European
Champions Alliance

European Cybersecurity Mapping 2026

European Cybersecurity Excellence

START-UP & SCALE-UP EDITION

powered by

IN CYBER FORUM

strategic sponsors

Atos

kuppingercole ANALYSTS

IONOS CLOUD

European
Champions Alliance

European Cybersecurity Mapping 2026

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION

strategic sponsors

Atos · IN CYBER FORUM · kuppingercole ANALYSTS · IONOS CLOUD

main sponsors

EclecticIQ · enclaive

community contributors

Ovens · GitGuardian · LANCOM SYSTEMS · RED ALERT LABS · wallix · XELERA

Europe has world-class innovators, researchers, and entrepreneurs. Yet its technology ecosystem remains fragmented and often lacks the scale needed to compete globally. At a time when technological leadership shapes economic strength, industrial resilience, and democratic sovereignty, Europe must ensure that the critical technologies of tomorrow are built and scaled here.

The European Champions Alliance (ECA) is a pan-European platform dedicated to the emergence and growth of Europe's next generation of technology champions. By connecting startups, scale-ups, corporates, investors, and policymakers across borders, ECA works to build the globally competitive companies Europe needs, while keeping critical technologies rooted in European ecosystems.

ECA's mission is to strengthen Europe's technological and economic autonomy by fostering collaboration across the innovation ecosystem. We empower startups and scale-ups to grow faster, connect actors across borders, and support the emergence of companies capable of shaping the technologies of tomorrow.

We do this in four ways: we **shape** the strategic conversation through ecosystem mappings and industry insights; we **connect** startups, corporates, investors, policymakers, and national associations to foster cross-border collaboration; we **navigate** complexity by providing strategic insights and access to key decision-makers; and we **make innovators shine** through events, publications, podcasts, and thought leadership platforms that showcase Europe's technology champions.

Europe has the talent and entrepreneurial energy to lead in critical technologies. The challenge is no longer innovation alone; it is **scale, visibility, and coordination.**

Because the technologies shaping the future should not only be global; they should also be European.

European
Champions Alliance

European Cybersecurity Mapping 2026

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION

In a year where cyber threats have accelerated in scale, intelligence, and systemic impact, the European Champions Alliance continues its mission to "Unite Europe's Innovators, Empower Tech Champions"

2026 marks a turning point. AI-enabled attacks, supply-chain entanglement, identity-based compromise, and looming post-quantum disruption are reshaping Europe's risk surface; and simultaneously redefining its innovation agenda.

As war looms around Europe more than ever in the last 80 years, it is also clear how much cyber attacks can be another way of disruption and toppling key assets and infrastructures. Against such hybrid warfare, Europe cannot entrust its cybersecurity to anyone else.

In this landscape, Europe needs more than resilience: it needs **strategic autonomy anchored in a strong, interconnected ecosystem of European cyber innovators.** This is precisely where the ECA acts; **connecting business with innovation, shaping the future, making innovators shine** to enable Europe's cybersecurity champions to scale.

ECA is also about **helping navigate complexity.** This new edition of the **European Cyber Mapping** embodies that ambition: giving structure to a fragmented market, accelerating cross-border visibility, and fostering trust between startups, corporates, investors, and public institutions.

By mapping the technologies that matter and the players shaping them, we aim to support Europe's transition from compliance-driven security to **performance-driven resilience,** and from dependency to **governed, sovereign choice.**

Europe has the talent, the regulation, and the market. What it needs now is orchestration; and the ECA is proud to help drive that momentum forward.

Dominique TESSIER
Head of Cybersecurity Operations
ECA

Andrea VAUGAN
General Secretary and Managing Director
ECA

Digital Dependencies: Sovereignty Put to the Test

Digital sovereignty has become a ubiquitous term. It structures political discourse, permeates industrial strategies, and stands as a marker of strategic ambition, both in France and more and more across Europe. Invoked so frequently, it has almost become consensual; and therefore, paradoxically, ineffective.

Behind this apparent consensus lies a more uncomfortable reality, one that remains largely absent from public debate: our technological and digital dependencies. Yet it is precisely here that sovereignty ceases to be a principle and becomes an operational constraint.

EUROPEAN INNOVATION: A NECESSARY, BUT INSUFFICIENT CONDITION

Europe is far from lacking innovation. In cybersecurity and digital trust, the European ecosystem is rich, creative, and dynamic. It is home to cutting-edge technologies, recognised expertise, and highly committed players. This innovation is a necessary condition for regaining control over our digital dependencies. Without indigenous innovation capacity, there can be no strategic autonomy or lasting resilience.

But innovation only matters insofar as it is grounded in a clear understanding of the market. Too often, it is driven more by abstract bets on the future than by a lucid reading of real-world uses, operational constraints, and the concrete needs of organisations. Useful innovation is not about anticipating a hypothetical future; it is about addressing today's problems while remaining adaptable.

INNOVATION, SOVEREIGNTY AND ECONOMIC VIABILITY ARE NOT THE SAME THING

It is time to dispel a structural ambiguity in the European debate: innovation, sovereignty, and business models do not automatically align. A company can innovate, be strategically relevant, contribute to European digital sovereignty; and still rely on a fragile or unsustainable business model.

This fragility is not a secondary issue. It directly affects companies' ability to endure, to invest, to scale internationally, and ultimately to carry real weight in global power dynamics. Sovereignty that is not supported by economically sound companies remains largely theoretical.

FRAGMENTATION AND THE CHALLENGE OF CONSOLIDATION

This economic issue directly reflects another structural characteristic of the European cybersecurity landscape: fragmentation. The market is made up of a multitude of innovative players, often positioned in very narrow niches, with offerings that struggle to gain visibility and coherence at scale.

Meanwhile, the global market is rapidly moving toward platformisation. Large players impose integrated solutions capable of covering broad perimeters, absorbing complexity, and establishing themselves as de facto standards. In this context, European dispersion is a strategic weakness.

This calls for investors willing not only to take risks, but also to support consolidation strategies; mergers, alliances, and structuring efforts. Investment should not merely fund innovation; it should enable the emergence of players of critical size, capable of competing over the long term.

EUROPEAN MARKET INTEGRATION: A STRATEGIC LEVER STILL UNDERUSED

Beyond consolidation, another major blind spot persists: the integration of the European market itself. Geographic, regulatory, cultural, and commercial fragmentation within the European Union still prevents the emergence of a truly unified internal cybersecurity market.

Strengthening European digital sovereignty does not primarily mean opposing extra-European markets; it means better integrating our own. As long as European companies must think country by country, regulation by regulation, they will remain structurally disadvantaged compared to competitors operating in large, homogeneous, and rapidly scalable domestic markets.

This lack of integration limits European players' ability to reach critical mass, standardise their offerings, and invest sustainably. It indirectly reinforces dependence on non-European solutions; not due to a lack of skills or technologies, but because of insufficient integrated market opportunities at continental scale.

Building a European cybersecurity market that is fluid, readable, and interoperable is therefore one of the most concrete; and most underestimated; levers of European digital sovereignty.

AN INTELLECTUAL DEPENDENCY AS WELL

Finally, and perhaps most critically, our dependencies are not only technological or industrial. They are also intellectual. We import solutions, but we also import analytical frameworks, strategic narratives, and ways of thinking about markets and risks. We increasingly assess our priorities using conceptual tools that are not our own.

This intellectual dependency constrains our ability to project ourselves, to structure our ecosystems, and to define our own value criteria. Thinking seriously about European digital sovereignty therefore requires reclaiming our analytical capacity; our ability to classify, map, and represent our markets on our own terms.

MAPPING TO ENABLE CHOICE

In a deeply interconnected world, sovereignty can only be relative and imperfect; but it can be lucid, organised, and resilient. That requires confronting our dependencies head-on, mapping them, prioritising them, and managing them.

This is precisely the ambition of this European Cybersecurity Mapping: to provide a market reading tool, not as an academic exercise, but as an instrument of intellectual autonomy and strategic decision-making. Because digital sovereignty does not begin with speeches. It begins when we accept to name, understand, and structure what binds us to others; in order to better choose what we truly want to control.

Guillaume TISSIER
Managing Director
INCYBER Forum - Europe

Welcome to the 2026 Edition of the European Cybersecurity Mapping.

Cybersecurity has been a recognized discipline for over thirty years. Yet, in 2026, we are witnessing a paradigm shift. This edition of the Mapping demonstrates that cybersecurity has ceased to be merely a technical requirement to become the absolute cornerstone of European independence.

To understand the state of our ecosystem, we must look at three critical forces:

- the geopolitical imperative for **Sovereignty,**
- the accelerating pace of **Innovation,**
- and the existential challenge of **Fragmentation.**

SOVEREIGNTY IS NO LONGER OPTIONAL

The boundaries between cybercrime, activism, and state-sponsored warfare have blurred. From the conflict in Ukraine to the sabotage of critical infrastructure and disinformation campaigns aimed at destabilizing democracies, the lesson is clear:

There is no political sovereignty without technological sovereignty.

For States and the EU, building a robust defense is mandatory. But this obligation extends to the private sector. With frameworks like **NIS2** and **DORA** fully influencing strategy, resilience is now a regulatory and operational necessity. Europe cannot afford to rely solely on external providers for its critical defense. We need a strong, local industrial base to guarantee control over our data and continuity of operations.

INNOVATION: THE AI PIVOT AND BEYOND

Despite its maturity, the sector is buzzing with vibrant innovation.

- **The AI Paradox:** Artificial Intelligence is reshaping the battlefield. It empowers defenders in EDR/NDR/XDR platforms but also arms attackers with tools to create elusive threats and deepfakes.
- **The Industrial Frontier (OT):** As automation connects factories to the cloud, OT security becomes a prime target. Europe remains a stronghold of engineering excellence here, well-positioned to secure these complex environments.
- **Future-Proofing:** Post-Quantum Cryptography is no longer science fiction but an immediate requirement. Simultaneously, a new market is emerging to secure AI itself protecting models from poisoning and manipulation.

THE FRAGMENTATION TRAP: A CALL FOR URGENT ACTION

Last year, we highlighted a clear warning sign: **only 23% of the vendors featured in our Mapping were scale-ups or large companies.** Fragmentation was already a structural weakness of the European cybersecurity ecosystem. Today, the gap has widened.

THE SCALE GAP

The ECA recently compared the revenues of the ten largest European cybersecurity vendors with those of the ten largest US players. The outcome is stark: a ratio of almost 1 to 10. Eight months later, as consolidation has continued to accelerate in the US and Israeli supplier landscape, this imbalance has only worsened.

THE CONSOLIDATION REALITY

Across the Atlantic, consolidation is moving fast and at scale. The multi-billion-dollar acquisition of Wiz by Google, the successive acquisitions carried out by Palo Alto Networks, or the acquisition of Armis by ServiceNow illustrate a clear strategy: building large, integrated platforms capable of sustaining massive R&D investments and rapidly integrating AI into cybersecurity offerings.

Europe has not remained silent. Some consolidation moves have emerged in OT security, Eastern European vendors are increasingly looking toward Western European players, and specialists in threat detection and analysis are joining forces to deliver more comprehensive solutions.

These signals are positive but the overall pace remains slow.

From the user's perspective, frustration persists. European customers still face a landscape dominated by niche players, many of which are too small to support the level of R&D effort that cybersecurity now requires, particularly as AI reshapes traditional security models.

We consider the consolidation of European cybersecurity vendors to be the single most critical strategic issue for our industry.

The talent is here.

The innovation is here.

The regulatory framework is here.

But without the industrial scale to back it up, we will remain dependent. We expect the new wave of AI-aided technologies to be the lever that finally unlocks these long-awaited moves.

This Mapping is a tool to drive those connections. Use it.

WHY THIS MAPPING?

Cybersecurity has become the backbone of Europe's digital resilience, economic competitiveness, and strategic autonomy. Yet the ecosystem that underpins it remains largely fragmented, under-mapped, under-funded, and under-recognized; both inside Europe and beyond. The ECA created this Mapping to address four fundamental needs.

1. VISIBILITY

Europe is full of world-class cybersecurity talent, deep-tech teams, and high-potential scale-ups; yet the landscape is difficult to see from the outside. Solutions are scattered across 20+ national ecosystems; many companies remain unknown beyond their home market. This Mapping acts as a **collective showcase,** making European capabilities visible to CISOs, investors, and policymakers alike.

2. DIGITAL SOVEREIGNTY

Dependence on foreign vendors creates strategic vulnerability. Frameworks like GDPR and NIS2 reinforce the need for trusted, European-controlled solutions; and buyers are increasingly demanding them. By identifying and structuring European players, this Mapping actively supports Europe's capacity to build a more resilient, autonomous industrial base. Cybersecurity is a sovereignty technology. Mapping it is a sovereignty action.

3. COLLABORATION AND CONSOLIDATION

European CISOs repeatedly flag the same frustration: too many fragmented point solutions, too little integration. This Mapping is more than a directory; it is a **tool for collaboration,** enabling companies to identify complementary technologies, build integrated solutions, and facilitate the cross-border partnerships and consolidation that Europe urgently needs.

4. STRATEGIC INTELLIGENCE

Beyond listing companies, this Mapping delivers actionable market intelligence: a structured view of 16 cybersecurity domains, country-by-country strengths and gaps, investment and technology trends, and a basis for policy recommendations. For buyers, it clarifies **who does what.** For innovators, **where to grow.** For institutions, **where to invest.**

WHAT'S NEW IN 2026?

The 2026 edition builds on the foundations of 2025 with clear advances in depth, quality, and community scale. Six key improvements set it apart.

MORE COMPANIES, BETTER DATA

This edition covers **significantly more companies (1,302 vs. 828 in 2025),** with cleaner classifications, more accurate country attribution, and refined maturity indicators throughout. We kept the same 16 categories to ensure year-over-year comparability, while delivering deeper insights into subcategory dynamics, scaling trajectories, and innovation hotspots.

RICHER INTERVIEWS

This year features an expanded set of conversations with scale-up founders, cybersecurity experts, investors, ecosystem leaders, and national associations; bringing real-world context and strategic perspectives from the people shaping Europe's cyber landscape.

NEW MACRO DATA FROM PARTNER ORGANISATIONS

For the first time, the Mapping integrates macro-level insights from ecosystem partners, including investment trends, regulatory impact, market dynamics, and European benchmarks; adding analytical depth and sharpness to the 2026 edition.

A GROWING COMMUNITY

The 2025 Mapping was widely read, shared, and praised across Europe. That enthusiasm translated directly into this edition: more actors contributed data, more organisations reached out proactively to participate, and the Mapping has become a **truly collective project.**

DISCLAIMER & HOW TO CONTRIBUTE

This Mapping has been compiled with the greatest care, drawing on extensive research and cross-validated data. Even so, in a fast-moving ecosystem, errors or omissions may occur. If you spot a mistake, a missing company, or outdated information, please reach out to us at cybermapping@european-champions.org.

We review all corrections and incorporate validated updates into our online platforms and future editions.

This Mapping is a community project; your contributions make it better every year.

STRATEGIC OUTLOOK 2026

Executive Synthesis
Cybersecurity as a Strategic Asset

By 2026, cybersecurity has completed its transition from a specialised IT function to a strategic asset class at the core of Europe's economic resilience and geopolitical autonomy.

This shift is no longer theoretical. It is the direct consequence of three converging forces: the industrialisation of cyber threats through automation and artificial intelligence; the full entry into force of a dense European regulatory framework; and a global consolidation cycle that is rapidly concentrating power, capital, and platforms, so far mostly outside Europe.

Cybersecurity now sits at the intersection of national security, economic competitiveness, and digital trust. Attacks no longer target only data or systems; they aim to disrupt operations, destabilise supply chains, and undermine confidence in institutions. As a result, cybersecurity spending has become structurally inelastic. While other segments of the technology sector have experienced corrections, cybersecurity continues to grow at double-digit rates, driven by necessity rather than optimism.

Yet Europe faces a structural dilemma. The continent excels at producing high-quality cybersecurity innovation particularly in deep tech, identity, cryptography, OT security, and threat intelligence but continues to struggle to transform these assets into large, independent platforms.

Fragmentation remains the defining weakness of the European ecosystem. Scale-ups emerge, consolidate local markets, and reach technical maturity, only to be acquired by non-European strategic buyers or private equity funds operating under non-European control.

Regulation has become Europe's most powerful lever. NIS2, the Cyber Resilience Act, and DORA have collectively shifted cybersecurity from discretionary spending to a legal and operational imperative. In doing so, they have created a vast addressable market particularly among SMEs and mid-sized industrial players while simultaneously raising the bar for vendor maturity, resilience, and scale.

This Strategic Outlook sets the context for the Mapping that follows. It explains why consolidation is accelerating, why certain categories dominate, why identity and infrastructure security have become central, and why Europe now faces a narrow window to convert regulatory strength and technological excellence into lasting industrial leadership.

"Cybersecurity is no longer a technical function. It is a condition for sovereignty."

MARKET TRAJECTORY & GROWTH SIGNALS

The European cybersecurity market continues to defy broader technology sector headwinds.

Growth projections for the 2026–2030 period remain consistently above general IT spending, positioning cybersecurity among the most resilient segments of the European digital economy.

According to consolidated market estimates, European cybersecurity spending reached **approximately €70–75 billion in 2025, representing roughly 26% of global cybersecurity spend.** Forecasts converge around a **compound annual growth rate (CAGR) of 11–13% through 2030–2033,** which would bring the market to **€150–165 billion by the early 2030s.** This sustained growth confirms that cybersecurity has shifted from a discretionary IT investment to a structural operational requirement.

THE RESILIENCE ANOMALY

Cybersecurity spending has become decoupled from traditional IT investment cycles. While cloud, SaaS, and enterprise software budgets experienced corrections in 2023–2024, cybersecurity maintained double-digit growth. The driver is not optimism, but necessity: regulatory enforcement, insurance pressure, and the rising cost of incidents have locked cybersecurity into a non-discretionary spending category.

REGIONAL ASYMMETRIES

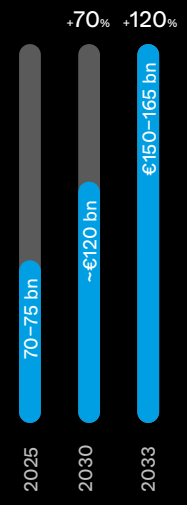
Growth is unevenly distributed across Europe. The **UK, Germany,** and **France** remain the largest markets in absolute terms, driven by enterprise and industrial demand. However, the fastest acceleration is occurring in **Southern Europe,** where **Italy** and **Spain** recorded **year-on-year growth rates of approximately +23% and +26% in 2025,** largely driven by the enforcement of NIS2 across industrial SMEs. Central and Eastern Europe plays a paradoxical role. Often underestimated, the region produces globally competitive cybersecurity champions while maintaining capital-efficient growth models. Companies in this region tend to internationalise later but scale aggressively once critical mass is reached, as illustrated by players such as **Bitdefender** (Romania), **ESET** (Slovakia) and **Nord Security** (Lithuania), the latter now valued at approximately **$3 billion** with sustained organic growth above **30% year-on-year.**

THE SCALE-UP PARADOX

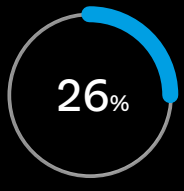
A persistent structural pattern defines European cybersecurity growth. Companies below a critical revenue threshold typically around **€10 million in annual recurring revenue (ARR);** remain heavily dependent on domestic markets, often generating more than **80% of revenues locally.** Once this threshold is crossed, internationalisation accelerates sharply, with mature scale-ups generating **40% or more of revenues outside their home market.** Some 25% of European cybersecurity vendors are now present in at least one more country than their original one.

At precisely this stage, capital intensity increases. European funding depth very often proves insufficient, pushing companies toward US capital or strategic exits. This dynamic explains the dense long tail of start-ups visible in the Mapping alongside a relatively small cohort of independent scale-ups. It also reveals a structural paradox: European capital and talent absorb the risk of the early stages, while US capital captures the value created in the scaling phase that follows.

PROJECTED EUROPEAN CYBERSECURITY MARKET SIZE (€ BILLIONS)



GROWTH TRAJECTORY



SHARE OF THE GLOBAL MARKET

Europe's Share of the Global Cybersecurity Market

Interview

KUPPINGERCOLE

STRATEGIC
SPONSOR

The current geopolitical turmoil has strengthened both the understanding of and demand for EU-sovereign solutions in cybersecurity and digital identity.

IDENTITY SECURITY: STILL A LONG WAY TO GO FOR OPTIMAL SECURITY POSTURE

Identity Security, the combination of Identity and Access Management (IAM) and Cybersecurity, is facing a series of challenges, from old but often underserved ones to major new ones. Amongst the long standing ones, we see the transition to passwordless, multi-factor authentication, the management of „non human" identities (NHI) such as in workloads, and securing OT (Operational Technology) as areas where many organizations still have a long way to go.

The major new challenge, without a doubt, is securing AI and its intersection withIdentity ("AIdentity"). While we see a lot of solutions emerging, these are mostly point solutions addressing certain aspects of AI security but missing the entire breadth and depth of challenges we are facing in this field.

Also, many organizations still must do the basics in both IAM and cybersecurity. In IAM, even fundamental workforce IAM processes for managing users and their entitlements frequently aren't solved well. Additionally, many organizations face a legacy challenge with IAM implementations that have become increasingly outdated and hard to manage after 10or more years since the initial deployment.

In cybersecurity, one of the biggest challenges stems from the multitude of tools. 70 or 80 different tools are more the norm than the exception for organizations. Integration and consistent management are both complex. This leads to a risk for a comprehensive cybersecurity posture, despite having many tools in place.

2027: THE YEAR OF NHI MANAGEMENT AND AI SECURITY

The good news is that the solutions in this space are evolving with considerable speed for addressing challenges such as NHI Management and AI Security. We are seeing major investments flowing into these areas and also into OT security.

While the latter area will be covered by isolated point solutions for longer, we expect to see broader, more feature-rich and integrated offerings for both the management of non-human identities, in particular workload identities, and for AI Security. These offerings will come from both start-ups and from established players in the market. While 2026 might still be a year driven by innovation, 2027 should be a year with a stronger focus on integration, while also keeping innovation at a high level.

This will be needed, with attackers continuing to move fast. Organizations will remain in a situation where they need continuous improvement in their cybersecurity posture and the investments needed for that to keep pace with the evolving cyber-attacks.

EUROPE'S PLAY: SOVEREIGNTY IN CYBERSECURITY AND DIGITAL IDENTITY

The current geopolitical turmoil has strengthened both the understanding of and demand for EU-sovereign solutions in cybersecurity and digital identity. While the former drives strengthening of IT security in general, the latter is pushing independence from the large U.S. cloud providers such as Google, Apple, Meta, Amazon, and others.

The ECA analysis as well as our research at KuppingerCole Analysts demonstrates that there exists a strong ecosystem of software vendors and service providers in Cybersecurity, IAM, and Sovereign Clouds. This ecosystem covers all relevant areas. Buyers should consider taking European solutions into consideration as alternatives. Many of the European solutions deliver technical excellence. For all major areas in Cybersecurity and IAM there are European offerings that are mature and feature-rich enough to provide a solid foundation for the requirements of organizations. An often-overlooked simple advantage of using European vendors is the proximity to their leadership and support teams.

For Digital Identity, the EU Digital Identity (EUDI) wallet(s) have the potential of being a game changer, delivering an interoperable and highly secure identity infrastructure across the EU. The power of the EUDI wallet becomes obvious when looking at the attempts of Google, Amazon, and other leading global players to play a role in that evolving ecosystem. Europe, in this area, is clearly in the driver's seat.

PLATFORMIZATION: CHALLENGE AND OPPORTUNITY

An often-discussed topic is security solution platformization. Every time a large vendor, especially in cybersecurity, acquires another vendor, the discussion of platformization reaches a new peak. Buyers are split between some that prefer unified sourcing that comes with platformization, and others that consider the risks of platformization larger than the advantages.

Platformization is not new in IT and cybersecurity. The discussion about "suite vs. best-of-breed" has run for decades in various areas of IT. There is no "wrong" or "right" in this debate, and virtually never is it about "only one suite/platform" or "everything best-of-breed". While the large platforms mainly come from U.S. vendors, European vendors can play a strong role with best-of-breed offerings. There also are significant opportunities for financial investors in building more comprehensive European platforms in cybersecurity and IAM...

It should be considered thatmodern modular software architectures, API-first approaches, and the rise of flexible, API-based orchestration leans to favoring best-of-breed over "over-platformization". It historically has been challenging to integrate 3rd-party sourced solutions without significant effort. Such solution combinations or "Fabrics", like the Identity Fabric defined by KuppingerCole Analysts, enables a phased migration and for eased integration with previously deployed solutions. In this way best-of-breed can give control back to customers.

TIME FOR STRONGER EUROPEAN SELF-ESTEEM

Europe has an ecosystem of available software and services across cybersecurity, IAM, Digital Identity, and sovereign clouds that is broader and more powerful than commonly understood. European buyers should take regionally sourced solutions into consideration. Moreover, it is a highly interesting playing field for financial investors, with well-engineered solutions available at lower valuations than in Silicon Valley. This, especially in the context of an increasing focus on EU digital sovereignty, provides strong growth opportunities for software vendors, cloud service providers, and the financial investors backing these companies.

Still, there is a need for fostering innovation, especially in the early stages of entrepreneurship, by strengthening funding and venture capital while also reducing bureaucratic barriers. The EU would be well-advised to favorl ndividual organizations over consortia in their funding, as the German SPRIND (agency for rapid innovation) does now. This will help accelerate the birth of Europe's own unicorns.

Martin KUPPINGER
Co-Founder
& Principal Analyst

KuppingerCole

REGULATION AS MARKET INFRASTRUCTURE

Europe's regulatory framework has become the single most important structural driver of cybersecurity demand. In 2026, regulation no longer shapes the market indirectly; it actively constructs it.

NIS2: FROM COMPLIANCE TO BUDGET ACTIVATION

The enforcement of NIS2 has expanded the cybersecurity market far beyond traditional critical infrastructure operators. Thousands of SMEs across manufacturing, logistics, energy, food production, and waste management now fall within its scope. For many, this marks their first sustained investment in cybersecurity. Demand is shifting toward solutions that combine risk management, monitoring, reporting, and operational support.

This has favoured vendors capable of delivering packaged, scalable offerings often via managed service providers over fragmented point solutions.

CYBER RESILIENCE ACT: SECURITY BY DESIGN

The Cyber Resilience Act has transformed embedded and firmware security into a market access condition. Hardware and IoT manufacturers can no longer treat security as an afterthought. This has created a powerful tailwind for European vendors specialising in embedded security, certification, and lifecycle compliance, reinforcing Europe's strengths in industrial and OT environments.

DORA AND SUPPLY CHAIN PRESSURE

For financial services and their suppliers, DORA has extended cybersecurity requirements deep into third-party ecosystems. Start-ups and scale-ups selling into regulated sectors now face longer sales cycles, higher assurance requirements, and growing pressure to demonstrate operational resilience. This dynamic favours consolidation and disadvantages undercapitalised niche players.

Collectively, these regulations reward scale, integration, and durability. Europe has created a regulatory moat but only companies capable of industrialising their offerings will fully benefit from it.

CAPITAL, INVESTMENT & THE EUROPEAN SCALE GAP

The post-2022 correction has fundamentally reshaped cybersecurity investment dynamics. The era of growth-at-all-costs has given way to a regime of selectivity, efficiency, and resilience.

CAPITAL CONCENTRATION

Overall funding volumes have stabilised, but capital is increasingly concentrated in fewer assets. Investors favour companies with recurring revenues, clear regulatory tailwinds, and paths to profitability. This has reinforced the position of later-stage scale-ups while increasing pressure on early-stage companies to demonstrate differentiation and traction earlier.

THE ROLE OF PRIVATE EQUITY

Private equity has become a central architect of the European cybersecurity landscape. Unlike traditional venture capital, PE firms bring consolidation expertise, long-term capital, and operational discipline. In identity, SecOps, and managed security, PE-backed buy-and-build strategies are now shaping the market structure.

THE SERIES B/C GAP

Despite progress, Europe still lacks sufficient depth to independently fund late-stage cybersecurity growth. As a result, US investors and strategic buyers continue to dominate the final stages of scaling. Sovereign and defence-linked funds are beginning to address this gap, but their impact remains uneven.

This structural imbalance directly feeds the consolidation dynamics analysed in the next section.

Interview

ATOS

STRATEGIC
SPONSOR

The human layer is also being upgraded for the AI era.

From your company vantage point, which cyber threats or attack patterns are currently the most critical for large organizations and public institutions across Europe? Which developments or weak signals are you monitoring most closely?

The most critical threat patterns for large enterprises and public institutions in Europe are the ones that combine scale, speed, and systemic impact. They don't just hit systems; they disrupt services, and force leadership decisions under extreme time pressure.

And that's why ransomware remains the highest-impact threat, now driven by multi-layer extortion, operational disruption, reputational intimidation, and ecosystem coercion. This is amplified by the industrialization of Ransomware-as-a-Service, and we now see AI-assisted negotiation support that makes extortion persistent, multilingual, and psychologically optimized.

In that same disruption-and-extortion playbook, we also see a sharp rise in DDoS as a pressure tool used to degrade services, distract responders, or raise the cost of delay. 2025 was a record year by volume, including extreme attacks measured in terabits per second and billions of packets per second across Europe.

We also see a consistent rise in identity-led compromise, including stolen credentials, session and token theft, over-privileged access, and manipulation of trusted workflows. And supply-chain compromise is increasingly central to high-impact incidents. A single upstream breach can cascade across dozens of organizations because trust is shared by design across software dependencies, managed services, cloud integrations, and federated identity. Finally, stealth intrusions and living-off-the-land are increasingly the default, with adversaries staying quiet until leverage is highest.

On emerging signals, we're tracking the collision of enterprise AI adoption and criminal innovation, and several patterns stand out:

1. **AI-enabled malware** that uses AI during runtime to dynamically generate commands, alter behavior, and evade static detection.

2. **Rogue criminal AI platforms** as FraudGPT, WormGPT, HackGPT and their many successors, lowering the barrier to entry and accelerating criminals' go-to-market.

3. **AI platforms** as targets: prompt injection, tool/plugin abuse, poisoning, and governance gaps that can turn trusted automation into an exfiltration or manipulation channel

4. **Deepfakes** are moving from novelty to operational fraud in executive and finance workflows.

5. **Quantum disruption** is shifting from theory to timeline as "Harvest today, decrypt tomorrow" threatens long-lived confidentiality, and "sign today, forge tomorrow" threatens the integrity of certificates, software updates, and digital trust.

Over the past months, what major evolution have you observed in terms of cybersecurity practices, organizational maturity, or defensive capabilities?

The most significant evolution we've observed is a mindset shift: European organizations are moving from cyber protection to cyber resilience. You can't prevent every intrusion, but you can control the blast radius and the clock. Cyber maturity in Europe is increasingly measured by one thing: how well you operate under attack.

In parallel, AI is reshaping both defense and risk across multiple layers, acting at the same time as an accelerator for defense and a new frontier to secure.

On the defensive side, we see the strongest value where AI reduces time and friction, for example, alert triage and investigation enrichment, support for threat hunting, and automation of identity entitlement reviews. At the same time, organizations are taking AI security by design far more seriously with stronger governance, data controls, access management, logging, red-teaming, and awareness of specific AI risks like prompt-injection and agents goal drift.

Zeina ZAKHOUR
Vice-President
Global CTO Cybersecurity

Atos

Interview

ATOS

STRATEGIC SPONSOR

And as AI agents enter workflows, IAM programs are adapting with unique identities for nonhuman actors, automated credential lifecycle, fine-grained authorization, and clear accountability for agent purpose and ownership.

The human layer is also being upgraded for the AI era. Employees are becoming AI-enhanced, and that changes both productivity and risk. The most mature organizations are moving beyond traditional awareness training toward AI literacy and behavior-based programs, teaching people how to use AI safely, how to recognize AI-powered attacks, and how to apply a stronger verify unusual requests reflex.

Finally, post-quantum is moving from theory to timetables in Europe. The EU coordinated roadmap sets clear milestones with a 2026 start line for Member States and a 2030 transition target for critical infrastructure. And this is already cascading through the partner and vendor ecosystem, as organizations start building their crypto inventories and put migration plans in motion.

Do you see concrete progress in anticipation, resilience, or crisis management among European organizations?

Yes, we see tangible progress and it's most visible in the organizations that have made resilience an operating practice that is repeatable and measurable. At Atos, we've anchored this approach with a SOC-driven resilience cycle of Prepare, Respond, Adapt.

- **Prepare:** we anticipate and reduce exposure before the crisis. That means clarified roles and decision rights, rehearsed playbooks, tabletop exercises aligned to modern extortion scenarios, restore drills that prove recovery time, segmentation that limits blast radius, and tighter control of supplier and privileged access.
- **Respond:** we optimize for speed and decisiveness. The focus is rapid detection and containment, especially identity containment, supported by pre-built escalation paths and communication routines so teams act decisively under pressure.
- **Adapt:** we institutionalize learning and turn every incident into improved posture. Post-incident learnings are translated into concrete control changes, detection tuning, and measurable improvements in time-to-contain, with continuous exposure reduction.

Overall, progress is uneven, but the direction is clear: the leaders are building cybersecurity as an operating discipline, designed for performance under pressure, not just prevention.

How is cybersecurity increasingly integrated into broader operational risks & governance frameworks? From your perspective, how do European regulations & frameworks contribute to structuring and strengthening this approach?

Cybersecurity is increasingly integrated into broader operational risk management because organizations now approach it in the same way they manage other threats to continuity. It is less about protecting IT and more about protecting the business. In mature European organizations, cyber is embedded into enterprise risk governance with defined risk appetite, named owners across business and support functions, tested controls, rehearsed escalation, and crisis management that link technical response to legal, communications, and operational decisions.

European regulation is accelerating this integration because it turns cybersecurity into a structured operating discipline. It creates a common language and governance baseline across security, risk, legal, procurement, and operations. That alignment is what makes anticipation, resilience, and crisis management real at scale. Indeed, Frameworks like NIS2 or DORA for financial services strengthen leadership accountability, incident handling and third-party expectations, while pushing organizations to industrialize reporting and escalation. The EU AI Act extends the same logic to AI-enabled operations, reinforcing governance and security-by-design where AI influences critical decisions.

In practice, this blended approach shows up in two concrete shifts. First, boards and executive committees are moving from control checklists to operational outcomes, with KRIs tied to detection, containment, recovery time, and service impact. Second, third-party and concentration risk is being treated as systemic risk, with tighter access governance, segmentation, and contractual obligations because supplier compromise can become enterprise disruption.

That's how cyber becomes manageable at scale: shared language, shared accountability, shared cadence.

How do you assess Europe's current position in cybersecurity – its strengths, dependencies & blind spots? What should be the top priorities to sustainably strengthen Europe's autonomy, resilience, and industrial competitiveness in this field?

Europe's position in cybersecurity is stronger than we often believe, but also more dependent than we like to admit. Europe is building rules, coordination, and resilience muscle at scale. The opportunity now is to convert that into strategic autonomy and industrial advantage.

WHERE EUROPE IS STRONG

Europe has a unique ability to align the levers that actually move the market: a clear regulatory framework, shared priorities, cross-border coordination, targeted funding, and a powerful standard-setting effect. When regulation is well designed, it does not just constrain organizations; it creates demand for solutions that are robust by default, interoperable, portable, secure, and maintainable. That alignment is a strategic asset, because it turns resilience requirements into an industrial runway for European capabilities

EUROPE'S DEPENDENCIES

Europe still relies heavily on a small number of non-European providers for key digital layers, including cloud platforms, identity stacks, productivity ecosystems, and parts of the security telemetry chain. Add globally interdependent hardware and compute supply chains, and the picture is clear: Europe's digital economy is strong, but parts of its foundation remain concentrated elsewhere.

EUROPE'S BLIND SPOTS

Systemic risk is still not stress-tested enough especially common-mode failures, supply-chain cascades, and concentration risk. Many organizations still do not quantify dependency exposure and the gap between plans and proven recovery remains wide at the pace modern threats demand. Identity sprawl is accelerating with automation and AI agents, creating nonhuman identities that governance models are still catching up with. And crypto visibility remains a blocker, especially as post-quantum timelines approach.

TOP PRIORITIES TO STRENGTHEN AUTONOMY, RESILIENCE, AND COMPETITIVENESS

Europe should prioritize sovereignty on systemic foundations. This includes European, or at least European-operable, capabilities for digital identity, privileged access, cryptography, and security detection and response. This is also where sovereignty risk must be quantified properly to help organizations adopt the right strategy on this front.

Second, autonomy has to be built through market demand, not slogans. Europe will not scale with intentions; it scales with market growth. Too often, organizations default to global platforms because they reduce perceived risk, or integration comfort, or even the cost of switching. The shift is to adopt European where it's strategic and where the sovereign risk is highest. The shift is also to invest more in European players, from startups to scale-ups to large industrial actors, accelerating the path to adoption at scale.

Third, Europe must treat the supply chain as a strategic asset. Security-by-design expectations of the EU Cyber Resilience Act should lift product quality and supplier assurance, while supply-chain concentration should be actively reduced through diversification, transparency, and enforceable requirements on critical dependencies.

Autonomy does not mean isolation. It means choosing partnerships and governing them properly with dependencies that are auditable and reversible, backed by continuity guarantees and realistic fallback options. That is how Europe stays open, but never blocked.

Europe has the ingredients: regulation that drives discipline, sectors that understand resilience, and a market big enough to set standards. The next step is execution at scale. That's how cyber becomes a competitive advantage, not just a defensive cost.

Interview

IONOS

STRATEGIC SPONSOR

To maintain competitiveness in 2026, Europe must bridge the “innovation-to-industrialization” gap by converting its world-class research into unified, global-scale platforms, particularly in AI-driven threat detection and post-quantum cryptography.

IONOS Cloud Startup Program

How do you see the role of European cloud and cybersecurity providers like IONOS in strengthening Europe’s digital sovereignty?

IONOS anchors European digital sovereignty by providing a legally autonomous cloud environment that serves as a definitive shield against extraterritorial jurisdictional risks, such as the US CLOUD Act. By supporting the “EuroStack” and offering sovereign Kubernetes frameworks like SUSE Rancher Prime and Red Hat OpenShift, we decouple European innovation from non-EU technical dependencies. This ensures that European businesses can scale within a secure, independent value chain that maintains strict operational and legal integrity.

What are the key cybersecurity and compliance challenges European organisations currently face when moving to the cloud?

European cybersecurity companies face a “scale-and-trust” deficit, where extreme market fragmentation necessitates costly integration efforts to compete with global platform providers. Despite the tailwinds of NIS2, growth is constrained by non-harmonized national procurement standards and a persistent lack of late-stage venture capital, which prevents specialized innovators from reaching global category leadership. To survive, these vendors must transition from niche specialists to interoperable ecosystem partners within a unified European digital framework.

In your view, where does Europe still need to strengthen its technological and infrastructural capabilities to remain competitive in cybersecurity?

To maintain competitiveness in 2026, Europe must bridge the “innovation-to-industrialization” gap by converting its world-class research into unified, global-scale platforms, particularly in AI-driven threat detection and post-quantum cryptography. We must urgently address the late-stage funding deficit to prevent promising scale-ups from seeking non-EU exits, ensuring that the “European Cyber Champions” of tomorrow remain under domestic ownership. Furthermore, securing our critical ICT supply chains requires a shift toward hardened, EU-based infrastructure that eliminates dependency on foreign proprietary stacks for essential public and private sector services.

How does the IONOS Cloud differentiate itself in the European cloud and cybersecurity landscape?

The IONOS Cloud differentiates through a "sovereign-by-design" model that prioritizes technical interoperability, exemplified by our 2026 validation for sovereign Kubernetes orchestration with SUSE. Rather than building a closed ecosystem, we act as a foundational enabler for European cybersecurity vendors, creating a transparent and legally shielded value chain. This approach combines absolute jurisdictional security with industry-leading price-performance, ensuring that sovereignty is a strategic performance driver rather than a compliance burden.

How does your offering contribute to resilience, compliance (e.g. NIS2, DORA, GDPR), and trust for European businesses and institutions?

IONOS strengthens European resilience by providing legally autonomous infrastructure that mitigates the jurisdictional risks inherent in non-EU cloud providers, satisfying the core sovereignty requirements of GDPR. Our platform natively supports NIS2 compliance and provides a strong foundation for DORA-regulated supply chains through high-availability architectures and the industry-leading BSI C5 certification, ensuring strict compliance for critical supply chains. By prioritizing open standards and local legal accountability, we enable businesses to build a foundation of trust while maintaining the strategic agility required to navigate Europe's evolving regulatory landscape.

Why did IONOS decide to support the European Cybersecurity Mapping initiative?

IONOS supports the European Cybersecurity Mapping initiative to foster a transparent and sovereign digital ecosystem that consolidates European innovation under a unified, legally autonomous framework. As a foundational infrastructure provider, we aim to bridge the visibility gap for specialized European cyber champions, enabling them to scale securely while ensuring the entire digital supply chain remains within local jurisdictional control. This strategic partnership reinforces our commitment to building an end-to-end European tech stack that prioritizes operational resilience and strategic independence.

Our Startup and ISV Partner Programs provide a strategic runway for European innovators, offering scalable sovereign infrastructure and direct access to our ecosystem of enterprise clients. By bridging the gap between technical development and market-ready compliance, we empower the next generation of European champions to lead with autonomy - scan the QR codes below to accelerate your growth.

IONOS CLOUD

IONOS is the leading digitalization partner and trusted cloud enabler for small and medium-sized businesses (SMBs). The company serves around 6.5 million customers and has a presence in 18 markets across Europe and North America, with its services being accessible worldwide. Its web presence and productivity portfolio caters to all digitalisation needs, providing domains, web hosting and website builders with AI capabilities, as well as eCommerce and online marketing tools. The company also offers cloud solutions for businesses looking to move their operations to the cloud as they expand and develop..

ionos.fr

Phillip MAASBERG
Senior Advisor Business Development Strategy & Planning and Global Startup Program Lead

IONOS

Interview

ENCLAIVE

MAIN
SUPPORTER

The question is no longer whether organisations will move sensitive workloads to the cloud; it is whether they can do so without being forced to extend blind trust to their infrastructure providers. This is today of course underlined and highlighted by the political pitfalls summed up in the sovereignty discussion.

Perimeter is dead. What is the 'last mile' of data protection?

When briefly taking the noise from the political domain out of the picture, the single most important shift we are witnessing is the collapse of the traditional security perimeter in the age of cloud and AI. For decades, cybersecurity was built around the assumption that you could draw a boundary around your infrastructure and defend it. That model is simply no longer viable. Today, sensitive workloads run across multiple clouds, AI models process confidential data in environments operated by third parties, and organisations are asked to "trust" infrastructure they do not own or control.

The critical issue this exposes is what I call the last mile of data protection: data while it is actively being processed. We have long been able to encrypt data at rest and in transit, but processing has remained a blind spot; a moment of exposure that every sophisticated attacker knows to target. Addressing this gap through hardware-based confidential computing is, in my view, the most urgent and consequential challenge in cybersecurity today. The question is no longer whether organisations will move sensitive workloads to the cloud; it is whether they can do so without being forced to extend blind trust to their infrastructure providers. This is today of course underlined and highlighted by the political pitfalls summed up in the sovereignty discussion.

How will AI and confidential computing create 'zero-trust compute'?

Over the next three years, I expect the convergence of AI and confidential computing to fundamentally reshape how we think about secure infrastructure. It can be similar as moving from HTTP to HTTPS in the browser when starting to secure communications. As enterprises deploy AI at scale; training models on proprietary data, running inference on sensitive inputs, building agentic systems that act autonomously; the attack surface expands dramatically. The data processed by these systems is often among the most valuable an organisation holds, and the current security models are not built to protect it.

What I anticipate is a structural shift toward "zero-trust compute": environments where security guarantees are enforced not by policy or contractual clauses, but by hardware-level isolation that no administrator, cloud provider, or insider threat can bypass. Organisations that build on this foundation today will have a significant competitive and compliance advantage as

regulation tightens and the threat landscape evolves being faster to transform and harvest the benefits of a truly secure digital supply chain.

Explain Europe's 'structural sovereignty gap.'

Europe occupies a paradoxical position. On the regulatory front, we are world leaders; GDPR set a global benchmark, and frameworks like NIS2 and the EU Data Act are pushing security standards in the right direction. European institutions understand the stakes of digital dependency better than most, and there is genuine political will to act.

Yet at the technology and infrastructure layer, Europe remains heavily dependent on a handful of non-European hyperscalers for the very cloud services that handle our most sensitive data. This creates a structural sovereignty gap: we write the rules, but we run our workloads on infrastructure governed by foreign jurisdictions and foreign legal frameworks. The good news is that European deep-tech companies; and the confidential computing ecosystem in particular; are building the technical foundation to close that gap. The challenge is speed and scale.

What is the single most impactful action Europe can take now?

The single most impactful action Europe could take is to create structured demand for sovereign, verifiable security in its public procurement and critical infrastructure requirements. Regulation alone is insufficient if the organisations subject to it have no practical, accessible alternative to the dominant hyperscalers. Europe needs to couple its regulatory ambition with procurement policies that actively favour solutions offering hardware-attested security and genuine data sovereignty; not just contractual promises.

Specifically, this means mandating confidential computing for workloads involving sensitive personal data, critical infrastructure, and AI systems operating in regulated sectors. The BSI and the gematik in Germany for example have started to move in that direction. What it needs now is the decisiveness to back its own ecosystem at scale and be willing to invest with usually younger and smaller European innovators, keeping some of the big global players in parts at arm's length without dropping the benefit from the international experience they bring. Thus playing the strength of Europe being used to operating in a collaborative cross company setup.

enclaive

Enclaive is Europe's leading confidential computing provider, empowering businesses to protect sensitive data across multi-cloud environments. By leveraging secure enclaves, we ensure applications and data remain confidential at runtime, even in untrusted infrastructures. Our solutions integrate seamlessly and comply with strict regulations, enabling secure innovation. Enclaive: Europe's top confidential computing for a safer digital future.

enclaive.io

Andreas WALBRODT
CEO

Enclaive

CONSOLIDATION, EXITS & THE SOVEREIGNTY LEAK

Consolidation is no longer optional; it is the dominant industrial logic of cybersecurity.

Platformisation, AI integration, and regulatory compliance all require scale, recurring revenues, and sustained R&D investment. Between 2024 and early 2026, Europe has witnessed an unprecedented wave of high-impact transactions that structurally reshaped its cybersecurity landscape.

LANDMARK EUROPEAN EXITS

Several transactions stand out as structurally decisive:

- **Hornetsecurity (Germany) → Proofpoint (USA):** completed in December 2025 for approximately $1.8 billion. At the time of acquisition, Hornetsecurity was serving more than 125,000 European SMEs through a network of 12,000+ MSPs, generating close to $200 million in ARR. While this exit validated Europe's ability to build profitable platforms, it also transferred a critical layer of SME email security and compliance infrastructure to US ownership.
- **Darktrace (UK) → Thoma Bravo (USA):** completed in October 2024 for $5.3 billion. One of Europe's rare cybersecurity decacorns, Darktrace was taken private after years of perceived undervaluation on the London Stock Exchange, highlighting the persistent valuation gap between European public markets and US private capital.
- **Tessian (UK) → Proofpoint (USA):** this acquisition removed a leading European player in human-layer security from the independent ecosystem, further consolidating US dominance in email security and data loss prevention.
- **Secure-IC → CADENCE (USA):** this fast scaling player expert in OT Security has finally found an US partner as the best solution to finance its development. Which reminds the acquisition of SENTRYO by CISCO IN 2019.

GLOBAL CONSOLIDATION WITH DIRECT EUROPEAN IMPACT

Several non-European transactions carry major implications for European buyers and vendors:

- **Alphabet (Google) → Wiz:** announced at $32 billion, this is the largest cybersecurity acquisition ever proposed. As of early 2026, the transaction remains under intense scrutiny by the European Commission, with the decision seen as a litmus test of Europe's willingness to act as a gatekeeper against hyperscaler dominance of the cloud security layer.
- **Palo Alto Networks → CyberArk:** announced in 2025 for approximately $25 billion, consolidating a dominant position in identity and privileged access management, a segment critical to European banking and critical infrastructure.
- **ServiceNow → Armis:** completed in 2025 for approximately $7.75 billion, reinforcing US control over OT and IoT asset visibility, a domain central to European industrial security.

THE STRUCTURAL SOVEREIGNTY LEAK

These transactions follow a consistent pattern: European companies incubate innovation, consolidate local markets, and reach operational maturity, only to exit to non-European platforms. In short, European capital bears the early-stage risk, while US capital harvests the returns of international scaling. While financially rational for founders and investors, this dynamic progressively shifts control over critical security layers email, identity, cloud posture, OT visibility outside Europe.

Without the emergence of large, European-led consolidators capable of executing similar platform strategies, Europe risks remaining structurally dependent on foreign-controlled security infrastructures, despite strong regulatory and technological foundations.

SNAPSHOT – KEY FIGURES & TRANSACTIONS (2024–2026)

EUROPEAN CYBERSECURITY AT A GLANCE

- Market size (Europe, 2025): **~€70–75 billion**
- Share of global cybersecurity spend: **~26%**
- Projected CAGR (2026–2033): **11–13%**
- Number of vendors mapped (2026): **800+ across 24 countries**
- Estimated talent gap (Europe): **300,000–350,000 cybersecurity professionals**

GROWTH HOTSPOTS

- Italy: **+23% YoY** (2025)
- Spain: **+26% YoY** (2025)
- Germany: **+14%** YoY (industrial & OT-driven)

CRITICAL REVENUE THRESHOLDS

- **€10m ARR:** inflection point for internationalisation
- **40% international revenue:** typical profile of mature European scale-ups

MAJOR TRANSACTIONS IMPACTING EUROPE

- Hornetsecurity → **Proofpoint** ($1.8bn)
- Darktrace → **Thoma Bravo** ($5.3bn)
- Tessian → **Proofpoint** (undisclosed)
- Google → **Wiz** ($32bn, pending EU decision)
- Palo Alto Networks → **CyberArk** ($25bn)
- ServiceNow → **Armis** ($7.75bn)

Interview

ECLECTICIQ

MAIN
SUPPORTER

Closer threat intelligence sharing between government and industry would also make a material difference. The threat picture is shared. The response shouldn't be fragmented.

What is the single most important issue or shift currently affecting your cybersecurity field?

The threat landscape has professionalised. The groups targeting organisations today, whether nation-state actors or criminal enterprises, operate with structure, discipline, and shared infrastructure. They iterate quickly, recycle what works, and coordinate in ways that most cyber defenders aren't built to match.

The stakes are real. Successful attacks disrupt critical services, expose sensitive data, undermine public trust, and in some cases threaten national infrastructure. The cost of getting this wrong has never been higher.

The response has to match the threat. Cyber defenders that rely on alerts and indicators alone are always playing catch-up. What separates effective programmes is the ability to understand the adversary, their motivations, their methods, and where they're likely to move next. Knowing what's coming matters more than reacting to what's already happened.

What key evolution do you expect to have the greatest impact in your domain over the next three years?

The pressure on organisations to demonstrate genuine cyber resilience is going to intensify significantly over the next three years. Regulators, boards, and insurers are all asking harder questions, and "we have the tools in place" is no longer a sufficient answer.

That's going to force a maturity shift in how security programmes are built and measured. Threat intelligence will move from being a technical input to a strategic one, something that informs business decisions, not just workflows. Organisations that build that capability now will be significantly better positioned as those expectations become the norm.

From your perspective, where does Europe stand today in your field compared to other regions?

Europe has built a serious regulatory foundation. NIS2, DORA, and the broader EU framework

represent genuinely ambitious thinking about what secure digital infrastructure should look like. That matters. Regulation shapes markets, and Europe is setting a standard that other regions are watching closely.

The opportunity now is on the vendor side. European cybersecurity capability is stronger than its reputation suggests. There are companies here doing genuinely world-class work in threat intelligence, detection, and response. The conditions for building a competitive European cybersecurity industry exist. What's needed is the confidence to back it.

The dependency on providers headquartered elsewhere is a choice, not an inevitability. As geopolitical pressures sharpen and data sovereignty moves up the agenda, European organisations have both the incentive and the means to change that. The foundation is there. This is a moment to build on it.

What concrete action would most help Europe progress in your cybersecurity domain?

Procurement and investment decisions need to reflect the strategic priorities Europe says it has. There are capable European cybersecurity companies that struggle to scale not because the technology isn't there, but because the institutional support, public sector procurement, growth capital, and coordinated policy, lags behind what exists in the US or Israel. That's a solvable problem, and there are encouraging signs that appetite is growing to solve it.

Europe's startup and scale-up ecosystem is genuinely strong. The talent is here, the ideas are here, and increasingly the ambition is here. What's needed is the institutional backing to let that ecosystem reach its potential rather than watching promising companies either stall or get acquired by non-European players before they can make an impact.

Closer threat intelligence sharing between government and industry would also make a material difference. The threat picture is shared. The response shouldn't be fragmented.

Europe has the expertise, the regulatory clarity, and a growing ecosystem ready to deliver. The work now is creating the conditions for that to scale.

EclecticIQ

EclecticIQ is the leading threat intelligence platform born in Europe, serving global enterprises and critical national infrastructure. Our AI-embedded platform improves workflows, reduces analyst fatigue, and empowers cyber defenders to neutralize critical cyber threats while maintaining data sovereignty and regulatory compliance. We help teams make smarter, faster decisions with solutions that reduce complexity and streamline threat detection and response.

eclecticiq.com

Cody BARROW
CEO

EclecticIQ

Interview

ADVENS

COMMUNITY
CONTRIBUTOR

Europe needs to close the gap between its regulatory ambition and its operational capacity. We have some of the most advanced cybersecurity frameworks in the world.

How do you define the role of Service Advisory players in today's European cybersecurity ecosystem?

Service Advisory players are the connective tissue of the cybersecurity ecosystem. They don't just respond to incidents; they help organizations understand their exposure, make sense of a fast-evolving threat landscape, and build strategies that are actually implementable. But beyond technical expertise, the most valuable thing an advisory partner can offer is trust. In a context where cyber threats are becoming more sophisticated and regulations more demanding, organizations don't need vendors; they need trusted partners who walk alongside them, challenge their assumptions, and help them build resilience from within. That is the relationship Advens has always strived to build with its clients.

What key challenges do European organizations face when structuring their cybersecurity strategy?

The gap between awareness and action remains the most persistent challenge. Most organizations understand they are exposed; but translating that awareness into a coherent, prioritized strategy is where many struggle. This is compounded by a shortage of skilled talent, increasing regulatory complexity with frameworks like NIS2, DORA and CRA, and the growing pressure to secure not just IT environments but operational technology as well. There is also a cultural dimension: cybersecurity is still too often perceived as a technical problem rather than a business and governance issue. Changing that framing is part of what a trusted advisory partner does; not just once, but continuously, as threats and organizations evolve together.

From your perspective, where does Europe still need to strengthen its cybersecurity advisory capabilities?

Europe needs to close the gap between its regulatory ambition and its operational capacity. We have some of the most advanced cybersecurity frameworks in the world, but not enough organizations; especially mid-sized ones; have

access to the advisory expertise needed to translate those frameworks into concrete actions. We also need to move away from a transactional model of cybersecurity services toward genuine, long-term trusted partnerships. Threats don't respect national boundaries, yet advisory ecosystems remain largely fragmented along country lines. Building shared methodologies, mutual recognition of expertise, and truly European advisory communities is where we still have significant work to do.

How does your organization differentiate itself in the Service Advisory landscape?

Advens is a mission-driven company; we believe that cybersecurity should serve people and society, not just commercial interests. That shapes everything we do, starting with how we define our role: not as a provider, but as a trusted partner embedded in our clients' long-term security journey. We combine deep technical expertise; including PDIS qualification from ANSSI, CERT label from BSI and recognition across European regulatory frameworks; with a human-centered advisory approach that prioritizes lasting resilience over short-term compliance. Operating across France, Spain, Italy, and Germany, we bring both local knowledge and a genuinely European perspective. And as a B-Corp certified organization, we hold ourselves accountable to standards that go beyond the bottom line; because trust, ultimately, is earned through consistency and integrity.

Benjamin LEROUX
Chief Marketing Officer

Advens

Interview

WALLIX

COMMUNITY
CONTRIBUTOR

In the age of AI, identity must move from visual trust to cryptographic trust.

AI-FORGED IDENTITIES: WHEN "SEEING IS BELIEVING" NO LONGER WORKS

Identity has always been the foundation of any Zero Trust architecture. If we cannot trust the identity requesting access (human or machine) then the entire security model collapses.

Artificial intelligence is now challenging this foundation. With deepfake video, cloned voices, and synthetic identities built from stolen and generated data, attackers can convincingly impersonate employees, executives, or service providers. These forged identities can manipulate helpdesks, bypass onboarding processes, or even pass video-based verification.

The challenge is that detection alone will not solve the problem. Deepfake detection technologies are already locked in a cat-and-mouse race with generative AI. Security strategies must therefore assume that a forged identity may occasionally pass initial verification.

This is where Identity and Access Management must evolve. Strong governance, least-privilege policies, and privileged access controls ensure that even if a fake identity enters the system, it cannot automatically access critical resources. Approval workflows, just-in-time privileges, and full session monitoring significantly reduce the potential impact of such attacks.

Looking forward, trusted digital identity frameworks such as eIDAS 2.0 and the EU Digital Identity Wallet could strengthen IAM by introducing cryptographic identity verification issued by trusted authorities. Combining these state-backed identities with enterprise IAM may become a key pillar of future Zero Trust strategies.

Because in the age of AI, identity must move from visual trust to cryptographic trust.

WALLIX (Euronext: ALLIX since 2015) is the European champion of cybersecurity, helping organisations secure their critical assets and shape their digital sovereignty. Built on European values of security and freedom, WALLIX empowers its customers to control their digital destiny through efficient, simple and cost-effective solutions.

wallix.com

Guido KRAFT
Field CISO
WALLIX

REGIONAL LENS: THE NORDIC MODEL

The Nordic cybersecurity ecosystem offers a condensed view of Europe's possible future.

High digital maturity, early regulatory adoption, and decisive private equity involvement have enabled the emergence of pan-European platforms in structurally critical domains.

Identity has become infrastructure rather than a feature. Signicat's trajectory illustrates how identity, trust services, and compliance can be consolidated into a single, scalable platform serving both private and public sectors across borders. In parallel, Logpoint demonstrates the convergence of SIEM, NDR, and automation into unified SecOps platforms, particularly attractive to MSSPs serving NIS2-regulated SMEs.

The region also highlights a structural shift away from public markets. The take-private of WithSecure reflects the difficulty of executing long-term industrial transformation under public market pressure, reinforcing the role of private capital as an architect of cybersecurity consolidation.

The Nordic model is not universally replicable, but it offers three transferable lessons: focus on infrastructure layers, accept consolidation as a strategy rather than a failure, and align capital, regulation, and technology around long-term resilience.

TECHNOLOGY SHIFTS THAT RESHAPE THE MAPPING

Artificial intelligence has become the primary force reshaping cybersecurity.

By 2026, up to **90% of Tier-1 SOC** alerts are handled through automated triage and enrichment, redefining the role of human analysts from operators to supervisors.

At the same time, security priorities are moving down the stack. Firmware, embedded systems, and OT environments are now prime targets, elevating the strategic importance of European expertise in industrial security. Cryptography has entered a new phase, with post-quantum readiness moving from research to procurement planning for governments and critical infrastructure operators, and slated to become a regulatory mandate under the next version of NIS2.

As AI becomes a key enabler across all types of IT-based activities, the impact of AI-enhanced cyber attacks is becoming a major concern. AI does not only expand the toolkit available to hackers, but amplifies their potential impact: a compromised AI system can wreak havoc. This risk is compounded by the growing adoption of robotics in industry, which widens the attack surface of industrial environments. Connected vehicles offer another illustration of these shifts toward broader impact and the growing importance of embedded security.

These shifts explain why the Mapping increasingly clusters around identity, threat management, OT security, AI and cryptography, while standalone point solutions face growing pressure to integrate or disappear.

CONSOLIDATION & INFLECTION POINTS (2024–2026)

- **OCT 2024:** Darktrace acquired by Thoma Bravo ($5.3bn) – signal of European public market undervaluation
- **MAR 2025:** Google announces $32bn acquisition of Wiz – triggers unprecedented EU antitrust scrutiny
- **JUL 2025:** Palo Alto Networks announces acquisition of CyberArk ($25bn)
- **OCT 2025:** ServiceNow completes acquisition of Armis ($7.75bn)
- **DEC 2025:** Proofpoint completes acquisition of Hornetsecurity ($1.8bn)

This sequence marks a decisive acceleration of platform-centric consolidation, with direct consequences for European sovereignty, procurement choices, and innovation pathways.

STRATEGIC TAKEAWAYS FOR THE ECOSYSTEM

For CISOs and buyers, consolidation, interoperability, regulatory alignment and uncontrolled dependency sharp reduction, are no longer optional. Vendor selection increasingly implies long-term purchase decisions.

For founders and scale-ups, scale is now existential. Interoperability, capital efficiency, and the ability to integrate into platforms will determine survival.

For investors, value creation is shifting decisively from tools to platforms. The winners of the next cycle will be those capable of sustaining long-term R&D and executing cross-border consolidation.

For policymakers and institutions, the challenge is no longer to stimulate innovation, but to convert regulatory power and public capital into durable industrial leadership. We are not the first ones to suggest this transition. The problem now is essentially political: when do European Institutions decide it's time no more to be a spectator but take cybersecurity as the key lever it is and embark on a real pro-independence policy ?

This Mapping translates these dynamics into concrete actors and categories. It is not a catalogue, but a decision tool.

ANALYSIS
& DEEP DIVES

EUROPE'S CYBERSECURITY ECOSYSTEM 2026

Density Achieved. Consolidation Required.

The 2026 European Cybersecurity Mapping identifies **1,302 cyber-security companies** across Europe. This is not the full market. Europe hosts more vendors than those mapped. But this dataset is sufficiently broad and structured to reveal something important: Europe has achieved innova-tion density.

What it has not yet achieved is **industrial concentration.**

Compared to 2025, when 828 companies were mapped, the ecosystem now shows a **60% expansion in coverage**.

This growth reflects deeper scrutiny, broader geographic inclusion, and improved ecosystem visibility, more than a pure explosion of new vendor creation.

The picture that emerges is nuanced. Europe's cyber ecosystem is vibrant, mature, sovereign and still fragmented.

GEOGRAPHY

The ranking of countries remains structurally consistent.

France leads with 24.6% of mapped vendors, followed by Germany at 13.5%, and the UK at 10.8%

The Netherlands (10.1%) and Switzerland (9%) also nurture strong startup and scale-up environments.

However, the UK's rise to third position reflects improved scrutiny more than sudden expansion

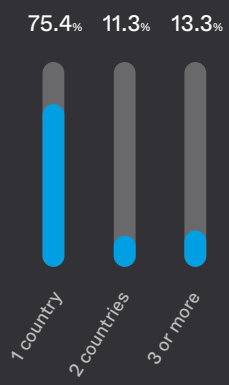
Eastern Europe and the Nordics continue to host several of the larger European cybersecurity players: ESET (Slovakia), Bitdefender (Romania), WithSecure (Finland), Outpost24 (Sweden), Nord Security (Lithuania), Signicat (Norway)

At the same time, six countries are clearly in growth mode: **Poland, Italy, Estonia, Spain, Denmark, Finland, Sweden**

Despite this broad distribution, one statistic defines the structural issue:

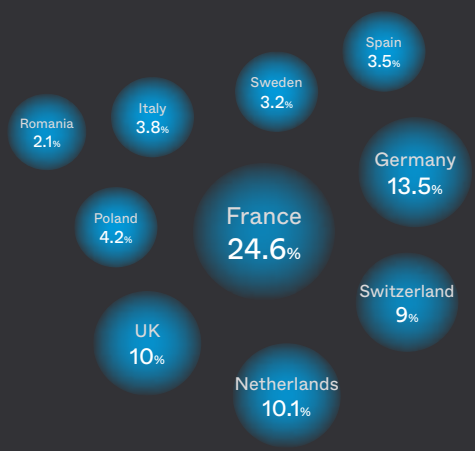
Cross-Border Footprint

NUMBER OF OPERATING COUNTRIES



Top Countries

SHARE OF MAPPED VENDORS

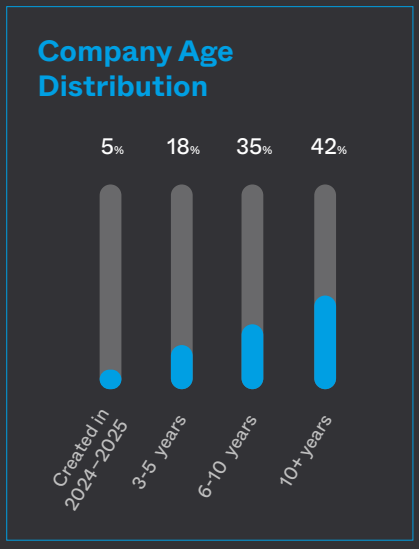


Europe's cybersecurity vendors remain primarily national players. The Single Market has not yet translated into a truly unified cybersecurity supply market.

ANALYSIS & DEEP DIVES

COMPANY AGE

For the first time, the Mapping integrates company age as a structured variable and the result is striking.



The main takeaway is clear:

Cybersecurity in Europe is no longer a nascent sector. It is an almost mature trade.

The rhythm of company creation is slowing. The industry is stabilizing.

However, maturity does not automatically translate into scale leadership.

Many European vendors are experienced.

Fewer have become continental or global champions.

COMPANY SIZE

The size distribution reveals the ecosystem's most persistent structural feature:

Nearly 71% of vendors have fewer than 50 employees.

Less than 5% exceed 500 employees.

To put this in perspective:

- Palo Alto Networks: 16,000 employees
- CrowdStrike: 10,400
- SentinelOne: 2,800

This employment gap explains much of Europe's competitive imbalance.

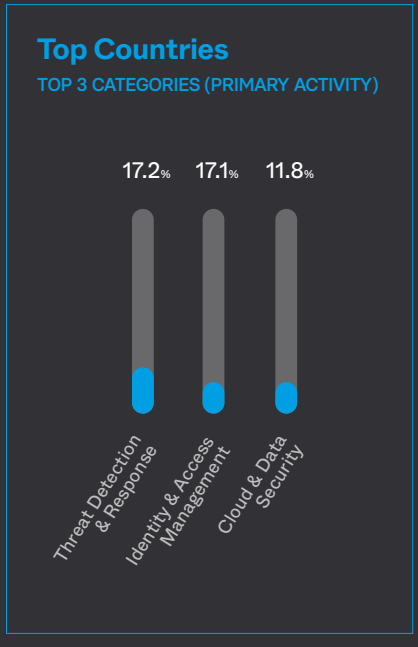
Smaller companies face greater difficulty in:

- Sustaining R&D intensity
- Funding commercial expansion
- Supporting global enterprise sales cycles

At a time when customers increasingly demand broader platforms rather than niche tools, this structural SME dominance becomes a constraint.

CATEGORIES

The top three cybersecurity categories remain unchanged compared to 2025:



These three domains dominate across the five largest countries: France, Germany, UK, Netherlands, Switzerland.

Threat Detection & Response

The historical backbone of cybersecurity from firewalls to EDR, NDR, XDR, now enters a new phase.

AI-based detection is reshuffling the landscape. Recent valuation drops among major US vendors suggest a transition phase in the market.

The open question:

Will the next generation be pure AI players or AI-enhanced cybersecurity specialists?

This shift may also increase the strategic importance of Cyber Threat Intelligence vendors, who provide the data feeding detection systems.

Identity & Access Management

IAM now slightly exceeds Cloud & Data Security.

IAM underpins zero-trust architecture — for both humans and machines.

It is also increasingly exposed to AI-forged identities and deepfake-enabled intrusion.

Identity may become one of the most contested battlegrounds of the next decade.

Vulnerability Management

Moving from one-shot scans to continuous evaluation, attack surface monitoring, predictive assessment, and supply-chain risk control.

This category is evolving toward integrated risk intelligence rather than simple scanning.

ANALYSIS & DEEP DIVES

Cryptography

Cryptography jumps from 12th to 5th position compared to 2025.

The pressure from quantum computing and the "steal now, decrypt later" threat is accelerating demand for post-quantum cryptography.

This is a strategic domain where Europe could lead.

OT Security

Still young. The race has only begun.

Few established global "kings" exist.

The window remains open.

AI Security & Integrity

Still below 3% overall, but growing.

When refined by company size:

- 6.1% of 11–50 employee companies
- 5.3% of 2–10 employee companies

This clearly signals a new creation wave.

AI systems themselves are vulnerable.

AI is also becoming the primary vector of attack and defense.

This dual role makes AI Security & Integrity likely the next strategic hotspot.

EUROPEANISATION

Encouragingly, in many major categories more than 25% of vendors operate in at least one additional European country.

Growing at European scale is no longer outside vendors' culture.

However, geographic presence does not equal revenue scale.

The revenue gap remains dramatic:

Top Vendor Revenue Gap

US VS EUROPE

Top 10 US vendors:

€33B total revenue

Top 9 European vendors:

€3.1B

Ratio:

10.69x

US vendors grow faster

15% excluding M&A effects

FRAGMENTATION

Fragmentation remains the defining structural issue. Consolidation is accelerating in the US: Palo Alto, Google/Wiz, ServiceNow/Armis, Protect AI.

Europe shows some M&A activity: Bitdefender/Mesh, Outpost24/Infinipoint, Seclab/Seckiot.

But the rhythm is slower.

There are few paths beyond fragmentation:

The good news: the window is open.

Even in mature domains, AI will reshuffle detection and response. European vendors must avoid building "me too" products and instead shoot for differentiation.

LEVER 3
Innovation

Unified capital markets and more strategic exit regulation are necessary to prevent premature external acquisitions.

LEVER 2
Capital

Public and private procurement policy must better steer orders toward scale-building.

LEVER 1
Demand

WHAT COMES NEXT

The Mapping is more than a list.

It can serve:

- Vendors seeking peer visibility
- Investors scouting consolidation targets
- Integrators mapping partnerships
- Buyers diversifying supply chains
- Analysts building independent European perspectives

Potential next steps:

- Creating category communities
- Deepening functional product analysis
- Measuring technological independence
- Providing a European analytical reference alternative to US consultancies

FINAL DIAGNOSIS

Europe's cybersecurity ecosystem is:

- Large
- Mature
- Technically competent
- Geographically broad
- Structurally fragmented

The next phase will not be defined by startup creation. It will be defined by consolidation, capital depth, and strategic coordination.

Europe has built the forest. It now needs stronger trees.

Interview

CESIN

While consolidation and platformization will be necessary in certain segments, European organizations already have the ability to build cybersecurity architectures based entirely on European solutions.
As the saying goes: where there's a will, there's a way.

THE ON-THE-GROUND REALITY FOR LARGE ORGANIZATIONS

From the perspective of CESIN members;CISOs, heads of cybersecurity, and senior cyber leaders; cyberattacks remain both highly frequent and increasingly impactful. According to the CESIN Barometer 2026, attempted attacks continue at scale, but there is a notable and encouraging trend: year after year, the number of successful and truly significant attacks is declining among member organizations.

Today, CESIN represents more than 1,200 members, with over 800 organizations actively contributing to the Barometer. This improvement clearly demonstrates that the sustained human and financial investments made by organizations are paying off. As illustrated during the Paris Olympic Games, cybersecurity can be effective when it is approached seriously, collectively, and in a coordinated manner.

This does not mean the threat is diminishing. Cybercriminals are becoming more efficient, and artificial intelligence is emerging as a powerful amplifier of attack capabilities. At the same time, however, cyber-defense systems are also benefiting from AI. These solutions are widely endorsed by CISOs; 88% consider them well adapted to current challenges; and AI is increasingly used to enhance detection, response, and overall effectiveness.

CYBER TRANSFORMATIONS: FROM 2023 TO 2027

There is a clear "before and after" marked by 2022 and the arrival of generative AI. While AI had already been used for years in cybersecurity; particularly in monitoring and supervision tools; the unprecedented speed at which generative AI has been adopted has profoundly disrupted CISO agendas.

Alongside Shadow IT, organizations are now facing Shadow AI. Security teams must deal with increasingly aggressive attack techniques, while simultaneously securing AI systems themselves as they are integrated into business processes. The CESIN Barometer confirms this shift: in 2025, the use of non-approved AI services became the most critical behavioral risk within organizations.

Looking ahead to 2027, securing AI usage and governance will be unavoidable challenges for both large enterprises and public administrations.

EUROPE'S POSITION THROUGH THE LENS OF USERS

Europe's dependency on foreign; and especially American; technology providers has become a growing concern for user organizations. This issue has gained renewed urgency in the context of geopolitical uncertainty and the unpredictability of recent U.S. political decisions, with their potential impact on the global economy.

In cybersecurity, however, the situation is more nuanced than in IT overall. The market remains highly fragmented, offering a wide range of solutions, including European alternatives. In its latest Cyber Panorama, CESIN, together with Hexatrust, identified more than 320 cybersecurity software solutions in France alone.

While consolidation and platformization will be necessary in certain segments, European organizations already have the ability to build cybersecurity architectures based entirely on European solutions. As the saying goes: where there's a will, there's a way.

STRENGTHENING THE EUROPEAN CYBERSECURITY ECOSYSTEM

Europe has many strengths: high-level talent, innovative solutions, and a sizeable market. Yet scaling remains a major challenge. Cybersecurity solutions are fragmented; and so is funding. Investor risk appetite remains limited, slowing down the emergence of European champions.

From a regulatory perspective, there is also a lack of strong incentives to favor European solutions, both in France and at the EU level. While the European Parliament has begun to address this issue, progress remains cautious and slow. To truly shift mindsets; starting with public-sector procurement; Europe must now move faster and more decisively.

CESIN

CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) is a French professional association dedicated to information and digital security. It brings together CISOs and cybersecurity experts to share knowledge, best practices, and experience through plenary sessions, working groups, thematic communities, and an annual congress. CESIN also conducts regulatory and vulnerability monitoring, and publishes white papers and an annual cybersecurity barometer for French organizations.

cesin.fr

Alain BOUILLÉ
General Delegate
CESIN

Interview

CAISSE DES DÉPÔTS

Cyber risk is now clearly identified within organizations: 92% rank it among the top five risks in their risk mapping, and 90% ensure regular monitoring at executive committee level.

OBSERVED DEVELOPMENTS AND POSITIVE SIGNALS

Over the past few years and as confirmed by the latest CESIN Barometer we have observed a decline in significant cyberattacks (40% in 2025 compared to 47% in 2024). However, when such attacks are successful, their consequences and overall impact on victims tend to be more severe.

Overall, efforts to improve cybersecurity levels continue across large companies and public administrations. As a result, the information systems of more mature organizations have become more resilient. That said, certain attack vectors remain preferred entry points for threat actors: the human factor (phishing, spear phishing, and smishing), which accounts for 55% of incidents; unpatched vulnerabilities (41%); and interconnections with third parties (35%).

Caisse des Dépôts has not been immune to these trends. Even though our cybersecurity maturity level is high, we decided to intensify our phishing simulation campaigns. We now conduct one exercise per month, combined with targeted awareness sessions for employees who clicked on phishing emails. Technical vulnerability levels and patching frequency are now monitored monthly through a cybersecurity dashboard shared with three members of the executive committee: the Chief Operating Officer, the Chief Risk Officer, and the Chief Executive Officer.

Finally, efforts to better control third-party cyber risks have been strengthened. The implementation of the Digital Operational Resilience Act (DORA) in the banking and insurance sectors has further raised contractual requirements and audit standards for outsourced service providers.

CYBERSECURITY, GOVERNANCE, AND RISK MANAGEMENT

Cyber risk is now clearly identified within organizations: 92% rank it among the top five risks in their risk mapping, and 90% ensure regular monitoring at executive committee level. Depending on the sector, cybersecurity may still be viewed primarily through a technical lens within IT departments.

The most mature organizations or those subject to regulatory requirements have chosen to position cybersecurity governance within their risk management functions. In these structures, while cyber threat detection and response remain critical, cyber risk mapping, controls, and reporting benefit from methodologies and experience developed for financial and other operational risks.

This governance model is the one implemented at Caisse des Dépôts.

EUROPEAN POSITIONING AND UPCOMING PRIORITIES

Geopolitical turbulence throughout 2025 has led to increased awareness among policymakers and business leaders in Europe of their technological dependence on American solutions and, to a lesser extent, Israeli solutions, which is nonetheless an important consideration in the cybersecurity domain.

Around two-thirds of companies surveyed by CESIN report being concerned by issues related to digital sovereignty and trusted cloud solutions (63%). At Caisse des Dépôts, the defense of sovereignty was already one of the three strategic priorities set by our new CEO, Olivier Sichel. In early 2026, he launched a dedicated program Horizon Numérique 2030 to mobilize all group capabilities in order to reduce the technological dependency of our information systems, notably through the procurement of sovereign solutions.

We also plan to increase our investment capacity in European technologies via Bpifrance's Deep Tech funds. Beyond the group itself, we are actively promoting the Digital Resilience Index, which aims to objectively measure sovereignty risk across eight dimensions: strategic and geopolitical, economic and legal, operational, security and continuity, environmental, technological, data and AI, and supply chain.

It is our collective responsibility to foster the emergence of innovative European solutions capable of scaling and competing with global leaders.

KEY CYBER TRENDS AND THREATS

The main cyber threat trend observed in 2025 and expected in the coming years stems from the faster adoption of artificial intelligence by attacker groups compared to cyber-defense teams. As a result, the number of discovered vulnerabilities is increasing, exploitation timelines are shortening, lateral movement within victims' information systems is accelerating, and data exfiltration incidents are becoming more frequent.

One of the key challenges in the coming semesters will be to reduce this asymmetry by automating incident response across all large enterprises and public administrations.

Caisse des Dépôts and its subsidiaries constitute a state-owned group providing long-term investment at the service of France's public interest and the country's economic development. It combines five areas of expertise: social policy (pensions, professional training, disability, old age and health), asset management, monitoring subsidiaries and strategic shareholdings management, business financing (with Bpifrance), and Banque des Territoires.

caissedesdepots.fr

Arnaud MARTIN

Director of Operational Risks
Group Risk Department

Caisse des Dépôts

European Cybersecurity Mapping 2026

AI SECURITY AND INTEGRITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: As AI systems become widespread, so do their specific vulnerabilities: compromised training data, prompt injection, user interface corruption, and loss of control over autonomous agents. A new generation of tools is emerging to counter these threats, safeguarding AI systems and data integrity, and preventing adversarial attacks, biases, and unauthorized manipulation.

Why Choose European Technology: As AI will percolate in all domains, making sure AI systems are trustworthy is essential. Developing an European industry to achieve this objective is therefore also essential. European technology offers a pathway to a strong economy and technological independence. Furthermore, European providers champion ethical AI aligned with EU principles, mitigating the risk of foreign dependencies that could introduce vulnerabilities or ethical concerns. Supporting them guarantees Europe's leadership in AI innovation and compliance with strict privacy laws.

Importance for European sovereignty: 10/10

AI technologies shape critical decisions across industries. Ensuring their security, the integrity of data used to develop the tools, and alignment with European ethical standards is essential for strategic independence and trustworthiness.

The Market That Didn't Exist Three Years Ago

kuppingercole ANALYSTS

MARKET CONTEXT

Every organization is now an AI company, whether it planned to be or not. Employees use ChatGPT, Claude, NotebookLM, and other AI-powered tools to draft emails, summarize documents, and write code. Business units have built retrieval-augmented generation systems on corporate data without consulting IT. Development teams integrate LLM APIs into customer-facing products on timelines that leave security reviews as an afterthought. This is the reality I encounter in advisory engagements across Europe: AI adoption has outpaced AI governance, and the security implications are only beginning to surface.

EUROPE'S COMPETITIVE ADVANTAGE

The EU AI Act establishes a regulatory framework that will shape this market for years. European vendors developing AI security tools understand the Act's risk classification system, documentation requirements, and conformity assessments better than US competitors often do. This matters because enterprises deploying high-risk AI systems need tooling that aligns with regulatory obligations, not generic security controls retrofitted with AI terminology.

The GDPR adds another layer. When LLMs process personal data, questions of lawful basis, data minimization, and the right to erasure become thorny. European vendors who have spent years building privacy-preserving architectures understand these problems from first principles, not as an export-market compliance exercise.

TECHNOLOGY EVOLUTION & TRENDS

The technology is evolving rapidly across several domains. Prompt injection remains the signature vulnerability of LLM-powered applications, and defenses are maturing from simple input filtering toward semantic analysis and multi-layered validation. Data loss prevention has gained new relevance; organizations need to prevent sensitive information from leaking into model prompts and training data. Runtime protection platforms now monitor LLM behavior for anomalies, toxic outputs, and policy violations. AI gateways sit between users and models, enforcing access controls and logging interactions for audit. Model supply chain security has emerged as a concern following demonstrations of backdoored models and poisoned training data. Each represents a distinct product category, though vendors are beginning to assemble broader platforms.

MARKET DYNAMICS

Market dynamics in AI security differ from those in mature cybersecurity segments. The space is young and fragmented, with venture funding continuing despite broader tech-sector pullbacks. I track roughly forty European vendors with credible AI security offerings, though definitions remain contested and many are pivoting from adjacent markets. Consolidation has begun. F5's acquisition of Heyhack and Palo Alto's purchase of Protect AI signal that platform vendors view AI security as strategic. European start-ups with strong technology but limited go-to-market reach are attractive acquisition targets, particularly those with EU AI Act compliance expertise built into their products.

FUTURE

The next two years will determine market structure. Enterprises are moving from experimentation to production AI deployments, and security requirements crystallize as systems handle real data and real decisions. I expect procurement to consolidate around vendors who address multiple AI security domains, rather than point solutions for individual attack vectors. European vendors have a window of opportunity as the EU AI Act compliance deadline approaches, and organizations seek partners who understand the regulatory landscape.

Those who build strong reference customers in regulated industries will have durable competitive positions. For investors, the logic is simple: AI security is not optional, the market is early, and European regulatory complexity strongly favors local expertise. Vendors who solve the compliance-plus-security problem will command premium valuations at exit.

Jonathan CARE
Lead Analyst
KuppingerCole Analysts AG

For detailed analysis, see:
Leadership Compass: Generative AI Defense
Whitepaper: Navigating the Future of Authentication in the Age of AI and Deepfakes

AI SECURITY AND INTEGRITY (1/2)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Advai	2020	GB London	11-50	EU			●		●												●	
ai+me	2023	GR Loannina	2-10	EU			●														●	●
AI-vidence	2020	FR Meudon	2-10	EU			●		●													
Anyway Systems		CH Lausanne	2-10	EU			●															
ASIMOB	2016	ES Bilbao	2-10	EU			●		●												●	
Calvin Risk	2022	CH Zurich		EU			●						●									●
Checkstep	2020	GB London	11-50	EU			●						●								●	
CiberTECCH	2023	PT Braganca	2-10	EU			●														●	
ClairVault	2023	CH Prilly	2-10	EU			●															
FLock.io	2022	GB London	11-50	EU			●			●		●										
Giskard	2021	FR Paris		EU			●	●														
Glaider	2024		2-10				●			●											●	●
Holistic AI	2020	GB San Fran.	11-50	NA EU			●		●				●									
INTA Systems	2020	IT Pisa	11-50	EU			●															
LABEL4.AI			2-10				●						●			●					●	
Lakera	2021	CH San Fran.	11-50	NA			●		●												●	●
Mindgard	2022	GB Boston	11-50	NA EU			●		●												●	
naaia.ai	2022	FR Paris	11-50	EU			●															
Numalis	2015	FR Montpellier	11-50	EU			●		●				●									
Oxford Dynamics	2020	GB Harwell	11-50	EU			●			●											●	
PowerBrain.Shop¬Æ	2019	NL Eindhoven	11-50	EU			●															
Safe Intelligence	2022	GB London	2-10	EU			●		●												●	

AI SECURITY AND INTEGRITY (2/2)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
SHIELD AI	2024	BE Brussels	2-10	EU			●			●											●	
Skyld AI	2021	FR Rennes	2-10	EU	●		●								●							
Stealthium	2024	US San Fran.	2-10	NA			●								●						●	
Surelio.ai			2-10				●															
Suzan AI		FR Paris	2-10	EU			●						●									
Validaitor	2022	DE Karlsruhe	11-50	EU	●		●						●									

Want to add your company or update your company information?

You can do it directly via our data portal: cybermapping.european-champions.org

Interview

CESIN

We are seeing the emergence of cybersecurity that is more professional, more organized, and more resilient.

KEY CYBER TRENDS AND THREATS

The key trends are clear in the CESIN 2026 Barometer: threats are becoming more geopolitical, more industrial, and more systemic.

They are shifting toward the supply chain, relying on the massive exploitation of vulnerabilities, and accelerating with AI.

Organizations are particularly exposed to non-sovereign cloud risks, poorly controlled third parties, and increasing technological complexity.

We are entering an era where cybersecurity is no longer confined to the internal perimeter but unfolds within a global, interconnected ecosystem often outside direct control.

POSITIVE SIGNALS AND MITIGATION CAPABILITIES

The CESIN 2026 Barometer sends very positive signals: organizations are becoming better prepared, better equipped, and more structured in managing cyber risk.

They are making progress in detection, prevention, and even response, with four out of five considering themselves ready to handle a major attack.

They are also strengthening their control of third-party risk: contractual clauses, security questionnaires, audits, cyber-rating…

And above all, they are gaining maturity: better visibility of assets, identification of the 'crown jewels,' more frequent crisis exercises. In short: despite high levels of threat, mitigation capabilities are clearly improving.

We are seeing the emergence of cybersecurity that is more professional, more organized, and more resilient. New regulations will also help raise the bar and enable a more global approach not only focused on 'crown jewels.'

CHANGES IN THE ROLE OF THE CISO AND INTERNAL POSTURE

Today, as explained in the WEF publication Elevating Cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs, the role of the CISO has fundamentally changed. We are no longer just system guardians: we have become central actors in corporate strategy, because cybersecurity directly influences resilience, trust, and an organization's ability to grow.

The CISO no longer simply protects: the CISO builds resilience. In a world where threats are systemic, security is not a state it is a permanent capacity to adapt, embedded in the organization's operations.

This transformation requires a deep shift in internal posture: we must influence, build alliances, speak the language of the business, and engage every function in risk management. Cybersecurity becomes a collective responsibility, a shared reflex.

Finally, the goal is no longer only to avoid crises: it is to turn cybersecurity into an accelerator of trust, innovation, and competitiveness. The organizations that will succeed are those that view cyber not as a constraint but as a strategic asset.

CISOs in small and medium-sized organizations need support to expand their skills, visibilityto increase their impact.

TECHNOLOGICAL DEPENDENCIES AND NON-EUROPEAN SUPPLIERS

Our technological dependence on non-European suppliers has become a full-fledged strategic risk. It is no longer just a cybersecurity issue: it is a matter of sovereignty, business continuity, and regulatory control.

Geopolitical fragmentation and globalized supply chains create systemic vulnerability. Every technological dependency outside Europe exposes us to extraterritorial laws, lack of transparency, and loss of operational control.

The CESIN Barometer quantifies this reality: organizations are deeply concerned about the risks tied to non-European cloud providers, extraterritoriality, and insufficient visibility on subcontractors. Incidents involving third parties are surging, and digital sovereignty is becoming a priority for most companies.

The message is clear: resilience also depends on our ability to manage and reduce technological dependencies. Reducing risk, diversifying suppliers, demanding transparency, and rebalancing our ecosystem are now imperatives not options. Several initiatives aiming to measure resilience and technological autonomy are underway; they must be tested and supported to properly manage this risk.

CESIN

CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) is a French professional association dedicated to information and digital security. It brings together CISOs and cybersecurity experts to share knowledge, best practices, and experience through plenary sessions, working groups, thematic communities, and an annual congress. CESIN also conducts regulatory and vulnerability monitoring, and publishes white papers and an annual cybersecurity barometer for French organizations.

cesin.fr

Frank VAN CAENEGEM
Vice President

VP CESIN

Cybersecurity VP
& CISO EMEA

Schneider Electric

European Cybersecurity Mapping 2026

APPLICATION SECURITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Applications are the top layer of the technology stack, sitting above infrastructure and base systems, making them a primary target. Dedicated tools protect applications from vulnerabilities throughout development and deployment, ensuring secure functionality. They prevent breaches from compromised websites or APIs and filter unauthorized Internet connections.

Why Choose European Technology: European companies deliver localized solutions that strictly adhere to EU standards. This ensures no data leaks to non-compliant jurisdictions, which is key to reinforcing Europe's strategic autonomy and building trust in secure application development.

Importance for European sovereignty: 7/10

Importance for European sovereignty: 7/10 While important for protecting software applications, the impact on sovereignty is more indirect. However, reliance on foreign tools could introduce risks like hidden vulnerabilities or backdoors.

Securing Modern Software Across Its Full Development and Runtime Lifecycle

kuppingercole ANALYSTS

MARKET CONTEXT

Application security is no longer a specialist topic reserved for development teams or security engineers. For most organizations, it has become a critical part of understanding and managing operational risks. Modern applications are built from loosely coupled components, APIs, cloud services, and third-party code, all of which change frequently. Vulnerabilities are no longer exceptional events but a predictable outcome of the scale and speed of modern development.

Regulatory frameworks such as NIS2 and DORA reflect this reality by explicitly linking secure software development and resilience to management responsibility. In advisory conversations, application security now comes up alongside business continuity, outsourcing risk, and audit readiness.

EUROPE'S COMPETITIVE ADVANTAGE

European vendors typically approach the market from a different angle than many global platform providers. Compliance with GDPR, data residency requirements, and sector-specific regulations is often built into product design rather than added later. This is important for application security because source code, logs, and runtime telemetry may be processed or stored outside production environments.

European vendors are generally clearer about where data is handled and under which legal framework, which simplifies procurement and risk assessments for regulated businesses. While this does not automatically translate into stronger functional capabilities, it often results in solutions that fit better with how European enterprises and public sector bodies operate. In the end, this helps eliminate the false dichotomy of balancing security and productivity that is often considered one of the leading reasons for data breaches and other cybersecurity incidents.

TECHNOLOGY EVOLUTION AND TRENDS

From a technological perspective, application security today looks very different from what it did even a few years ago. Static and dynamic testing are still part of the picture, but they are no longer enough on their own. Security controls are increasingly embedded directly into CI/CD pipelines, developer environments, and runtime platforms, where they can actually influence how software is built and operated. Software composition analysis has become table stakes, simply because most applications now consist largely of open-source and third-party components.

API security, once treated as a separate problem, is increasingly handled as part of application security proper, which mirrors the shift of business logic into APIs. AI-assisted analysis is being used to help teams deal with volume and prioritization, but it is not a silver bullet. In most organizations, skilled people are still needed to evaluate specific risks and set priorities accordingly.

MARKET DYNAMICS

The application security market remains fragmented and, at times, confusing for buyers. Large vendors continue to bundle application security into broader cloud, developer, or security platforms, often prioritizing integration and coverage over depth. Hyperscaler-native tools work well within a single ecosystem but tend to struggle in hybrid and multi-cloud environments common in Europe.

European specialists usually focus on narrower problem areas such as API security, vulnerability management, or compliance-oriented reporting. Consolidation is happening, but mostly in small steps, with acquisitions aimed at closing capability gaps rather than reshaping the market.

FUTURE

Regulations like the Cyber Resilience Act will increase pressure on application security vendors to demonstrate measurable risk reduction rather than just the number of detections. Integrations with identity, cloud security posture management, and software supply chain controls will become stronger, even further blurring the lines between cybersecurity disciplines.

Buyers will expect vendors to integrate into existing workflows and to operate within strict data protection constraints by design. Solutions that focus on well-defined problems, provide transparent data handling models, and scale through partnerships rather than platform expansion are more likely to succeed. In practical terms, this will matter more than the number of offered features over the coming years, particularly in the European market.

For detailed analysis, see:

Alexei BALAGANSKI
Lead Analyst
KuppingerCole Analysts AG

Leadership Compass: API Security and Management
Leadership Compass: Cloud Native Application Protection Platforms
Leadership Compass: Web Application and API Protection
Advisory Note: Vulnerability Management

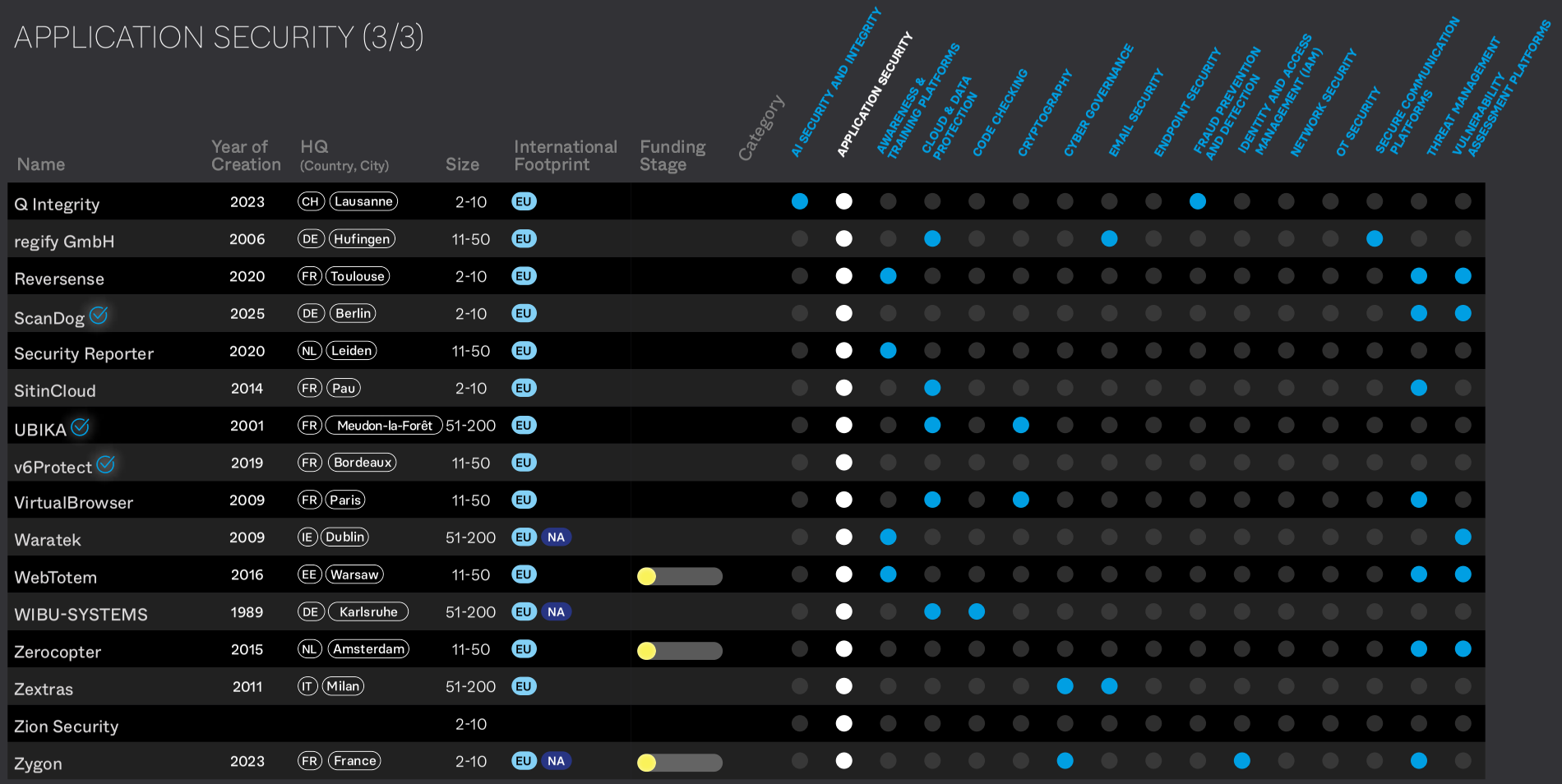
APPLICATION SECURITY (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
42Crunch	2016	IE Dublin	51-200	EU NA			○	●	○	○	○	○	●	○	○	○	○	○	○	○	●	●
Adaptive Shield		FR Tel Aviv	51-200	APAC			○	●	○	●	○	○	○	○	○	○	●	○	○	○	●	●
aicas	2001	DE Karlsruhe	51-200	EU NA			○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Airlock	2018	CH San Fran.	2-10	NA			○	●	○	●	○	○	○	○	○	○	●	○	○	○	○	○
Approov Mobile Security	2001	GB Edinburgh	11-50	EU NA			○	●	○	●	○	○	○	○	○	○	○	○	○	○	●	●
APPVISORY	2012	DE Hannover	11-50	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	●	○
AquilaX Security	2023	GB London	11-50	EU NA			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
ARCAD Software	1992	FR Chavanod	51-200	EU NA APAC			○	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
ATAKAMA Technologies	2015	FR La Ciotat	11-50	EU			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
Avanoo (ex-Sonar)	2023	FR Remote	2-10	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
BitSensor	2015	NL Eindhoven	11-50	EU			○	●	○	●	○	○	○	○	○	○	○	○	○	○	●	○
Blindspot Technologies	2023	CZ Prague	11-50	EU			○	●	○	●	○	○	○	○	○	○	○	●	○	○	●	○
BotGuard.ai	2025	GB London	2-10	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
bowbridge Software GmbH	2005	DE Walldorf	11-50	EU NA			○	●	○	○	○	○	○	○	●	○	○	○	○	○	●	○
Checkmarx Partner Hub	2006	US Paramus	501-1,000	NA			○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	●
CloudEssence		IL Tel Aviv	2-10	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	○	●	●
Codesealer A/S	2018	DK Copenhagen	11-50	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CryptoExperts	2009	FR Paris	2-10	EU			○	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○
Cryptosense	2013	FR Paris	11-50	EU			○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	●
digitronic computersysteme	1990	DE Chemnitz	11-50	EU			○	●	○	○	○	●	○	○	○	○	●	○	○	●	○	○
Equixly API Security		IT Verona	11-50	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	●	○

APPLICATION SECURITY (2/3)

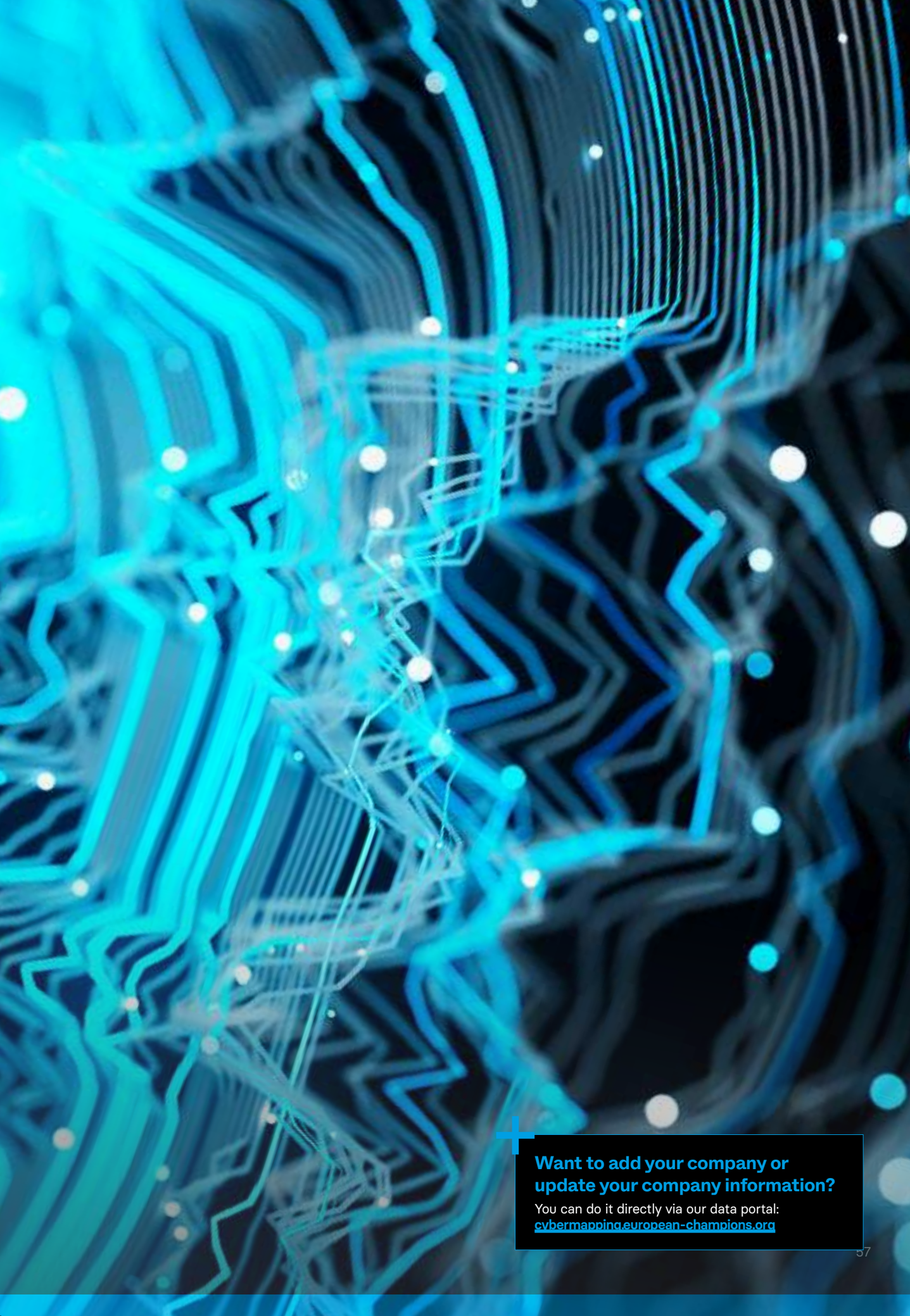
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
F3NIX	2024	FR Paris	2-10	EU			○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○
FTAPI Software GmbH	2010	DE Munich		EU			○	●	○	●	○	●	○	●	○	○	○	○	○	●	○	○
GitGuardian	2017	FR Paris		EU			●	●	○	○	●	○	○	○	○	○	●	○	○	○	●	●
Guardsquare	2014	BE Leuven	51-200	EU NA			○	●	○	○	○	○	○	○	○	○	○	○	○	○	●	●
Idyllum Labs	2020	EE Tartu	2-10	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	●	●
Ikusa Cybersecurity			2-10				○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	●
IriusRisk		ES Cuarte	51-200	EU NA			○	●	●	○	○	○	○	○	○	○	○	○	○	○	●	○
Jscrambler	2014	PT San Fran.	51-200	NA EU			○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	●
Keysight Device Security	2001	NL Delft	201-500	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	●
Merox	2018	FR Montpellier	11-50	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Modino.io	2021	PL Olsztyn	2-10	EU			○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Monit24	2010	PL Warsaw	11-50	EU			○	●	○	○	○	○	○	●	○	○	○	●	○	○	●	○
Mr Suricate	2015	FR Nantes	11-50	EU			○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Myra Security GmbH	2012	DE Munich	51-200	EU			○	●	○	○	○	○	○	○	○	●	○	●	○	○	●	○
NOVALYS	1998	FR Boulogne-Bill.	11-50	EU			○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Offensive 360	2017	NL Amsterdam	51-200	EU			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
OGO SECURITY	2018	FR Paris	11-50	EU			●	●	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Partisia	2008	DK Aarhus		EU			●	●	○	●	○	●	○	○	○	●	●	○	○	●	○	○
Patchstack	2017	EE Parnu	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●
Pluribus One	2015	IT Elmas	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	○
PortSwigger	2008	GB Knutsford	51-200	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	○
Probely		PT Porto	11-50	EU NA			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●

APPLICATION SECURITY (3/3)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
Q Integrity	2023	CH Lausanne	2-10	EU	
regify GmbH	2006	DE Hufingen	11-50	EU	
Reversense	2020	FR Toulouse	2-10	EU	
ScanDog	2025	DE Berlin	2-10	EU	
Security Reporter	2020	NL Leiden	11-50	EU	
SitinCloud	2014	FR Pau	2-10	EU	
UBIKA	2001	FR Meudon-la-Forêt	51-200	EU	
v6Protect	2019	FR Bordeaux	11-50	EU	
VirtualBrowser	2009	FR Paris	11-50	EU	
Waratek	2009	IE Dublin	51-200	EU NA	
WebTotem	2016	EE Warsaw	11-50	EU	
WIBU-SYSTEMS	1989	DE Karlsruhe	51-200	EU NA	
Zerocopter	2015	NL Amsterdam	11-50	EU	
Zextras	2011	IT Milan	51-200	EU	
Zion Security			2-10		
Zygon	2023	FR France	2-10	EU NA	

Category: AI SECURITY AND INTEGRITY; APPLICATION SECURITY; AWARENESS & TRAINING PLATFORMS; CLOUD & DATA PROTECTION; CODE CHECKING; CRYPTOGRAPHY; CYBER GOVERNANCE; EMAIL SECURITY; ENDPOINT SECURITY; FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM); NETWORK SECURITY; OT SECURITY; SECURE COMMUNICATION PLATFORMS; THREAT MANAGEMENT; VULNERABILITY ASSESSMENT PLATFORMS



Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

European Cybersecurity Mapping 2026

CLOUD AND DATA PROTECTION

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: The goal is simple: ensure data is protected from all risks whether from hacking, malice, negligence, system disruption, or failure. This is achieved by securing cloud environments and sensitive data through a suite of measures: secure storage and backup, air-gapping, anonymization (including encryption), rigorous access control, and compliance measures.

Why Choose European Technology: European vendors not only protect sensitive data from illicit access but also guarantee it remains within EU jurisdictions, offering robust protection without exposure to foreign surveillance laws. This empowers governments and businesses to maintain data control and achieve core sovereignty objectives.

Importance for European sovereignty: 10/10

Data sovereignty is a cornerstone of European independence. Cloud solutions directly affect data privacy, compliance (GDPR), and resilience against external control.

Data Protection and Cloud Resilience

kuppingercole ANALYSTS

MARKET CONTEXT

The EU cloud services market, estimated at over €80 billion and growing by 24% annually, is predominantly dominated by US providers, claiming around 70% of the market share. This expansion is poised to speed up with the adoption of GenAI. While data protection is crucial, cloud cyber resilience has become the primary concern. Service outages, like the recent one from AWS, demonstrate the significant impact on EU organizations.

A central sovereignty issue is governmental overreach, especially in geopolitical conflicts, making cloud services reliant on cross-border infrastructure particularly vulnerable. This situation underscores the need to focus on preventing lock-in and preparing exit strategies.

The EU GDPR and EU–U.S. Data Privacy Framework partially address data protection. However, US laws like the CLOUD Act allow the US government access to data beyond its borders, straining trust in US-based cloud services for EU organizations.

EU COMPETITIVE ADVANTAGE

These dynamics give EU-based cloud services a competitive advantage, alongside tools mitigating risks linked with non-EU cloud providers. Security and compliance responsibility is split between the provider and the customer. Many cloud-related incidents stem from customers failing to establish adequate controls. EU regulations like NIS2 and DORA require organizations to enforce controls, but lack of standardization creates lock-in issues.

TECHNOLOGY EVOLUTION AND TRENDS

Cloud services rely on proprietary technology for scalability and automation, mostly owned by non-EU providers. OpenStack and SUSE stand as alternatives, but the EU lacks prominent SaaS options for office automation.

Technologies like identity and access management are vital, as most cyberattacks begin with credential theft. Encryption safeguards data at rest, yet key protection is crucial. Pseudonymization allows for secure data sharing, aligning with ENISA recommendations.

Data backup and recovery remain critical. Tools in this domain prevent both lock-in and lock-out, with innovations in backup formats enabling environment conversion and immutability safeguarding against ransomware.

MARKET DYNAMICS

The US-based hyperscale providers have embarked on projects to deliver their cloud services in an EU-sovereign way. For example, by delivering the service from an EU-owned and operated partner like Google and S3NS. There are some EU-owned and operated cloud IaaS services led by OVHcloud in France. These still account for less than 15% of the EU cloud market.

FUTURE

The EU has the knowledge and competence to provide its own cloud technologies, but it is too late in the market evolution to play catch up. The market for cloud services in the EU will continue to be based on US technology stacks. These will be delivered through EU partners for those market areas that demand the highest level of sovereignty and are willing to pay the premium price.

The market in data protection add-on tools and services will continue to grow in the areas of managed cloud services, data protection, and compliance. This market for IaaS related security tools is consolidating into one for platforms as opposed to point products.

The market for cyber resilience tools and services around cloud services will grow strongly because of the increasing dependence on these services as well as the high levels of both economic and geopolitical cyber threats.

Mike SMALL
Senior Analyst
KuppingerCole Analysts AG

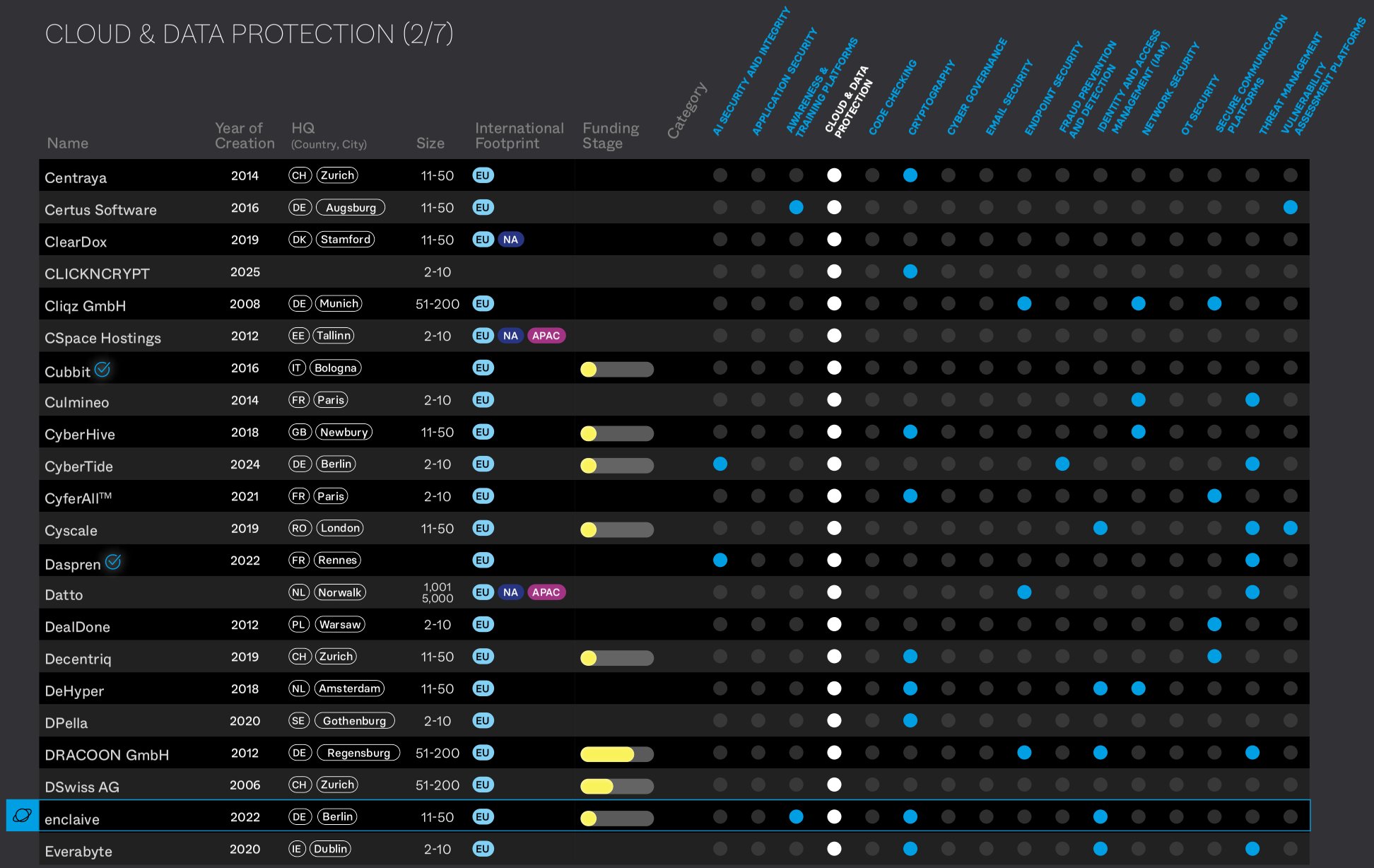
For detailed analysis, see:

Leadership Compass: Cloud Native Application Protection Platforms (CNAPP)
Leadership Compass: Cloud Backup for AI Enabled Cyber Resilience
Leadership Compass: Data Governance
Leadership Compass: Enterprise Secrets Management
Leadership Compass: Cloud Infrastructure Entitlement Management (CIEM)

CLOUD & DATA PROTECTION (1/7)

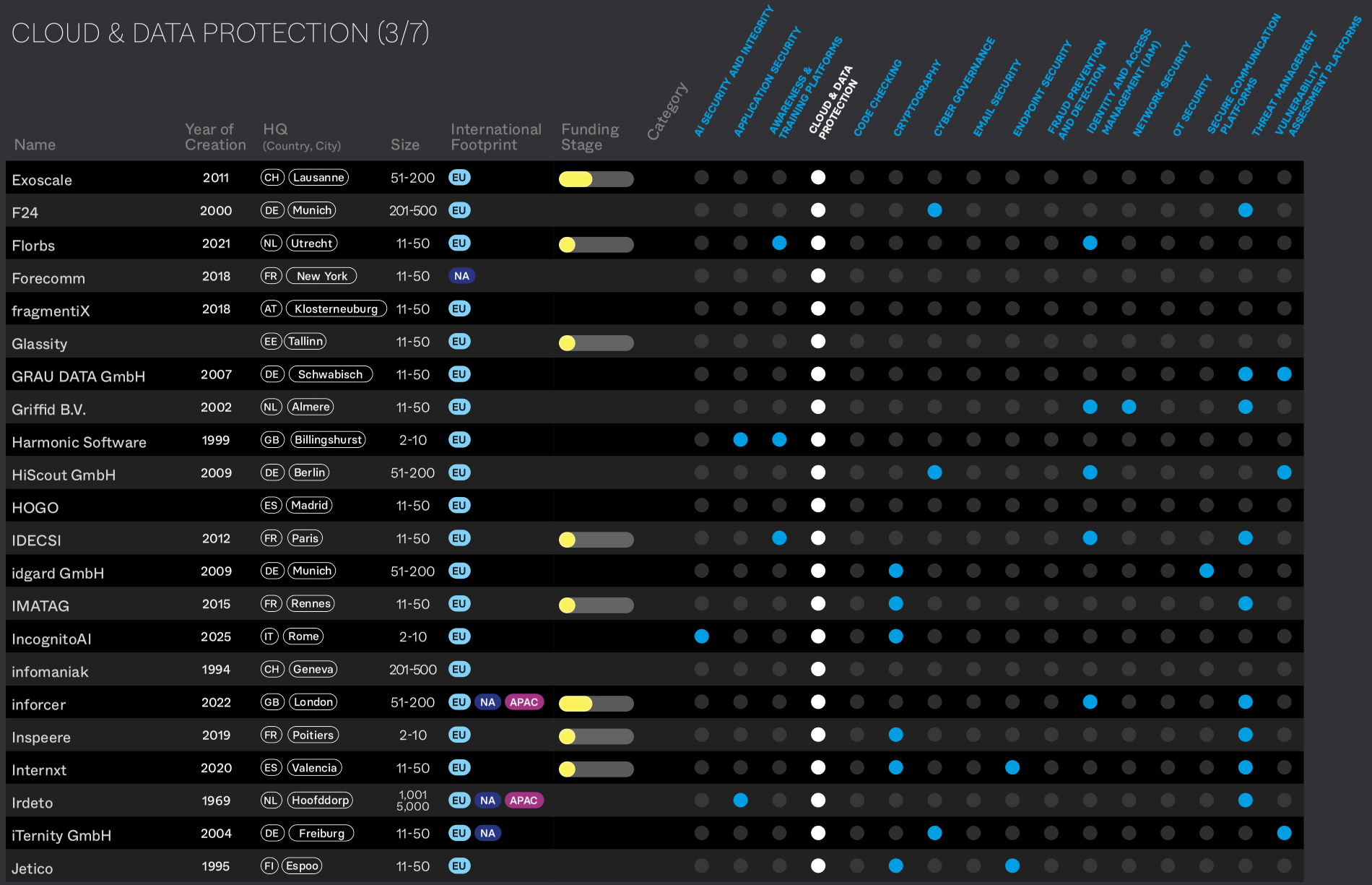
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Accolm		SE Stockholm	11-50	EU NA						●					●			●				
Acronis	2003	CH Schaffhausen	1,001 5,000	EU NA APAC	●					●				●	●						●	
Aegis Technologies			2-10							●			●								●	
aiomics	2025	DE Berlin	2-10	EU	●					●			●									
Aleph	2012	FR Villefranche	11-50	EU						●											●	
AO DATA CLOUD		ES Sabadell	11-50	EU				●		●					●			●			●	
Aqua Global	1983	GB London	51-200	EU				●		●											●	
Arbit Cyber Defence	2006	DK Hvidovre	11-50	EU						●							●			●	●	
ARCANO. Stay Safe.		CH Zurich	2-10	EU						●												
ARKHINEO	2001	FR Paris	1,001 5,000	EU						●		●										
arzen		FR Rennes	2-10	EU						●												
Astran		FR Paris	11-50	EU						●		●	●								●	
Atempo	1992	FR Massy	201-500	EU	●					●				●							●	
AUCAE	2019	FR Toulouse	2-10	EU				●		●			●								●	
Avaneidi S.p.A.		IT Saronno	2-10	EU	●			●		●												
Beyond Civic AG	2022	CH Luzern	2-10	EU						●												
bifrost security	2022	SE Stockholm	2-10	EU	●					●											●	●
Binary Bunker GmbH	2024	DE Hamburg	2-10	EU						●		●								●		
Blancco France & Afrique	1998	FR Lille	201-500	EU						●			●									
BlueFinch-ESBD NL	2011	NL Rijswijk	11-50	EU						●												
Breezy AI			2-10							●			●								●	
CanaryBit	2020	SE Stockholm		EU	●					●		●	●									

CLOUD & DATA PROTECTION (2/7)



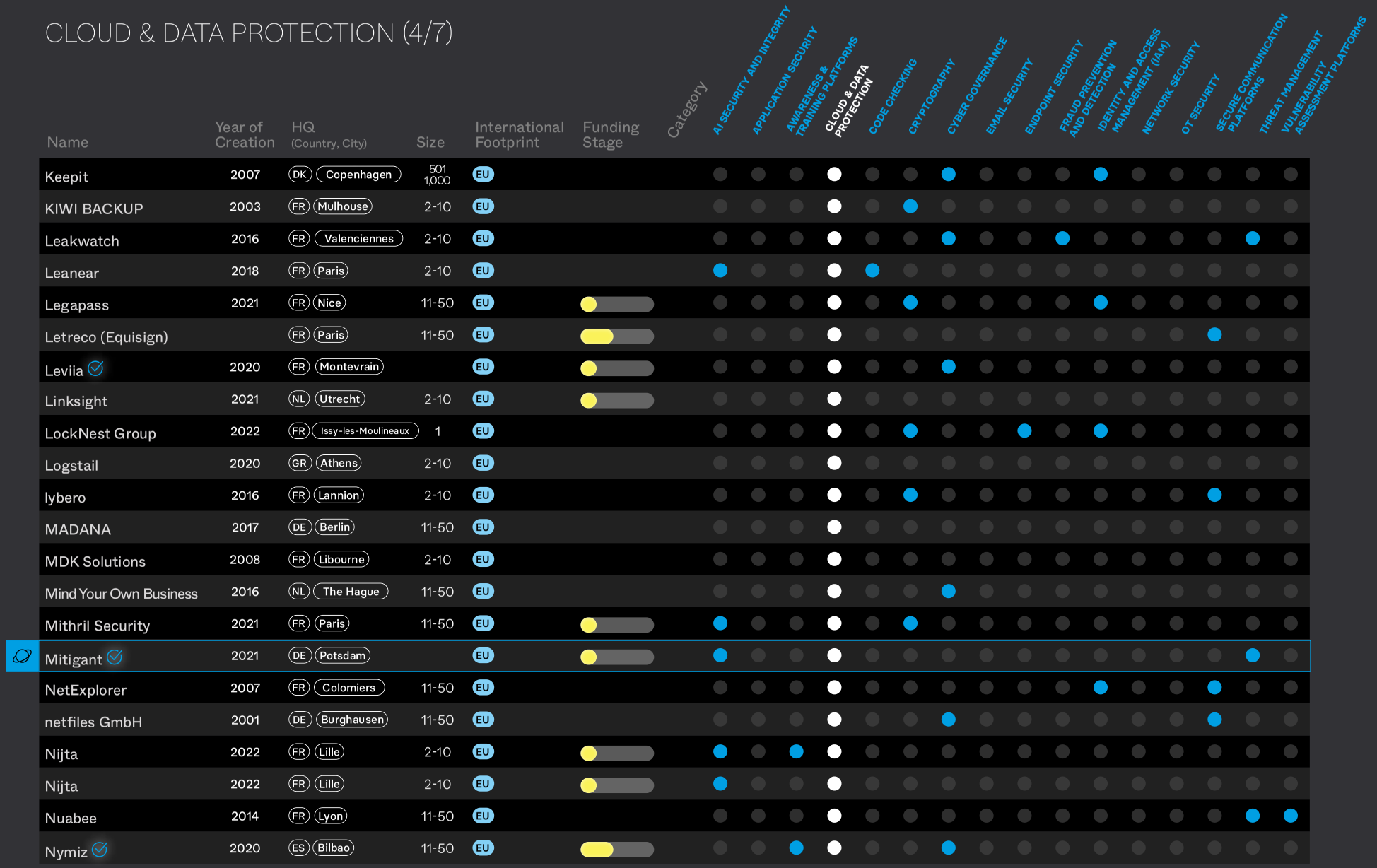
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
Centraya	2014	CH Zurich	11-50	EU		
Certus Software	2016	DE Augsburg	11-50	EU		
ClearDox	2019	DK Stamford	11-50	EU NA		
CLICKNCRYPT	2025		2-10			
Cliqz GmbH	2008	DE Munich	51-200	EU		
CSpace Hostings	2012	EE Tallinn	2-10	EU NA APAC		
Cubbit	2016	IT Bologna		EU		
Culmineo	2014	FR Paris	2-10	EU		
CyberHive	2018	GB Newbury	11-50	EU		
CyberTide	2024	DE Berlin	2-10	EU		
CyferAll™	2021	FR Paris	2-10	EU		
Cyscale	2019	RO London	11-50	EU		
Daspren	2022	FR Rennes		EU		
Datto		NL Norwalk	1,001 5,000	EU NA APAC		
DealDone	2012	PL Warsaw	2-10	EU		
Decentriq	2019	CH Zurich	11-50	EU		
DeHyper	2018	NL Amsterdam	11-50	EU		
DPella	2020	SE Gothenburg	2-10	EU		
DRACOON GmbH	2012	DE Regensburg	51-200	EU		
DSwiss AG	2006	CH Zurich	51-200	EU		
enclaive	2022	DE Berlin	11-50	EU		
Everabyte	2020	IE Dublin	2-10	EU		

CLOUD & DATA PROTECTION (3/7)



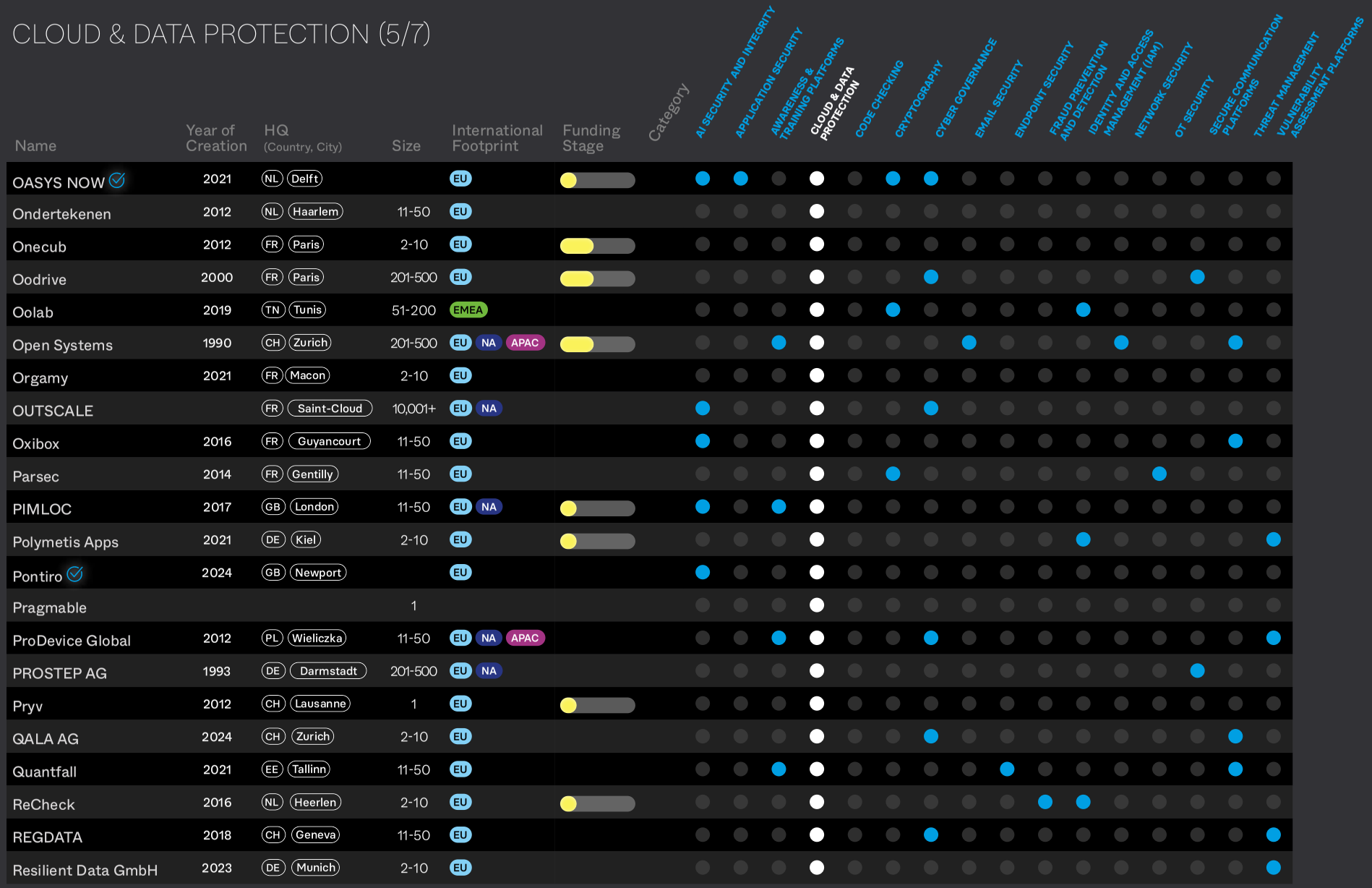
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
Exoscale	2011	CH Lausanne	51-200	EU	
F24	2000	DE Munich	201-500	EU	
Florbs	2021	NL Utrecht	11-50	EU	
Forecomm	2018	FR New York	11-50	NA	
fragmentiX	2018	AT Klosterneuburg	11-50	EU	
Glassity		EE Tallinn	11-50	EU	
GRAU DATA GmbH	2007	DE Schwabisch	11-50	EU	
Griffid B.V.	2002	NL Almere	11-50	EU	
Harmonic Software	1999	GB Billingshurst	2-10	EU	
HiScout GmbH	2009	DE Berlin	51-200	EU	
HOGO		ES Madrid	11-50	EU	
IDECSI	2012	FR Paris	11-50	EU	
idgard GmbH	2009	DE Munich	51-200	EU	
IMATAG	2015	FR Rennes	11-50	EU	
IncognitoAI	2025	IT Rome	2-10	EU	
infomaniak	1994	CH Geneva	201-500	EU	
inforcer	2022	GB London	51-200	EU NA APAC	
Inspeere	2019	FR Poitiers	2-10	EU	
Internxt	2020	ES Valencia	11-50	EU	
Irdeto	1969	NL Hoofddorp	1,001 5,000	EU NA APAC	
iTernity GmbH	2004	DE Freiburg	11-50	EU NA	
Jetico	1995	FI Espoo	11-50	EU	

CLOUD & DATA PROTECTION (4/7)



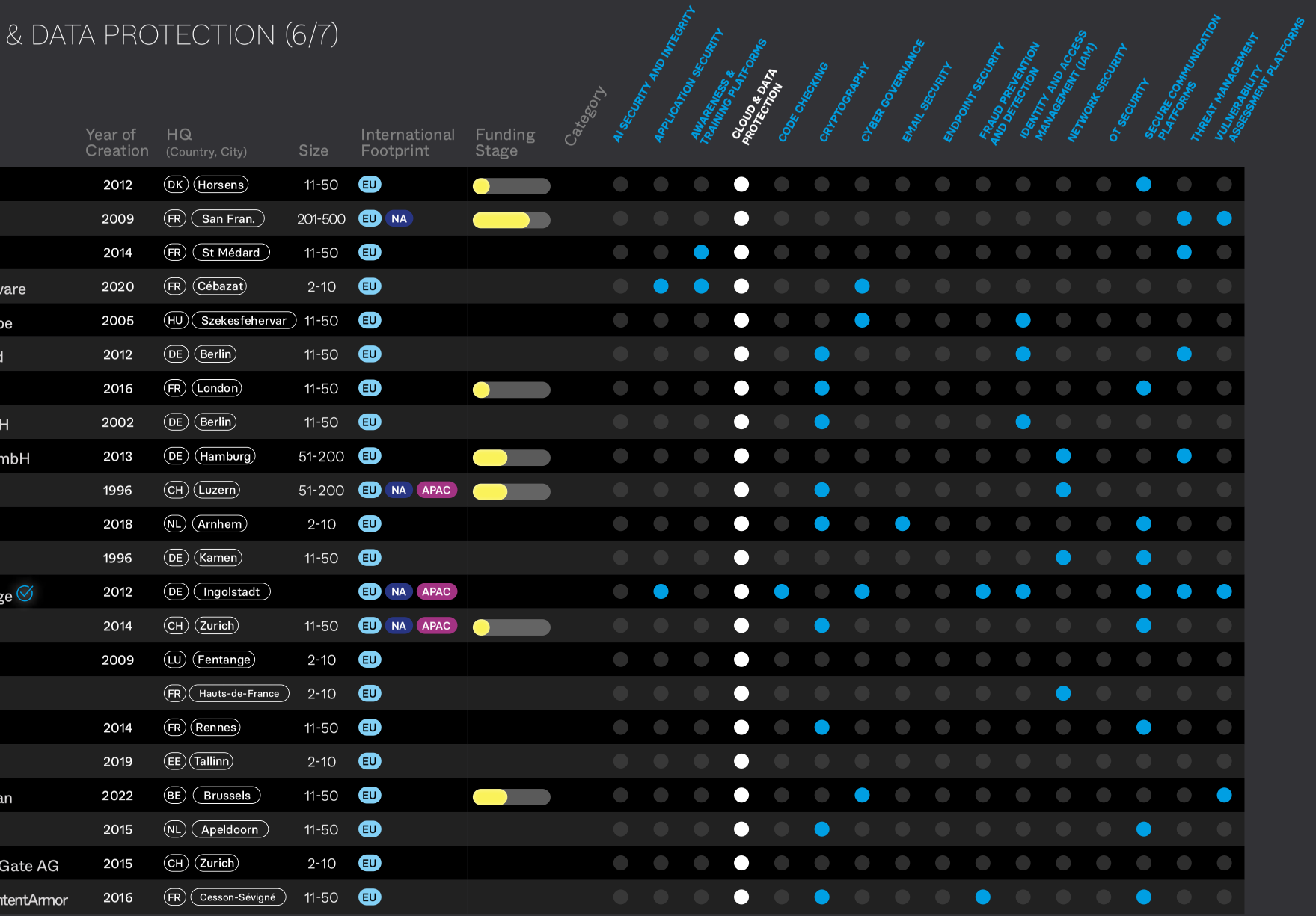
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Keepit	2007	DK Copenhagen	501 1,000	EU						●			●				●					
KIWI BACKUP	2003	FR Mulhouse	2-10	EU						●		●										
Leakwatch	2016	FR Valenciennes	2-10	EU						●			●			●					●	
Leanear	2018	FR Paris	2-10	EU			●			●	●											
Legapass	2021	FR Nice	11-50	EU						●		●					●					
Letreco (Equisign)		FR Paris	11-50	EU						●										●		
Leviia	2020	FR Montevrain		EU						●			●									
Linksight	2021	NL Utrecht	2-10	EU						●												
LockNest Group	2022	FR Issy-les-Moulineaux	1	EU						●		●			●		●					
Logstail	2020	GR Athens	2-10	EU						●												
lybero	2016	FR Lannion	2-10	EU						●		●								●		
MADANA	2017	DE Berlin	11-50	EU						●												
MDK Solutions	2008	FR Libourne	2-10	EU						●												
Mind Your Own Business	2016	NL The Hague	11-50	EU						●			●									
Mithril Security	2021	FR Paris	11-50	EU			●			●		●										
Mitigant	2021	DE Potsdam		EU			●			●											●	
NetExplorer	2007	FR Colomiers	11-50	EU						●						●				●		
netfiles GmbH	2001	DE Burghausen	11-50	EU						●			●							●		
Nijta	2022	FR Lille	2-10	EU			●		●	●												
Nijta	2022	FR Lille	2-10	EU			●			●												
Nuabee	2014	FR Lyon	11-50	EU						●											●	●
Nymiz	2020	ES Bilbao	11-50	EU					●	●			●									

CLOUD & DATA PROTECTION (5/7)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
OASYS NOW	2021	NL Delft		EU	
Ondertekenen	2012	NL Haarlem	11-50	EU	
Onecub	2012	FR Paris	2-10	EU	
Oodrive	2000	FR Paris	201-500	EU	
Oolab	2019	TN Tunis	51-200	EMEA	
Open Systems	1990	CH Zurich	201-500	EU NA APAC	
Orgamy	2021	FR Macon	2-10	EU	
OUTSCALE		FR Saint-Cloud	10,001+	EU NA	
Oxibox	2016	FR Guyancourt	11-50	EU	
Parsec	2014	FR Gentilly	11-50	EU	
PIMLOC	2017	GB London	11-50	EU NA	
Polymetis Apps	2021	DE Kiel	2-10	EU	
Pontiro	2024	GB Newport		EU	
Pragmable			1		
ProDevice Global	2012	PL Wieliczka	11-50	EU NA APAC	
PROSTEP AG	1993	DE Darmstadt	201-500	EU NA	
Pryv	2012	CH Lausanne	1	EU	
QALA AG	2024	CH Zurich	2-10	EU	
Quantfall	2021	EE Tallinn	11-50	EU	
ReCheck	2016	NL Heerlen	2-10	EU	
REGDATA	2018	CH Geneva	11-50	EU	
Resilient Data GmbH	2023	DE Munich	2-10	EU	

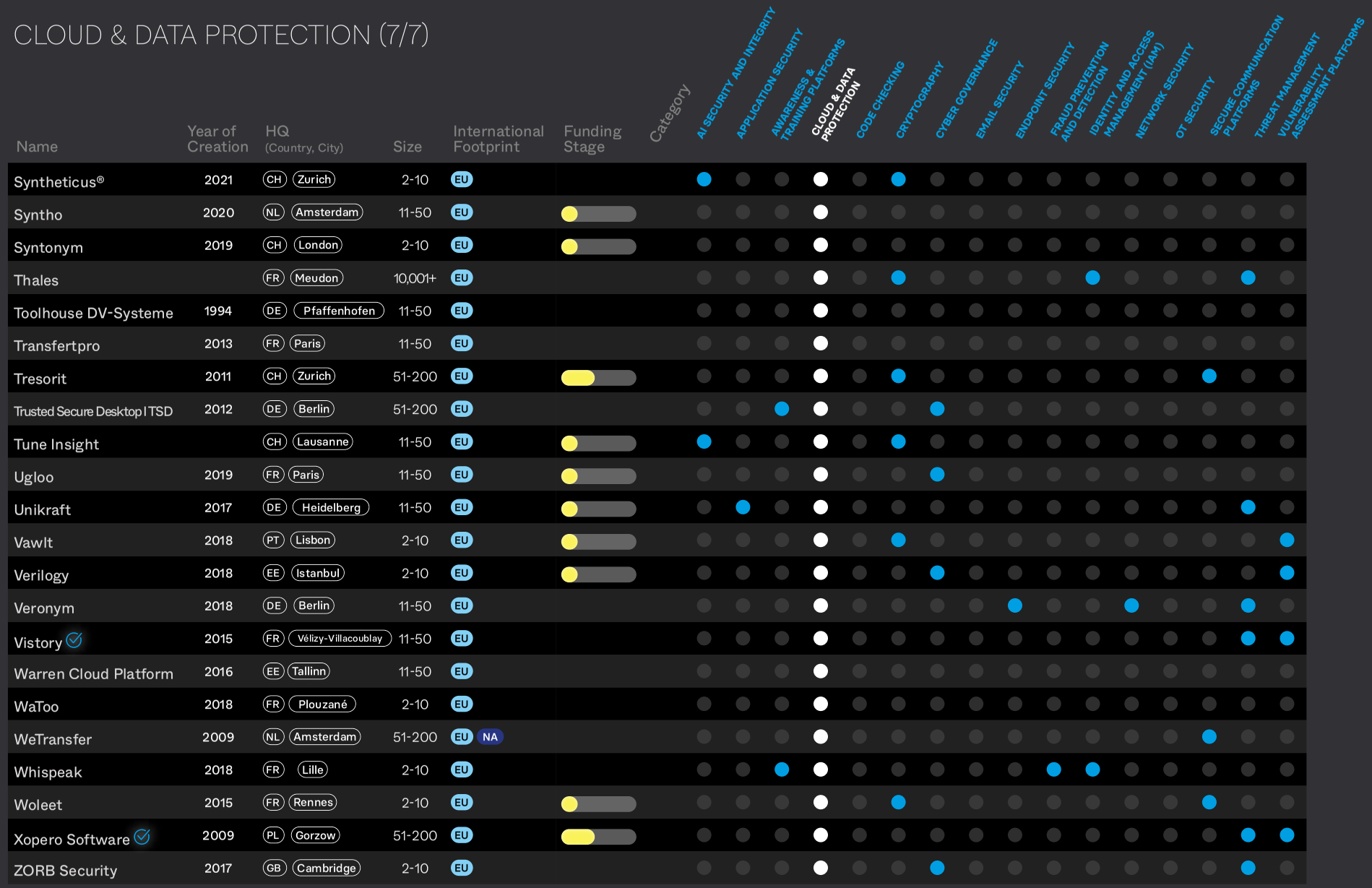
CLOUD & DATA PROTECTION (6/7)



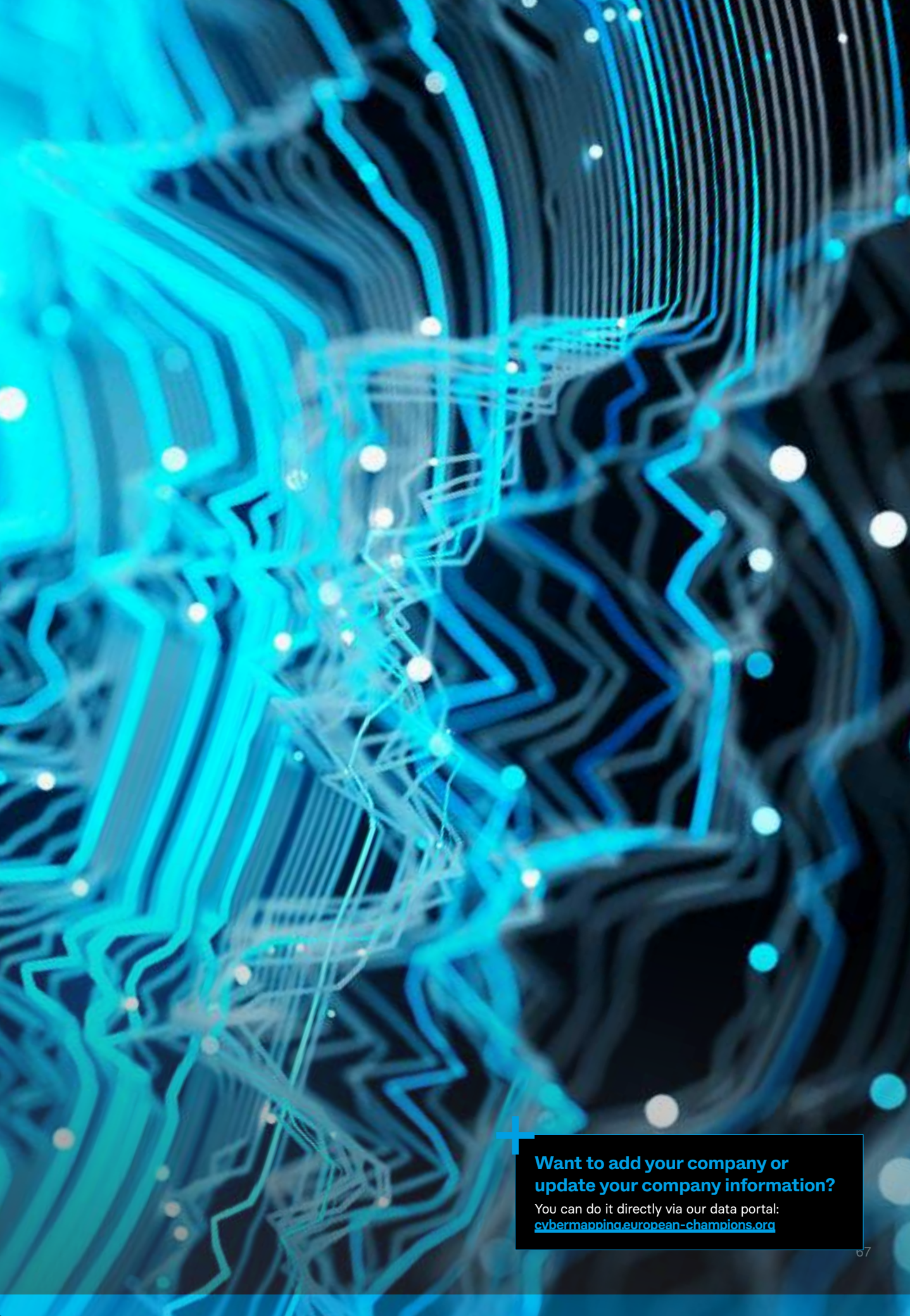
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
RushFiles	2012	DK Horsens	11-50	EU	
Scality	2009	FR San Fran.	201-500	EU NA	
SCILLE	2014	FR St Médard	11-50	EU	
scredIn software	2020	FR Cébazat	2-10	EU	
Seacon Europe	2005	HU Szekesfehervar	11-50	EU	
Search Guard	2012	DE Berlin	11-50	EU	
Secretarium	2016	FR London	11-50	EU	
secrypt GmbH	2002	DE Berlin	11-50	EU	
Secucloud GmbH	2013	DE Hamburg	51-200	EU	
Secude	1996	CH Luzern	51-200	EU NA APAC	
SecuDoc	2018	NL Arnhem	2-10	EU	
SECUDOS	1996	DE Kamen	11-50	EU	
SecurityBridge	2012	DE Ingolstadt		EU NA APAC	
Securosys	2014	CH Zurich	11-50	EU NA APAC	
SeeZam S.A.	2009	LU Fentange	2-10	EU	
Semicube		FR Hauts-de-France	2-10	EU	
Shadline	2014	FR Rennes	11-50	EU	
Skudo OÜ	2019	EE Tallinn	2-10	EU	
StackGuardian	2022	BE Brussels	11-50	EU	
Storro	2015	NL Apeldoorn	11-50	EU	
Swiss Cyber Gate AG	2015	CH Zurich	2-10	EU	
Synamedia ContentArmor	2016	FR Cesson-Sévigné	11-50	EU	

Category: AI SECURITY AND INTEGRITY; APPLICATION SECURITY; AWARENESS & TRAINING PLATFORMS; CLOUD & DATA PROTECTION; CODE CHECKING; CRYPTOGRAPHY; CYBER GOVERNANCE; EMAIL SECURITY; ENDPOINT SECURITY; FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM); NETWORK SECURITY; OT SECURITY; SECURE COMMUNICATION PLATFORMS; THREAT MANAGEMENT; VULNERABILITY ASSESSMENT PLATFORMS

CLOUD & DATA PROTECTION (7/7)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
Syntheticus®	2021	CH Zurich	2-10	EU		Cloud & Data Protection
Syntho	2020	NL Amsterdam	11-50	EU		Cloud & Data Protection
Syntonym	2019	CH London	2-10	EU		Cloud & Data Protection
Thales		FR Meudon	10,001+	EU		Cloud & Data Protection
Toolhouse DV-Systeme	1994	DE Pfaffenhofen	11-50	EU		Cloud & Data Protection
Transfertpro	2013	FR Paris	11-50	EU		Cloud & Data Protection
Tresorit	2011	CH Zurich	51-200	EU		Cloud & Data Protection
Trusted Secure Desktop I TSD	2012	DE Berlin	51-200	EU		Cloud & Data Protection
Tune Insight		CH Lausanne	11-50	EU		Cloud & Data Protection
Ugloo	2019	FR Paris	11-50	EU		Cloud & Data Protection
Unikraft	2017	DE Heidelberg	11-50	EU		Cloud & Data Protection
VawIt	2018	PT Lisbon	2-10	EU		Cloud & Data Protection
Verilogy	2018	EE Istanbul	2-10	EU		Cloud & Data Protection
Veronym	2018	DE Berlin	11-50	EU		Cloud & Data Protection
Vistory	2015	FR Vélizy-Villacoublay	11-50	EU		Cloud & Data Protection
Warren Cloud Platform	2016	EE Tallinn	11-50	EU		Cloud & Data Protection
WaToo	2018	FR Plouzané	2-10	EU		Cloud & Data Protection
WeTransfer	2009	NL Amsterdam	51-200	EU NA		Cloud & Data Protection
Whispeak	2018	FR Lille	2-10	EU		Cloud & Data Protection
Woleet	2015	FR Rennes	2-10	EU		Cloud & Data Protection
Xopero Software	2009	PL Gorzow	51-200	EU		Cloud & Data Protection
ZORB Security	2017	GB Cambridge	2-10	EU		Cloud & Data Protection



Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

European Cybersecurity Mapping 2026

AWARENESS & TRAINING PLATFORMS

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Secure operations depend not just on robust tools but also on high staff awareness and constant vigilance. These platforms, through training, security exercises, and crisis simulations, raise cybersecurity awareness and equip employees to detect anda respond effectively to threats.

Why Choose European Technology: European awareness platforms align training with EU-specific threats and regulatory requirements, delivering culturally relevant, localized content to maximize organizational readiness.

Importance for European sovereignty: 7/10

Awareness and training are essential for resilience but have a lower direct impact on sovereignty compared to technologies securing infrastructure or data.

Continuous Awareness Programs for a Regulation-Driven Threat Landscape

MARKET CONTEXT

Security awareness training has moved beyond its original role as a compliance exercise. Now it is increasingly treated as a structural control to address one of the most persistent weaknesses in security: human behavior. Even organizations with mature technical defenses continue to see phishing, social engineering, credential misuse and accidental data exposure as primary attack vectors.

European regulation reinforces this development. NIS2, DORA, and GDPR set expectations that organizations manage staff-related security risks in a structured and ongoing manner. As a result, traditional annual training cycles are giving way to continuous awareness programs and microlearning approaches. This trend is further accelerated by AI-enabled phishing and impersonation techniques, which increase the scale and sophistication of malicious attacks.

EUROPEAN COMPETITIVE ADVANTAGES

European vendors rarely dominate this market in terms of global presence, but they can compete on different fundamentals. Their solutions are designed with privacy by default in mind. Conservative data collection, transparent processing, and a practical interpretation of GDPR Article 28 responsibilities are common. In regulated industries, these qualities have become meaningful selection criteria, amplified by broader discussions around digital sovereignty.

Public sector organizations, financial institutions, and critical infrastructures increasingly favor EU-based hosting, as well as local operational presence and transparent ownership. US vendors often provide broader international coverage and more mature global rollout capabilities, but European providers tend to perform best where regulatory knowledge, cultural context, and procurement realities matter most. This is especially valid for multinational deployments, where content coverage, analytics consistency, and cross-jurisdiction delivery remain a major challenge.

TECHNOLOGY EVOLUTION AND TRENDS

Most sensibilization platforms have long been SaaS-based, but their architectures are evolving toward tighter integration, higher automation, and continuous delivery models. Security awareness tools are increasingly connected to IAM, email security, governance, and HR systems. Static content delivery is being replaced by a contextual and event-driven approach, where observed user behavior triggers targeted follow-up actions.

This reflects a broader shift toward operational models that treat human behavior as a measurable and manageable risk factor. AI and machine learning are applied cautiously, mainly to improve targeting, personalization, and campaign effectiveness. Differentiation increasingly depends on the ability to demonstrate auditable and defensible behavioral impact. Metrics are moving away from completion rates to prioritization, risk reduction, and maturity assessment across defined behavior categories. Microlearning formats continue to gain traction as part of continuous reinforcement strategies.

MARKET DYNAMICS

The market remains fragmented. Pure-play awareness vendors coexist with broader security, compliance, and governance platforms that include training as one component of a larger suite. Buyers often balance depth and behavioral effectiveness against the convenience of bundled offerings, especially where training is driven by compliance or GDPR requirements. Phishing simulations and baseline training typically serve as entry points, followed by role-specific and risk-adaptive programs.

Build-versus-buy decisions frequently result in hybrid approaches. Organizations may rely on external platforms for orchestration, measurement, and reporting while retaining control over internally developed, culture-specific content. For smaller vendors, realistic exit strategies are more often tied to acquisition than to independent global expansion.

FUTURE

Over the next several years, security awareness platforms are likely to become more tightly integrated with enterprise risk management and identity-centric security architectures. The central challenge will be demonstrating measurable risk reduction without eroding employee trust or violating privacy expectations. Buyers will increasingly look for evidence of sustained behavioral change rather than just participation metrics.

As European regulations extend security expectations across a wider range of organizations, vendors must combine regulatory credibility with strong integration capabilities. Long-term success will depend less on feature breadth and more on measurable impact, interoperability, and the ability to maintain trust with both employees and regulators.

Kai BOSCHERT

Senior Advisor
& Deputy CISO

KuppingerCole Analysts AG

For detailed analysis, see:

Advisory Note: Security for the Agile IT

Blog: Training Non-techies on Cybersecurity Awareness

Blog: Cybersecurity Awareness – Are We Doing Enough?

AWARENESS & TRAINING PLATFORMS (1/3)

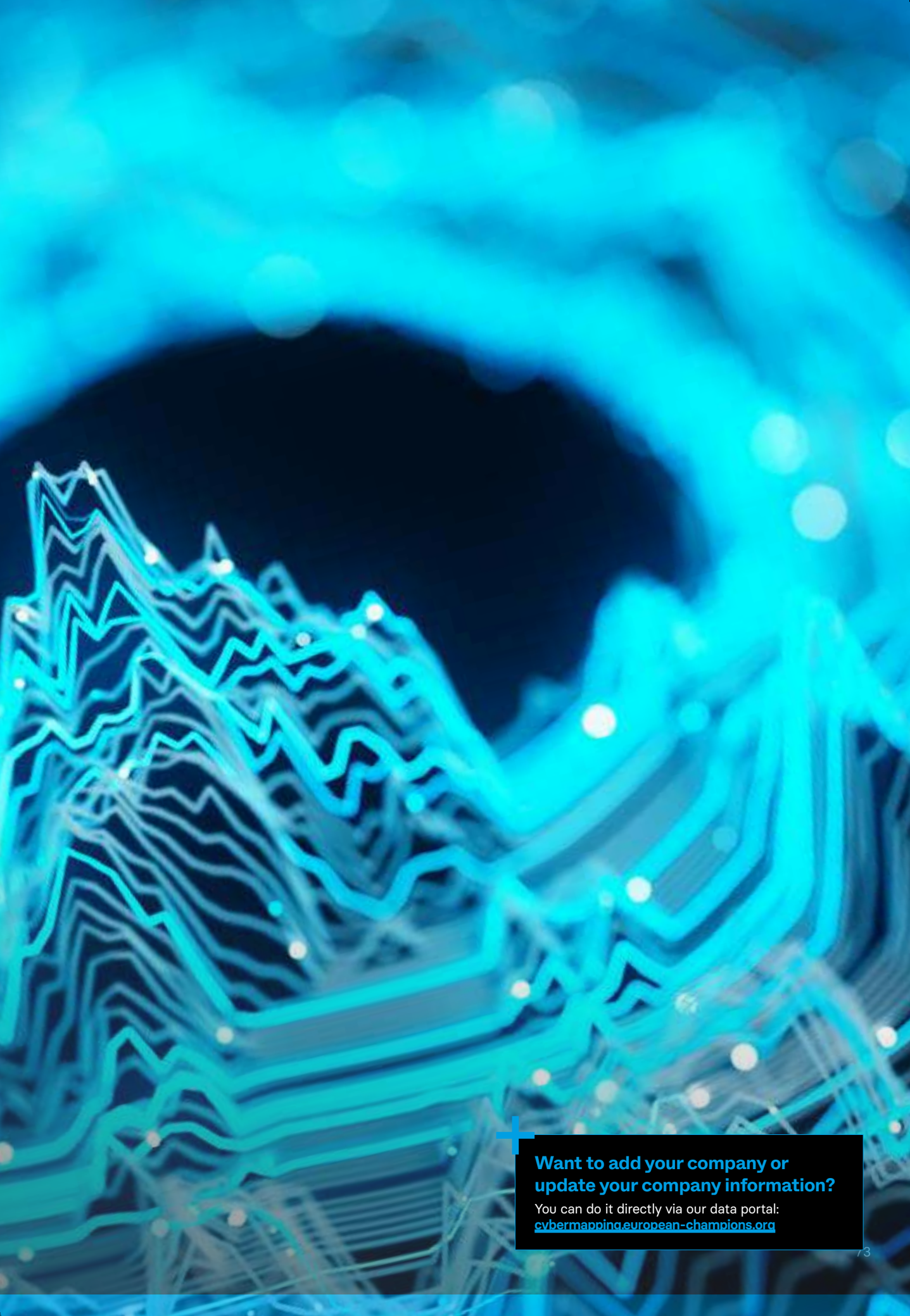
Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Alcyconie	2018	FR Rennes	11-50	EU					●				●							●		
APT Defend	2018	PL Warsaw	2-10	EU					●											●		
Arsen Security	2021	FR Paris	2-10	EU					●						●					●		
BackBox.org	2010	IT Turin	2-10	EU				●	●													
Badrap Oy	2017	FI Oulu	2-10	EU					●											●	●	
BlackStork.io	2023	NL Amsterdam	2-10	EU					●				●									
Boxphish	2018	GB Leeds	11-50	EU					●					●						●		
Brain Technologies	2015	FR San Mateo	51-200	NA					●													
Brightside AI	2023	CH Lausanne		EU					●						●						●	
CDeX	2022	PL Poznan	11-50	EU					●													
Conscio Technologies		FR Paris	11-50	EU					●													
CTF Tech	2020	EE Tallinn	11-50	EU					●											●		
CultureAI	2015	GB Manchester	11-50	EU			●		●											●		
Cyber Guru	2017	IT Rome	51-200	EU					●				●									
Cyber Struggle	2019	EE Bilbao	11-50	EU NA					●					●						●		
CYBERDISE Cybersecurity	2023	CH Zug		EU					●											●		
CybExer Technologies	2016	EE Tallinn	51-200	EU			●		●											●		
Cypaw	2018	GB Welwyn Garden	2-10	EU					●							●				●		
Erium	2012	FR Paris	51-200	EU					●	●										●		
Gottaphish	2022	FR Pessac	2-10	EU					●						●					●		
Hack The Box	2017	GB Folkestone	201-500	EU					●						●					●		
HackTheBox - Dr. AITH	2022	IN Kanpur	1	APAC					●													

AWARENESS & TRAINING PLATFORMS (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
HookPhish	2024	GB West End	2-10	EU					●						●					●		
Immersive	2017	GB Bristol	201-500	EU NA				●	●											●		
IT-Seal GmbH	2016	DE Darmstadt	11-50	EU					●				●							●		
Kamav©	2020	FR Paris	11-50	EU					●			●								●		
Keepnet	2017	GB London	11-50	EU NA					●				●							●		
KnowBe4		FR Clearwater	1,001-5,000	NA					●			●	●							●		
Kymatio	2017	ES Madrid	11-50	EU					●							●				●		
LePhish		FR Paris	2-10	EU					●				●							●		
LUCY Awareness		CH Cham	11-50	EU					●											●		●
MetaCompliance		GB London	201-500	EU NA					●				●							●		
Misja	2018	PL Krakow	2-10	EU					●													
Moxso		DK Copenhagen	51-200	EU					●						●							
ONYL Rocks		FR Lyon	2-10	EU					●				●									
OutThink	2015	US New York	51-200	NA EU APAC					●							●				●		
Paratus Systems	2014	EE Pune	11-50	APAC					●													
Phished		BE Leuven	11-50	EU					●													
PWNX		IT Rome	2-10	EU			●		●											●		
Riot	2020	FR San Fran.	51-200	NA EU					●				●							●		
SecDojo	2021	FR Guyancourt	11-50	EU					●			●								●		
Secure Practice	2017	NO Trondheim		EU					●													
SecureFlag		GB London	11-50	EU				●	●													
sequal	2020	CH Ecublens	2-10	EU					●													

AWARENESS & TRAINING PLATFORMS (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
SimuPhish	2024	GB Global	51-200	EU		AWARENESS & TRAINING PLATFORMS
SiteBell			2-10			AWARENESS & TRAINING PLATFORMS
SoSafe		DE Cologne	201-500	EU		AWARENESS & TRAINING PLATFORMS
usecure	2016	GB Manchester	11-50	EU		AWARENESS & TRAINING PLATFORMS



Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

European Cybersecurity Mapping 2026

CODE CHECKING

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: As code development grows in complexity, incorporating third-party components and AI-aided tools, code verification is now mandatory. These tools analyze source code for vulnerabilities, bugs, and compliance issues, ensuring a secure development lifecycle.

Why Choose European Technology: European providers focus on transparency and compliance, aligning security practices with EU norms. Supporting them mitigates the risks of international dependency and directly enhances Europe's cybersecurity independence.

Importance for European sovereignty: 8/10

Secure software development is vital for ensuring no hidden backdoors or vulnerabilities are introduced, particularly for critical applications in sensitive industries.

Keeping Software Secure Even When Code Writes Itself

kuppingercole ANALYSTS

MARKET CONTEXT

In modern software development, source code analysis is increasingly part of how organizations manage risk across the entire development lifecycle. Applications are assembled from custom code, open-source components, and infrastructure definitions, often developed by distributed teams under time pressure. Now, code checking is expected to provide continuous assurance rather than episodic review.

Regulatory initiatives like the Cyber Resilience Act strongly emphasize secure development, transparency, and the ability to demonstrate due diligence. Code checking can produce evidence about how the software is built, what it contains, and how risks are identified, prioritized, and addressed. It has become integral component of governance, auditability, and digital resilience.

EUROPE'S COMPETITIVE ADVANTAGE

European providers in this space tend to focus on open formats, explainable findings, and deployment models that allow organizations to retain control over source code and analysis metadata. For many enterprises, especially in regulated sectors, this approach reduces friction during procurement and internal risk assessments.

EU vendors often position code analysis as part of broader governance frameworks. Rather than focusing solely on detecting issues, tools emphasize auditability, ownership, and traceability across development stages and teams. This aligns well with customer expectations around accountability and long-term maintenance.

TECHNOLOGY EVOLUTION AND TRENDS

Traditional static analysis remains important, but it is now complemented by software composition analysis, secret detection, infrastructure-as-code checks, and Software Bill of Materials (SBOM) processing. These capabilities increasingly fall under the umbrella of software supply chain security, reflecting the reality that many critical risks originate from dependencies rather than their own code.

A newer factor is the rapid rise of "vibe coding," where developers use AI-assisted platforms to generate applications quickly, without a substantial understanding of how the resulting code works or what dependencies it introduces. While this approach accelerates development, it also increases the likelihood of hidden flaws, unsafe defaults, missing security controls, and poorly understood transitive dependencies. Recent incidents with vibe-coded apps shipped with massive security gaps illustrate that speed does not remove the need for testing, vulnerability analysis, or code review.

As a result, modern tools must assume less developer insight and compensate with stronger automated inspection, contextual validation, and policy enforcement. This applies not only to human-written code, but also to code produced by AI systems and embedded into projects through automated pipelines.

MARKET DYNAMICS

The market for code checking tools remains fragmented. Some vendors focus narrowly on code analysis, while others position themselves as broader platforms covering build integrity, dependency management, and policy enforcement. This gives buyers flexibility, but it also creates a risk of overlapping tools that generate large volumes of findings without improving decision-making.

In Europe, buyers often prioritize interoperability and deployment control over comprehensive platform coverage. Tools that integrate cleanly with existing development environments and security processes tend to gain more traction than those that replace entire systems.

FUTURE

Code checking is likely to focus more on the ability to show what was checked, when, and with what outcome rather than the quantity of checks themselves. SBOMs, lifecycle-wide visibility, contextual prioritization, and policy-driven validation will play a larger role, especially in regulated industries. The growth of vibe coding only reinforces this direction.

AI-generated code must still meet the same security, quality, and compliance requirements as traditionally developed software. Future tools will need to extend existing governance frameworks to cover these development platforms, treating them as part of the software supply chain. They become even more important as assumptions about developer intent and expertise become less reliable.

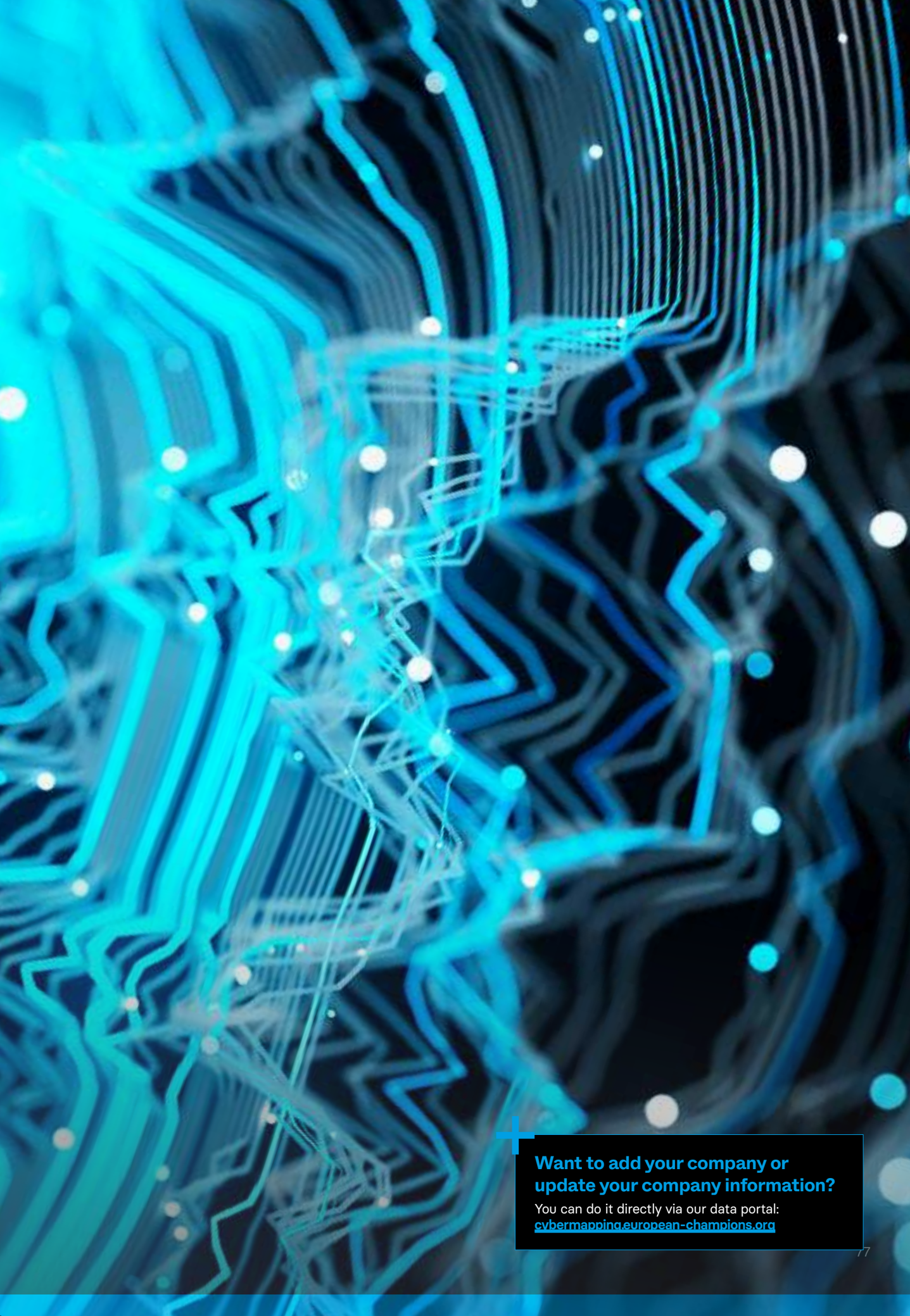
Alexei BALAGANSKI
Lead Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Software Supply Chain Security
Blog: Software Supply Chain Security - Are You Importing Problems?
Advisory Note: SBOM as a Core Element of Cyber Resilience

CODE CHECKING

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
AbsInt GmbH	1998	DE Saarbrucken	11-50	EU			○	●	●	○	●	○	○	○	○	○	○	○	○	○	○	●
Codean	2020	NL Utrecht	2-10	EU			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
CodeClarity		LU Luxembourg	2-10	EU			○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Continus.io	2020	FR Paris	2-10	EU			○	●	○	○	●	○	●	○	○	○	○	○	○	○	○	●
DCODX	2019	EE Amsterdam	2-10	EU			○	●	●	○	●	○	○	○	○	○	○	○	○	○	○	●
Decentralized Intelligence AG		CH Zug	2-10	EU			●	○	○	○	●	○	○	○	○	○	○	○	○	●	○	○
Fendora	2025	DE Berlin	2-10	EU			●	●	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Glev			2-10				○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Percepio®	2009	SE Vasteras	11-50	EU			○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Securify	2012	NL Amsterdam	11-50	EU			○	●	○	○	●	○	○	○	○	○	○	○	○	●	○	○
SignPath GmbH	2017	AT Vienna	51-200	EU			○	○	○	○	●	●	●	○	○	○	○	○	○	○	○	○
Sonar	2008	CH Vernier		EU NA APAC			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
TASKING		DE Munich	201-500	EU NA APAC			○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Threatray	2018	CH Biel	2-10	EU			○	○	○	○	●	○	○	○	●	●	○	○	○	●	○	○
TrustInSoft	2013	FR Paris	11-50	EU NA			○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
Yagaan	2010	FR Paris	51-200	EU			○	●	●	○	●	○	○	○	○	○	○	○	○	●	○	●



Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

RED ALERT LABS

COMMUNITY CONTRIBUTOR

Europe should accelerate harmonised standards and practical implementation guidance so manufacturers can move from “policy” to repeatable workflows, testing paths, and evidence packs.

What is the most important signal, trend, or risk you are currently observing in your cybersecurity domain?

The strongest signal right now is that cybersecurity for connected products is becoming a market access requirement, not an optional engineering add-on. The risk is no longer only “being attacked”, it is being unable to demonstrate control over vulnerabilities, updates, and supply-chain exposure when customers or authorities ask for proof. In practice, this means “cybersecurity” is increasingly evaluated through evidence - SBOMs, vulnerability handling processes, secure update capability, and incident responsiveness - turning compliance-grade lifecycle governance into a prerequisite for procurement, certification, and regulatory acceptance.

In your specific field, what does Europe do well; and where is improvement urgently needed?

Europe’s strength is clear, structured regulation that pushes industry toward measurable security outcomes. The CRA is a major step because it anchors security-by-design and lifecycle obligations for products with digital elements, including expectations around vulnerability handling and updates.

The weakness is execution at scale. Many teams still face fragmented tooling, inconsistent interpretations across countries and schemes, and slow time-to-evidence. That friction will become more visible as CRA obligations drive more audits, documentation, and readiness checks.

What single priority should Europe address to strengthen its position in your domain?

One priority, make CRA compliance operational and scalable. Europe should accelerate harmonised standards and practical implementation guidance so manufacturers can move from “policy” to repeatable workflows, testing paths, and evidence packs. If CRA becomes easy to implement consistently across the single market, Europe strengthens both security and competitiveness.

RED ALERT LABS

Red Alert Labs is an international cybersecurity lab specializing in IoT security. They offer innovative consulting, evaluation, and certification services for IoT products, processes, and services, covering the entire spectrum from chip to cloud. Their AI-driven innovation, CyberPass, is a SaaS platform that equips enterprises with a cost-effective and scalable solution to assess and manage the cybersecurity compliance of connected products. Let’s get you read for the Cyber Resilience Act (CRA).

redalertlabs.com

Roland ATOUI
Managing Director
Red Alert Labs

Interview

GITGUARDIAN

COMMUNITY CONTRIBUTOR

We must address the AI security gap urgently. As organizations deploy autonomous AI agents creating millions of new non-human identities, European vendors should lead in securing them, particularly given our AI governance frameworks.

How do you define the role of cybersecurity software vendors in today's European cybersecurity ecosystem?

European cybersecurity vendors play a dual role: delivering world-class security solutions that compete globally while strengthening Europe's digital sovereignty. This means building technologies that protect against evolving threats while operating within frameworks that respect European values around data privacy and regulatory compliance.

We also serve as an innovation engine. With less venture capital than U.S. or Israeli ecosystems, European vendors must be exceptionally innovative, talented, and focused.

What key challenges do European organizations face when selecting and deploying cybersecurity solutions?

The primary challenge is navigating complex, overlapping regulations, NIS2, DORA, GDPR, the Cyber Resilience Act, with different timelines. This creates paralysis where compliance becomes a checkbox exercise rather than meaningful risk reduction. Organizations don't know where to start.

Second, there's a procurement bias toward U.S. vendors, even when European alternatives exist. CISOs often perceive American solutions as more mature simply because those ecosystems have been funded more aggressively. Unfortunately, that also applies to some large European enterprises. They will prefer to buy established solutions from US vendors because they feel like it's a "safe" choice. This means European vendors must work harder both in the US and Europe to demonstrate the same level of credibility, even when their technology is far superior.

Finally, organizations are drowning in alerts from fragmented point solutions. They need integrated platforms that reduce complexity and automate remediation without requiring large security teams.

From your perspective, where does Europe still need to strengthen its technological capabilities in cybersecurity?

We must address the AI security gap urgently. As organizations deploy autonomous AI agents creating millions of new non-human identities, European vendors should lead in securing them, particularly given our AI governance frameworks.

We also need more category-defining companies with global scale. This requires aggressive international expansion, particularly into North America.

European founders often underestimate the importance of establishing U.S. presence early.

How does GitGuardian differentiate itself in the competitive cybersecurity software landscape?

GitGuardian focuses exclusively on securing non-human identities and secrets, a problem most vendors treat as secondary. While competitors build broad platforms, we've invested seven years becoming the world's leading solution for secrets security, reflected in our #1 position on GitHub globally with 550,000+ developers using our tools.

Our differentiation comes from comprehensive detection (code, collaboration tools, AI agent workspaces), intelligent prioritization that eliminates alert fatigue, and remediation orchestration connecting detection to action. We face Microsoft, GitHub, and Wiz, but they approach secrets as one feature among many. We detect exposures they miss and have the lowest false-positive rate in the market.

Our European heritage is also strategic. We can hire excellent engineers in Europe and we understand compliance natively. Yet we compete globally: 70% of our revenue comes from North America, proving European technology can win when the product excels.

How does your solution contribute to strengthening European digital sovereignty and resilience?

GitGuardian addresses a fundamental sovereignty question: who controls the credentials granting access to Europe's most sensitive systems? By helping organizations discover, govern, and protect these credentials, we reduce risks from both malicious breaches and unauthorized access.

We enable compliance with European regulations through continuous monitoring and full audit trails for NIS2, DORA resilience testing for financial institutions, and GDPR breach prevention. As a French-founded company with R&D in Europe, we give organizations a sovereign alternative that understands their regulatory context and won't be subject to foreign government data requests.

Finally, we support European competitiveness in AI deployment. Organizations cannot adopt AI agents safely without securing secrets and credentials. Each agent needs credentials to access data. By providing governance infrastructure that makes AI adoption secure, we enable European companies to innovate confidently without compromising values or security.

GitGuardian

GitGuardian protects the enterprises against leaked secrets and mismanaged identities. As you know, exposed secrets are exploited in more than 80% of today's breaches. We are the developer wingman at every step of the development life cycle and we enable security teams with automated vulnerability detection and remediation. We strive to develop a true collaborative Non-Human Identity security platform including Secrets Security, NHI Governance and AI Agents security.

gitguardian.com

Eric FOURRIER
Co-Founder & CEO

GitGuardian

European Cybersecurity Mapping 2026

CRYPTOGRAPHY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Cryptography provides the essential encryption solutions for secure and confidential data storage, processing, and communication. However, the landscape is shifting rapidly. Quantum computers will soon be able to break classical encryption, introducing a "steal now, decrypt tomorrow" threat for sensitive, long-term data. Quantum Proof Cryptography (QPC) is already necessary to prepare for this transition, and regulators are moving to phase out classical algorithms.

Why Choose European Technology: New cryptography will be a key component of data protection and communication security. EU-based cryptographic solutions adhere to strict privacy standards, avoiding vulnerabilities coming from foreign legislation. Using European vendors reinforces trust, ensures GDPR compliance, and strengthens Europe's autonomy in critical security infrastructure. Crucially, European researchers, vendors, and integrators possess remarkable expertise in the field of QPC.

Importance for European sovereignty: 10/10

Cryptography underpins the security of all digital communications. Control over encryption technologies is fundamental to European sovereignty and independence from foreign surveillance.

Protecting Digital Trust in a Highly Regulated Post-Quantum World

kuppingercole ANALYSTS

MARKET CONTEXT

Cryptography provides a secure foundation for nearly every digital system. It powers sensitive communications, identity verification, data protection, and software integrity, yet remains almost invisible to end users. As digital infrastructures become more open and interconnected, cryptography has evolved from a technical concern into a matter of strategic risk management.

Growing awareness of quantum computing has amplified this shift. Even before practical quantum computers exist, malicious actors are already collecting encrypted data today with the expectation that it can be decrypted once quantum-capable systems become available. This "harvest now, decrypt later" risk makes long-term data confidentiality a current concern rather than a future one. Regulations like GDPR, NIS2, and DORA implicitly require strong cryptographic controls, even if they lack specific recommendations for implementing them. Cryptography is therefore an area where failure is not immediately visible, but the consequences could be catastrophic.

EUROPE'S COMPETITIVE ADVANTAGE

Europe has a long-standing and often underestimated strength in cryptographic research and engineering. European vendors and academics alike have played a major role in the development and evaluation of modern, post-quantum cryptographic algorithms. They also usually have a much stronger focus on data protection, privacy, and transparency, driven by both ethical considerations and regulatory expectations.

Maintaining data residency, enforcing strict control over key material, and preventing extraterritorial exposure are considered design prerequisites, not optional features. For governments, critical infrastructures, and regulated industries, this alignment is essential. Control over cryptographic technologies is therefore closely tied to European digital sovereignty, arguably more than in any other security domain.

TECHNOLOGY EVOLUTION AND TRENDS

Modern cryptography is undergoing a slow but profound transition. Classical public key algorithms remain widely used, but the industry has largely accepted that they are insufficient in the long term. Post-quantum cryptography is moving from theory into early implementations and migrations, even though reliable quantum computers are not yet available. This shift has brought cryptographic agility into focus as a core architectural requirement. Future systems must be able to replace algorithms, parameters, and protocols without disruptive redesigns, something many existing deployments are not prepared for.

At the same time, cryptography is becoming more tightly integrated into security architectures, including key management, hardware security modules, secure enclaves, and identity systems. Phishing-resistant authentication methods based on cryptographic primitives are also gaining importance. Despite increased automation and abstraction, cryptography remains unforgiving when implemented incorrectly (which continues to be a reality for many businesses).

MARKET DYNAMICS

The cryptography market remains fragmented and difficult to assess. Large technology providers embed cryptographic capabilities deep into operating systems, cloud platforms, and hardware, often limiting visibility and choice. Specialized vendors focus on individual areas such as key management, hardware security modules, or post-quantum cryptography, but their solutions are often very technical and overlooked by mainstream buyers.

In Europe, smaller niche vendors play a strong role in high-assurance and government-mandated use cases. Market consolidation is limited by national security and certification requirements. While this can frustrate buyers looking for platform solutions, it also supports cryptographic agility and reduces dependency on single vendors.

FUTURE

Cryptography should be evaluated based on preparedness rather than immediate return on investment. Organizations will be expected to show that their cryptographic architectures can evolve to address post-quantum migration requirements and long-term confidentiality concerns. Cryptographic agility will be a deciding factor, not just the choice of available algorithms.

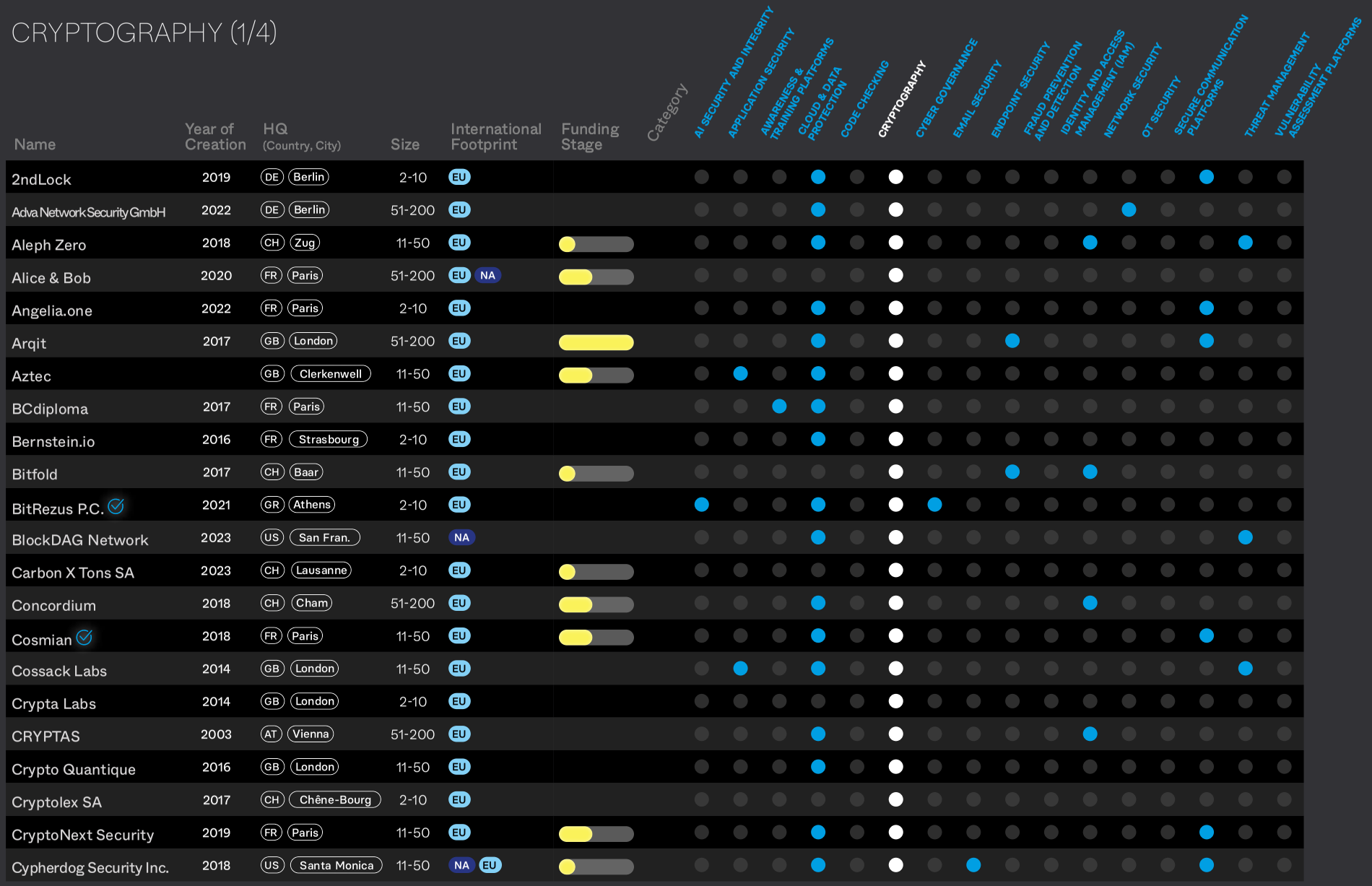
Solutions must support algorithm replacement, provide migration paths without significant downtime, and integrate with existing IAM and application security architectures. Transparency around implementation choices, certification status, and jurisdictional exposure will matter more than claims of cryptographic strength. In cryptography, trust is slow to build, easy to lose, and rarely forgiven once broken.

Alexei BALAGANSKI
Lead Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Blog: Cyber Resilience
Buyer's Compass: Cyber Risk Quantification Solutions
Leadership Compass: Cloud Security Posture Management (CSPM)
Leadership Compass: Identity and Access Governance

CRYPTOGRAPHY (1/4)

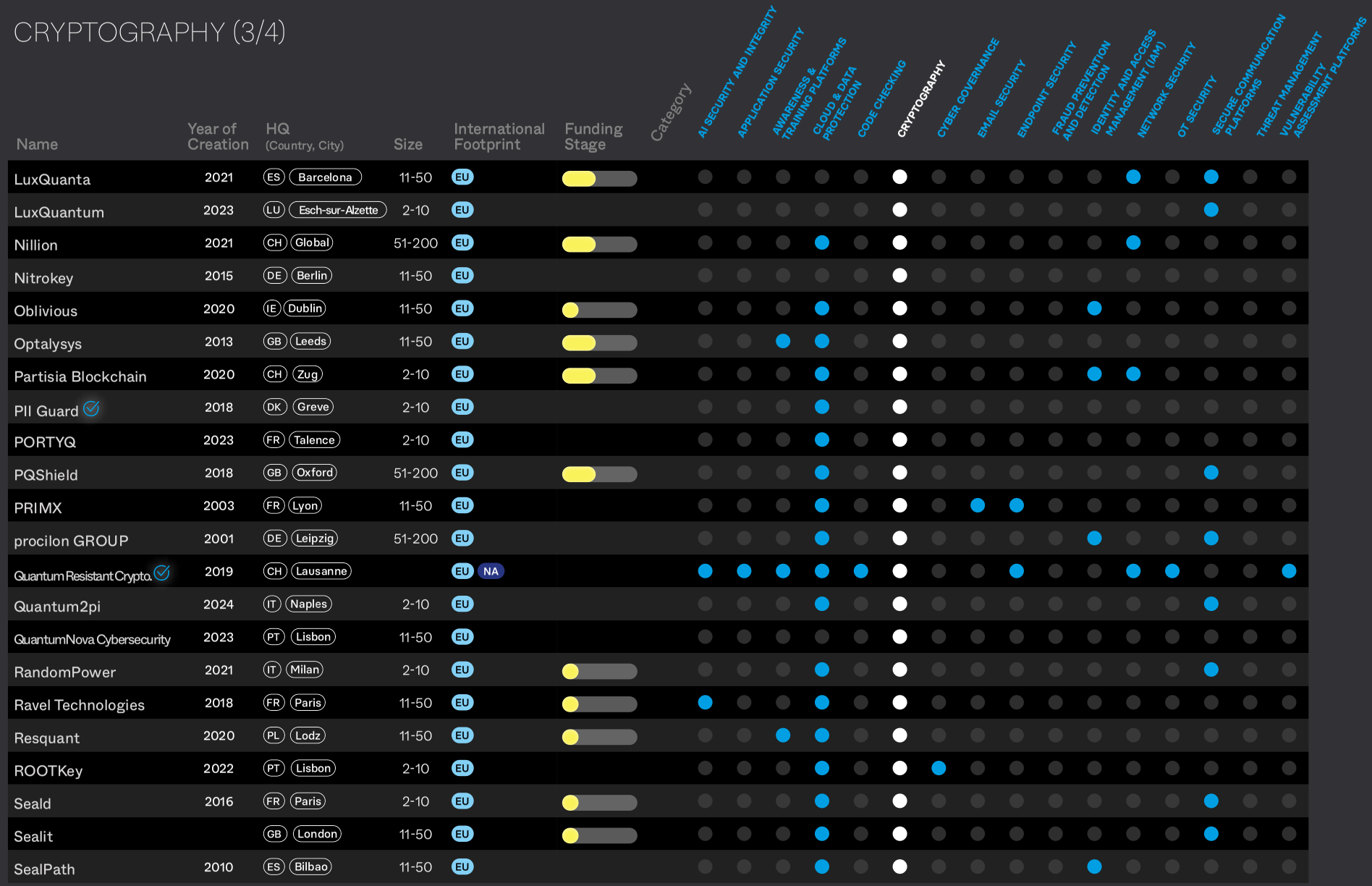


Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
2ndLock	2019	DE Berlin	2-10	EU		CRYPTOGRAPHY
Adva Network Security GmbH	2022	DE Berlin	51-200	EU		CRYPTOGRAPHY
Aleph Zero	2018	CH Zug	11-50	EU		CRYPTOGRAPHY
Alice & Bob	2020	FR Paris	51-200	EU NA		CRYPTOGRAPHY
Angelia.one	2022	FR Paris	2-10	EU		CRYPTOGRAPHY
Arqit	2017	GB London	51-200	EU		CRYPTOGRAPHY
Aztec		GB Clerkenwell	11-50	EU		CRYPTOGRAPHY
BCdiploma	2017	FR Paris	11-50	EU		CRYPTOGRAPHY
Bernstein.io	2016	FR Strasbourg	2-10	EU		CRYPTOGRAPHY
Bitfold	2017	CH Baar	11-50	EU		CRYPTOGRAPHY
BitRezus P.C.	2021	GR Athens	2-10	EU		CRYPTOGRAPHY
BlockDAG Network	2023	US San Fran.	11-50	NA		CRYPTOGRAPHY
Carbon X Tons SA	2023	CH Lausanne	2-10	EU		CRYPTOGRAPHY
Concordium	2018	CH Cham	51-200	EU		CRYPTOGRAPHY
Cosmian	2018	FR Paris	11-50	EU		CRYPTOGRAPHY
Cossack Labs	2014	GB London	11-50	EU		CRYPTOGRAPHY
Crypta Labs	2014	GB London	2-10	EU		CRYPTOGRAPHY
CRYPTAS	2003	AT Vienna	51-200	EU		CRYPTOGRAPHY
Crypto Quantique	2016	GB London	11-50	EU		CRYPTOGRAPHY
Cryptolex SA	2017	CH Chêne-Bourg	2-10	EU		CRYPTOGRAPHY
CryptoNext Security	2019	FR Paris	11-50	EU		CRYPTOGRAPHY
Cypherdog Security Inc.	2018	US Santa Monica	11-50	NA EU		CRYPTOGRAPHY

CRYPTOGRAPHY (2/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
CYSEC	2018	CH Lausanne	11-50	EU						●		●					●	●				
Data-Warehouse GmbH	1987	DE Ottobrunn	11-50	EU								●	●									●
DCD-SEMI	1999	PL Bytom	11-50	EU			●			●		●										
DROON	2019	FR Paris	11-50	EU						●		●			●							
DuoKey	2021	CH Lausanne	11-50	EU						●		●										
Dyne.org foundation	1999	NL Amsterdam	11-50	EU						●		●					●					
Eperi GmbH	2003	DE Pfungstadt		EU						●		●		●						●		
eSignus	2018	ES Gran Canaria	2-10	EU								●				●	●					
essendi it Group	2000	DE Schwabisch Hall	51-200	EU								●	●									●
Evervault	2019	US New York	11-50	NA EU						●		●				●						●
Eviden		FR Bezons	10,001+	EU						●		●					●			●		
Forkbomb BV	2022	NL Amsterdam	2-10	EU						●		●				●						
HENSOLDT	2017	DE Taufkirchen	5,001-10,000	EU								●					●	●		●		
ID Quantique	2001	CH Geneva	51-200	EU								●					●		●			
IDEMIA		FR Courbevoie	10,001+	EU NA APAC								●			●	●						
iliadata		FR Paris	2-10	EU						●		●										
INTAGIUM	2024	DE Dresden	2-10	EU						●		●							●			
KeeeX	2014	FR Marseille	11-50	EU						●		●							●			
KETS Quantum Security	2016	GB Bristol		EU						●		●							●			
Kin AI	2023	DK Copenhagen	11-50	EU			●			●		●										
Kobra Infosec	2005	DE Teutschenthal	11-50	EU								●										
Linksight	2021	NL Utrecht	2-10	EU					●	●		●										

CRYPTOGRAPHY (3/4)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
LuxQuanta	2021	ES Barcelona	11-50	EU								●					●		●			
LuxQuantum	2023	LU Esch-sur-Alzette	2-10	EU								●							●			
Nillion	2021	CH Global	51-200	EU						●		●					●					
Nitrokey	2015	DE Berlin	11-50	EU								●										
Oblivious	2020	IE Dublin	11-50	EU						●		●				●						
Optalysys	2013	GB Leeds	11-50	EU					●	●		●										
Partisia Blockchain	2020	CH Zug	2-10	EU						●		●				●	●					
PII Guard	2018	DK Greve	2-10	EU						●		●										
PORTYQ	2023	FR Talence	2-10	EU						●		●										
PQShield	2018	GB Oxford	51-200	EU						●		●								●		
PRIMX	2003	FR Lyon	11-50	EU						●		●		●	●							
procilon GROUP	2001	DE Leipzig	51-200	EU						●		●				●				●		
Quantum Resistant Crypto.	2019	CH Lausanne		EU NA			●	●	●	●	●	●			●			●	●			●
Quantum2pi	2024	IT Naples	2-10	EU						●		●								●		
QuantumNova Cybersecurity	2023	PT Lisbon	11-50	EU								●										
RandomPower	2021	IT Milan	2-10	EU						●		●								●		
Ravel Technologies	2018	FR Paris	11-50	EU			●			●		●										
Resquant	2020	PL Lodz	11-50	EU					●	●		●										
ROOTKey	2022	PT Lisbon	2-10	EU						●		●	●									
Seald	2016	FR Paris	2-10	EU						●		●								●		
Sealit		GB London	11-50	EU						●		●								●		
SealPath	2010	ES Bilbao	11-50	EU						●		●				●						

CRYPTOGRAPHY (4/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
SEALSQ		FR Meyreuil	51-200	EU						●		●					●					
SECQAI	2021	GB London	2-10	EU			●			●		●										
Secrets Vault	2024	ES Barcelona	2-10	EU						●		●					●					
Sintecs	2000	NL Hengelo	51-200	EU								●								●		
Specfile.pl	2015	PL Poznan	2-10	EU						●		●								●		
SSLok		FR								●		●										
Swisstronik	2022	CH Zug	11-50	EU						●		●					●					
Sygnanet	2021	PL Poznan	2-10	EU								●	●							●		
Syndesis Security			1						●			●	●									●
TACEO	2022	AT Graz	11-50	EU			●			●		●										
Thales Cybersecurity		US Austin	1,001-5,000	NA EU				●		●		●					●					
Vaultree	2020	IE Cork	51-200	EU			●			●		●										
Verifoxx	2020	GB London	2-10	EU			●			●		●										
Xiphera Ltd.	2017	FI Espoo		EU						●		●			●			●	●	●		
Zama	2020	FR Paris	51-200	EU						●		●								●		

Interview

HEXATRUST

The consolidation of European forces could be built at the condition of developing financing consolidation and growth operations through European funds on one side and developing joint procurement mechanisms at the European level to enable scaling across the continent on the other side.

What are the perspectives for the European cyber and cloud market?

Digital technology has no borders, but it does have an identity and rules. The distinctiveness of trusted European digital technology is based on both pillars: secure-by-design and privacy-by-design principles; something we can be proud of. The standards we must collectively apply such as GDPR, NIS 2 Directive, Cyber Resilience Act, Cybersecurity Act, CAIDA, EUCS are European regulations. Digital strategy must therefore be approached at the scale of the European continent in order to promote a consolidated and mature Digital Single Market and to meet the digital needs of 450 million European citizens.

It is under these conditions that representative European champions in cybersecurity and tech will be able to emerge. All the initiatives led by ECA, Hexatrust, Forum INCYBER, and KuppingerCole are essential to building this path forward. The objective is to create an EU tech reference framework independent from Gartner and non-European (particularly U.S.) analysts, one that would take into account European specificities in its evaluation criteria.

How does Hexatrust see the evolution of cybersecurity needs and the market in France and beyond?

Hexatrust represents more than 160 French or European entities, which together generate approximately €15 billion in revenue. If we look at the capability offering we represent; or the one mapped in the Cyber Panorama we developed in partnership with CESIN based on the NIST framework; we are pleased to see that we cover the needs of the French cybersecurity market. We are also able to address the broader European market, as a number of our members are already established across Europe.

With your experience leading an association that brings together a significant number of software vendors, what would help accelerate the consolidation of European forces?

The consolidation of European forces could be built at the condition of developing financing consolidation and growth operations through European funds on one side and developing joint procurement mechanisms at the European level to enable scaling across the continent on the other side.

After much hesitation, French public authorities (less clearly elsewhere in Europe for now) seem willing to act through the lever of public procurement; and private procurement where possible. What is your view? A flash in the pan, or genuine commitment?

Public procurement has never been so positively framed in rhetoric. It is encouraging to hear that European preference is no longer taboo. Henna Virkkunen highlights the risks of instrumentalizing our digital dependencies and reminds us that our competitiveness and security require us to reduce reliance on third-country technologies. Similarly, Stéphane Séjourné, through his call for "Made in Europe," unambiguously defends European preference. The objective is to use public procurement as a lever to secure our value chains and strengthen our industrial autonomy.

However, when it comes to concrete action, the situation is more uncertain. For example, regarding digital platforms, projects supported by France 2030 were not selected; under a DARPA-style logic; to address ministerial needs. Concerning EUCS, once again the outlook is not favorable for France. Europe is still not assuming that our "privacy by design" model should be applied in and out of Europe, despite the resistance of our allies in the United States.

In any case, for more than 10 years Hexatrust has consistently advocated for digital resilience built upon a strong and mobilized European cybersecurity and cloud industrial sector. This is why we officially contributed to the consultation on the revision of the European public procurement framework last January and we will be committed throughout the whole process of revision of the public procurement directive in 2026.

Finally, I advocate for a digital renewal consisting of doubling the investments we make each year in European companies in order to generate €690 billion over the next decade and create 500,000 jobs in Europe.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Hexatrust, the group of French and European champions in cybersecurity and trusted cloud.

Hexatrust is a non-profit association (loi 1901) that brings together and unites French and European champions in cybersecurity, trusted cloud, and digital workplace.

Hexatrust member companies are start-ups, SMEs, and mid-sized enterprises, including software publishers, solution providers, and service companies at the cutting edge of technology and innovation; the finest French gems in cybersecurity and trusted cloud.

hexatrust.com

Jean-Noël DE GALZAIN
President

Hexatrust

European Cybersecurity Mapping 2026

CYBER GOVERNANCE

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Cybersecurity extends beyond tools; it is fundamentally dependent on management commitment, staff engagement, clear rules aligned with business processes, and organizational agility. EU regulations like NIS2 mandate clear accountability. Governance systems are designed to help organizations define and manage cybersecurity policies, ensure compliance, conduct risk assessments, and support strategic decision-making.

Why Choose European Technology: European providers deliver solutions specifically tailored to the EU's legal landscape, ensuring full compliance with data protection laws. This allows governments and companies to maintain decisive control over their security policies and strategic decision-making.

Importance for European sovereignty: 10/10

Strong governance frameworks ensure that Europe's cybersecurity strategies are aligned with its regulations and strategic goals, reducing dependence on external standards or guidance.

Ensuring Cyber Resilience

kuppingercole ANALYSTS

MARKET CONTEXT

Cybersecurity threats are prevalent, requiring all organizations to address them. In 2025, major European companies like Jaguar Land Rover faced cyberattacks, causing significant disruptions and financial losses. Cyber governance involves leadership, policies, and processes to manage these risks in a business-aligned manner. The NIS2 directive mandates cyber risk management as a board-level obligation, while DORA creates a unified resilience regime for the financial sector, focusing on risk lifecycle functions such as identification, protection, detection, response, recovery, learning, and communication, integrating governance into operational resilience.

Unlike the US NIST Cybersecurity Framework, NIS2 specifies what organizations must implement but not how. Many EU organizations utilize ISO/IEC 27001:2022 for structured information security management, fostering governance and risk management. This opens the market to diverse frameworks, platforms, and tools that define accountability, manage risk, demonstrate compliance, and support cyber governance. These tools include Governance, Risk & Compliance (GRC) Platforms, Risk Assessment Tools, Identity Governance, and Administration (IGA) systems, supported by security event monitoring and vulnerability assessment tools.

EUROPEAN COMPETITIVE ADVANTAGES

The EU excels in consulting services around cyber governance and tool configuration, identifying, managing, and governing real cyber-risks. EU vendors assist in building processes and configuring tools for EU-specific obligations, including governance accountability, evidence trails, incident reporting, and risk management under NIS2 and DORA. DORA's scrutiny of ICT concentration risk and oversight of third-party providers increases demand for risk tooling compatible with EU regulations, offering tailored features meeting supervisory expectations. EU organizations prefer suppliers within EU jurisdiction, aligning with NIS2's varying national implementations.

ENISA plays a key role in shaping EU cybersecurity practices, issuing guidance for EU policy and regulation. EU vendors closely follow ENISA publications to update templates, control mappings, and reporting structures as needed.

TECHNOLOGY EVOLUTION & TRENDS

Traditionally based on quarterly reviews, modern governance requires near-real-time compliance and risk management assurance. Consequently, governance platforms now offer continuous monitoring and automated control testing.

Cloud services, often non-EU, have reshaped governance, introducing new risks and new security tools like Cloud Security Posture Management (CSPM), Data Security Posture Management (DSPM), and SaaS Security Posture Management (SSPM). Governance for Generative AI (GenAI) is also emerging. Supply chain and third-party governance are essential, driven by NIS2 and DORA's focus on ICT third-party risk management.

Challenges include aligning security spending with cyber risk. Traditional control lists and scorecards, along with simplistic risk measurements like CVSS scores, fall short. Risk quantification models and tools have emerged to measure risks financially.

Cyber Risk Quantification (CRQ) evaluates cyber risks financially, aiding data-driven cybersecurity investment decisions. It uses statistical methods to assess the likelihood and impact of cyber incidents using internal and external data, translating risks into monetary values to align security posture with business goals. CRQ complements Continuous Threat Exposure Management (CTEM), which prioritizes exploitable exposure identification to enhance technical security.

FUTURE

Future cyber governance will emphasize continuous, measurable, regulator-aligned assurance, requiring organizations to demonstrate the effectiveness of policies and controls across systems, clouds, and third-party networks. NIS2, DORA, and ENISA guidance push EU cyber governance beyond checkbox compliance toward operational resilience and accountability.

Integrated with technology management, cyber governance will encompass asset visibility, secure configuration, incident readiness, and recovery. DORA formalizes this model for financial services. Moving toward quantified risk assessments will justify cybersecurity investments and effective risk management.

Mike SMALL
Senior Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Enterprise Secrets Management
Blog: Strong Authentication in a Post-Quantum World
Blog: Quantum Computing Horizons in Cybersecurity

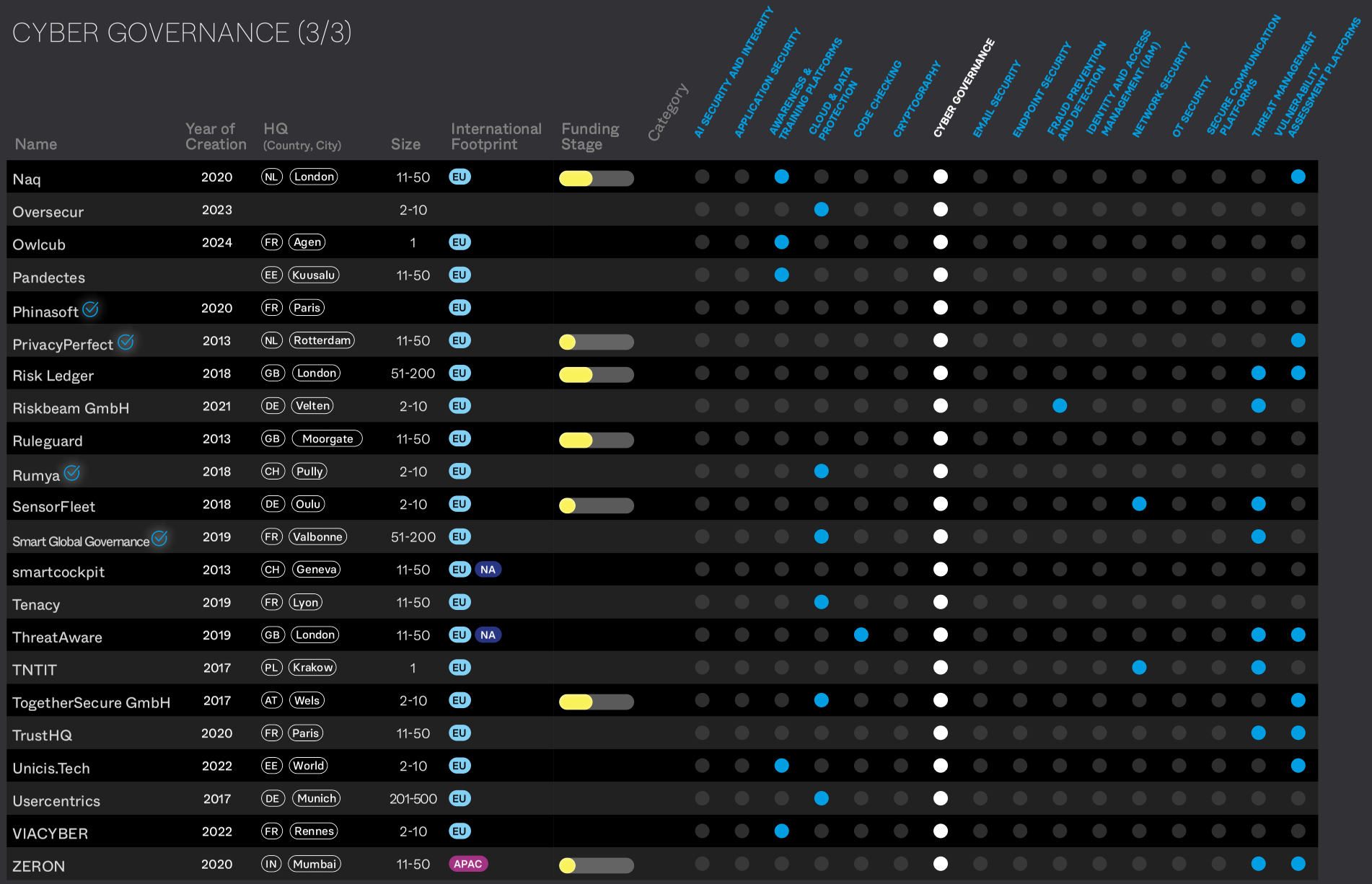
CYBER GOVERNANCE (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Acuity Risk Management	2005	GB London	11-50	EU									●									●
ai.esra	2024	IT Turin	11-50	EU									●									
AKARION	2017	DE Munich	11-50	EU									●								●	●
ALL4TEC	1998	FR Change	11-50	EU					●				●									
Apomatix	2017	GB London	11-50	EU									●									●
Bastion Technologies	2022	FR Paris	11-50	EU									●		●						●	●
Board of Cyber	2022	FR Sèvres	11-50	EU									●				●					●
Bubo Cybersec		FR Gardanne	2-10	EU						●			●				●				●	
CALPANA	2005	AT Linz	51-200	EU									●									
CalQRisk		IE Shannon	11-50	EU									●								●	●
Capptions	2017	NL Rotterdam	11-50	EU									●									
Citicus Limited	2000	GB London	11-50	EU									●						●			
Compleye.io	2018	NL Amsterdam	2-10	EU					●	●			●									
ComplyCloud	2017	DK Copenhagen	51-200	EU			●		●				●									
ComplyDo (YC F25)	2025	DE Berlin	2-10	EU									●									
CONTECHNET GmbH	2007	DE Pattensen	11-50	EU					●				●									●
Copla	2023	LT Kirkwall	11-50	EU					●				●								●	●
CyberVadis	2016	FR Paris	201-500	EU NA									●								●	●
Cynomi	2021	IL Herzliya	51-200	APAC									●									
Cyrima		PL Warsaw	2-10	EU					●				●								●	●
CyTailor	2021	FR Paris		EU					●	●			●									●
Dastra	2020	FR Paris	11-50	EU					●	●			●									

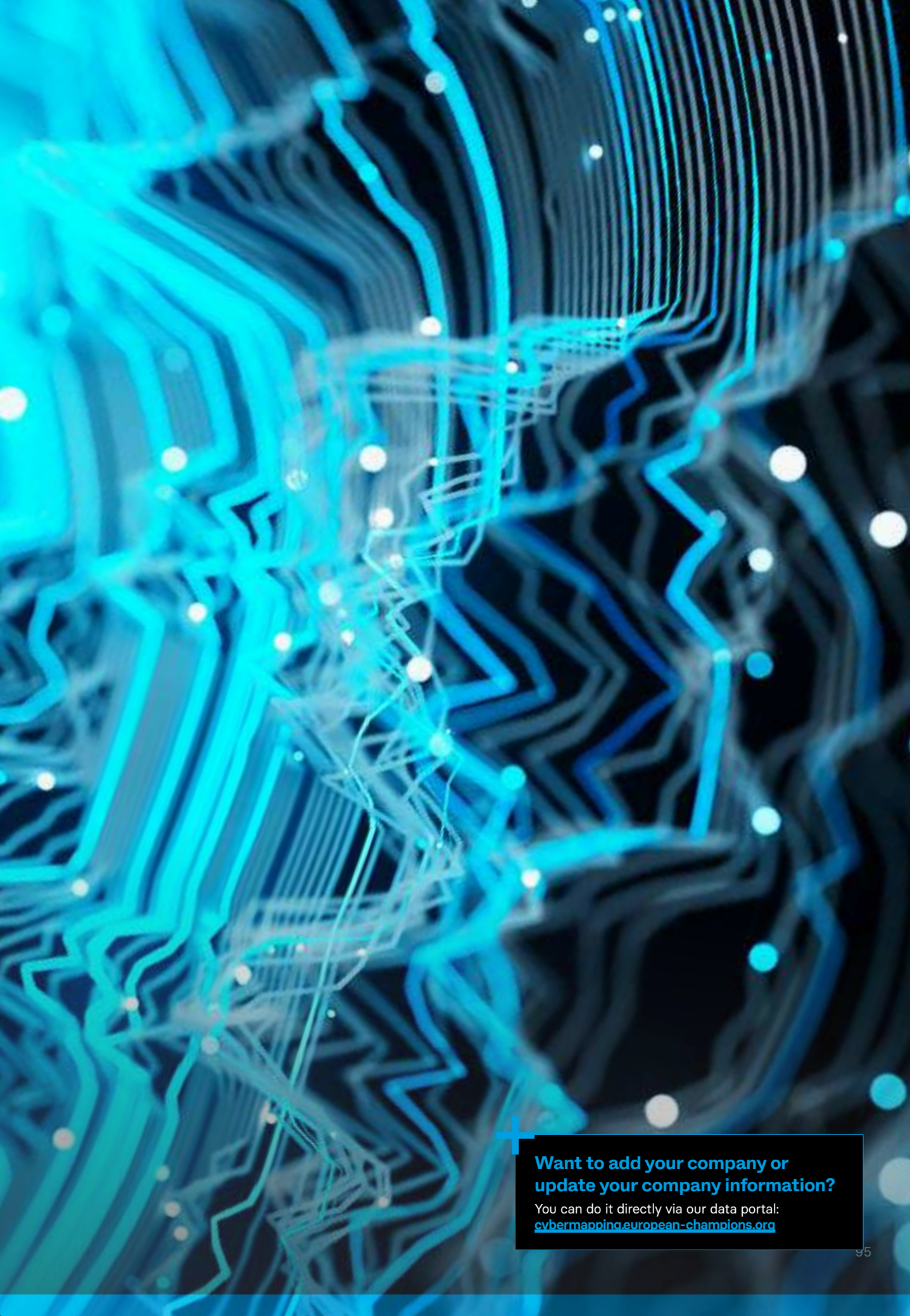
CYBER GOVERNANCE (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Data Legal Drive	2018	FR Neuilly-sur-Seine	51-200	EU									●									
Dataships	2019	US Sausalito	11-50	EU NA									●	●								
Didomi		FR Paris	51-200	EU						●			●									●
DPOrganizer	2015	SE Stockholm	11-50	EU					●				●									
Dream On Technology	2024	FR Lyon		EU NA					●				●								●	
DYNATRUST	2022	FR Lille	2-10	EU					●				●								●	
ECOMPLY.io	2017	DE Munich	2-10	EU						●			●									●
EDICIA	2003	FR Nantes	11-50	EU					●				●								●	
eramba	2011	GB London	11-50	EU					●				●									
Examin		FR Paris	11-50	EU					●				●									●
Eyako	2021	FR Saint-Denis	2-10						●				●									
Fabor	2023	FR Paris	2-10	EU									●									
FeelAgile	2007	FR Paris	11-50	EU					●				●									
Galink	2024	FR Paris		EU									●								●	
Hamyn√§		FR Lille	2-10	EU					●				●			●						
ibi systems GmbH	2012	DE Regensburg	11-50	EU					●				●									
Intuitem	2018	FR Vélizy-Villacoublay	11-50	EU					●	●			●									
IRM360	2017	NL Deventer	11-50	EU					●				●							●		●
Keepabl	2017	GB London	11-50	EU					●				●			●						
Kertos	2021	DE Munich	51-200	EU									●									
Leto	2021	FR Paris	2-10	EU			●		●	●			●									
Logmanager	2014	CZ Prague	11-50	EU					●				●								●	
MOB.ID		NL Amsterdam	11-50	EU									●			●						

CYBER GOVERNANCE (3/3)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Naq	2020	NL London	11-50	EU					●				●									●
Oversecur	2023		2-10							●			●									
Owlcub	2024	FR Agen	1	EU					●				●									
Pandectes		EE Kuusalu	11-50	EU					●				●									
Phinasoft	2020	FR Paris		EU									●									
PrivacyPerfect	2013	NL Rotterdam	11-50	EU									●									●
Risk Ledger	2018	GB London	51-200	EU									●								●	●
Riskbeam GmbH	2021	DE Velten	2-10	EU									●			●					●	
Ruleguard	2013	GB Moorgate	11-50	EU									●									
Rumya	2018	CH Pully	2-10	EU					●				●									
SensorFleet	2018	DE Oulu	2-10	EU									●					●			●	
Smart Global Governance	2019	FR Valbonne	51-200	EU					●				●								●	
smartcockpit	2013	CH Geneva	11-50	EU NA									●									
Tenacy	2019	FR Lyon	11-50	EU					●				●									
ThreatAware	2019	GB London	11-50	EU NA						●			●								●	●
TNTIT	2017	PL Krakow	1	EU									●					●			●	
TogetherSecure GmbH	2017	AT Wels	2-10	EU					●				●									●
TrustHQ	2020	FR Paris	11-50	EU									●								●	●
Unicis.Tech	2022	EE World	2-10	EU					●				●									●
Usercentrics	2017	DE Munich	201-500	EU					●				●									
VIACYBER	2022	FR Rennes	2-10	EU					●				●									
ZERON	2020	IN Mumbai	11-50	APAC									●								●	●



Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

European Cybersecurity Mapping 2026

EMAIL SECURITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Email security aims to protect systems from common threats like phishing, spam, malware, and unauthorized access. This domain is rapidly evolving with the emergence of AI-aided attacks, even as the security technology itself benefits from AI capabilities. Industry trends also show Threat Management solutions integrating the email vector into their core functions.

Why Choose European Technology: European providers prioritize privacy and sovereignty by strictly operating within GDPR-compliant frameworks. This guarantees secure communication, free from risks associated with third-country laws, and strengthens Europe's control over its digital communication channels.

Importance for European sovereignty: 8/10

Email remains a key vector for phishing, stealing credentials and cyberattacks. European solutions reduce exposure to foreign surveillance or data processing laws, safeguarding sensitive communications.

The Universal Door That Must Be Secured

MARKET CONTEXT

Email is the gift that keeps giving for cybercriminals. What other IT system provides threat actors with unfettered access to users at enterprises around the world for essentially no cost? In addition, because of its ease of use, openness, and flexibility – email will carry text in any language, file attachments of any type, and links to any website – it directly helps cybercriminals deploy ransomware, conduct espionage, lift account logins, and steal intellectual property.

Email has thus become a key tool in most attacks. In fact, the Verizon DBIR report for 2025 notes that ~60% of all breaches included some form of human interaction, typically via email. It thus follows that email security is of the utmost importance and has earned its position as a core security control for all organizations. While NIS2, DORA, GDPR and other EU regulations don't specifically address email security, because of its prevalence as an attack vector, it is very much in scope for them.

EUROPE'S COMPETITIVE ADVANTAGE

The criticality of strong email security can also be demonstrated by the sheer number of security vendors that provide it. In the most recent KuppingerCole Leadership Compass on email security, 49 vendors were highlighted that provide various forms of email security. Four vendors covered in this report have a primarily European focus, namely: Mailinblack, Xorlab, SpamTitan, and Retarus. These vendors are of specific interest for organizations requiring data sovereignty as they emphasize GDPR/NIS2 regulatory compliance by design and provide data residency within EU data centers.

MARKET DYNAMICS

All email security vendors fall into 1 of 4 categories: Vendors that provide built-in email security as part of the email service itself, namely Microsoft 365 and Google Workspace, Vendors of Secure Email Gateways (SEGs) that inspect inbound and outbound mail via an independent cloud service, Integrated Cloud Email Security (ICES) systems that connect via APIs to the cloud-based email platforms, and finally, Supplementary Email Security Services that provide encryption, file sandboxing, browser isolation and other email-centric services as extensions to email security systems.

TECHNICAL EVOLUTION AND TRENDS

Among the notable trends with email security systems is the increasing reliance on AI-based analytics. Vendors are integrating AI to enhance threat detection, enabling more precise identification of phishing and BEC attacks. This trend reflects the need for solutions capable of analyzing vast volumes of data to efficiently distinguish between legitimate and malicious emails. There is also a marked shift towards providing multi-channel security solutions. As businesses extend their communication systems to include Microsoft Teams, Slack, and Zoom, many email security vendors have expanded their protections to encompass these communications applications as well. DLP integration within email security systems is also gaining traction as businesses seek to improve their prevention of sensitive data leakage.

For the roughly 50% of organizations that go beyond using the built-in security of Microsoft 365 and Google Workspace, a handful of vendors own most of the market, with the remaining dozens sharing the rest. As demand continues to grow, driven by the evolving nature of cyber threats, I anticipate continued innovation and accelerated vendor consolidation. New entrants are introducing pioneering techniques and established players are likely to engage in strategic acquisitions to enhance their portfolios.

FUTURE

European-focused vendors have the continued opportunity to provide email security centric services that strike the right balance between security for the enterprise, regulatory compliance, and privacy for the individual employee. The focus remains clear: providing comprehensive and adaptive email security that protects against sophisticated threats while facilitating safe and efficient communication. For as long as email remains a primary communication "door", email security will continue to be a critical control.

Matthew GARDINER
Fellow Analyst
KuppingerCole Analysts AG

For detailed analysis, see:
Leadership Compass: Email Security
Buyer's Compass: Email Security

EMAIL SECURITY

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
BlueMind		FR Labège	11-50	EU										●						●		
CipherMail	2007	NL Amsterdam	2-10	EU								●		●						●		
Clearswift Cyber Security		DE Cologne	201-500	EU					●					●		●					●	
comcrypto GmbH	2014	DE Chemnitz	11-50	EU								●		●						●		
Egress		GB London	201-500	EU NA						●				●			●				●	
Fortyx Security	2024	GB London	2-10	EU			●							●		●						
Halon	2010	SE Gothenburg	11-50	EU NA										●				●			●	
Libraesva	2013	GB London	11-50	EU NA					●	●				●							●	
Mailinblack	2003	FR Marseille	51-200	EU					●					●			●					
MailStore Software GmbH	2006	DE Viersen	11-50	EU										●								
Mailvelope	2012	DE Zellingen	2-10	EU								●		●						●		
Mimecast	2003	GB London	1,001-5,000	EU NA APAC					●	●				●							●	
Proton	2014	CH Geneva	501-1,000	EU								●		●			●			●		
Retarus	1992	DE Munich	201-500	EU NA APAC										●								
Secuserve	2003	FR Paris	11-50	EU										●								
Smartlockr	2014	NL Amsterdam	11-50	EU						●				●							●	
xorlab	2015	CH Stadtkreis 11	11-50	EU					●					●							●	
Zertificon Solutions GmbH	2004	DE Berlin	51-200	EU						●		●		●						●		
Zivver	2015	NL Amsterdam	51-200	EU						●				●							●	

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

TRUST VALLEY

Trust is no longer defensive; it shapes who wins contracts and builds durable alliances.

DIGITAL TRUST: THE INVESTMENT OPPORTUNITY DEFINING TOMORROW'S ECONOMY

Digital trust has moved beyond compliance. It is becoming a decisive competitive advantage and a structural pillar of the global economy.

The digital economy already represents roughly 15–17% of global GDP, exceeding USD 16 trillion in value according to OECD and World Economic Forum analyses. This value must be protected. At the same time, cyber risk is intensifying: over 90% of large organizations have adjusted their cybersecurity strategies in response to geopolitical volatility. The expansion of digital activity without corresponding trust infrastructure creates systemic vulnerability.

Trust Valley was created by EPFL to address precisely this gap. Every transaction, data exchange, and digital interaction depends on trust. Yet many organizations still operate with fragmented security and governance models. Digital trust provides the integrated framework that enables secure scale.

Switzerland offers a uniquely strong environment for building trusted digital solutions. Ranked first globally in innovation by the Global Innovation Index, the country combines political neutrality, regulatory predictability, and institutional stability. Trust Valley leverages this environment to connect startups, enterprises, investors, and public actors around a shared ambition: making trust operational at scale.

Digital trust is compelling for investment and growth in three ways.

First, growth acceleration. Trust increasingly influences revenue. Enterprises select vendors based on demonstrable security, governance, and transparency. Startups that embed resilience from day one close partnerships faster. Talent gravitates toward organizations that treat cybersecurity and data responsibility as strategic priorities. Trust is no longer defensive; it shapes who wins contracts and builds durable alliances.

Second, ecosystem dynamics. Trust does not scale in isolation. Trust Valley brings together startups, corporates, investors, and public institutions within a structured environment. Collaboration reduces fragmentation and accelerates adoption. Anchored in Switzerland and founded by EPFL with strong public and private partners, the ecosystem combines scientific depth with institutional credibility. This matters when companies expand across borders and operate in increasingly regulated environments.

Third, a mindset shift. Traditional cybersecurity focuses on preventing loss. Digital trust goes further: it designs systems that enable transactions, international expansion, and long-term confidence. This distinction changes capital allocation.

Investors are funding not only tools that block threats, but infrastructure that allows the digital economy to grow securely. As trust becomes foundational, sustained investment follows.

Trust Valley positions itself as an execution-oriented platform. Since inception, it has supported more than 250 startups and innovation projects in cybersecurity and digital trust. Portfolio companies have collectively raised over CHF 400 million, demonstrating that trusted technology is scalable and globally relevant.

Its structured programs; Tech4Trust, Trust Village incubators, Trust4SMEs, and international GovTech initiatives; connect research, innovation, capital, and enterprise demand within one coherent framework. A key barrier to adoption is not technical capability but strategic understanding. Many boards still treat trust as a compliance topic rather than a growth lever. Trust Valley translates technical complexity into business language and demonstrates measurable return on investment through practical case examples.

The beneficiaries of digital trust extend across the ecosystem.

Solution providers gain from structural demand expansion as organizations seek integrated, resilient systems rather than isolated tools. Enterprises strengthen resilience, reduce regulatory friction, and reinforce stakeholder confidence. In a context of geopolitical fragmentation, trusted infrastructure becomes a strategic asset enabling cross-border growth.

Investors access a high-growth segment aligned with regulatory momentum and structural digitalization. Early-stage cybersecurity innovators, system integrators, and advisory platforms represent scalable opportunities. At the systemic level, higher trust standards reduce collective risk and increase economic stability through positive network effects.

The key message is clear: digital trust is not emerging; it is foundational. The strategic question is whether organizations approach it proactively within a coordinated ecosystem or react after incidents occur.

In a world defined by geopolitical volatility, rising cybercrime, and regulatory complexity, trusted digital infrastructure underpins sovereignty, competitiveness, and sustainable growth. Digital trust is one of the defining structural investment themes of the coming decade. Those who align early will help shape tomorrow's markets.

TRUST VALLEY
Ensuring Safe Digital Growth

The Trust Valley is a public-private partnership aimed at promoting the excellence of the Lake Geneva region in the field of digital trust and cybersecurity.

Public authorities, academic institutions and economic players are joining forces to promote this unique centre of expertise and encourage the emergence of innovative projects.

trustvalley.swiss

Lennig PEDRON
CEO

Trust Valley

European Cybersecurity Mapping 2026

ENDPOINT SECURITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: With the rise of mobile devices, extended enterprises, and remote working, an increasing number of IT system accesses originate from user endpoints. These devices must be protected from cyber threats, spyware, and embedded malware to ensure safe network access. Modern tools increasingly leverage AI and automated processes to detect malicious attempts, including zero-day attacks.

Why Choose European Technology: European vendors offer solutions specifically tailored to local privacy regulations and sovereignty concerns. This ensures safe, compliant, and independent endpoint protection for both businesses and governments.

Importance for European sovereignty: 10/10

Endpoint protection is a key part of Threat management. It is therefore a decisive element of zero trust and ability to stop attacks including zero day ones. Dependence on foreign endpoint solutions, however, can still introduce vulnerabilities.

Threat Containment Starts on the Endpoint

kuppingercole ANALYSTS

MARKET CONTEXT

Every endpoint represents an entry point for attackers and has effectively become the new network perimeter. Breaches, ransomware attacks, and account takeovers frequently start on laptops, servers, mobile devices, and Internet of Things (IoT) devices. The General Data Protection Regulation (GDPR), Network and Information Security Directive 2 (NIS2), Digital Operational Resilience Act (DORA), and Artificial Intelligence Act (AI Act) make endpoint security a board-level topic.

EUROPEAN COMPETITIVE ADVANTAGES

European endpoint security vendors have a competitive advantage because they tend to build for EU digital sovereignty and regulatory compliance and work collaboratively in regional clusters. Privacy by design shapes telemetry collection, retention, and admin access. Many provide EU data centers, EU support teams, and specific support for compliance with GDPR Article 28. They also enable customers to keep logs and incident data inside the EU and to meet NIS2 and DORA demands for evidence that controls are in place and to limit the impact of cyber incidents. The Electronic Identification, Authentication and Trust Services 2.0 (eIDAS 2.0) regulation ensures that endpoints have cryptographically verifiable identities, while the Cyber Resilience Act (CRA) rewards secure software supply chains, which are being increasingly targeted by attackers.

TECHNOLOGY EVOLUTION & TRENDS

Endpoint security is moving from signature scanning to behavior-focused prevention and recovery. Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) systems continue to converge into Endpoint Protection Detection and Response (EPDR). Agents collect more runtime signals and enforce policy locally. Central consoles run as SaaS and expose secured Application Programming Interfaces (APIs). Integration with Security Incident and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems is another trend aimed at improving reporting and case handling. Vendors are increasingly adding automation to contain incidents quickly, limit impact, and shorten recovery time by isolating compromised endpoints, restoring endpoints to a known good state, and forcing credential resets. Machine Learning (ML) improves detection for fileless attacks and living-off-the-land activity, while Generative Artificial Intelligence (GenAI) is being used to support analyst workflows, fine-tune policies, and summarize investigations.

MARKET DYNAMICS

The European endpoint security market is mature yet crowded. Platform vendors drive standardization on a single agent for cost control and audits. Mergers and acquisitions favor add-on acquisitions in threat research, device management, and response automation. Many CISOs choose "buy" over "build" due to NIS2 timelines and talent gaps. Adoption follows a "lift and shift" pattern from legacy antivirus to EPDR, leading to tighter links with SIEM and identity. Startups win by solving a specific endpoint problem well, strict EU residency, and transparent support locations, ownership, and data flows. But growth demands global expansion.

FUTURE

Over the next 24 to 36 months, I expect the way European organizations manage and secure their endpoint devices will align tightly with identity controls and reporting rules under NIS2. The AI Act will pressure vendors to explain model use and oversight. The CRA will push deeper checks for firmware integrity and signed updates. DORA audits will also raise expectations for evidence, testing, and continuity. Buyers should demand EU data residency, test recovery, and validate GDPR Article 28 clauses. Investors should favor vendors that can translate EU regulations into product design and market messaging and can sell and support through partners in multiple European markets. Vendors should plan early for expansion beyond the home market, plus building cross-border support.

Warwick ASHFORD
Senior Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Endpoint Protection Detection & Response (EPDR)

Whitepaper: NIS2 Starts with Securely Managed Endpoints

ENDPOINT SECURITY (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
2NS Cybersecurity Oy		FI Espoo	11-50	EU	
Actinis	2020	EE Tartu	2-10	EU	
allpriv	2023	FR Barcelona	11-50	EU	
Apostrophy			11-50		
AppSense		US Sunnyvale	1,001-5,000	NA	
Avast		CZ Prague	1,001-5,000	EU	
AwaCloud	2016	FR Paris	2-10	EU	
AxBx	1999	FR Villeneuve-D'Ascq	11-50	EU	
baramundi software	2000	DE Augsburg	201-500	EU NA	
Becrypt	2001	GB London	51-200	EU	
Binarii Labs	2021	IE Dublin		EU NA APAC	
BitNinja Security	2014	HU Debrecen	11-50	EU	
BlueVoyant	2017	NL New York	501-1,000	NA EU	
BullGuard		GB London	1	EU	
Cenobe Cybersecurity	2019	GR Athens	11-50	EU	
ControlUp Spain	2008	ES Madrid	201-500	EU	
Cortado	2015	DE Berlin	51-200	EU NA APAC	
Cyberlib	2025	FR Malakoff	11-50	EU	
Cyberscope		GR Rhodes	11-50	EU	
DongIT	2011	NL Leiden	11-50	EU	
DriveLock SE	1999	DE Munich	51-200	EU	
EPSEED	2020	FR Nice	2-10	EU	

ENDPOINT SECURITY (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
FileWave	1992	CH Wil	51-200	EU NA APAC											●		●					●
Fitsec Ltd	2009	FI Espoo	2-10	EU					●						●						●	●
i-Guard	2014	FR Paris	11-50	EU			●								●						●	
Inpedio	2015	NL The Hague	11-50	EU								●			●			●			●	
ITWatch	2017	DK Copenhagen	2-10	EU											●							
KERYS Software	2024	FR Palaiseau	2-10	EU											●							
Ledger		FR Paris	501-1,000	EU						●		●			●							
LogSentinel	2017	NL Naarden	11-50	EU					●				●		●						●	●
Matrix42	1992	DE Frankfurt	501-1,000	EU											●							
MITE3 Cybersecurity	2018	NL Zwolle	2-10	EU					●				●		●							●
mnemonic	2000	NL Oslo	201-500	EU NA											●							
Nexthink	2004	CH Prilly	1,001-5,000	EU NA APAC					●						●						●	
Northwave Cyber	2006	NL Utrecht	201-500	EU					●				●		●						●	●
Nucleon Security	2019	FR Paris	11-50	EU					●						●						●	
ORSEC Technologies	2023	FR St-Jacques-de-la-Lande	11-50	EU											●			●			●	●
Pinewood	1994	NL Delft	51-200	EU											●							
Pradeo	2010	FR Paris	51-200	EU NA			●								●						●	●
PROGET	2007	PL Bielsko-Biala	11-50	EU					●						●						●	
SecuLution GmbH	2001	DE Werl	11-50	EU			●								●						●	
Senturo	2023	GB London	11-50	EU											●						●	●
Shindan.io			2-10												●						●	
Silverskin Information	2009	FI Helsinki	11-50	EU			●		●						●							●

ENDPOINT SECURITY (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
SURF SECURITY	2021	GB London	11-50	EU						●					●		●				●	
Tesorion	2018	NL Leusden	51-200	EU											●		●	●			●	
TRAPMINE	2016	EE Tallinn	2-10	EU											●						●	●
Trend Micro		JP Tokyo	5,001 10,000	EU NA APAC									●		●			●			●	
TYREX CYBER	2016	FR Clichy	11-50	EU											●							
WithSecure	1988	FI Helsinki	1,001-5,000	EU NA						●					●		●				●	
X-Systems B.V.	2016	NL The Hague	11-50	EU											●					●	●	

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

DIGITALLEAD

Europe's cybersecurity would benefit from stronger coordination, faster innovation-to-market pathways, and greater visibility of European solutions.

Can you present your organization, its objectives and achievements?

We strengthen Danish ICT companies and digital businesses by connecting entrepreneurs, companies, and researchers in a strong network. Through events, collaborations, and joint projects, we turn digital innovation into growth, with a focus on green, efficient, and secure digital solutions that boost competitiveness and address societal challenges.

You have kindly supported the setup of the ECA European Cybersecurity Vendors Mapping: can you tell us why?

DigitalLead supports the ECA European Cybersecurity Vendors Mapping as it increases visibility and market access for European cybersecurity vendors, especially SMEs and scale-ups. It helps Danish companies scale beyond national markets and strengthens European cybersecurity value chains through cross-border collaboration, aligning with DigitalLead's mission to promote innovation, competitiveness, and trusted European technologies.

Is cybersecurity an important issue in your national context?

Cybersecurity is a strategic priority in Denmark and closely linked to digital competitiveness, resilience, and trust. As one of Europe's most digitalized countries, Denmark creates significant value through digital technologies but also faces increased cyber threats. Consequently, cybersecurity is no longer seen as a purely technical issue, but as a core business and leadership concern that impacts operations, compliance, reputation, and long-term competitiveness, in line with European regulations such as NIS2, the Cyber Resilience Act, and GDPR.

How could you present the local cybersecurity industry (vendors, service providers)?

The Danish cybersecurity landscape is dominated by specialized vendors focusing on niches like identity management, OT/ICS security, threat detection, and privacy technologies. This makes them valuable partners in European value chains, even as SMEs or scale-ups. DigitalLead acts as a neutral innovation platform, connecting vendors, users, researchers, and public stakeholders, supporting innovation projects, matchmaking, and user-driven solution development. It also contributes to national coordination, including operating the Danish National Coordination Centre (NCC-DK) with CenSec.

In your opinion, what could Europe do better regarding cybersecurity?

Europe's cybersecurity would benefit from stronger coordination, faster innovation-to-market pathways, and greater visibility of European solutions. Fragmentation across countries, clusters, and regulations limits collective capacity. Supporting adoption especially for SMEs and critical infrastructure requires not just regulation, but innovation support, testing environments, and accessto trusted European technologies. Strengthening digital sovereignty demands a balanced focus on technology, market access, interoperability, and partnerships..

For your own organization, how far are you taking part in or promoting joint European initiatives?

DigitalLead actively promotes joint European initiatives by connecting Danish cybersecurity companies to European networks, partnerships, and funding opportunities.

We work to position Danish vendors within broader European value chains and encourage collaboration across borders, sectors, and disciplines. By supporting European mappings, joint innovation projects, and cross-national partnerships, DigitalLead contributes to building a stronger and more coherent European cybersecurity ecosystem based on shared values, trust, and competitiveness.

DigitalLead

DigitalLead is Denmark's national cluster for digital technologies and serves as a focal point for digital innovation - both for companies that develop digital solutions, as well as for other sectors that need innovative digital solutions.

DigitalLead thus constitutes a unique platform for innovation and growth in the interaction between business, research and educational institutions, public authorities and citizens.

digitallead.dk

European Cybersecurity Mapping 2026

IDENTITY AND ACCESS MANAGEMENT (IAM)

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Identity and the ability to define and manage access rights is a cornerstone of security. Identity has become a prime target for criminals, who are increasingly using AI to forge identities. IAM systems manage user identities and access permissions, adapting to this new threat landscape. They are crucial for ensuring secure and authorized access, especially as more IT systems migrate to the Cloud.

Why Choose European Technology: European IAM providers guarantee that sensitive access credentials remain secure and compliant with EU regulations, such as eIDAS2. Supporting these technologies reduces dependency on external solutions and significantly enhances trust in European digital identity frameworks.

Importance for European sovereignty: 10/10

IAM systems control access to sensitive data and infrastructure. A loss of control over these systems could severely impact sovereignty, making European solutions essential.

Identity at the Core: The Foundation of Cybersecurity, Governance and Digital Trust

MARKET CONTEXT

Improper identity and credential management maintains the leading role as a root cause in roughly one-fifth to over one-half of data breaches, and its role is even greater when considering access and escalation issues. As an advisor, I see relevant regulations driving the need for strong identity governance and administration to ensure compliance. This makes IAM the key foundation of cybersecurity across the workforce, cloud, SaaS, APIs, DevOps, and third-party access.

EUROPEAN COMPETITIVE ADVANTAGES

European vendors in the IAM space benefit from their specific positioning. Their strong traditional presence in regulated industries like finance and healthcare gives them firsthand experience with EU regulations like the Digital Operational Resilience Act (DORA) and Network and Information Security Directive 2 (NIS2). Their ability to handle and store personal data in Europe ensures strong General Data Protection Regulation (GDPR) compliance and supports digital sovereignty.

Trusted decentralized identities issued by governments or banks in the Netherlands and Nordic European countries drive pioneering IAM innovations, like decentralized identities and digital wallets. This gives European vendors unique positioning and expertise in addressing regulatory and industry-specific requirements within IAM, including privileged, administrative access and the wave of new types of non-human identities.

TECHNOLOGY EVOLUTION & TRENDS

I observe a structural transformation away from monolithic IAM stacks, isolated point solutions, and organizational silos. This move is driven by architectural modularization, automation, AI, and APIs as the glue connecting components and capabilities. Organizations are embracing Identity Fabrics, enabling greater scalability, composability, and orchestration across heterogeneous identity systems. This shift aligns with increasingly distributed IT environments and multi-cloud strategies.

Non-Human Identities (NHIs) are no longer hype. Agents, workloads, machines, and containers are rapidly becoming crucial innovation enablers for any organization due to APIs, IoT, and emerging agentic AI. Maintaining visibility, managing lifecycles, providing just-in-time least privilege access, in-session analytics, and automation are essential to impose control and governance.

I see dynamic authorization evolving through AI-driven, context-aware decision-making. Real-time signals and continuous evaluation enable adaptive enforcement models that integrate authorization with detection and response, which makes fine-grained policy-based access control (PBAC) a core Zero Trust enabler. Passive authentication will further establish identity as a core security layer.

MARKET DYNAMICS

The IAM market is characterized by a multitude of specialized and emerging vendors alongside established IAM providers, each catering to different facets of identity management. As such, it is fragmented yet evolving towards consolidation.

This is particularly evident in Consumer Identity and Access Management (CIAM), where niche players create innovative solutions. I expect consolidation to happen, especially for NHI vendors as strategic acquisition targets for IAM, PAM, secrets management, and DevOps platform vendors.

Similarly, modernization will make traditional IGA vendors consider acquiring cloud-native challengers to expand their solutions.

FUTURE

I expect the IAM market to transform significantly in the next 2-3 years: orchestration will emerge as the control plane, decoupling logic from systems. The EU Digital Identity Wallet will accelerate decentralized identity. AI will drive autonomous identity at scale, extending governance to non-human and AI-driven identities.

Investors should look at enabling technologies instead of full IAM stacks. As the market consolidates, orchestration layers, non-human identity management, policy engines, and identity security components are expected to be prime acquisition targets, possibly as soon as 2026.

Buyers should focus on architectural flexibility, policy-based authorization, and the convergence of IAM with security operations, rather than niche features. Decentralized credentials and strong governance for machine and AI agent identities will be essential.

For vendors to succeed, faster modularization and automation are key. I consider integrating orchestration and AI-driven governance essential. European vendors will increasingly combine this with meeting regulatory standards and addressing digital sovereignty.

Matthias REINWARTH
IAM Practice Director
KuppingerCole Analysts AG

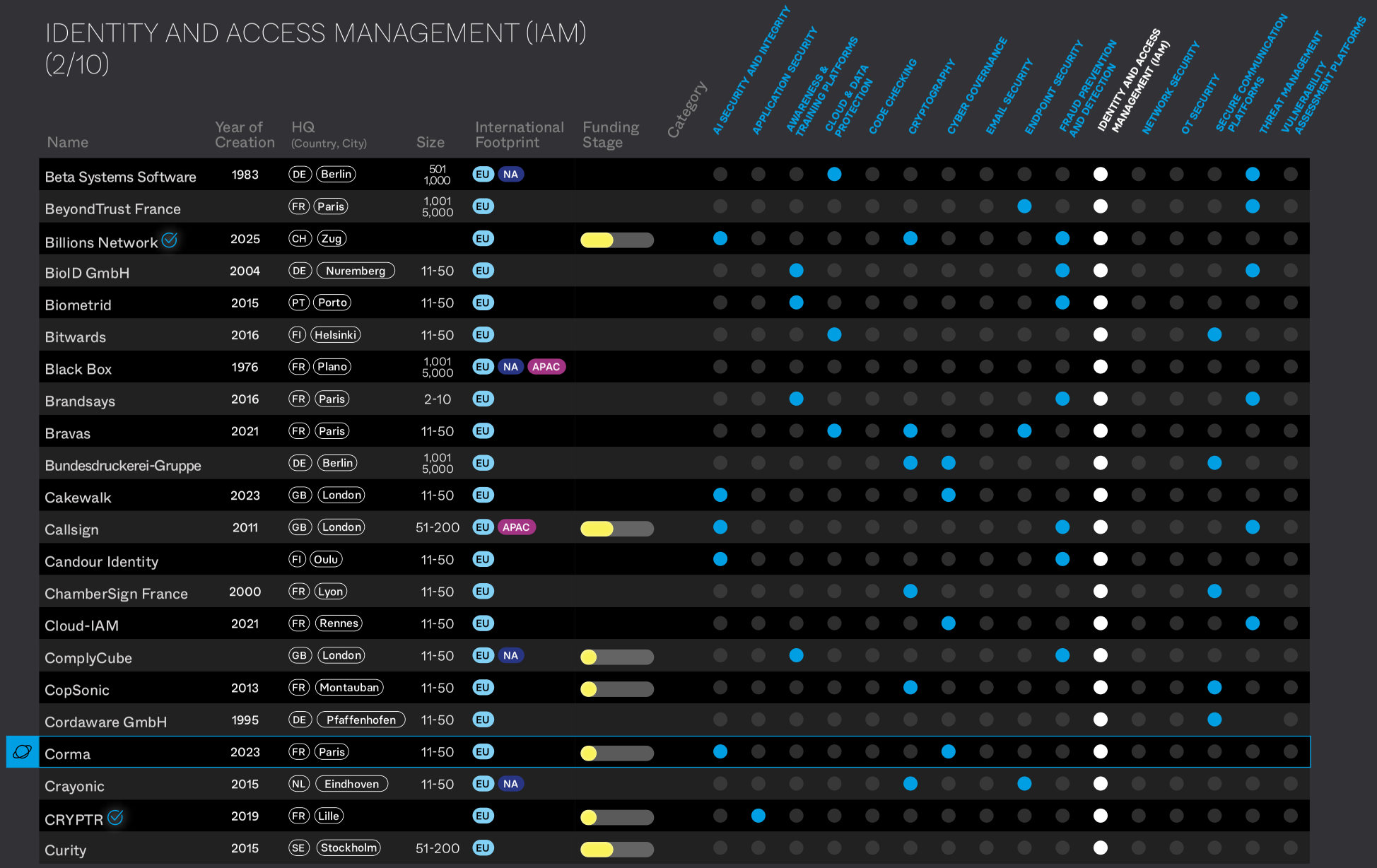
For detailed analysis, see:

Leadership Compass Identity Fabrics
Leadership Compass Non-Human Identity Management
Leadership Compass Consumer Identity and Access Management (CIAM)

IDENTITY AND ACCESS MANAGEMENT (IAM) (1/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
10Duke	2007	GB London	11-50	EU						●							●					
1Password	2005	CA Toronto	1,001 5,000	NA						●					●		●					
1TrueID	2016	IT Chiari	11-50	EU						●		●					●					
20face	2016	NL Enschede	11-50	EU			●		●								●					
2-Controlware		NL Breda	11-50	EU													●					
8Layers	2024	ES Madrid	2-10	EU			●						●				●				●	
A3BC GROUP	2018	FR Rennes	11-50	EU						●		●					●					
Access Informer Security	2011	CH Zug	2-10	EU									●				●					
achelos GmbH	2008	DE Paderborn	51-200	EU					●			●	●				●				●	
Admin By Request		DK San Fran.	501 1,000	EU NA													●					
AID:Tech	2016	IE Dublin	11-50	EU											●		●					
AirID GmbH	2004	DE Oberhausen	11-50	EU								●			●		●					
amitego	2003	CH Wangen	11-50	EU											●		●		●			
ANGOKA	2019	GB Belfast	11-50	EU													●	●	●		●	
Applied Risk	2012	NL Amsterdam	11-50	EU					●								●		●		●	●
Atos		FR Bezons	10,001+	EU NA APAC			●						●				●				●	
Authentiq	2015	NL Utrecht	2-10	EU								●					●			●		
AUTHENTIQ8 ME	2025	GB London	2-10	EU								●			●		●					
AuthGate B.V.	2019	NL Hengelo		EU								●			●		●		●	●		
AuthN by IDEE	2015	DE Munich	11-50	EU					●						●		●					
Axiomatics	2006	US Chicago	51-200	EU NA						●							●				●	
BAYOOSOFT		DE Darmstadt	51-200	EU								●		●			●					

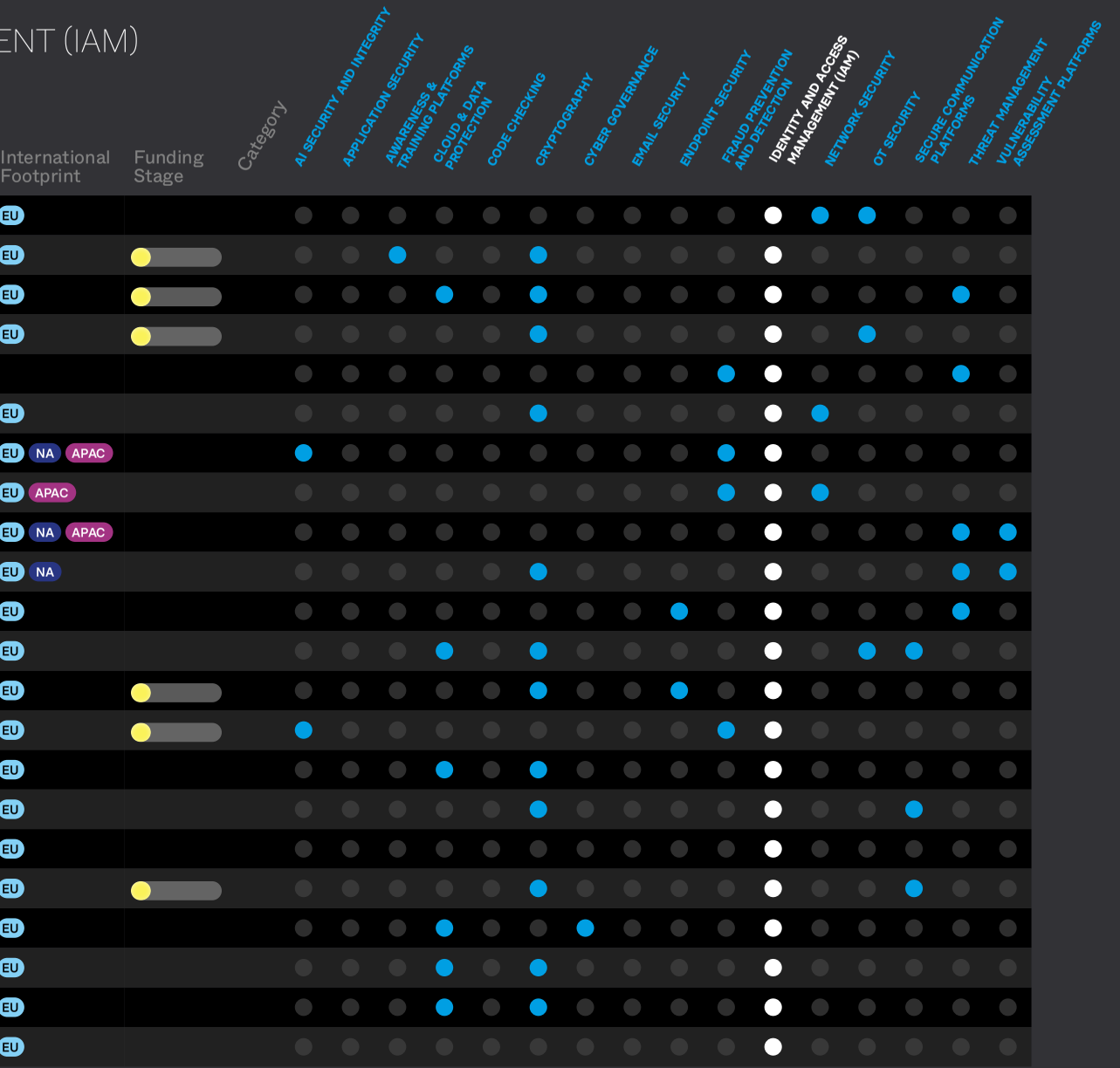
IDENTITY AND ACCESS MANAGEMENT (IAM) (2/10)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
Beta Systems Software	1983	DE Berlin	501 1,000	EU NA	
BeyondTrust France		FR Paris	1,001 5,000	EU	
Billions Network	2025	CH Zug		EU	
BioID GmbH	2004	DE Nuremberg	11-50	EU	
Biometrid	2015	PT Porto	11-50	EU	
Bitwards	2016	FI Helsinki	11-50	EU	
Black Box	1976	FR Plano	1,001 5,000	EU NA APAC	
Brandsays	2016	FR Paris	2-10	EU	
Bravas	2021	FR Paris	11-50	EU	
Bundesdruckerei-Gruppe		DE Berlin	1,001 5,000	EU	
Cakewalk	2023	GB London	11-50	EU	
Callsign	2011	GB London	51-200	EU APAC	
Candour Identity		FI Oulu	11-50	EU	
ChamberSign France	2000	FR Lyon	11-50	EU	
Cloud-IAM	2021	FR Rennes	11-50	EU	
ComplyCube		GB London	11-50	EU NA	
CopSonic	2013	FR Montauban	11-50	EU	
Cordaware GmbH	1995	DE Pfaffenhofen	11-50	EU	
Corma	2023	FR Paris	11-50	EU	
Crayonic	2015	NL Eindhoven	11-50	EU NA	
CRYPTR	2019	FR Lille		EU	
Curity	2015	SE Stockholm	51-200	EU	

IDENTITY AND ACCESS MANAGEMENT (IAM) (3/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
cyberelements		FR Sausheim	51-200	EU		
Cyberneid	2019	IT Naples	2-10	EU		
Cybernetica	1997	EE Tallinn	201-500	EU		
Cyberus Labs		PL Katowice	2-10	EU		
CyEx	2020		11-50			
DAASI International	2000	DE Tubingen	11-50	EU		
Daon		IE Fairfax	201-500	EU NA APAC		
DERMALOG Identification	1995	DE Hamburg	201-500	EU APAC		
Detack Group	2001	DE Ludwigsburg	11-50	EU NA APAC		
Device Authority	2014	GB Reading	11-50	EU NA		
deviceTRUST GmbH	2016	DE Darmstadt	11-50	EU		
DEVITY	2021	DE Paderborn		EU		
DigiFlak	2013	EE Tallinn	11-50	EU		
Digital Fingerprints	2017	PL Katowice	11-50	EU		
Digitalberry	2014	FR Issy-les-Moulineaux	11-50	EU		
DOCAPOSTE	2007	FR Ivry-sur-Seine	5,001 10,000	EU		
Egonym	2021	CH Zurich	2-10	EU		
eID Easy	2014	EE Tallinn	2-10	EU		
Elimity	2017	BE Mechelen	11-50	EU		
Engity	2022	DE Munich	11-50	EU		
EVERTRUST	2017	FR Paris	11-50	EU		
Evolveum	2011	SK Bratislava	11-50	EU		



IDENTITY AND ACCESS MANAGEMENT (IAM) (4/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Excalibur	2016	SK Poprad	11-50	EU				●	●								●			●		
ExcID		GR Athens	2-10	EU						●		●					●					
Fidentity Visitor Management		CH Fayetteville	11-50	NA									●				●					
filancore	2019	DE Limburgerhof	11-50	EU						●		●					●			●		
Fudo Security Polska	2012	PL Warsaw		EU						●						●	●		●	●	●	
Futurae Technologies	2016	CH Zurich	51-200	EU												●	●				●	
Gataca	2018	ES Madrid		EU NA						●			●			●	●			●		
Giesecke+Devrient	1852	DE Munich	10,001+	EU						●		●					●					
Gimly	2021	NL Amsterdam	2-10	EU													●					
Global ID SA @ EPFL	2016	CH Lausanne	2-10	EU										●			●					
heylogin	2020	DE Braunschweig	11-50	EU				●	●								●					
HIAsecure	2017	FR Neuilly-sur-Seine	2-10	EU								●					●					
HSB identification		NL Woerden	11-50	EU											●		●					
HTS Hi-Tech Services	2013	IT Udine	11-50	EU								●					●				●	●
ID Control	2005	NL The Hague	11-50	EU				●					●				●				●	
ID Security	2008	CH Rapperswil	11-50	EU						●		●		●			●					
IDAKTO	2019	FR Paris	51-200	EU						●			●				●					
Identeco	2020	DE Bonn	2-10	EU						●							●				●	
IDENTT		PL Wroclaw	11-50	EU			●		●							●	●					
IDEX Biometrics		NO Oslo	51-200	EU NA										●			●			●		
IDlayr	2020	GB London	11-50	EU											●		●				●	
IDnow	2014	DE Munich	501 1,000	EU			●									●	●					

IDENTITY AND ACCESS MANAGEMENT (IAM) (5/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
IDtech	1985	BE Belgium	11-50	EU					●						●		●					
Idura	2013	DK Copenhagen	11-50	EU								●					●			●		
ILEX-International	1970	FR Clichy	10,001+	EU					●								●					
Impierce Technologies	2022	NL Houten	2-10	EU						●		●					●					
IN Groupe	1538	FR Paris	1,001 5,000	EU						●		●					●					
Infraray GmbH	1998	DE Berlin	11-50	EU											●		●	●				●
INTALIO Open Source	2011	PL Poznan	11-50	EU													●					
Inverid	2013	NL Enschede	51-200	EU												●	●					
inWebo Group	2021	FR Paris	51-200	EU						●							●					
iProov		GB London	51-200	EU NA APAC													●					
Iriscan	2019	EE Tallinn	2-10	EU													●					
Ironchip	2017	ES Barakaldo	11-50	EU									●				●				●	
ISARS	2017	FR Poigny-la-Forêt	2-10	EU								●					●					●
KeoPass		FR Vannes	2-10	EU								●					●					
Keyless	2019	GB London	51-200	EU APAC													●					
KeyTalk	2004	NL Amersfoort	11-50	EU								●					●			●		
KIWI.KI GmbH	2012	DE Berlin		EU											●		●	●				
KOBIL	1986	DE Worms	201-500	EU NA												●	●			●		
Lab A Part	2015	GB Cambridge	2-10	EU				●				●					●					
Labyrinth Cyber	2021	GB London	11-50	EU													●					
Leonardo	1948	IT Rome	10,001+	EU NA APAC													●	●		●	●	
LINAGORA	2000	FR Issy-les-Moulineaux	201-500	EU NA													●					

IDENTITY AND ACCESS MANAGEMENT (IAM) (6/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
LockSelf	2014	FR Asnières-sur-Seine	51-200	EU													●					
LuxTrust S.A.	2005	LU Capellen	51-200	EU								●					●			●		
MaskTech GmbH	2002	DE Nuremberg	11-50	EU								●					●			●		
MayBind	2025		2-10				●										●					
MAYI ID	2024		51-200														●					
Memority	2018	FR Tallinn	11-50	EU						●		●					●					
Memority	2023	FR Puteaux	51-200	EU						●		●					●					
MIRACL	2011	GB London	11-50	EU													●					
Multilogin	2015	EE Tallinn	51-200	EU													●					
MultiSense	2015	NL Amsterdam	11-50	EU			●										●				●	
MyCena®	2016	GB London	11-50	EU NA								●	●				●				●	
My-Money biometric	2017	IT Padova	2-10	EU						●						●	●					
Namirial	2000	FR Senigallia	501 1,000	EU								●					●			●		
Nect	2017	DE Hamburg	51-200	EU			●					●					●					
NeoCheck	2017	ES Castellon	2-10	EU												●	●				●	
neomia	2021	FR Sausheim	2-10	EU			●										●					
NEOWAVE	2007	FR Gardanne	2-10	EU								●					●			●		
Nevis Security	2020	CH Zurich	51-200	EU													●					
Nexis	2009	DE Regensburg		EU						●			●				●					
NextDay.Vision SA	2017	CH Courroux	2-10	EU								●					●			●		
Nexus IN Groupe	1984	SE Stockholm	201-500	EU APAC						●		●					●				●	
NordPass	2019	NL Netherlands	201-500	EU								●					●				●	

IDENTITY AND ACCESS MANAGEMENT (IAM) (7/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
Notarify	2018	IT Milan	11-50	EU APAC		Identity and Access Management (IAM)
Omada	2000	DK Copenhagen	201-500	EU NA		Identity and Access Management (IAM)
oneIDentity+		DE Ismaning	2-10	EU		Identity and Access Management (IAM)
OneVisage	2016	CH Lausanne	2-10	EU		Identity and Access Management (IAM)
OneWave	2016	FR Rennes	11-50	EU		Identity and Access Management (IAM)
OneWelcome		NL Amersfoort	51-200	EU		Identity and Access Management (IAM)
OOTENTIK	2022	FR Les Milles	1	EU		Identity and Access Management (IAM)
Open Sezam	2022	FR Puteaux	2-10	EU		AI Security and Integrity; Secure Communication Platforms
Oribi MobileID	2016	NL Oisterwijk	2-10	EU		Awareness & Training Platforms; Vulnerability Assessment Platforms
passbolt		LU Luxembourg	11-50	EU		Cloud & Data Protection; Cryptography
Password Crypt	2016	DK Naestved	2-10	EU		Identity and Access Management (IAM)
PayByFace	2018	NL Bucharest	11-50	EU		Fraud Prevention and Detection; Secure Communication Platforms
perc.pass			2-10			Identity and Access Management (IAM)
Pointsharp	2006	SE Stockholm	51-200	EU		Identity and Access Management (IAM)
Pointsharp Germany	2006	DE Freiburg	51-200	EU		Cryptography; Cyber Governance
Precise Biometrics	1997	SE Lund	51-200	EU NA		Awareness & Training Platforms; Endpoint Security; Threat Management
Privately SA	2014	CH Lausanne	2-10	EU		AI Security and Integrity; Awareness & Training Platforms; Threat Management
Privy		US New York	11-50	NA		Cloud & Data Protection; Cryptography
Procivis	2008	CH Kielce	2-10	EU		Identity and Access Management (IAM)
ProID		CZ Zlin-Stipa	201-500	EU		Cloud & Data Protection; Cryptography
PSYND	2012	CH Geneva	2-10	EU		Identity and Access Management (IAM)
PXL Vision	2017	CH Zurich	51-200	EU		Identity and Access Management (IAM)
Radiant Logic		FR San Rafael	51-200	NA		Identity and Access Management (IAM)

IDENTITY AND ACCESS MANAGEMENT (IAM) (8/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
RCDevs Security		LU Esch	11-50	EU			○	○	○	●	○	●	○	○	○	○	●	○	○	●	○	○
ReachFive	2014	FR Paris	11-50	EU			○	○	○	●	○	○	●	○	○	○	●	○	○	○	○	○
reBop	2020	FR Paris	2-10	EU			○	○	●	●	○	●	○	○	○	○	●	○	○	○	○	○
Reemo	2021	FR Paris	11-50	EU			○	○	○	○	○	○	○	○	●	○	●	○	○	○	●	○
Relock		US Austin	2-10	NA			○	○	○	○	○	●	○	○	○	○	●	○	○	○	○	○
Riptides	2025	HU Budapest	2-10	EU			○	○	○	○	○	●	○	○	○	○	●	●	○	○	○	○
Rublon	2011	PL Zielona Gora	11-50	EU			○	○	○	○	○	○	○	○	●	○	●	●	○	○	○	○
Rubycat		FR Cesson-Sévigné	11-50	EU			○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	●
SailPoint	2005	GB Austin	1,001 5,000	EU NA APAC			○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Sala Secure Oy	2024	CH Jyvaskyla	2-10	EU			○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○
Sandgrain	2021	NL Eindhoven	2-10	EU			○	○	○	●	○	○	○	○	○	○	●	○	○	○	○	●
Saporo	2021	CH Lausanne	11-50	EU NA			○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	●
Secfense	2018	PL San Fran.	11-50	EU NA			○	○	○	○	○	○	○	○	●	○	●	○	○	○	●	○
secunet Security Networks AG	1997	DE Essen	1,001 5,000	EU			○	○	○	●	○	●	○	○	○	○	●	●	○	●	○	○
Securivy	2020	PL Poznan	11-50	EU			○	○	○	○	○	○	○	○	○	○	●	●	○	○	●	○
Sedicii	2013	IE Waterford	11-50	EU			○	○	○	○	○	●	○	○	○	○	●	○	○	○	●	○
ShareID	2020	FR Paris	11-50	EU NA			○	○	●	○	○	○	○	○	○	○	●	○	○	○	●	○
Signicat	2006	NO Trondheim	501 1,000	EU			○	○	○	○	○	○	●	○	○	●	●	○	○	○	○	○
signotec GmbH	2000	DE Ratingen	11-50	EU			○	○	○	○	○	●	○	○	○	○	●	○	○	●	○	○
SIVIS GmbH		DK Karlsruhe	11-50	EU			○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Skribble	2018	CH Zurich	51-200	EU			○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
SMS PASSCODE	2005	DK Brondby	11-50	EU NA			○	○	○	●	○	○	○	○	○	○	●	○	○	○	●	○
SonicBee	2020	NL Utrecht	11-50	EU			○	○	○	●	○	○	●	○	○	○	●	○	○	○	○	○

IDENTITY AND ACCESS MANAGEMENT (IAM) (9/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
Specops Software	2001	SE Stockholm	51-200	EU NA		AWARENESS & TRAINING PLATFORMS; IDENTITY AND ACCESS MANAGEMENT (IAM); SECURE COMMUNICATION PLATFORMS
SSH Communications	1995	FI Helsinki	51-200	EU NA APAC		IDENTITY AND ACCESS MANAGEMENT (IAM)
swIDch Ltd	2018	GB London	11-50	EU		EMAIL SECURITY; IDENTITY AND ACCESS MANAGEMENT (IAM); OT SECURITY
SwissSign AG	2001	CH Glattbrugg	51-200	EU		IDENTITY AND ACCESS MANAGEMENT (IAM)
Systancia	1998	FR Sausheim	51-200	EU		IDENTITY AND ACCESS MANAGEMENT (IAM); NETWORK SECURITY; OT SECURITY
Syteca		US Waltham	51-200	NA		AWARENESS & TRAINING PLATFORMS; IDENTITY AND ACCESS MANAGEMENT (IAM); SECURE COMMUNICATION PLATFORMS
Tekalis	2019	FR Rennes	2-10	EU		CLOUD & DATA PROTECTION; CRYPTOGRAPHY; CYBER GOVERNANCE; IDENTITY AND ACCESS MANAGEMENT (IAM)
tenfold Software		US New York	11-50	EU NA		IDENTITY AND ACCESS MANAGEMENT (IAM)
Topicus KeyHub	2014	NL Deventer	1,001 5,000	EU		IDENTITY AND ACCESS MANAGEMENT (IAM)
Transmitio	2014	FR Bordeaux	2-10	EU		CLOUD & DATA PROTECTION; CYBER GOVERNANCE; IDENTITY AND ACCESS MANAGEMENT (IAM)
Trust Stamp	2015	US Atlanta	51-200	EU NA		IDENTITY AND ACCESS MANAGEMENT (IAM)
TrustBuilder	2010	FR Paris	51-200	EU		FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM)
Trusted Accounts	2022	AT Dornbirn	2-10	EU		AWARENESS & TRAINING PLATFORMS; FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM)
TrustSEC	2016	PL Szczecin		EU		AI SECURITY AND INTEGRITY; APPLICATION SECURITY; CLOUD & DATA PROTECTION; CRYPTOGRAPHY; CYBER GOVERNANCE; IDENTITY AND ACCESS MANAGEMENT (IAM); SECURE COMMUNICATION PLATFORMS
ubiqu	2010	NL Delft	11-50	EU		CLOUD & DATA PROTECTION; CRYPTOGRAPHY; IDENTITY AND ACCESS MANAGEMENT (IAM)
Ubisecure	2002	GB London	51-200	EU		CYBER GOVERNANCE; FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM)
Unosecur	2021	DE Berlin	11-50	EU		CLOUD & DATA PROTECTION; IDENTITY AND ACCESS MANAGEMENT (IAM); SECURE COMMUNICATION PLATFORMS
Vaulteq	2015	NL Amsterdam	2-10	EU		CLOUD & DATA PROTECTION; IDENTITY AND ACCESS MANAGEMENT (IAM)
Vaultys	2022	FR Haguenau	2-10	EU		IDENTITY AND ACCESS MANAGEMENT (IAM)
Veintree SAS	2017	CH Fillinges	2-10	EU		CLOUD & DATA PROTECTION; CRYPTOGRAPHY; IDENTITY AND ACCESS MANAGEMENT (IAM)
Vereign AG	2017	CH Zug	11-50	EU		CRYPTOGRAPHY; EMAIL SECURITY; IDENTITY AND ACCESS MANAGEMENT (IAM); SECURE COMMUNICATION PLATFORMS
Veridos	2015	DE Berlin	501 1,000	EU NA		CRYPTOGRAPHY; IDENTITY AND ACCESS MANAGEMENT (IAM)
Veriff	2015	EE New York	201-500	EU NA		AI SECURITY AND INTEGRITY; FRAUD PREVENTION AND DETECTION; IDENTITY AND ACCESS MANAGEMENT (IAM)

IDENTITY AND ACCESS MANAGEMENT (IAM) (10/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage
Verimi	2017	DE Berlin	51-200	EU	
Virtual Vaults	2014	FR Rotterdam	51-200	EU	
WALLIX Group	2003	FR Paris	201-500	EU NA	
WebID		DE Berlin	201-500	EU	
Wecan	2015	CH Geneva	201-500	EU	
WISeKey SA	1999	CH Geneva	51-200	EU	
XignSys GmbH	2016	DE Gelsenkirchen	11-50	EU	
Xolphin B.V.	2002	NL Alkmaar	11-50	EU	
Ydentic	2016	NL Zwolle	11-50	EU	
Yneuro	2019	FR Paris	2-10	EU	
Yorba	2022	PT Lisbon	2-10	EU NA	
Yoti	2014	GB London	201-500	EU	
YourID Foundation	2019	NL Amsterdam	2–10	EU	
Yousign	2013	FR Paris	51-200	EU	
Youverse		PT Lisbon	11-50	EU	
Yubico	2007	SE Stockholm	201-500	EU NA	
zally®	2022	GB Manchester	11-50	EU	
Zamna	2016	GB London	11-50	EU	
ZealiD	2014	SE Stockholm	11-50	EU	
ZenyWay	2015	FR Paris	2-10	EU	
ZEPCAM	2009	NL Zaltbommel	11-50	EU	
ZITADEL	2020	CH San Fran.	11-50	EU NA	
ZYNYO	2016	NL Hengelo	11-50	EU	

Interview

PAC

In the general context of the software and IT services markets, the cybersecurity segment occupies a strategic and essential place.

For nearly 50 years, PAC has established itself as a leading strategy and marketing specialist for players in the digital, IT services and software sectors. Its European coverage is virtually complete in terms of analysis, and its network of subsidiaries (France, Germany, UK, Romania) and partners (Italy, Spain, Northern Europe, etc.) enables it to provide dedicated services in most of the markets it covers.

PAC's DNA is very similar to that of ECA: a culture deeply rooted in Europe: respecting the diversity of countries, methodologies adapted to European specificities, prestigious references among major European groups, but also numerous SMEs and mid-cap companies in their ecosystems. It also shares a desire to contribute to the emergence of European champions, which has been achieved in the IT Services sector with Capgemini, Atos, T-Systems, etc., which are among or close to the top 10 worldwide.

In the general context of the software and IT services markets, the cybersecurity segment occupies a strategic and essential place. Along with artificial intelligence and data analytics, it is also a very dynamic sector, characterized by the creation of numerous companies, start-ups, scale-ups, etc., alongside global leaders, most of which originate from the North American market.

The emergence of European leaders in these fields is a key factor, not only for the future of the software/IT services industry, but also for ensuring the sovereignty of European businesses and administrations. This is why the "Cyber mapping" initiative, successfully launched by ECA a few years ago, is important and should serve as a basis for action plans supporting an independent strategy for our continent.

According to PAC, the European software and IT services market related to cybersecurity will be worth almost €45 billion in 2025, representing more than 10% of a total market estimated at nearly €400 billion. By 2029, European cybersecurity could reach €65 billion, with average annual growth of 10%, which is 5 to 8 points above IT spending growth, and then will represent more than 13% of the total market.

What will be the drivers of this very dynamic growth?

They will be of various kinds:

Demand from large users will remain strong, but the main driver will be small and medium-sized enterprises, which have been relatively inactive until now but are becoming increasingly aware of the risks involved and the need for reliable solutions. At the same time, outsourcing to specialised external players will grow. Many user companies will be less and less able to handle increasingly sophisticated applications and tools on their own.

A host of new regulations from the European Union and local governments will force customers and suppliers to increase their investments or migrate from existing solutions. These include, in particular the NIS2 directives, the DORA law and the Cyber Resilience Act (CRA). Most of these regulations have a significant impact on applications, infrastructures and information systems governance.

This will result in a boom in this market segment over the next few years, with repositioning, new opportunities, etc. In this context, it is important that the many European companies involved in cybersecurity markets seek to reach critical thresholds by relying on powerful investors, contributing to mergers, moving towards successful partnerships and innovating.

We are convinced that the existence of this ECA mapping will contribute to raising awareness and bringing about positive developments for European cybersecurity activities.

Pierre Audoin Consultants (PAC) was born out of a vision – entrepreneur Pierre Audoin's vision of a market research and consulting firm that would help businesses navigate the ever-changing technology landscape. Since its inception in 1976 in Paris, PAC has grown to become a trusted source of market intelligence and strategic guidance in the IT sector.

pacanalyst.com

Daniella CAMPBELL
CEO
PAC GROUP

Jean-François PERRET
Associate Director
PAC GROUP

European Cybersecurity Mapping 2026

FRAUD PREVENTION AND DETECTION

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Fraud has escalated from a nuisance to an industry, often leveraging AI to generate fake identities and communications. Prevention must also be industrialized. These tools detect, prevent, and respond to fraudulent activities using advanced behavioral analytics and machine learning techniques.

Why Choose European Technology: European providers offer fraud detection solutions tailored to EU-specific challenges and regulations. Their localized expertise enhances both trust and compliance, allowing businesses to securely handle sensitive financial and personal data.

Importance for European sovereignty: 6/10

Although critical for financial security, its sovereignty impact is relatively low compared to infrastructure-focused categories. European solutions are still important for trust and compliance.

Protection for businesses, government organizations, and consumers

kuppingercole ANALYSTS

MARKET CONTEXT

Fraud impacts individuals and practically every type and size of organization, from for-profit businesses to non-profits to government agencies. Digital fraud takes many forms, including Account Takeover (ATO), New Account Fraud (NAF), financial scams, policy abuse, and bot-perpetrated automated fraud and abuse as examples. The European Banking Authority (EBA) stated in their Consumer Trends Report 2024/25 that "Payment fraud is still the most significant issue... such as 'Authorised Push Payment' (APP) fraud, where the payer is manipulated into making a payment to the fraudster."

The European Union (EU) revised Payment Service Directive (PSD2) mandated Strong Customer Authentication (SCA) when it took effect, and that has helped to reduce ATOs, but "the EBA observed that... fraudsters managed to adapt their techniques, giving rise to fraud types of a more complex nature, in particular leveraging social engineering."

Fraud Reduction Intelligence Platforms (FRIPs) are technical solutions that consume multiple intelligence feeds and risk signals and assess the likelihood that a particular transaction may be fraudulent in real-time.

EUROPEAN COMPETITIVE ADVANTAGES

FRIP solutions offered by European vendors adhere to GDPR and PSD2 and are working toward PSD3. Many FRIP solution providers from outside these regions have also largely complied with these regulations, but European vendors, in some instances, have taken more care to protect personal information embedded in risk signals. Several FRIP specialists operate across the EU, in countries such as Cyprus, Czechia, Finland, France, Hungary, Italy, Ireland, and Portugal.

TECHNOLOGY EVOLUTION & TRENDS

Most FRIP solutions are cloud-based Software-as-a-Service (SaaS) systems, accessed via Application Programming Interfaces (APIs). FRIP solutions are composed of six technical capabilities: Identity Verification (IDV), compromised credential intelligence, device intelligence, user behavioral analysis (UBA), behavioral biometrics, and bot detection/management. The first five of these functions require the processing of what is considered personal information in multiple jurisdictions; thus, great care must be taken to adhere to GDPR.

MARKET DYNAMICS

The FRIP market is mature. There are 25+ vendors operating in both the FRIP for finance and eCommerce spaces. This market is dominated by credit bureaus and IAM service providers. The smaller specialists in the field generally offer competitive advantages by providing more specific functions. Examples are those that provide more rigorous IDV, behavioral biometrics, or bot detection. Organizations in other sectors, such as technology, eCommerce, or government, by default select FRIP specialist firms with experience in their verticals.

FUTURE

It is imperative for FRIP vendors to keep current on fraudster tactics, especially those that are focused on specific industries. Financial scams outpaced ATO attacks in 2024, and FRIP providers have pivoted to be better able to detect and interdict scams as they happen.

Outside of finance, FRIP solution providers must focus on escalating bot attacks, distinguishing human users from AI agents, and evaluating agentic AI behavior. Moreover, as fraudsters increasingly abuse guest checkout, return, and review/comment policies, these FRIP solutions must adapt to the new attack vectors.

European FRIP vendors will continue to have opportunities to distinguish themselves from external competitors by promoting GDPR and PSD2 adherence and integrating with regional Identity Providers (IdPs) and supporting electronic IDentification, Authentication, and trust Services (eIDAS).

For investors that want to elevate and support EU-based FRIP services, there are many smaller companies in this space spread around Europe.

John TOLBERT
Director of Cybersecurity Research
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Fraud Reduction Intelligence Platforms – eCommerce

Leadership Compass: Fraud Reduction Intelligence Platforms - Finance

FRAUD PREVENTION & DETECTION (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Acoru		ES Madrid	11-50	EU			●									●					●	
Acuminor	2018	SE Stockholm	11-50	EU												●						
Adresta AG	2019	CH Zurich	2-10	EU												●						
AdvanThink (ISoft)	1990	FR Saint-Aubin	51-200	EU			●									●						
Andrupos BV	2016	NL The Hague	2-10	EU				●								●					●	
Authena	2018	CH Zug	11-50	EU												●						
Behavox	2014	GB London	201-500	EU NA APAC					●							●					●	
Bleckwen	2017	FR Paris	11-50	EU			●									●						
BusinessForensics		NL The Hague	11-50	EU												●					●	●
Cambridge Intelligence	2011	GB Cambridge	51-200	EU NA												●	●				●	
CAV Solutions	2020	EE Nomme	2-10	EU NA												●						
Cleafy	2014	IT Milan	51-200	EU			●									●					●	
Clearspeed	2016	GB San Diego	51-200	NA					●							●					●	
CoDe_RTD	2020	IT Turin	2-10	EU			●									●						
Cursor Insight		GB London	11-50	EU												●	●					
Cybertonica Ltd	2015	GB London	11-50	EU			●									●	●				●	
cyex	2018	EE Tallinn	2-10	EU			●		●							●					●	
Dark Entry	2022	NL Amsterdam	11-50	EU												●					●	●
DecisionRules.io	2020	US Wilmington	51-200	NA EU			●									●						
DeepView	2018	GB Bishops Cleeve	2-10	EU					●	●						●						
Doppel	2022	US Covina	51-200	NA					●					●		●					●	
EBRAND	2006	LU Leudelange	201-500	EU NA												●					●	●

FRAUD PREVENTION & DETECTION (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Elliptic	2013	GB London	51-200	EU NA APAC			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○
ENAI	1946	NL Capelle	11-50	EU			○	○	●	○	○	○	○	○	○	●	○	●	○	○	●	○
Evina	2018	FR Paris	51-200	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Factology.Systems	2019	EE Tallinn	2-10	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Feedzai	2011	PT Lisbon	501-1,000	EU NA APAC			●	○	○	○	○	○	○	○	○	●	●	○	○	○	●	○
ForenSwiss	2024		2-10				●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
fraud0.com	2020	DE Munich	11-50	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
FraudBuster	2010	FR Vélizy-Villacoublay	11-50	EU			○	○	○	○	○	○	○	○	○	●	○	●	○	○	●	○
Fraudio	2019	NL Amsterdam	11-50	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
FraudShield Security	2023	HU Budapest	2-10	EU			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○
Integritee	2021	CH Zurich	11-50	EU			○	○	○	●	○	●	○	○	○	●	○	○	○	●	○	○
LastingAsset		GB Edinburgh	2-10	EU			○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○
Mavin	2020	NL The Hague	2-10	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Meelo		FR Marcq-En-Baroeul	11-50	EU			●	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○
Nefture	2022	FR Paris	2-10	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	●
Netcraft	1994	GB London	201-500	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	●
Newgen Payments	2015	NL Amsterdam	11-50	EU APAC			○	○	○	●	○	○	○	○	○	●	●	○	○	○	○	○
Ondato	2018	GB London	51-200	EU			○	○	○	○	○	○	○	○	○	●	●	○	○	○	●	○
Ondorse	2021	FR Paris	11-50	EU			○	○	○	○	○	○	●	○	○	●	●	○	○	○	○	○
Palturai	2014	DE Hofheim	51-200	EU			○	○	○	○	○	○	●	○	○	●	○	●	○	○	○	○
Prooftag®	2004	FR Montauban	11-50	EU NA			○	○	○	○	○	○	○	○	○	●	○	○	○	●	●	●
qKey	2009	NL Delft	11-50	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○

FRAUD PREVENTION & DETECTION (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Ripjar	2013	GB Cheltenham	51-200	EU			○	○	○	○	○	○	○	○	○	●	●	○	○	○	●	○
Scantrust	2014	CH Lausanne	11-50	EU			○	○	○	●	○	○	○	○	○	●	●	○	○	○	○	○
Securely	2019	NL Eindhoven	2-10	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
Sensity	2018	NL Amsterdam	11-50	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
SICPA	1927	CH Lausanne	1,001 5,000	EU NA APAC			○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
Sis ID	2016	FR Lyon	51-200	EU			○	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○
Smart Protection	2015	ES Madrid	51-200	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
summitto	2017	NL Amsterdam	2-10	EU			○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○
Sumsub	2015	CY Limassol		EU NA APAC			○	○	○	○	○	○	○	○	○	●	●	○	○	○	●	○
SurePay	2016	NL Utrecht	51-200	EU			○	○	○	●	○	○	○	○	○	●	○	○	○	○	●	○
Sygno		NL Leusden	11-50	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
ThreatFabric	2015	NL Amsterdam	51-200	EU NA			○	○	○	○	○	○	○	○	●	●	○	○	○	○	●	○
T-Mining	2016	BE Antwerpen	11-50	EU APAC			○	○	○	○	○	●	○	○	○	●	●	○	○	●	○	○
Travatar.ai	2020	PL Pulawy	2-10	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
TrueScreen	2022	IT Bologna	11-50	EU			○	○	○	○	○	●	○	●	○	●	○	○	○	○	○	○
Trustpair	2017	FR Paris	51-200	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	○	●
UrbanFox	2015	IE Dublin	2-10	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Vespia		EE Tallinn	2-10	EU			○	○	○	○	○	○	○	○	○	●	●	○	○	○	●	○
Vestigit	2018	PL Wroclaw	11-50	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Vistalworks OÜ	2019	NL Glasgow	2-10	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	●
Vyntra Global		CH Yverdon	51-200	EU			●	○	○	○	○	○	○	○	○	●	○	○	○	○	●	○
Wakweli		CH Geneva	11-50	EU			○	○	○	●	○	●	○	○	○	●	○	○	○	○	○	○

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

European Cybersecurity Mapping 2026

NETWORK SECURITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Networks are constantly exposed to unauthorized access, attacks, and breaches. This challenge is magnified by the development of new protocols and the expanding network footprint, particularly with the growth of connected industry and critical systems. Network security systems detect anomalies and suspicious activities to enable a rapid response before a compromise can occur.

Why Choose European Technology: European network security providers guarantee the operational continuity and resilience of key infrastructures, while considering EU-specific threat landscapes. Their localized expertise and alignment with regional regulations ensure secure and sovereign network operations.

Importance for European sovereignty: 10/10

Networks form the backbone of digital infrastructure. Securing them with European technologies is crucial to maintaining control over critical communications and data flows.

Network-Centric Detection and Response for Modern Threats

kuppingercole ANALYSTS

MARKET CONTEXT

For years, organizations have relied on legacy firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to protect their networks. However, these tools are often labor-intensive to manage and prone to generating too many false positives. Many organizations now also require additional visibility at the network layer. Network Detection and Response (NDR) has emerged as the next generation of network security, using ML to monitor traffic patterns, metadata, and device communications. This enables teams to detect sophisticated threats, such as DNS tunneling, data exfiltration, and zero-day exploits, that evade traditional tools. Today, NDR is often integrated into broader XDR suites to provide a comprehensive view of the threat landscape across network, cloud, and identity layers.

EUROPE'S COMPETITIVE ADVANTAGE

Due to Europe's stringent regulatory framework, including NIS2, DORA, and GDPR, European network security vendors will likely differentiate themselves through privacy-preserving analytics and industry specialization. European vendors must build native reporting and governance capabilities into their NDR/XDR platforms. AI can detect threats from metadata without decrypting the payload. This enables vendors to protect highly sensitive networks in the healthcare and banking sectors without violating privacy rights or creating pools of decrypted data. Additionally, the push for cloud sovereignty in Europe is a significant factor that is causing European organizations, especially government entities, to choose local providers over non-European vendors.

TECHNOLOGY EVOLUTION & TRENDS

AI- and ML-driven security is becoming mainstream. It enables faster threat detection and automated responses against sophisticated attacks. One major trend is using ML to improve anomaly detection at the network level. Modern NDR solutions include encrypted traffic analysis (ETA), a capability that identifies threats within encrypted data without the need for full decryption. Some innovative vendors offer sensor less solutions that provide effective monitoring capabilities without deploying physical agents.

MARKET DYNAMICS

As enterprises realize that traditional tools such as EDR and SIEM cannot sufficiently secure modern network layers, sophisticated threats are pushing them to invest in more sophisticated network-level defense solutions. Market growth is driven by the shift to hybrid and multi-cloud environments, as well as the expanded network attack surface created by 5G and IoT devices. Despite the high demand, the market faces challenges such as high implementation costs, deployment complexity, and the need for specialized expertise.

These factors, alongside privacy concerns, can pose significant barriers for smaller organizations. NDR remains the best option for SMBs that want to directly monitor their network traffic, as broader XDR is often too costly to implement. Large enterprises should instead consider XDR solutions for their ability to correlate telemetry across multiple security domains, such as endpoint, cloud, network, and identity, to provide a unified defense against sophisticated, multi-vector attacks.

FUTURE

As encryption becomes even more pervasive, traditional deep packet inspection will become less effective. This will force NDR to invest more in ETA, behavioral modeling, and alternative telemetry sources instead of relying on payload visibility. Consistent cross-domain visibility and analytics will be a key differentiator for future network security platforms due to heterogeneous network infrastructure, including on-premises, multi-cloud, OT, IoT, and 5G. XDR platforms depend on NDR-grade network analytics to detect lateral movement and attacker behavior.

Meanwhile, NDR vendors are expanding their telemetry coverage and response integrations to remain relevant within broader security ecosystems. AI leverages basic anomaly detection for large-scale correlation, forensics support, and semi-automated responses, thus accelerating SOC workflows and analyst decision-making. Future network security solutions will be more XDR-aligned, analytics-driven, and automation-centric.

ABOUT THE AUTHOR

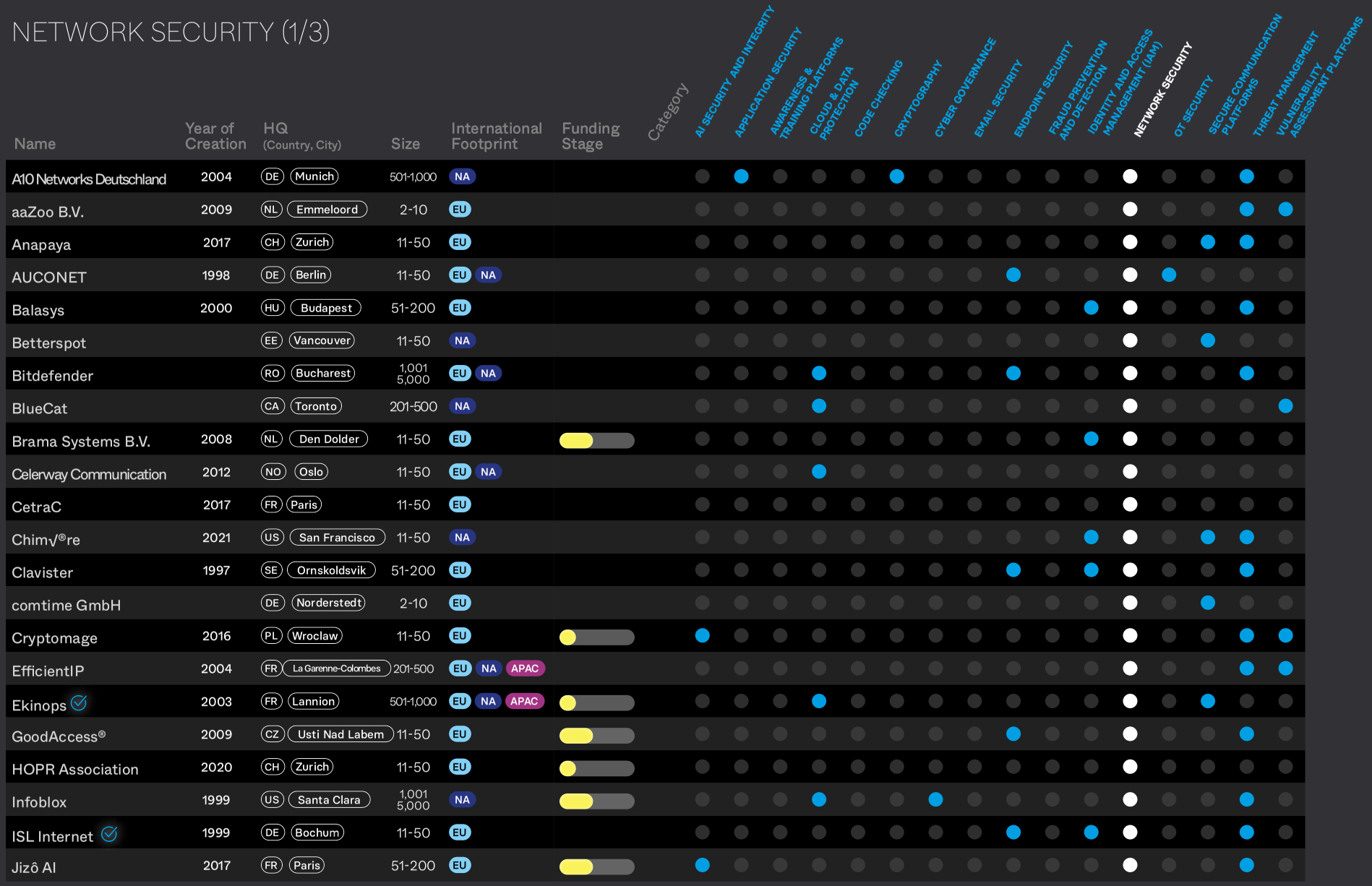
Osman Celik is a Research Analyst at KuppingerCole Analysts AG with expertise in ASM, Brand Protection, Web Application and API Protection (WAAP), NDR, and XDR.

Osman CELIK
Research Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Network Detection and Response
Leadership Compass: eXtended Detection and Response
Buyer's Compass: Network Detection and Response
Buyer's Compass: eXtended Detection and Response

NETWORK SECURITY (1/3)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
A10 Networks Deutschland	2004	DE Munich	501-1,000	NA				●				●						●			●	
aaZoo B.V.	2009	NL Emmeloord	2-10	EU														●			●	●
Anapaya	2017	CH Zurich	11-50	EU														●		●	●	
AUCONET	1998	DE Berlin	11-50	EU NA										●				●	●			
Balasys	2000	HU Budapest	51-200	EU												●		●			●	
Betterspot		EE Vancouver	11-50	NA														●		●		
Bitdefender		RO Bucharest	1,001 5,000	EU NA					●					●				●			●	
BlueCat		CA Toronto	201-500	NA					●									●				●
Brama Systems B.V.	2008	NL Den Dolder	11-50	EU												●		●				
Celerway Communication	2012	NO Oslo	11-50	EU NA					●									●				
CetraC	2017	FR Paris	11-50	EU														●				
Chim√®re	2021	US San Francisco	11-50	NA												●		●		●	●	
Clavister	1997	SE Ornskoldsvik	51-200	EU										●		●		●			●	
comtime GmbH		DE Norderstedt	2-10	EU														●		●		
Cryptomage	2016	PL Wroclaw	11-50	EU			●											●			●	●
EfficientIP	2004	FR La Garenne-Colombes	201-500	EU NA APAC														●			●	●
Ekinops	2003	FR Lannion	501-1,000	EU NA APAC					●									●		●		
GoodAccess®	2009	CZ Usti Nad Labem	11-50	EU										●				●			●	
HOPR Association	2020	CH Zurich	11-50	EU														●				
Infoblox	1999	US Santa Clara	1,001 5,000	NA					●				●					●			●	
ISL Internet	1999	DE Bochum	11-50	EU										●		●		●			●	
Jizô AI	2017	FR Paris	51-200	EU			●											●			●	

NETWORK SECURITY (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Keezel	2015	NL Amsterdam	2-10	EU NA			●					●						○			●	
LANCOM Systems	2002	DE Wurselen	201-500	EU						●								○				
Link11 GmbH		DE Frankfurt	51-200	EU NA			●											○			●	
LORIOT	2015	CH Langnau Am Albis	11-50	EU						●								○		●		
Missing-Link Oy	2015	FI Tampere	2-10	EU						●								○			●	
Morphean SA	2009	CH Fribourg	11-50	EU						●								○			●	
NACVIEW	2012	PL Poznan	11-50	EU										●		●		○			●	
Napatech	2003	DK Soeborg	51-200	EU NA						●								○			●	
NCP engineering GmbH	1986	DE Nuremberg	51-200	EU NA										●				○		●		
NetWitness	1997	NL Boston	1,001 5,000	NA			●							●				○			●	
Nexufend GmbH	2024	AT Brunn Am Gebirge	2-10	EU						●		●						○				
Nord Security		LT Vilnius	1,001 5,000	EU						●		●				●		○			●	
P1 Security	2011	FR Paris	11-50	EU														○				●
P4S	2022	FR Paris	2-10	EU								●						○			●	
Paessler GmbH	1997	DE Nuremberg	201-500	EU														○				
Profitap	1984	NL Eindhoven	11-50	EU						●								○			●	
ProvenRun	2009	FR Paris	11-50	EU														○				
RebelRoam	2015	EE Tallinn	11-50	EU														○				
Securepoint GmbH	1997	DE Luneburg	201-500	EU					●					●	●			○				
SecurityGen	2022	GB London	11-50	EU					●									○			●	●
SensorFu	2017	DE Oulu	2-10	EU														○			●	●
Sentinel	2018	EE Cosmos	11-50									●			●			○		●		

NETWORK SECURITY (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category
SnowHaze		CH Zurich	2-10	EU		
Snowpack	2021	FR Orsay	11-50	EU		
SUNERIS SOLUTION		FR Vélizy-Villacoublay	51-200	EU		
TDT AG	1978	DE Essenbach	11-50	EU		
TheGreenBow	1998	FR Paris	11-50	EU		
Whalebone	2016	CZ Brno	51-200	EU		

AI SECURITY AND INTEGRITY
APPLICATION SECURITY
AWARENESS & TRAINING PLATFORMS
CLOUD & DATA PROTECTION
CODE CHECKING
CRYPTOGRAPHY
CYBER GOVERNANCE
EMAIL SECURITY
ENDPOINT SECURITY
FRAUD PREVENTION AND DETECTION
IDENTITY AND ACCESS MANAGEMENT (IAM)
NETWORK SECURITY
OT SECURITY
SECURE COMMUNICATION PLATFORMS
THREAT MANAGEMENT
VULNERABILITY ASSESSMENT PLATFORMS

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

THE NETHERLANDS ORGANISATION FOR APPLIED SCIENTIFIC RESEARCH (TNO)

THE NATIONAL RESEARCH INSTITUTE FOR MATHEMATICS AND COMPUTER SCIENCE IN THE NETHERLANDS (CWI)

Cryptography is a foundational element of trust in our digital society.

A PRESENT-DAY, SYSTEM-WIDE CHALLENGE

Quantum computing continues to advance towards capabilities that could break much of today's public-key cryptography within the lifecycle of digital systems currently in use. Although large-scale quantum attacks are not yet a reality, the combination of complex migration, long system lifecycles and "harvest-now, decrypt-later" threats make early action essential today.

Regulation further reinforces this urgency. Authorities around the world are moving to phase out algorithms that are vulnerable to quantum attacks. The US National Institute for Standards and Technology (NIST), for instance, plans to deprecate the use of RSA and elliptic curve cryptography by 2035. As a result, postponing post-quantum cryptography (PQC) migration increasingly carries not only security risk but also the risk of non-compliance.

Unfortunately, PQC migration is not a simple algorithm swap. It is a system-wide transformation affecting cryptographic libraries, communication protocols, hardware implementations, embedded devices and operational processes. These technical changes are tightly coupled to complex supply chains and long product lifecycles, exposing dependencies across hardware, software, and vendors that are difficult and costly to resolve later. Legacy systems, in particular, further amplify this challenge.

This has triggered various organizations to act now and not later. The PQC migration has begun, and success will depend on treating PQC not as a standalone cryptographic upgrade, but as a coordinated, ecosystem-level effort requiring long-term planning and cross-industry alignment.

STRATEGIC DEPENDENCIES AND EUROPE'S SOVEREIGNTY

Cryptography is a foundational element of trust in our digital society. It underpins secure communication , data protection and the reliable operation of critical infrastructures. Losing control over cryptographic capabilities creates structural dependencies that can weaken strategic autonomy. This control extends beyond algorithms alone and includes implementations, key management, validation and certification processes.

The PQC migration therefore raises critical questions about Europe's ability to retain control over its cryptographic building blocks. At the same time, it offers an opportunity to strengthen collaboration between European research, industry, and government, while simultaneously enhancing cyber security, innovation capacity, and technological sovereignty. PQC can thus play an important role in shaping the future of Europe's digital security and independence.

A CATALYST FOR EU CYBERSECURITY ECOSYSTEM

While the risk to Europe's autonomy is real, PQC migration also offers a strategic opportunity. European researchers have played a decisive role in the development of global PQC standards. This provides a solid foundation to develop a flourishing European market for PQC-enabled products and services.

However, Europe has long struggled to consistently translate research into scalable, widely deployable, and trusted industrial solutions. This is a challenge that extends well-beyond the area of PQC.

PQC can act as a catalyst to bridge this gap. As a shared, long-term challenge, it offers a unique opportunity to align research institutes, technology providers, manufacturers, governments, and regulators around a common objective. If approached strategically, PQC can drive the strengthening of Europe's cybersecurity market and establish trusted supply chains for cryptographic components.

A FOUNDATIONAL BUILDING BLOCK FOR CYBERSECURITY BY DESIGN

A strong cryptographic foundation should be embedded in the design of digital systems rather than applied as an afterthought. Ideally, it is resilient to future developments, incorporating agile and updatable architectures and using modular and verifiable cryptographic implementations. Newly designed systems can adopt these principles from the start, but many legacy systems were never designed to accommodate cryptographic migrations.

At the same time, the PQC transition presents a unique opportunity to clean up and modernise existing cryptographic infrastructures. Organisations can increase their preparedness not only for quantum-enabled attacks, but also for future cryptanalytic advances or the development of more efficient cryptography. The PQC migration is thus an opportunity to raise the overall level of cyber hygiene, not just swapping cryptographic algorithms.

CONCLUSION

PQC should be treated as a present-day design obligation not a future upgrade. Addressing PQC by design is essential to protect long-term data, ensure system resilience, and safeguard European digital sovereignty.

A coherent approach can transform a disruptive threat into a strategic European advantage. Achieving this will require a strengthened European community that extends beyond cryptographic expertise alone. Initiatives such as the European Conference on PQC Migration help bring together researchers, industry, and government, while resources like the PQC Migration Handbook provide concrete action perspectives.

Thomas ATTEMA
Researcher Cryptology

The Netherlands Organisation for Applied Scientific Research (TNO)

The National Research Institute for Mathematics and Computer Science in the Netherlands (CWI)

ECA MEMBER

Interview

LANCOM SYSTEMS

COMMUNITY CONTRIBUTOR

WHAT IS THE MOST IMPORTANT SIGNAL, TREND, OR RISK YOU ARE CURRENTLY OBSERVING IN YOUR CYBERSECURITY DOMAIN?

The most striking trend we are currently seeing is certainly the growing awareness of existing technological dependencies and the consequences they entail. For example, AI-driven exploitation of vulnerabilities is currently one of the fastest-growing risks. Yet the AI sphere of influence continues to be dominated by global, non-European players. In addition, there is a growing trend toward attacks targeting identities and supply chains, where cyberattacks on non-European suppliers can have significant impact on local businesses. This gives rise to an increased demand for European solutions aimed at making supply chains more resilient.

IN YOUR SPECIFIC FIELD, WHAT DOES EUROPE DO WELL AND WHERE IS IMPROVEMENT URGENTLY NEEDED?

Europe is a hotbed of innovation. This strength is particularly evident in the field of IT security, both in terms of components and devices. Many suppliers offer cutting-edge features and high-quality products. However, the ecosystem remains highly fragmented, and there is a lack of European leaders with a global footprint. This is also due to the disjoined nature of the European market. Furthermore, while the EU's legal framework for cybersecurity is already well advanced, adoption varies across member states, creating a gap in capabilities. This complicates efforts to foster cooperation on joint solutions.

WHAT SINGLE PRIORITY SHOULD EUROPE ADDRESS TO STRENGTHEN ITS POSITION IN YOUR DOMAIN?

To establish itself as a genuine counterweight in the global IT security landscape, Europe must recognize its own strengths and overcome the fragmentation of expertise, technologies, and capabilities. True cyber resilience can only be built collectively. At LANCOM Systems, we collaborate with trusted European partners to build a robust IT security ecosystem. The "European Cybersecurity Mapping" initiative pursues exactly the same goal and serves as an indespensable tool to promote visibility and cohesion within an industry that lies at the heart of Europe's digital resilience and sovereignty.

LANCOM SYSTEMS

LANCOM Systems is a leading European manufacturer of network and security solutions for business and the public sector. The portfolio includes hardware (WAN, LAN, WLAN, firewalls), virtual network components, cloud-based software-defined networking (SDN), and solutions for remote and mobile access.

lancom-systems.com

Robert MALLISON
Co-CEO

LANCOM Systems

European Cybersecurity Mapping 2026

OT SECURITY

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: As industry accelerates global automation and connected manufacturing, a new class of attacks has emerged, targeting disruption of operations or theft of Intellectual Property. Operational Technology (OT) Security systems protect industrial and critical infrastructure including sensors, communication, and data processing from these targeted cyber threats.

Why Choose European Technology: European providers deeply understand the unique requirements of regional industrial environments and ensure compliance with EU safety and security standards. Their expertise is crucial to strengthening Europe's ability to independently secure its critical infrastructure.

Importance for European sovereignty: 10/10

OT Security protects critical infrastructure like energy, transport, and water systems. This category is central to sovereignty, as foreign interference could have catastrophic impacts.

Adapting Industrial Security to Hyperconnected Operations

kuppingercole ANALYSTS

MARKET CONTEXT

Early operational technology adopters were the utilities (such as energy, oil & gas, water & wastewater). It is now a diverse industry sector comprised of agriculture, building management, healthcare, manufacturing, and smart cities, which includes V2X (vehicle-to-anything) and utilities. While in the past OT infrastructure was treated as a separate environment from IT, there are now pressures to move towards a more integrated architecture. Organizations want to ensure that OT infrastructure is managed to the same standards that are imposed on the IT environment and that corporate SOCs have visibility over the OT infrastructure.

There are two trends forcing this integration: Industrial IoT (IIoT) and 5G networks. IIoT utilizes internet technology, encouraging alignment with corporate governance procedures. 5G makes a compelling argument for adoption within OT environments, strengthening the push for integration.

Government regulation is most intensive in the utilities segment, where duty-of-care obligations apply. Controls address both compromise prevention and incident response. In Europe, the NIS2 Directive defines requirements for essential and important industrial sectors, while the Cyber Resilience Act establishes cybersecurity rules for product vendors. IEC 62443 provides a framework for managing technical infrastructure, and Germany's IT-SIG 2.0 sets more prescriptive requirements for public OT environments.

EUROPE'S COMPETITIVE ADVANTAGES

European companies currently hold several advantages. They are home to major OT device suppliers with proven track records. As the US becomes more insular under the current administration, global opportunities exist for European companies to expand their markets.

Europeans also have extensive experience in deploying telecommunications services, developing industry specifications, and integrating private and public 5G services. This positions Europe well to benefit from the transition of telcos from phone services to business support services, where they can supply both the 5G network services needed for OT architectures and the cloud services for OT management.

Europe maintains a distinct advantage in discrete manufacturing. New and refurbished facilities are deploying IIoT devices rather than PLCs and sensor arrays, and private 5G rather than WiFi or Ethernet. Europe's leadership in vehicle manufacturing will also require rapid deployment of smart city infrastructure to support V2X devices.

TECHNOLOGY EVOLUTION AND TRENDS

In legacy OT environments, controllers are separate from sensors and actuators. IIoT devices combine these elements with logic control functions previously provided by PLCs and SCADA systems. An IIoT device can measure temperature or pressure and take action, such as opening or closing a valve, based on pre-programmed instructions. These devices also include integrated communications for management purposes.

5G is having a similarly large effect. It provides fine-grained control over communication links, optimizing them for specific device requirements. Devices communicating small amounts of data periodically no longer require dedicated fixed lines. Network slicing can provide the segmentation that OT environments typically require, supporting the layered architecture defined by the Purdue model.

MARKET DYNAMICS

Demand is growing fastest in manufacturing, healthcare, and smart cities. Manufacturing growth comes from automation and Industry 4.0 initiatives. Healthcare facilities are adopting OT for building management, medical device connectivity, and patient safety systems. Smart cities bring together transport, utilities, and public services on shared infrastructure.

Emerging segments such as V2X, agriculture, and water management represent newer areas for OT adoption. These markets are newer but expanding as sensor costs fall and connectivity improves. The shift from wired to wireless OT networks supports this growth, particularly in environments where cabling is impractical.

FUTURE

New technology is opening an expanding market for IIoT and 5G suppliers. Advances in industrial infrastructure capabilities, combined with lower costs, are creating good opportunities for vendors able to take advantage. IT and OT integration will continue to change how industrial environments operate.

Graham WILLIAMSON
Fellow Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Secure Remote Access for OT/ICS
Leadership Compass: Zero Trust Network Access
Guide: OT, ICS, and SCADA – What Every Cybersecurity Expert Should Know

OT SECURITY (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
4Secure Ltd	2003	GB Northampton	11-50	EU															●	●	●	
Acklio	2016	FR Cesson-Sevigné	11-50	EU								●						●	●	●		
AIoTrust	2023	FR Villeurbanne	2-10	EU															●			
AMDT	2007	DE Landau	201-500	EU NA								●							●		●	●
ANZENA Sp. z o.o.	2012	PL Katowice	11-50	EU															●			
asvin GmbH	2018	DE Stuttgart	11-50	EU								●							●		●	●
Atlantis Cyber Security	2023	NL Haarlem	2-10	EU													●		●		●	●
BaseN	2001	FI Helsinki	51-200	EU NA					●										●		●	
Bertin Technologies	1956	FR Montigny	501-1,000	EU NA										●					●		●	
BifrostConnect	2018	DK Copenhagen	11-50	EU															●			
Busit	2016	FR Nice	11-50	EU															●			
BYSTAMP	2016	FR Vannes	11-50	EU								●					●		●	●		
CLEARSY	2001	FR Aix-en-Provence	51-200	EU															●		●	●
Cognite	2016	US Tempe	501-1,000	EU NA			●				●								●			
Cyberium		FR Paris	2-10	EU															●			
Cybershen	2022	FR Paris	2-10	EU								●		●					●		●	
Cybus	2015	DE Hamburg	51-200	EU					●			●							●			
DTSecLabs	2024	DE Berlin	2-10	EU															●		●	●
emproof	2021	NL Eindhoven	11-50	EU			●				●			●					●		●	
eShard	2015	FR Pessac	11-50	EU APAC			●				●								●			●
Exein	2018	IT Rome	11-50	EU NA			●							●					●		●	●
floLIVE	2015	GB London	51-200	EU					●								●	●	●			
Foundries.io	2017	GB Cambridge	11-50	EU					●					●					●			●

OT SECURITY (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
genua gmbh	1992	DE Kirchheim	201-500	EU									●				●	○	●	●	●	
Hilscher Gesellschaft	1986	DE Hattersheim	201-500	EU NA APAC						●							●	○				
HiveMQ	2012	DE Landshut	51-200	EU														○				
Hudson Cybertec	2012	NL Rijswijk	11-50	EU					●				●					○			●	
ICsec	2018	PL Poznan	11-50	EU													●	○			●	
iExec	2016	FR Lyon	11-50	EU						●		●						○	●			
INCERT GIE	2012	LU Leudelange	51-200	EU						●		●						○				
Infineon Technologies		DE Neubiberg	10,001+	EU NA APAC								●			●		●	○				
IoT.bzh		FR Lorient	11-50	EU														○				
Kentix GmbH	2010	DE Idar-Oberstein	51-200	EU													●	○			●	
Kontron Europe		DE Ismaning	5,001 10,000	EU NA														○				
Kudelski IoT	1951	CH Cheseaux	1,001 5,000	EU														○			●	●
Loctio	2019	GR Aiyaleo	11-50	EU						●		●						○			●	
MetaMind Innovations	2021	GR Kozani	11-50	EU			●											○			●	
Missionware		GR Thessaloniki	2-10	EU														○				
MON5	2022	IT Bologna	2-10	EU								●						○			●	●
NanoLock Security	2017	DE Hod Hasharon	11-50	APAC								●						○			●	●
narrowin	2020	CH Basel	2-10	EU														○				
Nautilus OT	2023	NL Haarlem	2-10	EU			●											○			●	●
ondeso	2010	DE Regensburg	11-50	EU										●				○				●
OneKey	2020	HK Hong Kong	11-50	APAC								●		●			●	○				
OT-Secure B.V.	2024	NL Den Dolder	2-10	EU								●						○				●
P4 Companies	2014	FR Chicago	501-1,000	NA														○				

OT SECURITY (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Parcoor	2019	FR Lyon	2-10	EU			●								●				○		●	
PHYSEC GmbH	2016	DE Bochum	51-200	EU								●							○		●	
Red Alert Labs	2017	FR Alfortville	11-50	EU					●				●						○		●	●
Rhebo OT & IIoT Security	2014	DE Leipzig	11-50	EU														●	○		●	
S2GRUPO		ES Valencia	501-1,000	EU															○			
SANCTUARY	2021	DE Darmstadt	11-50	EU									●						○		●	
Scalys	2017	NL Hengelo	2-10	EU						●					●			●	○	●		
Seckiot	2020	FR Paris	11-50	EU															○		●	●
Seclab	2011	FR Montpellier	11-50	EU														●	○			●
SeedFence			2-10																○			
SEEMS S.A.	2017	GR Thessaloniki	11-50	EU															○			
Steryon	2024	ES Barcelona	2-10	EU									●						○		●	●
Swissbit AG	2001	CH Bronschhofen	201-500	EU NA						●		●			●				○			
Systerel	2001	FR Aix-en-Provence	51-200	EU							●	●	●						○			
Tarides	2018	FR Paris	11-50	EU				●	●	●									○			
Tiempo Secure	2007	FR Montbonnot	11-50	EU						●			●						○	●		
Tisalabs Limited	2017	IE Cork	11-50	EU					●									●	○		●	●
TofuPilot		CH Lausanne	2-10	EU															○			
Trout	2022	FR Paris	11-50	EU NA												●	●		○			
Trusted Objects		FR Aix-en-Provence	2-10	EU										●		●			○		●	●
TTTECH		AT Vienna	1,001 5,000	EU														●	○			
uCORE Systems	2022	DE Weiterstadt	2-10	EU															○		●	
Utimaco	1983	DE Aachen	501-1,000	EU NA APAC						●		●				●			○	●		
Zafehouze Ltd.	2021	DK Jyllinge	11-50	EU															○			

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

FRAUNHOFER

The European Union has adopted the Artificial Intelligence Act, which provides the most comprehensive regulatory framework for AI to date.

The arrival of generative artificial intelligence systems has fundamentally altered how digital content is produced, distributed, and evaluated. Texts, images, audio, and video can now be created or manipulated at a quality level that is increasingly indistinguishable from conventionally produced material, both for human observers and for many automated detection methods. This development expands creative and economic possibilities but simultaneously undermines established mechanisms for assessing authenticity, provenance, and credibility. In particular, the fabrication of persuasive but entirely synthetic "evidence" lowers the threshold for fraud, disinformation, and targeted deception.

In response, the European Union has adopted the Artificial Intelligence Act, which provides the most comprehensive regulatory framework for AI to date. A central element of this regulation is the obligation to label content that has been generated or significantly altered by AI. Anchored in Article 50, this labeling duty is designed to enhance transparency and traceability in digital environments. Providers of AI systems are required to implement machine-readable markings for AI-generated or AI-manipulated content, including texts, images, audio, and video. The objective is to enable auditors, supervisory authorities, media organizations, and other stakeholders to reliably identify the origin and transformation history of digital content.

Technically, the landscape of potential labeling methods is heterogeneous and characterized by trade-offs. Inserted metadata and cryptographic signatures (including standards such as C2PA) allow relatively straightforward public verification and can document provenance and editing histories, but are vulnerable to loss or stripping during content processing. Visible watermarks are accessible and intuitive but may impair media quality and are often removable. Invisible watermarks, whether symmetric or asymmetric, promise higher robustness against common transformations, yet either require trusted third parties for detection (symmetric) or remain less mature and weaker in practice (asymmetric). Fingerprinting, which infers AI origin by matching content-specific features against provider-maintained databases, can be robust but depends on provider cooperation and does not enable fully public verification.

No single approach currently satisfies all regulatory and practical requirements simultaneously. It is therefore plausible that multi-layered solutions, combining several complementary methods, will be needed. More fundamentally, the labeling obligation should not be understood as a purely technical fix but as one component of a broader trust infrastructure for digital information. Its effectiveness will depend on the interplay between clear legal norms, technically sound and standardized implementations, institutional workflows, and informed users. In this sense, labeling AI-generated content provides a focal point where legal regulation, technical innovation, and information-scientific theory converge to support more transparent and trustworthy digital ecosystems.

Fraunhofer SIT

ATHENE National Research Center for Applied Cybersecurity

The Fraunhofer-Gesellschaft, headquartered in Germany, is one of the world's leading organizations for applied research. It plays a major role in innovation by prioritizing research on cutting-edge technologies and the transfer of results to industry to strengthen Germany's industrial base and for the benefit of society as a whole. Since its founding as a nonprofit organization in 1949, Fraunhofer has held a unique position in the German research and innovation ecosystem.

fraunhofer.de

Prof. Dr. Martin STEINEBACH

Head of the Media Security and IT Forensics department

Fraunhofer Institute for Secure Information Technology SIT

European Cybersecurity Mapping 2026

SECURE COMMUNICATION PLATFORMS

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Safe communication, collaboration, and the distribution of uncompromised messages are essential for both business operations and institutional work. Secure Communication Platforms provide encrypted channels for secure messaging, data exchange, collaborative work, and videoconferencing systems.

Why Choose European Technology: European vendors design platforms fully compliant with GDPR and local sovereignty concerns, ensuring that critical communications remain under European jurisdiction and control.

Importance for European sovereignty: 9/10

Secure communication is vital for governments, businesses, and individuals. European platforms ensure confidential information remains within trusted borders.

Where Privacy Meets Enterprise Reality

kuppingercole ANALYSTS

MARKET CONTEXT

The post-pandemic shift to hybrid work exposed a fundamental weakness in organizational communication. Consumer messaging apps have become de facto business tools almost overnight, and security teams have spent the past years trying to regain control. Regulatory pressure compounds the problem. NIS2 imposes strict incident notification requirements that break down when sensitive discussions occur on platforms with no audit trail. Financial services firms face MiFID II and DORA obligations that require communications retention and surveillance. Healthcare providers must demonstrate GDPR compliance for patient-related discussions. The regulatory environment has transformed secure communications from a nice-to-have into a compliance imperative.

EUROPE'S COMPETITIVE ADVANTAGE

European vendors have clear advantages here. Privacy engineering is baked into how they build products, not bolted on afterward to satisfy a checklist. Several German and Swiss providers have built their architectures around zero-knowledge principles, where even the vendor cannot access message content. Threema's approach is instructive: messages are encrypted on the device before transmission, keys never leave the user's possession, and the company cannot obtain the original data because it lacks the technical means to do so. This matters when your customers include government ministries, defense contractors, and organizations handling classified information. The Schrems II decision continues to haunt US platform providers, and European alternatives can sidestep the entire debate about transatlantic data flows. I have procurement decisions in critical infrastructure sectors where European ownership was a hard requirement.

TECHNOLOGY EVOLUTION & TRENDS

Secure messaging has matured considerably. Early solutions forced users to choose between security and usability, and usability predictably won. Modern platforms have closed that gap. End-to-end encryption now extends beyond text to voice, video, and file sharing without degrading the experience. Federation protocols enable secure communication across organizational boundaries without requiring everyone to use the same platform. Integration with enterprise systems matters more than standalone security features. Organizations want secure chat embedded in their workflows, connected to identity providers, appearing in their compliance archives, and subject to the same policy controls as email.

MARKET DYNAMICS

The market remains surprisingly fragmented. A handful of established players serve government and defense, but the broader enterprise market has yet to consolidate around clear leaders. European vendors are trying to scale but face real obstacles. Most lack the sales and marketing resources of U.S. competitors, and the European market itself is fractured across languages and procurement cultures. Recent acquisitions suggest that larger security vendors view secure communications as a platform play rather than a point solution. I expect continued M&A activity, with identity and access management vendors particularly interested in expanding into the communications layer.

FUTURE

Secure messaging, collaboration, and identity are converging. The EU Digital Identity Wallet rollout will eventually enable verified identity in communications, a development that could benefit European vendors familiar with the eIDAS 2.0 framework. Quantum-resistant cryptography will become a procurement requirement within five years; vendors who begin transitioning now will have a story to tell, while those who wait will face costly retrofits. For buyers evaluating platforms today, I would prioritize interoperability and standards compliance over proprietary feature sets. For investors, the exit opportunities lie in vendors who have solved the enterprise integration problem, not those competing purely on encryption strength. The latter is becoming commoditized; the former remains difficult to get right.

Jonathan CARE
Lead Analyst
KuppingerCole Analysts AG

For detailed analysis, see:
Market Compass: Secure Collaboration
Leadership Compass: Identity Governance and Administration

SECURE COMMUNICATION PLATFORMS (1/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
9Solutions Global	2009	SE Helsingborg	51-200	EU										●						○	●	
Aangetekend	2011	NL Utrecht		EU								●	●							○		
ARC Data Shield	2022	FR Pays de La Loire	2-10	EU			●											●	●	○		
ARMA INSTRUMENTS	2017	NL Mijdrecht	51-200	EU								●		●						○		
Belledonne Communications	2009	FR Grenoble	11-50	EU																○		
Beyond Encryption	2013	GB Fareham	51-200	EU																○		
blackned GmbH		DE Heimertingen	201-500	EU										●				●		○		
CEO-Vision SAS	2010	FR Archamps	11-50	EU																○		
Compumatica secure	1991	NL Uden	51-200	EU								●		●				●	●	○		
Crypho	2012	NO Tonsberg	2-10	EU						●		●								○		
Cyber Attack - CBA	2021	ES Roqueta	2-10	EU					●											○	●	
ERCOM	1986	FR Vélizy-Villacoublay	51-200	EU						●		●								○		
Fragmentalis	2022	IT Milan		EU				●		●		●						●	●	○		
Garrison	2014	GB London	51-200	EU														●		○	●	
Infobip	2006	GB London	1,001 5,000	EU NA APAC												●				○		
infodas	1974	DE Cologne	201-500	EU								●								○	●	●
innovaphone	1997	DE Sindelfingen	51-200	EU						●										○		
Inseqr	2018	PL Warsaw	11-50	EU					●											○	●	
Intercope	1982	DE Hamburg	51-200	EU								●			●					○		
Interpeer gUG	2022	DE Greifenberg	2-10	EU								●								○		
Invis Wearables		PL Warsaw	2-10	EU																○		
Jalios	2001	FR Le Chesnay	51-200	EU																○		

SECURE COMMUNICATION PLATFORMS (2/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Jamespot	2005	FR Montreuil	11-50	EU																●		
LiveDrop	2021	NL Eindhoven	11-50	EU	●										●					●		
Messagenius	2014	GB London	11-50	EU	●				●						●					●		
Messente Communications	2013	EE Pelgulinn	11-50	EU					●							●	●			●		
Msafe Secure	2012	NL Ijsselstein	11-50	EU					●											●		
MyTutela	2017	IT Rome	2-10	EU	●				●											●		
NEXIMS	2008	FR Boulogne-Billancourt	11-50	EU APAC												●				●	●	
NFON AG	2007	DE Munich	201-500	EU	●				●											●		
Olvid	2019	FR Paris	2-10	EU						●						●				●		
OnePrivacy S.A.	2017	LU Windhof	2-10	EU					●	●										●		
Private Discuss		FR Limonest	11-50	EU												●				●	●	
PRIVUS	2016	CH Zug	2-10	EU					●	●										●		
PureSquare	2006	VG Virgin Islands	201-500	NA						●							●			●		
RealTyme	2020	CH Geneva	11-50	EU					●	●										●		
Salt Communications	2013	GB Belfast	11-50	EU	●				●	●										●		
Sectra	1978	SE Linkoping	1,001 5,000	EU NA APAC						●								●	●	●	●	
Secusmart	2007	DE Dusseldorf	51-200	EU	●					●										●		
SHAREKEY Swiss AG	2018	CH Zug	11-50	EU					●	●										●		
Surfshark	2018	LT New Town	201-500	EU										●						●	●	
Threema	2012	CH Pfaffikon	51-200	EU					●	●										●		
Tixeo	2003	FR Montpellier	11-50	EU					●	●										●		
Treebal Pro	2021	FR Rennes		EU					●		●									●		

SECURE COMMUNICATION PLATFORMS (3/3)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
TRUSTZONE	2004	DK Copenhagen	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
WATCHA	2016	FR Lyon	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Wayren	2020	EE Tallinn	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Whaller	2013	FR Suresnes	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Wimi	2010	FR Paris	51-200	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
YEO Messaging	2017	GB London	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
YoGoKo	2014	FR Cesson-Sévigné	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○

Want to add your company or update your company information?

You can do it directly via our data portal:
cybermapping.european-champions.org

Interview

GREATER GENEVA BERN AREA

Switzerland has a strong incentive to invest in cyber resilience.

YOUR ACTIVITY

Greater Geneva Bern area (GGBa) is the investment promotion agency for Western Switzerland, covering the cantons of Geneva, Vaud, Fribourg, Neuchâtel and Bern. Our mission is to support foreign companies, primarily from Europe, North America and Asia, in their establishment and growth in Switzerland. We work closely with cantonal authorities, innovation agencies, academic institutions and technology parks.

Our objectives are to attract high value-added activities, strengthen local innovation ecosystems, and support sustainable economic development. Over the years, we have supported numerous companies in sectors such as cybersecurity, digital technologies, life sciences and advanced manufacturing, helping them navigate regulatory frameworks, identify suitable locations, and connect with talent, research and funding partners.

We supported the European Cybersecurity Alliance (ECA) vendor mapping initiative because visibility and structure matter. As Switzerland hosts a dense cybersecurity ecosystem, contributing to a European-level mapping helps position Swiss actors within the broader market and improves transparency for customers and partners. It reinforces Europe's strategic autonomy in cybersecurity.

YOUR ASSESSMENT OF CYBERSECURITY IN SWITZERLAND

Cybersecurity is a critical issue in Switzerland. As a highly digitalized economy hosting international organizations, financial institutions, critical infrastructures and industrial IP, Switzerland has a strong incentive to invest in cyber resilience. This is reflected in national strategies, public-private cooperation and sustained investment in research and innovation.

The local cybersecurity industry is mature and diverse, covering software vendors, managed security service providers, consulting firms and highly specialized niche players. This ecosystem is anchored in strong innovation hubs and technology parks across Western Switzerland. In Vaud, the Unlimitrust Campus in Prilly is a flagship site dedicated to digital trust and cybersecurity. Geneva benefits from Campus Biotech and from its concentration of international organizations and financial institutions, generating strong demand for cybersecurity solutions related to data protection and critical infrastructures. Neuchâtel relies on the Microcity innovation pole, closely linked to applied research in secure hardware, embedded systems and industrial cybersecurity. Fribourg's blueFACTORY innovation district supports applied digital and Industry 4.0 projects, including cybersecurity for manufacturing and infrastructure.

In Bern, innovation sites such as Bernapark, combined with the presence of federal institutions, foster expertise in e-government, public-sector IT security and national critical systems.

EUROPEAN PERSPECTIVE

Europe could improve coordination and speed. Fragmentation of markets, standards and procurement remains a challenge for cybersecurity vendors trying to scale. Stronger alignment between regulation, funding instruments and industrial policy would help European companies compete globally, while maintaining high standards of trust and data protection.

At GGBa, we actively promote European collaboration by connecting companies with cross-border partners, research programs and innovation networks. We encourage participation in European initiatives and consistently position Western Switzerland as an open, reliable and cooperative location within the European cybersecurity landscape.

For cybersecurity companies, establishing a local team in Switzerland offers direct access to trusted customers, cutting-edge research, skilled talent and a stable regulatory environment; GGBa is available to support companies at every stage of this process and invites interested actors to get in touch.

Greater Geneva Bern area (GGBa) is the investment promotion agency for Western Switzerland, bringing together the cantons of Bern, Fribourg, Vaud, Neuchâtel and Geneva. Its mission is to provide support to foreign companies allowing them to get established quickly and develop their activities in the region.

ggba.swiss

Thomas BOHN
CEO

GREATER GENEVA BERN AREA

European Cybersecurity Mapping 2026

THREAT MANAGEMENT

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Threat Management is a core security domain. Threats are now ubiquitous, moving beyond simple external assaults, and AI-aided attacks make distinguishing between genuine threats and normal access increasingly difficult. These systems use proactive and reactive strategies to identify, analyze, and mitigate cyber threats. The toolkit is rounded out by capabilities like cyber threat intelligence and deception tools. Increasingly AI-driven and automated, they allow cybersecurity teams to focus on critical issues. We foresee major evolutions in this domain as AI will become, on one side a key vector of malicious attacks, and on the other side, the core of anomaly detection and interpretation.

Why Choose European Technology: European providers deliver solutions tailored to local regulatory frameworks and threat landscapes, ensuring the trusted and sovereign management of cybersecurity risks and all related user data.

Importance for European sovereignty: 10/10

Threat management tools are key to detecting and responding to cyber threats, ensuring strategic independence in dealing with evolving risks.

From Reactive Defense to Continuous Threat Exposure Management

kuppingercole ANALYSTS

MARKET CONTEXT

For the past decade ethical hacking and red teaming have been standard practices for identifying organizational security gaps. However, these practices were usually performed on demand, leaving environments unmonitored most of the time. Recently, the industry has shifted from a reactive defense posture to a proactive one, with vendors investing heavily to create tools that automate security assessment and validation. As organizations adopt cloud-native architectures and remote work practices, their attack surface expands.

Modern threat management enables teams to discover unknown assets and detect active attacker behavior and system misconfigurations that human analysts might overlook. Additionally, the increasing number of known vulnerabilities makes manual prioritization of threats a bottleneck for human-led SOC teams.

Organizations can now identify and remediate sophisticated AI-driven threats before they are leveraged by cybercriminals by using Threat Management tools such as Threat Detection and Response (TDR), Attack Surface Management (ASM), and Threat Intelligence Platforms (TIPs).

Meanwhile, TDR has evolved from siloed security controls into a continuous, cross-layer capability that extends to endpoints, networks, cloud workloads, and applications. Organizations need solutions that offer real-time detection, behavioral analytics, and automated responses to identify threats that bypass legacy tools.

EUROPE'S COMPETITIVE ADVANTAGE

When NIS2 and DORA are fully implemented European vendors will have a significant advantage by embedding security control groups into their solutions and technical architectures, thereby achieving compliance by design. Unlike their global counterparts, who may fail to support GDPR and localized data residency laws, EU-based providers can assist organizations in complying with jurisdictional security and privacy laws.

TECHNOLOGY EVOLUTION & TRENDS

The most obvious market trend is that vendors now provide greater visibility and mapping of attack surfaces instead of just conducting static vulnerability scanning. In most cases, ASM and Continuous Threat Exposure Management (CTEM) solutions offer the same functionality. Another trend is the implementation of agentic AI to automate detection, prioritization, and remediation efforts across both threat management and active response. However, organizations do not yet trust machine-led decision making, although this may change.

In the TDR domain behavior-based analytics and network-centric detection are gaining importance as attackers can often evade signature-based controls. Vendors are expanding their detection capabilities to include network traffic analysis (NTA), cloud runtime telemetry, and application-layer signals. This convergence is driving closer alignment between threat management, NDR, and XDR systems.

MARKET DYNAMICS

The number of baseline functions required from threat management vendors has nearly doubled compared to previous years, reflecting a shift toward developing out-of-the-box capabilities rather than complementary third-party integrations. The market is consolidating as customers seek unified platforms that combine External Attack Surface Management (EASM), Cybersecurity Asset Attack Surface Management (CAASM), and Digital Risk Protection capabilities. Large platforms are acquiring niche specialists to build all-in-one threat management suites. However, there is still a strong demand for standalone TIPs for precise threat intelligence.

FUTURE

We should expect agentic AI to be more involved in threat prioritization and remediation. AI-led automation will also reduce analyst alert fatigue and result in fewer false positives. Human analysts will likely monitor agentic AI decisions rather than being completely replaced by AI. TDR will become more autonomous and predictive, with AI-driven systems correlating exposure data, attacker behavior, and environmental context to interrupt attacks proactively. Solutions such as software supply chain security and brand protection tools, as well as native Cyber Threat Intelligence feeds, will likely become integral parts of threat management solutions.

Osman CELIK
Research Analyst
KuppingerCole Analysts AG

For detailed analysis, see:
Leadership Compass: Attack Surface Management
Buyer's Compass: Brand Protection

THREAT MANAGEMENT (1/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
2501.ai		FR Paris	2-10	EU			●			●											○	
3CORESec	2019	PT Lisbon	2-10	EU																	○	
6cure	2010	FR Herouville-Saint-Clair	11-50	EU					●								●				○	
Aagon GmbH	1992	DE Soest	51-200	EU										●		●					○	●
Abstract Security	2023	US San Fran.	11-50	NA			●			●											○	
Agam Security	2016	CH Lausanne	2-10	EU																	○	
Alekso	2018	FR Le Plessis-Robinson	11-50	EU						●							●				○	
allentis		FR Paris	11-50	EU													●				○	●
Allgeier CyRis GmbH		DE Bremen	51-200	EU																	○	
AMG INFORMATIQUE	1970	FR Dijon	11-50	EU						●							●				○	
AMPEG GmbH	1994	DE Bremen	2-10	EU								●				●					○	●
ANOZR WAY	2019	FR Cesson-Sévigné	11-50	EU					●						●	●					○	
Arcabit	2004	PL Warsaw	11-50	EU										●							○	●
Athesya	2020	FR Paris	2-10	EU												●	●				○	●
Attic BV	2020	NL Zevenbergen	11-50	EU					●							●					○	
Axence	2005	PL Krakow	51-200	EU					●					●							○	
Baffin Bay Networks	2017	SE Stockholm	11-50	EU				●									●				○	
Ballpoint	2023	FR London	2-10	EU																	○	
BeAI Srl	2025	IT Seregno	2-10	EU			●			●											○	
Beelzebub			2-10						●							●					○	
Beware Cyberlabs	2018	FR Bordeaux	2-10	EU					●												○	
Binalyze	2018	EE Tallinn		EU NA			●							●	●						○	

THREAT MANAGEMENT (2/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
BlackDice Cyber	2019	GB Leeds	11-50	EU			●										●				○	
BlackfishID		ES Madrid	2-10	EU					●					●							○	●
BLOCKAPT	2019	GB Southwark	11-50	EU										●	●						○	●
BreacHunt	2020	FR Paris	1	EU												●					○	
Bureau Veritas Cybersecurity		NL Amsterdam	201-500	EU					●				●								○	●
C2SEC INC	2016	CH Redmond	11-50	EU NA																	○	
CacheGuard Technologies	2009	FR Paris	2-10	EU													●				○	●
ChapsVision		FR Suresnes	501-1,000	EU			●						●								○	
CHEOPS TECHNOLOGY	1998	FR Canejan	501-1,000	EU						●							●				○	●
Chorus Intelligence	2011	GB Woodbridge	51-200	EU NA						●						●					○	
CloudGuard	2020	GB Manchester	11-50	EU					●								●				○	●
Cloudsmith	2016	GB Donegall	51-200	EU						●											○	●
Cogninn	2017	GR Athens	11-50	EU																	○	
Coinnect	2019	CH Mendrisio	11-50	EU					●							●					○	
Comand AI	2023	FR Paris	11-50	EU			●			●			●								○	
consistec	2000	DE Saarbrucken	51-200	EU												●		●	●		○	
Cortex Security S.A.			2-10				●			●											○	
CounterCraft	2015	US New York	51-200	EU NA												●					○	
CrowdSec	2020	FR Paris	11-50	EU												●		●			○	
Custocy	2018	FR Labège	11-50	EU			●										●				○	
CybaVerse	2018	GB Portsmouth	11-50	EU					●							●					○	●
cybee.ai	2024	CH Zurich	11-50	EU						●				●		●					○	

THREAT MANAGEMENT (3/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
CybelAngel	2013	FR Paris		EU NA			○	○	○	○	○	○	○	○	●	●	○	○	○	○	●	●
CYBERA	2022	CH New York	11-50	EU NA	▬		○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
CyberCyte	2018	GB Reading	11-50	EU			○	○	○	○	○	○	●	○	○	○	●	○	○	○	●	●
CYBER-DETECT	2017	FR Nancy	11-50	EU			○	○	●	○	○	○	○	○	●	○	○	○	○	○	●	○
CyberOwl	2016	GB London	11-50	EU APAC			○	○	●	○	○	○	○	○	○	○	○	●	●	○	●	○
Cybersense GmbH		DE Dortmund	11-50	EU			○	○	○	●	○	○	○	○	○	○	○	●	○	○	●	○
CyberseQ	2021	DE Hamburg	2-10	EU			○	○	●	●	○	○	○	○	○	○	○	○	○	○	●	○
CyberTrap	2015	AT Vienna		EU			○	○	○	○	○	○	○	●	●	○	●	○	○	○	●	○
Cyberwise	2018	NL Amsterdam	11-50	EU			○	○	○	○	○	○	○	○	○	○	●	●	○	●	●	
Cybi	2022	FR Villers-les-Nancy	2-10	EU			●	○	○	○	○	○	○	○	○	○	○	○	○	●	●	
CybSafe		GB London	51-200	EU	▬		○	○	●	○	○	○	○	○	●	○	○	○	○	●	○	
Cydea	2019	GB Abingdon	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	
CyNation	2015	GB London	11-50	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	●	○	
CYQUEO	2003	DE Munich	11-50	EU			○	○	○	○	○	○	○	●	●	○	○	●	○	●	○	
Cytidel	2022	IE Castlebar	11-50	EU	▬		○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	
Cywise	2018	FR Paris	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	●	
DarkFindR	2024	FR Paris					○	○	○	○	○	○	●	○	○	●	○	○	○	●	○	
Darktrace	2013	GB Cambridge	1,001 5,000	EU			○	○	○	○	○	○	○	●	○	○	○	●	○	●	○	
Data for Ethic	2019	FR Fontenay-sous-Bois	2-10	EU			●	○	●	○	○	○	○	○	○	○	○	○	○	●	○	
DataDome	2015	FR New York	51-200	EU NA APAC	▬		●	○	●	○	○	○	○	○	●	○	○	○	○	●	○	
Dataxium	2019	FR Neuilly-sur-Seine	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	●	
Dattak	2021	FR Paris	11-50	EU	▬		○	○	●	○	○	○	○	○	○	●	○	○	○	●	●	

THREAT MANAGEMENT (4/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Dectar	2017	IE Dublin	11-50	EU			○	○	○	○	○	○	○	●	○	○	●	○	○	○	●
Dedge Security	2023	ES Madrid	2-10	EU			●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Deep Secure	2010	GB Malvern	51-200	EU			○	○	○	○	○	○	○	●	○	○	●	○	○	○	○
Deepinfo	2017	FR Istanbul	11-50	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	○	●
defants	2021	FR Cesson-Sévigné	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
DEFION Security	1997	NL Eu	51-200	EU			○	●	○	○	○	○	●	○	○	○	○	○	○	○	●
DefSecIntel Solutions		EE Tallinn	51-200	EU			●	○	○	○	○	○	○	○	○	○	●	●	○	○	○
Defused	2023	FI Espoo	2-10	EU			○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
DFLabs		IT Milan	501-1,000	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	○
DomainTools	2004	ES Seattle	51-200	NA			○	○	○	●	○	○	○	○	○	●	●	○	○	○	○
Dreamlab Technologies	1997	CH Bern	51-200	EU APAC			○	○	○	○	○	○	○	○	○	○	●	○	○	○	●
Dubex	1997	DK Glostrup	51-200	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
DYNANIC	2021	CZ Kralovo Pole	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
easylience®	2016	FR Paris & Rennes	11-50	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	○
EclecticIQ	2014	NL Amsterdam		EU NA			○	○	●	○	○	○	●	○	○	○	○	○	○	○	○
Elasticito	2017	GB London	2-10	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	○	○
Enablon		NL Bois-Colombes	501-1,000	EU NA			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Energy Logserver	2015	PL Warsaw	11-50	EU			○	○	●	○	○	○	○	○	○	○	●	○	○	○	○
Engave	2010	PL Warsaw	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enginsight GmbH	2017	DE Jena	51-200	EU			○	○	○	○	○	○	○	●	○	○	●	○	○	○	●
Ermes Browser Security	2017	IT Turin	11-50	EU			○	○	●	○	○	○	○	●	○	○	○	○	○	○	○
ESET	1992	SK Bratislava	1,001 5,000	EU NA APAC			○	○	○	○	○	○	○	●	○	○	○	○	○	○	○

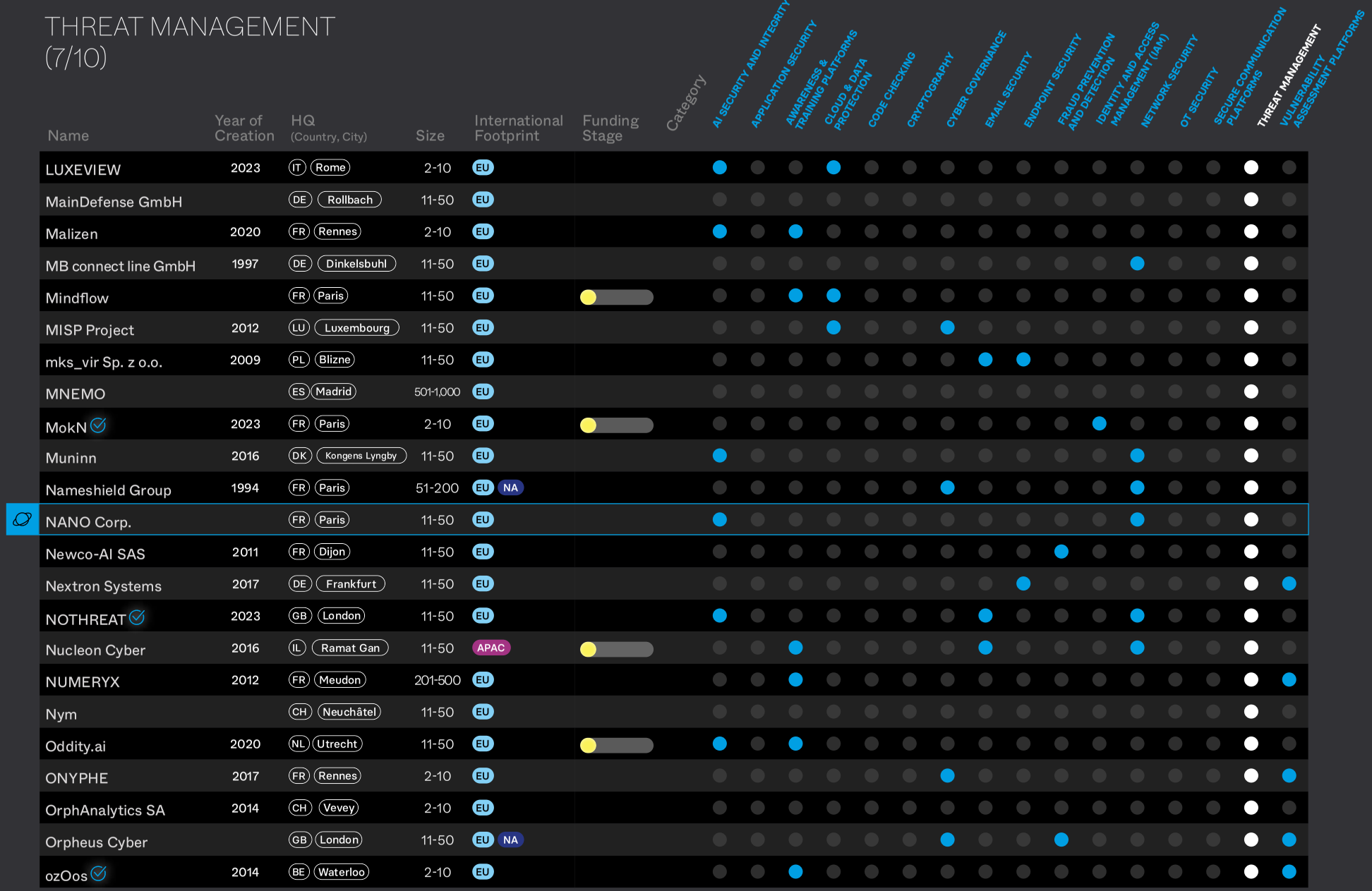
THREAT MANAGEMENT (5/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
ESIA S.A.	2011	BE Sprimont	11-50	EU			○	○	●	○	○	○	○	○	○	○	●	○	○	○	●	○
Euler Data Solutions	2021	FR Bordeaux	51-200	EU			●	○	○	○	○	○	●	○	○	○	○	○	○	○	●	○
Evidantly CYBER BV	2015	NL Rotterdam	2-10	EU			●	○	○	○	○	○	●	○	○	●	○	○	○	○	●	○
EXB Software	1989	NL Rotterdam	51-200	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	○
Exeon Analytics	2016	CH Zurich	51-200	EU			●	○	○	○	○	○	○	○	○	○	○	●	●	○	●	○
Eye Security	2020	NL The Hague	201-500	EU			○	○	●	○	○	○	○	○	●	○	○	○	○	○	●	○
FELWY			2-10				●	○	○	○	○	○	○	○	●	○	○	○	○	○	●	○
Filigran	2022	FR New York	201-500	EU NA APAC			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	○
Flare	2017	CA Montreal	51-200	NA			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○
ForenSOC			1				○	○	○	●	○	○	○	○	○	○	○	○	○	○	●	○
ForestGuard	2022	TR Istanbul	2-10	EU			●	○	○	●	○	○	○	○	○	○	○	○	○	○	●	○
FortIT AG	2019	CH Zurich	11-50	EU			○	○	○	●	○	○	●	○	○	○	●	○	○	○	●	●
Fox-IT	1999	NL Delft	201-500	EU			○	○	●	○	○	○	●	○	○	●	○	○	○	○	●	○
Friend MTS	1998	GB London	51-200	EU APAC			○	○	○	●	○	○	○	○	○	○	●	○	○	○	●	●
FRISS	2006	NL Utrecht	201-500	EU NA			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○
F-Secure Corporation	1988	FI Helsinki	501-1,000	EU NA APAC			○	○	○	○	○	○	○	○	●	●	●	●	○	○	●	○
G DATA CyberDefense	1985	DE Bochum	501-1,000	EU			○	○	●	○	○	○	○	○	●	○	●	○	○	○	●	○
Gambit Cyber	2024	NL Leiden	2-10	EU			●	○	○	○	○	○	●	○	○	○	○	○	○	○	●	●
GATEWATCHER	2015	FR Paris	51-200	EU			●	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○
GLIMPS	2019	FR Cesson-Sévigné	51-200	EU			●	●	○	○	○	○	○	○	○	○	○	○	○	○	●	●
GRCcontrol B.V.	2008	NL Deventer	11-50	EU			○	○	○	○	○	○	●	○	○	○	○	○	○	○	●	○
GREYCORTEX		CZ Brno	11-50	EU			●	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○

THREAT MANAGEMENT (6/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Hacknowledge SA	2016	CH Morges	51-200	EU			○	○	○	○	○	○	○	●	○	○	●	○	○	○	●	●
Hafnova	2024	CH Lausanne	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
HarfangLab	2018	FR Paris	51-200	EU			○	○	○	○	○	○	○	●	○	○	○	○	○	○	●	●
Haruspex Cybersecurity	2016	IT Pisa	11-50	EU			●	○	○	○	○	○	●	○	○	○	○	○	○	○	●	●
Hexegic	2009	GB London	51-200	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	○
HOLIS	1995	FR Paris	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
HumanFirewall		GB London	51-200	EU			○	○	●	○	○	○	○	●	○	○	○	○	○	○	●	○
IGEL Technology	2001	DE Bremen	201-500	EU NA			○	○	○	●	○	○	○	○	●	○	○	○	○	○	●	○
KARUS Security	1986	AT Vienna	51-200	EU			○	○	○	○	○	○	○	●	●	○	○	○	●	○	●	○
Illumio	2013	DE Sunnyvale	501-1,000	NA			●	○	○	●	○	○	○	○	○	○	○	●	○	○	●	○
Immunity Systems	2015	PL Warsaw	11-50	EU			○	●	●	○	○	○	○	○	○	●	○	○	○	○	●	○
IntelexVision	2017	GB London	51-200	EU			●	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
iTrust	2003	FR Cham	11-50	EU			○	○	○	○	○	○	○	○	○	●	○	○	○	○	●	●
Karsa Oy	2016	FI Helsinki	11-50	EU			○	○	○	○	○	○	○	○	●	○	○	●	○	○	●	○
keyIT sa	2021	CH Marly	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Krakinsight	2025	CH Lausanne	2-10	EU			○	○	○	○	○	○	○	○	○	○	●	●	○	○	●	○
Labyrinth Security	2019	PL Zabrze	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	●	○	○	●	○
Linkurious	2013	FR Montreuil	51-200	EU NA			●	○	○	○	○	○	○	○	●	○	○	○	○	○	●	○
LogCraft		FR Paris	2-10	EU			○	○	●	○	○	○	○	○	●	○	○	○	○	○	●	○
Logmind		CH Lausanne	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Logpoint	2001	DK Copenhagen	201-500	EU NA			○	●	●	○	○	○	○	○	●	○	○	○	○	○	●	○
Look Up	2022	FR Toulouse	11-50	EU			○	○	○	●	○	○	●	○	○	○	○	○	○	○	●	○
Lupovis		GB Glasgow	11-50	EU			●	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○

THREAT MANAGEMENT (7/10)



Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
LUXEVIEW	2023	IT Rome	2-10	EU			●			●											○	
MainDefense GmbH		DE Rollbach	11-50	EU																	○	
Malizen	2020	FR Rennes	2-10	EU			●		●												○	
MB connect line GmbH	1997	DE Dinkelsbuhl	11-50	EU													●				○	
Mindflow		FR Paris	11-50	EU					●	●											○	
MISP Project	2012	LU Luxembourg	11-50	EU						●			●								○	
mks_vir Sp. z o.o.	2009	PL Blizne	11-50	EU										●	●						○	
MNEMO		ES Madrid	501-1,000	EU																	○	
MokN	2023	FR Paris	2-10	EU												●					○	
Muninn	2016	DK Kongens Lyngby	11-50	EU			●										●				○	
Nameshield Group	1994	FR Paris	51-200	EU NA									●				●				○	
NANO Corp.		FR Paris	11-50	EU			●										●				○	
Newco-AI SAS	2011	FR Dijon	11-50	EU											●						○	
Nextron Systems	2017	DE Frankfurt	11-50	EU										●							○	●
NOTHREAT	2023	GB London	11-50	EU			●						●				●				○	
Nucleon Cyber	2016	IL Ramat Gan	11-50	APAC					●				●				●				○	
NUMERYX	2012	FR Meudon	201-500	EU					●												○	●
Nym		CH Neuchâtel	11-50	EU																	○	
Oddity.ai	2020	NL Utrecht	11-50	EU			●		●												○	
ONYPHE	2017	FR Rennes	2-10	EU									●								○	●
OrphAnalytics SA	2014	CH Vevey	2-10	EU																	○	
Orpheus Cyber		GB London	11-50	EU NA									●			●					○	●
ozOos	2014	BE Waterloo	2-10	EU					●												○	●

THREAT MANAGEMENT (8/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Panop.io	2024	CH Prilly	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Passguard	2021	NL Leusden	2-10	EU	●		○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Periphery	2023	GB Leeds	2-10	EU	●		●	○	○	○	○	○	○	○	○	○	○	○	●	○	●	●
Phishermen	2017	NL Delft	2-10	EU			○	○	●	○	○	○	○	●	○	●	○	○	○	○	●	○
Pikered	2020	IT Milan	2-10	EU			●	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
PinakashieldTech	2025	EE Tallinn	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
PRODAFT	2012	NL Yverdon-les-Bains	51-200	EU			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	○
P-X Systems	2015	NL Amsterdam	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	●	●	○	●	○
Qevlar AI	2023	FR Paris		EU NA	●		○	○	○	○	○	○	●	●	○	●	○	○	○	○	●	○
QuoScient	2016	DE Frankfurt	2-10	EU			○	○	●	○	○	○	○	○	○	●	○	○	○	○	●	●
RAVIB	2012	NL The Hague	1	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	○
RazorSecure	2014	GB Basingstoke	11-50	EU	●		○	○	○	○	○	○	○	○	○	○	○	●	●	○	●	○
Redamp.io	2012	CZ Brno	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	●	○	○	●	○
RedCarbon	2020	IT Turin	11-50	EU			●	○	●	○	○	○	○	○	○	○	○	○	○	○	●	○
Resilium.AI		FR Paris	11-50	EU			○	○	●	●	○	○	○	○	●	○	○	○	○	○	●	○
Resistine	2021	CZ Berlin	11-50	EU	●		●	○	○	●	○	○	○	○	○	○	○	●	○	○	●	○
Retactic	2023	DE Mannheim	2-10	EU			○	○	●	○	○	○	○	●	●	○	○	○	○	○	●	○
Ria21 - TotalGAC	2021	ES Vigo	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	●	○	●	○
RIFFSEC	2022	PL Warsaw	2-10	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	○	●	●
Rudder	2010	FR Paris	11-50	EU			○	○	○	●	○	○	●	○	○	○	○	○	○	○	●	●
Sagenso	2019	PL Rzeszow	11-50	EU	●		○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	●
SCASSI		FR PS/TL/MD	51-200	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	●
SecureMe2 Cyber Security	2016	NL Barendrecht	11-50	EU			○	○	○	○	○	○	●	○	○	○	○	●	○	○	●	○

THREAT MANAGEMENT (9/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
SecureVisio	2010	PL Rzeszow	51-200	EU			●			●											●	●
SECWATCH B.V.	2005	NL Almere	11-50	EU					●												●	●
seedata.io	2021	GB London	2-10	EU					●								●				●	
Sekoia.io	2022	FR Rennes		EU						●			●		●		●				●	
SenseOn	2017	GB London	51-200	EU			●								●		●				●	
Sensoworks	2020	IT Rome	11-50	EU			●														●	●
Serenicity	2018	FR Saint-Étienne	11-50	EU											●		●				●	
Serverius IT infrastructure	2009	NL Apeldoorn	51-200	EU						●							●				●	
Sharelock	2017	IT Rome		EU			●									●					●	
SharkGate		FI Helsinki	11-50	EU NA					●						●						●	●
Shift Technology	2013	FR Paris	501-1,000	EU NA			●									●					●	
Siren	2014	NL Galway	51-200	EU NA					●							●					●	
Stoik	2023	FR Brisbane	2-10	APAC																	●	
Stormshield	2014	FR Issy-les-Moulineaux	201-500	EU						●					●			●	●		●	
Sycope	2019	PL Warsaw	11-50	EU													●				●	
SYLink Technologie	2017	FR Clermont-Ferrand	11-50	EU													●			●	●	●
SYLink Technologie	2017	FR Clermont-Ferrand	11-50	EU																	●	
Tadaweb	2011	LU Luxembourg	51-200	EU					●						●						●	
TandemTrace		ES Madrid	2-10	EU NA			●		●												●	
TeamFence SA	2024	CH Lugano	2-10	EU																	●	
TEHTRIS	2010	FR Pessac	201-500	EU NA					●					●			●				●	
Tenzir	2017	DE Hamburg	11-50	EU					●								●				●	
TeskaLabs	2014	CZ Prague	11-50	EU						●						●				●	●	

THREAT MANAGEMENT (10/10)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Tetrane	2011	FR Mâcon	11-50	NA				●													●	●
ThreadStone Cyber Security	2014	NL Rotterdam	11-50	EU					●												●	●
Threat Status	2017	GB Fareham	11-50	EU					●						●	●					●	
Tines	2018	IE Dublin	201-500	EU NA					●	●											●	
Tracebit	2023	GB London	11-50	EU						●											●	
Tranquil IT	2002	FR St Sébastien	11-50	EU					●							●					●	
Tremau	2021	FR Paris	11-50	EU			●		●												●	
Trinity Cyber	2016	US Bowie	11-50	NA										●			●				●	●
TROPICO Security	2025	IT Milan	2-10	EU			●										●				●	
TrustPort	2008	CZ Brno	11-50	EU								●		●	●						●	●
UBCOM	2014	CH Martigny	2-10	EU					●					●							●	●
Uncovery	2021	FR Paris	2-10	EU																	●	●
Unknown	2022	PT Porto	2-10	EU										●		●					●	
Validato	2021	GB Cheltenham	11-50	EU					●												●	●
VirtualMetric	2014	NL Amsterdam	11-50	EU					●	●											●	
VMRay	2013	DE Bochum		EU NA																	●	
Vulidity GmbH	2018	DE Burghausen	2-10	EU					●						●						●	●
WaryMe	2016	FR Cesson-Sévigné	11-50	EU					●											●	●	
Whisper	2025	NL Amsterdam	2-10	EU			●								●						●	
XM Cyber	2016	DE Tel Aviv	201-500	NA APAC					●												●	●
XNETSOLUTIONS	2003	DE Herrenberg	51-200	EU																	●	
Zynap		ES Barcelona	11-50	EU			●		●												●	

European Cybersecurity Mapping 2026

VULNERABILITY ASSESSMENT PLATFORMS

BY CATEGORY

Legend

ECA MEMBERS

DATA VERIFIED BY THE COMPANY

Short Pitch: Before mitigating threats, organizations must gain a clear view of their most probable attack vectors to effectively prioritize countermeasures. This is a management imperative, especially under EU NIS2 regulation, given constantly shifting attack surfaces and the impact of third-party components. Vulnerability Assessment systems identify and prioritize system weaknesses. The field is evolving from instantaneous evaluation to continuous assessment, incorporating supply chain analysis, code verification, and providing insights into the most probable and business-impacting attacks thanks to attack surface analysis. This forms a sound basis for configuring IT protection, defining resilience policy, and planning future improvements.

Why Choose European Technology: European platforms ensure that sensitive assessment data remains within EU jurisdictions, aligning with privacy and sovereignty goals. This commitment promotes trust and transparency in securing organizational systems.

Importance for European sovereignty: 10/10

Identifying and addressing vulnerabilities is critical for protecting systems and infrastructure. European solutions ensure sensitive security data stays within trusted jurisdictions.

Assessment and Risk-Based Prioritization to Address Vulnerability Fatigue

MARKET CONTEXT

Today, periodic vulnerability scans are considered insufficient as attackers now utilize sophisticated Tactics, Techniques, and Procedures (TTPs) and target new vulnerabilities daily. While manual penetration testing was the standard in the past, the increasing complexity and frequency of cyberattacks leave organizations highly vulnerable without real-time monitoring and risk assessment tools. To keep pace with adversaries, security teams must significantly reduce their Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to vulnerabilities.

Consequently, organizations require their exposures to be continuously identified and prioritized based on their criticality and relevance to the business. This level of proactive defense can be achieved through modern solutions such as Automated Penetration Testing, Pen Testing as a Service (PTaaS), BAS, Dynamic Application Security Testing (DAST), SaaS Security Posture Management (SSPM), and ASM tools.

EUROPEAN COMPETITIVE ADVANTAGES

European vendors in the vulnerability assessment market benefit from strong regulatory requirements that drive demand for compliance-ready solutions. Frameworks such as GDPR, NIS2, and the Cyber Resilience Act force organizations to adopt vulnerability management and 24-hour incident reporting.

TECHNOLOGY EVOLUTION & TRENDS

ASM and CTEM vendors are the primary drivers of emerging technologies in this market. The larger and more fragmented an organization's exposed IT estate becomes, the more it requires automation that acts like a reconnaissance team rather than a static catalogue. Consequently, the traditional static inventory model is being replaced by the dynamic validation of vulnerabilities. Simply listing system vulnerabilities is no longer sufficient. Most vendors now provide exploitability scores that reflect the real-world risk to the organizations. Rather than relying solely on the Common Vulnerability Scoring System (CVSS), risk scoring is contextualized and enriched by Cyber Threat Intelligence (CTI) feeds.

Regulatory compliance is another significant driver of technology and trends in this market. Many vendors offer compliance mapping capabilities to facilitate adherence to regional regulations. In addition, many solutions now natively support MITRE ATT&CK mapping, as well. This framework provides a globally recognized view of adversary TTPs based on real-world observations. It also serves as a structured catalogue of attacker behavior during actual attacks, covering steps from initial access to final impact.

MARKET DYNAMICS

Market consolidation is active in vulnerability assessment. Large vendors are acquiring solutions to round out their portfolios. Meanwhile, hyperscalers continue to raise their baseline functions by embedding native vulnerability and web scanning into their security suites. Customer adoption typically begins with compliance-driven scanning and patch management workflows and expands to include continuous discovery, systematic control validation, and application testing. There is a growing emphasis on reducing the "noise" and operationalizing exploitability. While the core of the vulnerability market is mature, the periphery is fragmented, driven by adjacent alternatives such as ASM, DAST, BAS, SSPM, and automated pen testing/PTaaS.

FUTURE

Standalone vulnerability scanners will either be absorbed into broader platforms or become obsolete. Capabilities borrowed from various tools will likely converge into unified platforms that continuously discover assets, validate security controls, test applications, and simulate attack paths. As hyperscalers further simplify baseline scanning, differentiation will shift toward advanced prioritization, contextual risk scoring, and automated remediation that links findings directly to security workflows.

Innovation will be dominated by agentic AI, which will enable autonomous agents to perform continuous virtual red teaming. These agents will independently plan and execute sophisticated attack chains to identify vulnerabilities that pose a real risk to business logic and data. I believe that vulnerability assessment tools will significantly reduce vulnerability fatigue in the near future.

Osman CELIK
Research Analyst
KuppingerCole Analysts AG

For detailed analysis, see:

Leadership Compass: Attack Surface Management
Buyer's Compass: Attack Surface Management
Blog: Why We Need to Map Our Attack Surface

VULNERABILITY ASSESSMENT PLATFORMS (1/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
1Strike.ai		PL Warsaw	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●
ACI Risk Measure ApS	2023	DK Copenhagen	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Aegis Security	2017	PL Warsaw	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
AFINE	2015	PL Warsaw	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Agnostic Intelligence		CH Zug	2-10	EU			○	○	○	●	○	○	●	○	○	○	○	○	○	○	●	●
Aikido Security	2022	BE Belgium	51-200	EU NA			○	●	○	●	○	○	○	○	○	○	○	○	○	○	●	●
Alpha Strike Labs	2017	DE Berlin	11-50	EU			○	○	○	○	○	○	●	○	○	○	○	○	○	○	●	●
Amn Brains	2020	FR Rennes	2-10	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	○	●
Arvato Systems		DE Gutersloh	1,001 5,000	EU			○	○	○	●	○	○	●	○	○	○	○	○	○	○	○	●
Boltonshield AG	2020	CH Zurich	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
Bug Bounty Switzerland	2020	CH Zurich	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
Bugbounter	2020	EE Tallinn	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
bugshell	2021	DE Berlin	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
C2 RISK	2015	GB London	11-50	EU			○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	●
Catcher24	2022	NL Amsterdam	2-10	EU			○	○	●	○	○	○	○	○	○	○	●	○	○	○	●	●
Citalid	2017	FR Paris	51-200	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	○	●	●
code4thought	2017	GB Holloway	11-50	EU			●	○	●	○	○	○	●	○	○	○	○	○	○	○	○	●
Cognitechs	2016	CH Plan-les-Ouates	2-10	EU			●	○	○	○	○	○	●	○	○	○	○	○	○	○	●	●
Condignum GmbH		AT Vienna	11-50	EU			○	●	○	○	○	○	●	○	○	○	○	○	○	○	●	●
Cyber Boxer	2017	EE Tallinn	2-10	EU APAC			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Cyber Cert Labs	2022	IE Dublin	2-10	EU			○	●	●	○	○	○	●	○	○	○	○	○	○	○	○	●
CyberDart	2023	IT Rome	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	●
Cyberday	2013	FI Tampere	11-50	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	●	●

VULNERABILITY ASSESSMENT PLATFORMS (2/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
CyberSmart	2016	GB London	51-200	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
Cyberwatch	2015	FR Massy	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
CyCommSec	2018	PL Warsaw	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
CyLock	2022	IT Rome	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
CyQuant	2018	CH Zurich	2-10	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	●	○	●
CYRATING	2017	FR Paris	2-10	EU			○	○	○	○	○	○	●	○	○	●	○	○	○	○	○	●
Cytix	2022	GB Manchester	2-10	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	●
Cyver.io	2020	NL Amsterdam	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Debricked	2018	SE Malmo	11-50	EU			●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	●
Deepengine	2024	CH Zurich	2-10	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
DEFENDERBOX	2024	DE Kreuztal	2-10	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
DefendSphere	2025	ES Valencia	2-10	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	●	○	●
DRIVESEC	2017	IT Turin	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
Edgescan	2011	IE Dublin	51-200	EU NA			○	●	○	○	○	○	○	○	○	○	○	○	○	●	○	●
Egerie	2016	FR Toulon	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
ENTRYZERO	2024	DE Bochum	2-10	EU			●	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●
Escape		US San Fran.	11-50	NA EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Ethiack	2022	PT Coimbra	11-50	EU			○	●	○	○	○	○	○	○	○	○	○	○	○	●	○	●
Exalens	2015	NL London	11-50	EU			○	○	○	○	○	○	○	○	○	○	●	●	○	●	○	●
FB Pro GmbH	2016	DE Grolsheim	11-50	EU			○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
GObugfree AG	2020	CH Zurich	11-50	EU			○	○	●	○	○	○	○	○	○	○	○	○	○	●	○	●
Greenbone AG	2008	DE Osnabrueck	51-200	EU			○	○	●	○	○	○	●	○	○	○	○	○	○	○	○	●
Guardian360 B.V.	2015	NL Utrecht	11-50	EU			○	○	○	○	○	○	○	○	○	○	●	○	○	●	○	●
HackenProof	2017	EE Tallinn	11-50	EU			○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	●

VULNERABILITY ASSESSMENT PLATFORMS (3/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Hackerium	2022	IE Dublin	2-10	EU				●													●	●
Hacksessible			2-10																		●	●
Hackuity	2018	FR Lyon	51-200	EU APAC					●												●	●
Hackurity	2021	NL Rotterdam	2-10	EU					●												●	●
Hadrian	2021	NL Amsterdam	51-200	EU											●						●	●
Haryon	2021	FR Bègles	2-10	EU					●												●	●
Hoxhunt	2016	FI Helsinki	201-500	EU NA			●		●												●	●
Immunefi		SG Singapore	11-50	APAC				●	●												●	●
ImmuniWeb	2019	CH Geneva	51-200	EU NA				●													●	●
Insiber.com	2022	NL Amsterdam	2-10	EU								●									●	●
JUNE FACTORY	2014	CA Hamilton	11-50	NA																		●
LocateRisk		DE Darmstadt	11-50	EU								●									●	●
LockEM	2023	PT Leiria	2-10	EU								●									●	●
Make It Home Safe Inc.®	2017	FR Pittsburgh	2-10	NA												●				●	●	●
Mind The Hack	2022	GR Palaion Faliron	11-50	EU					●												●	●
Moabi.com	2019	FR Paris	11-50	EU NA					●	●												●
Nova Leah	2015	IE Dundalk	11-50	EU								●									●	●
noways		FR Paris	2-10	EU						●							●					●
ONEKEY	2020	DE Dusseldorf	11-50	EU						●								●			●	●
OnSecurity	2018	GB Bristol	51-200	EU					●												●	●
ORBIK Cybersecurity	2023	ES Mondragon	11-50	EU														●			●	●
Outpost24		SE Karlskrona	201-500	EU NA				●				●									●	●
OverSOC		FR Lille	11-50	EU																		●

VULNERABILITY ASSESSMENT PLATFORMS (4/4)

Name	Year of Creation	HQ (Country, City)	Size	International Footprint	Funding Stage	Category	AI SECURITY AND INTEGRITY	APPLICATION SECURITY	AWARENESS & TRAINING PLATFORMS	CLOUD & DATA PROTECTION	CODE CHECKING	CRYPTOGRAPHY	CYBER GOVERNANCE	EMAIL SECURITY	ENDPOINT SECURITY	FRAUD PREVENTION AND DETECTION	IDENTITY AND ACCESS MANAGEMENT (IAM)	NETWORK SECURITY	OT SECURITY	SECURE COMMUNICATION PLATFORMS	THREAT MANAGEMENT	VULNERABILITY ASSESSMENT PLATFORMS
Patrowl.io	2020	FR Paris	11-50	EU																	●	●
Persistent Security		BE Eupen	2-10	EU					●												●	●
Phoenix Security	2021	GB London	11-50	EU NA				●		●											●	●
Plexicus | AI & ASPM	2025	ES Bilbao	11-50	EU NA			●			●												●
ProHacktiv	2022	MX Mexico City	2-10																			●
Protostars		IE Dublin	2-10	EU			●						●									●
Purplemet	2019	FR Paris	2-10	EU																		●
Pwn & Patch		FR Nanterre	11-50	EU											●						●	●
RedMimicry GmbH	2023	DE Berlin	2-10	EU										●							●	●
RESHAPE.SYSTEMS	2024	CH Lausanne	2-10	EU																		●
ResilientX Security	2022	GB London	11-50	EU				●									●				●	●
scanmeter	2023	CH Zurich	2-10	EU				●													●	●
Scovery	2023	FR Paris	2-10	EU									●								●	●
Sekost	2021	FR Rennes	2-10	EU																		●
Synacktiv	2012	FR Paris	51-200	EU																		●
TeamSystem Cybersecurity		IT Milan	11-50	EU																		●
Trustable	2022	FR Paris	11-50	EU					●				●								●	●
UNGUESS	2015	IT Milan	51-200	EU					●												●	●
XeOps.ai	2025	FR Paris	11-50	EU																		●
YesWeHack	2015	FR Paris	51-200	EU APAC				●	●												●	●
Yogosha	2015	FR Paris	11-50	EU					●												●	●
Ystorian	2023	CH Geneva		EU						●			●		●						●	●

Fraunhofer SIT

Interview

Dr.-Ing. Steven ARTZ

Coordinator Department
Automatic Vulnerability
Scanning and Verification

Fraunhofer SIT Institute

CYBERSECURITY IN EUROPE: WHERE DO WE GO?

The world is changing rapidly and so is cybersecurity. Geopolitical conflicts manifest in cyberattacks, threatening critical infrastructure even in times and places without open warfare. In addition to espionage and information retrieval, we now face threats of sabotage, e.g., backdoors or vulnerabilities that could allow an attacker to disable systems when requested. At the same time, the capabilities of organized cybercrime groups are increasing with diversified business models and black markets on which malicious experts provide services and products.

As today's main technology driver, AI assists attackers and defenders alike. Although public AI services attempt to put guardrails in place, these filters can often be circumvented. The resulting capability shift allows novice attackers such as political activists to conduct attacks that were previously out of reach, while sophisticated threat actors can exploit efficiency gains to scale and move faster.

On the other hand, we as cybersecurity researchers must find techniques for AI-based protection and defense. Using AI for better anomaly detection, for automated risk-driven response, for identifying vulnerabilities before attackers exploit them, and for automatically fixing vulnerable systems configurations and software code, present opportunities not only for academic advancement, but also for the industrial players of tomorrow. Aside from classical attack and defense, how can we as IT security researchers enable companies to securely reap the benefits of AI? How do we ensure that AI coding assistants write secure code? How do we ensure that attackers do not compromise AI-based business processes, e.g., by injecting prompts or manipulating the training data? As cybersecurity researchers, we are the ones who make the difference between blindly trusting systems (or missing chances out of fear by rejecting AI technology) and a risk-aware, secure use of what will undoubtedly shape our future well beyond traditional IT.

AI provides opportunities if we identify and use them wisely. There is a well-funded public research sector across Europe working on innovative AI-based cybersecurity technologies. Universities and research institutions publish world-class papers on novel attacks and defenses. There is a broad pool of talent and expertise that we can build upon if we set the right priorities. We need to bring this expertise into the market, into products and services that sell, that can sustain themselves, and that can generate revenue to re-invest into the further development of these products and services.

Europe might not have hyperscalers offering GPU capacity at the level of large US-based entities. Building such infrastructure costs exorbitant amounts of money, and the hardware needs regular replacement to keep up with GPU evolution. Such vast investment needs businesses at a scale currently unknown in Europe. Even in the US, it remains to be seen whether the expensive buildup in capacity will be met with profits at the same rate and scale.

Instead of competing at scale with massive datacenters, European AI technology, especially in the field of cybersecurity, should play out its unique advantages. As Europeans, we have lived the concepts of privacy, decentralized and federated infrastructure and control for decades. In cybersecurity, this allows for resilience. If one protective system is compromised but there are five others with different ideas and different implementations, attackers face serious challenges. If many companies offer similar services and one falls into the control of an unfriendly non-EU state, we can simply pick one of their competitors. While this approach may not be as shiny as multi-trillion US companies, it uses key European competencies to build resilience. We don't need to run the biggest AI models in the biggest datacenters to have the best models for the use cases that drive our economies and societies.

Such ecosystems do not grow from isolation but from cooperation, between EU Member States, but also between academia and industry. We need to bridge the gap between basic research and products by fostering applied research institutions sitting at the intersection of academia and industry, not only on paper, but engrained in the foundations of these institutions. While by no means perfect, Fraunhofer is based on a co-funding model of tying government funding to the amount of industry project money. We only get taxpayer money if industry puts their money on the table as well.

Europe has a bright future in AI-driven cybersecurity if we focus on our challenges and our values. We need to harvest the potential of all Member States – not through ultra-large companies or governmental funding schemes that give out free money that evaporates, but through shared responsibility – between Member States, between academia and industry, between people. We should not ty to copy the US or China but instead focus on our own European way forward – resilience, sovereignty, and prosperity through decentralized cooperation for mutual benefit.

Interview

We must support our own references and standards.

I think the main challenge for cyber-resilience will always be agility. We now need dynamic systems that can bounce back quickly after an attack, and this recovery has to be faster and faster. This is also a challenge in teaching, as we need to transmit this mindset to our students, before they build the European infrastructures of tomorrow.

In my field of cryptography, the transition to Post-Quantum Cryptography is everything. Quantum computing could have been the end of data security, but it ends up being a massive driver for innovation. Our goal is to stay ahead of the curve, by building new secure schemes today against an adversary that is still beyond the horizon, and we need to do that without sacrificing any functionality. Europe has a phenomenal history in mathematics, which lets us lead this transition.

Beyond standardizing PQC, the improvements of Fully Homomorphic Encryption and Secure Multi-Party Computation are phenomenal. These tools allow us to work together across borders while strictly enforcing our privacy standards. Down the line, we could hope to securely query and retrieve answers from AI models controlled by adversaries.

The European cybersecurity market has a lot of potential. Our biggest strengths are our deep tech expertise, the world-class talent coming out of our universities, and a culture of "security and privacy by design.

Historically, our blind spots have been a fragmented internal market and a lack of late-stage funding, leading our best startups to either struggle to scale globally or simply to get swallowed up by foreign tech giants right when they were getting ready. This is clearly improving, with the right mix of awareness, regulatory alignment, and European-level investment. Once the mix is right, there is a potential for a huge boom of the ecosystem.

We must support our own references and standards. Europe has to assert its technical vision globally. Building our own standards is the only way to guarantee strategic autonomy, and be sure there are no hidden backdoors. We have the right level of expertise in science, engineering and regulatory capacity to do so, we should definitely stop waiting for another entity to decide for us.

Right now, the level of cooperation across Europe is encouraging. Framework programs have done a great job building bridges between universities in different member states. But we still need a much tighter feedback loop between fundamental research, applied defense operations, and industry.

I want to see massive, joint European projects tackling the deployment of PQC. A perfect example is the future European Digital Identity Wallet, frankly, it is beyond surprising that this hasn't been fully integrated yet. We need large-scale initiatives that seamlessly connect all the players.

© École polytechnique - J.Barande

Olivier BLAZY
Professor in Cybersecurity
École polytechnique

Scientific Director
CIEDS


European
Champions Alliance

European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION

CONCLUSIONS OF THE EUROPEAN CYBERSECURITY MAPPING

Europe's cybersecurity ecosystem is larger, more mature, and more strategically aware than ever before. The 1,302 companies mapped in this edition are not just a list; they are proof that the talent, the technology, and the ambition exist. What remains to be built is the scale, the coordination, and the collective will to act on that potential.

The analysis in this Mapping points consistently in one direction: consolidation is no longer optional, and Europe's window to shape it on its own terms is narrow. The regulatory framework is in place. The innovation is here. What the ecosystem now needs is for buyers to choose European, for investors to back European growth at scale, for policymakers to convert regulatory strength into industrial strategy; and for the companies themselves to look beyond their home markets and build the bridges that make a unified European cybersecurity industry possible.

This Mapping is ECA's contribution to that effort; a tool for connection, visibility, and strategic decision-making. But it is only as powerful as the community that uses it and helps it grow. If you are a founder, an investor, a CISO, an institution, or an ecosystem builder, we invite you to be part of this project: share it, act on it, challenge it, and help us improve it.

To our sponsors: your support makes this initiative possible. Without you, there is no Mapping; and without the Mapping, a part of Europe's cybersecurity ecosystem remains invisible. To our contributors and partners: every data point shared, every correction submitted, every interview given has made this edition more accurate and more valuable. And to everyone who reads and uses this Mapping: thank you for believing that a stronger, more sovereign European cybersecurity industry is worth building; together.

No Sponsors, no Mapping *Our Deepest Thanks!*

The European Cybersecurity Mapping exists for one simple reason: because a committed community believes in the importance of strengthening Europe's digital resilience. At the heart of this community are our sponsors, the organisations that choose not only to support a project, but to invest in a vision.

We are profoundly grateful to all the sponsors of the 2026 edition.

Your support does far more than fund a publication.

It brings this entire Mapping to life.

Thanks to you, we are able to:

- research and structure hundreds of companies across Europe.
- engage experts and contributors in dozens of countries.
- analyse trends, markets, and technologies in depth.
- produce high-quality interviews and macro insights.
- and distribute this Mapping freely to thousands of professionals, policymakers, and innovators.

You enable us to make European cybersecurity **visible, understandable, and accessible;** not just to experts, but to the entire digital ecosystem.

strategic sponsors

Atos · IN CYBER FORUM · kuppingercole ANALYSTS · IONOS CLOUD

main sponsors

EclecticIQ · enclaive

community contributors

Ovens · GitGuardian · LANCOM · RED ALERT LABS · wallix · XELERA

A Contribution to Europe's Digital Sovereignty

Our sponsors share a common belief: that Europe needs strong local champions, trusted technologies,and a resilient cybersecurity industry.

Your support demonstrates a commitment to:

- European digital sovereignty.
- open and collaborative innovation.
- responsible data governance.
- and the emergence of the next generation of European champions.

Because of you, we can showcase European excellence to corporations, investors, public institutions, and international markets.

A Growing Community We're Proud to Build Together

The 2025 Mapping was read, shared, and celebrated across Europe; and it was your support that allowed that momentum to grow.

In 2026, our community is larger than ever, and your contribution is one of the key reasons why more organisations are joining, sharing data, and reaching out to participate.

You help us build not just a document, but a living ecosystem. Thank You for Believing in This Project. To every sponsor, thank you for your trust, your encouragement, and your belief in what we are building together.

Your support is essential.
Your involvement is inspiring.
Your commitment makes this Mapping possible.

Together, we are not just documenting the cybersecurity landscape. We are helping shape the future of European cybersecurity.

Transparency, Trust, and Use of Funds

All funds received from our sponsors are entirely dedicated to the European Cybersecurity Mapping and related activities. The project is run on a strictly non-profit basis: sponsorship contributions are used exclusively to cover the concrete costs required to deliver this initiative, including data collection and processing, analysis, design and layout, printing, project management, associated events, website maintenance, and communication and dissemination efforts.

Our commitment to transparency and trust is not declarative but operational. Each year, the use of funds is presented and reviewed during the ECA General Assembly, and as stated in the statutes of the European Champions Alliance our expenses are examined by independent auditors. Sponsorship does not influence the methodology, content, or analysis of the Mapping.

Should any funds remain once the project costs are fully covered, they are reinvested in the actions of the European Champions Alliance (ECA) in support of its mission to strengthen Europe's cybersecurity ecosystem and digital sovereignty.

METHODOLOGY

The European Cybersecurity Mapping 2026 is the result of a long-term, structured, and iterative research effort conducted by the European Champions Alliance (ECA).

It combines historical data, multi-source analysis, and direct ecosystem engagement to deliver a reliable and actionable representation of Europe's cybersecurity landscape.

This edition builds on the 2025 Mapping, itself grounded in more than five years of continuous research and observation of the European cybersecurity ecosystem. This longitudinal approach ensures consistency over time, enables meaningful year-over-year comparisons, and allows the Mapping to capture structural trends rather than short-term signals.

SCOPE

The Mapping focuses exclusively on cybersecurity start-ups and scale-ups headquartered in Europe.

For the purposes of this study, Europe is defined as:

- the European Union
- the United Kingdom
- and Switzerland

Only companies with their operational and strategic headquarters located in these geographies are included. Subsidiaries of non-European groups are excluded.

This choice reflects the Mapping's core objective: to assess Europe's capacity to build and retain sovereign cybersecurity capabilities.

DATA SOURCES

The Mapping relies on a combination of complementary data sources to ensure depth, accuracy, and cross-validation:

- The historical ECA Cybersecurity Mapping database, continuously enriched since 2020.
- Publicly accessible professional and financial databases, including LinkedIn, Crunchbase, and PitchBook.
- Company websites, public filings, press releases, and freely available online information.
- Direct ecosystem intelligence gathered through interviews, events, and interactions with founders, investors, corporates, and institutions.

All company profiles were systematically reviewed and updated as part of the 2026 edition, with particular attention paid to company status, positioning, category assignment, and geographical footprint.

DIRECT COMPANY VALIDATION

To reinforce data quality and limit interpretation bias, all identified companies were contacted directly and invited to review and confirm the information collected about them.

While participation was voluntary and not all companies responded, a significant share of the ecosystem actively contributed to this validation process.

Validated inputs were integrated into the final dataset. For non-responding companies, information was retained only when corroborated by multiple reliable public sources.

INTEGRATION AND CLASSIFICATION

All collected and validated data was consolidated into a single structured dataset and classified according to the Mapping's analytical framework.

This structure is designed to make the Mapping usable not only as a visual landscape, but as a strategic tool for analysis, comparison, and decision-making.

A LIVING REFERENCE

The European cybersecurity ecosystem evolves rapidly. New companies emerge, others consolidate, pivot, or exit. The Mapping reflects the state of the ecosystem at the time of publication, based on the best information available.

It is not intended as a static directory, but as a living reference. Readers, founders, investors, associations, and institutions are encouraged to contribute corrections, updates, and additions to improve future editions.

This methodology reflects ECA's commitment to transparency, rigor, and neutrality; and underpins the Mapping's ambition:

to serve as the trusted reference for understanding, connecting, and scaling Europe's cybersecurity ecosystem.

TEAM & CREDITS

EDITORS-IN-CHIEF

Andrea VAUGAN and Dominique TESSIER
European Champions Alliance (ECA)

DATA COLLECTION & ANALYSIS

Stéphane GENDREL
Augment

DESIGN

INCYBER Forum design team
Special thanks to Marie-Laurence BICKEL

DISTRIBUTION

European Champions Alliance (ECA)

ACKNOWLEDGEMENTS

From the European Champions Alliance, we would like to warmly thank Stéphane GENDREL and Marie-Laurence BICKEL for their commitment, support, and close collaboration throughout the production of this Mapping. Their contributions were instrumental in bringing this edition to completion.

We also extend our sincere thanks to all sponsors, interviewees, partners, and contributors who shared their time, insights, and expertise. Their valuable input and engagement made this Mapping possible and significantly enriched the quality of the analysis.

European
Champions Alliance

HOW TO CITE AND REUSE THIS MAPPING

Building Europe's Future Together

REQUIRED ATTRIBUTION

Any reuse of content from this Mapping must include the following elements:

1. **Source name**
   European Champions Alliance (ECA)
2. **Title of the publication**
   European Cybersecurity Mapping 2026 – Start-up and Scale-up Landscape
3. **Year of publication**
   2026
4. **License**
   Creative Commons Attribution 4.0 International (CC BY 4.0)
5. **Link to the source (when applicable)**
   www.european-champions.org

STANDARD CITATION EXAMPLE

Short version (for slides, charts, visuals):

> Source: European Champions Alliance (ECA), European Cybersecurity Mapping 2026, CC BY 4.0

Full version (for reports, articles, academic or policy documents):

> Source: European Champions Alliance (ECA), European Cybersecurity Mapping 2026 – Start-up and Scale-up Landscape, 2026. Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). www.european-champions.org

EXAMPLE USE CASES

Using a chart or graphic in a presentation
Add the following in the footer or caption:

> © European Champions Alliance (ECA), European Cybersecurity Mapping 2026; CC BY 4.0

Quoting analysis in an article or report
Include a source note such as:

> Analysis based on data from the European Cybersecurity Mapping 2026, European Champions Alliance (ECA).

Adapting or remixing content (e.g. reworking a chart or dataset)
Indicate that changes were made:

> Adapted from: European Champions Alliance (ECA), European Cybersecurity Mapping 2026, CC BY 4.0.

WHAT IS NOT ALLOWED

- Implying endorsement by the European Champions Alliance without prior written consent
- Removing attribution or license references
- Presenting reused content as original work

QUESTIONS OR PERMISSIONS BEYOND CC BY 4.0

For uses not covered by the CC BY 4.0 license (e.g. exclusive use, co-branding, or official endorsements), please contact:

cybersecurity@european-champions.org

European
Champions Alliance

European Cybersecurity Mapping 2026

European Cybersecurity Excellence

START-UP & SCALE-UP EDITION

powered by

IN CYBER FORUM

strategic sponsors

Atos

kuppingercole ANALYSTS

IONOS CLOUD