



European
Champions Alliance

European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP & SCALE-UP EDITION

powered by

IN CYBER
FORUM

gold sponsors





European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION

The European Champions Alliance (ECA) promotes European technology and European values. We believe that Europe's strategic economic autonomy can be strengthened through a conscious business-related interdependence between European companies and all participants of the European economic ecosystem.

Europe must build a strong regional economic network to foster innovation and technologies. Embedding this network in the global world economy is indispensable, but should not prevent us from putting the defense of European interests and values at the center.

To achieve this goal, the ECA builds bridges between national ecosystems, SMEs, companies and other supporters of the tech ecosystem in Europe. We harness the power of smart collaboration and accelerate the growth of Europe's digital champions.

We want start-ups founded in Europe to take the technological lead in key technologies of the future, remain in European hands, and accompany, support and protect our citizens and industries in the digital age!

We are proud to present to you the new 2025 European Cybersecurity Start-up and Scale-up Mapping, designed by the European Champions Alliance with the valuable help of INCYBER FORUM.

WHY ANOTHER CYBERSECURITY MAPPING?

Our objective is three folds:

- Illustrate the dynamism and creativity of Europe's cybersecurity-focused vendors, which are growing in so many different parts of Europe
- Provide key insights into the technology and business trends in cybersecurity
- Point the way to the success of true European Champions.

Dynamism: We feature 828 companies from 24 countries. Together, they cover all the major cybersecurity threats, including the most malicious, such as zero-day attacks, supply chain lateral attacks, AI-based social engineering or threats to industrial OT systems.

Cybersecurity is an area that US (and often Israeli-American) companies are promoting. On the other hand, while we recognise that US players are often good salesmen and lobbyists, we believe that the European

industry presents an offer that is equal to that of these players, both in terms of functional coverage and efficiency, as well as technical stability.

Full threat coverage: European vendors cover all threat segments, including the most sophisticated and emerging attack vectors. It is useful to quote the [recent report](#) by the European Agency for the Security of Information Technology (ENISA), which details the main types of attacks observed in Europe over the last period. If we compare this solid analysis with this mapping, we can see that there is no attack segment that is not addressed by several European vendors.

Trends: This mapping shows an exceptional focus of vendors on "Threat Management". This is an evolution that has been constant for the last 5 years. Vendors tend to respond to the fact that many new types of attacks are appearing every day and that their infiltration path into the user's system is becoming more and more unpredictable. So we see a lot of R&D aimed at controlling the unexpected and stopping the most stealthy attacks.

Will this trend lead to a new landscape where users can benefit from a one-stop shop for cybersecurity? We believe that as criminals innovate, vendors will continue to offer brand-new solutions. On the other hand, we think vendors should take into account the growing demand from users to benefit from fully integrated solutions that offer at least a broad range of functionality.

Another area where vendors are coming out in force is "Data Protection". The idea here is resilience: whatever shields you have around or even within your IT system, someone can find their way into some part of it, so users should not only reduce their exposure but also the impact of a successful attack.

No data loss and the ability to recover quickly are the keywords. And efficient data protection is at the heart of it.

Of course, there are different ways of protecting data, such as using truly secure storage or encrypting data wherever it is stored.

Incidentally, data is another area where the European offer is fundamentally different. Europe values data ownership and privacy, whereas US vendors often do not care about capturing users' data (and that is a bit of an understatement).

Beyond these two areas, we can see some other trends. Email security remains a key area, as phishing is a major means of infiltration. The application layer (e.g. web and API filtering) should not be neglected, as these attack vectors can be underestimated. IAM (Identity and Access Management) remains an essential element of security, especially as so many organisations move their processes and data to the cloud. Industrial OT security is becoming a major issue as industry becomes a matter of connected sensors and monitoring.

If you had to sum up all these functional areas in a few words, it would probably be "Zero Trust" and "resilience". This probably starts with looking at our IT systems differently: building systems where a successful intrusion cannot do much harm and cannot disrupt the whole operation.

SO WHAT ARE THE CHALLENGES?

While it's important for European vendors to continue to adapt to an evolving threat landscape and take advantage of new technologies such as AI, they must also take into account the following issues:

User demand: it tends to be for easy-to-use solutions. Fragmented offerings create an integration problem that users are increasingly reluctant to accept. Vendors could consider articulating their offers so that users are not forced to do the work of integration.

Consolidation: Articulation between different products could be a first step, but cybersecurity is a field that requires constant R&D efforts, so it could one day be difficult to support such efforts if the commercial surface is not wide enough. The US has largely started down this path. European vendors are also facing this strategic challenge.

Financing: As cybersecurity vendors scale and begin to see consolidation as a necessary horizon, one way or another, the ability of the European financial sector to support such a move will be called into question. Mario Draghi's and Enrico Letta's reports call for the creation of a single European financial market. Needless to say, we agree.

We sincerely hope that you will enjoy the interviews and insights presented in this mapping. Our goal is to provide valuable perspectives and contribute meaningfully to the growth and development of the European cybersecurity ecosystem.

Together, let's continue to strengthen and innovate in the vital field of European cybersecurity.



Dominique TESSIER
Head of Cyber
ECA



Andrea VAUGAN
Secretary General
ECA



Valentin VANDEKERCHOVE
Data Project Lead
ECA, ESSEC/Telecom Paris

IN CYBER
FORUM
EUROPE

1-3 APRIL
2025
LILLE GRAND PALAIS

➤ europe.forum-incyber.com

IN CYBER
FORUM
USA

17-18 JUNE
2025
SAN ANTONIO, TEXAS, USA

➤ usa.forum-incyber.com

IN CYBER
FORUM
CANADA

14-15 OCT.
2025
PALAIS DES CONGRÈS, MONTRÉAL

➤ canada.forum-incyber.com

IN CYBER
FORUM
JAPAN

DEC. 2025
TOKYO, JAPAN

➤ japan.forum-incyber.com

Promoting innovation and bolstering investment

Eight of the top ten countries on the 2024 National Cyber Security Index are European. This ranking reflects their success in implementing legal, technical, organizational, operational, and international cooperation measures to effectively manage cyber risks.

This maturity also translates to the economic front, with the European cybersecurity market valued at approximately €130 billion annually, growing at a rate of 17% per year. The sector is powered by a dynamic ecosystem of around 60,000 companies and 660 centers of expertise specializing in cybersecurity.

However, these achievements should not overshadow the numerous challenges faced by Europe's cybersecurity ecosystem: the lack of global leaders, fragmented solutions, disjointed intra-European markets, and dependency on U.S. infrastructures, to name a few. In an era defined by the "platformization" and "cloudification" of the digital and cybersecurity landscape, these challenges are substantial.

This is where the European Champions Alliance's mapping of European cybersecurity providers proves invaluable. It offers a comprehensive overview of the European cybersecurity industry, highlighting its strengths and weaknesses alike. Beyond mere observation, the ultimate goal is clear: to act decisively on key levers that address weaknesses and capitalize on strengths—whether through investment, industrial policy, enhanced interoperability between solutions, or improved procurement policies for businesses and public organizations.

The InCyber Forum – Europe is fully committed to supporting the European cyber ecosystem with two key priorities: promoting innovation and bolstering investment. This commitment is exemplified by the InCyber Start-up Award, which annually recognizes particularly promising start-ups, and the Invest InCyber Day, held alongside the Forum, where public and private investors, investment bankers, corporations, and accelerators gather to explore major market trends.

We are therefore delighted to partner with the European Champions Alliance on this mapping initiative!



Guillaume TISSIER
Managing Director
INCYBER FORUM EUROPE



Editors-in-Chief

Andrea Vaugan, Managing Director
and Secretary General, European
Champions Alliance

Dominique Tessier, Head of Cyber-
security, European Champions
Alliance

Data Analysis

Valentin Vandekerchove

Graphic Designer

Marie-Laurence Bickel, INCYBER

Contributors

Guillaume Tissier, INCYBER
Marco Eckardt, ECA
Lauri Ylä-Mononen, ECA
Ignacio Sbampato, ECA
Georgios Kotsougianis, ECA
Patrick Hollenbeck, ECA

Distribution

European Champions Alliance
FORUM INCYBER
Postal and online distribution

Printing

Publisher of this Document
European Champions Alliance

Contact

Email: [cybermapping@
european-champions.org](mailto:cybermapping@european-champions.org)

Website: european-champions.org

Recommended Citation

European Champions Alliance (Ed.)
Cybersecurity Focus Group
European Cybersecurity Mapping 2025
Paris, 2025

About the European Champions Alliance

The European Champions Alliance
is a non-profit association founded
in 2020 as a business-driven and
inclusive platform to help small,
fast-growing businesses create
more European tech champions.

COPYRIGHT NOTICE

© European Champions Alliance
(ECA), 2025

This publication is licensed under
CC-BY 4.0. Unless otherwise noted,
the reuse of this document is autho-
rized under the Creative Commons
Attribution 4.0 International (CC BY
4.0) license ([https://creativecommons.
org/licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/)). This means
that reuse is permitted, provided that
appropriate credit is given to the
European Champions Alliance and any
changes made are clearly indicated.

For any use or reproduction of photos,
graphics, or other materials that
are not under the copyright of
the European Champions Alliance,
permission must be sought directly
from the copyright holders.

TABLE OF CONTENT

INTRODUCTION	9
SPONSORS	12
METHODOLOGY	16
INTERVIEWS & MAPPING	18
VALUE CHAIN IN CYBERSECURITY	70
CONCLUSION	114

European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION



European Cybersecurity Mapping 2025

European Cybersecurity Excellence
START-UP AND SCALE-UP EDITION

ACKNOWLEDGEMENTS

The European Champions Alliance (ECA) would like to express its heartfelt gratitude to all the partners, stakeholders, and contributors who have supported the development of this mapping project. We are particularly thankful to Incyber for their invaluable support in helping us bring this initiative to life. Their commitment and dedication to fostering a stronger European cybersecurity ecosystem have been instrumental in this project's success.

We would also like to acknowledge the **input and collaboration of various ecosystem players, industry experts, and associations** who shared their insights, feedback, and expertise, enriching the content and scope of this mapping. Their contributions ensure that this work reflects the dynamic and diverse European cybersecurity landscape.

INTRODUCTION

DISCLAIMER

This cybersecurity mapping has been compiled for informational purposes only and is accessible free of charge. While we have made every effort to provide accurate and up-to-date information, we cannot guarantee the accuracy of the categorization or completeness of the list of companies included.

CATEGORIZATION AND CORRECTIONS

Companies included in this mapping may not be assigned to the most appropriate category. If your company is listed and you believe it has been miscategorized or omitted, please contact us at cybermapping@european-champions.org to request rectification or provide additional information. We welcome your feedback to improve the quality of this mapping.

INTERVIEWS AND OPINIONS

This mapping contains interviews with various experts and stakeholders. The views and opinions expressed in these interviews are solely those of the interviewees and do not necessarily reflect the views or opinions of our organization or its members.

USE OF INFORMATION

This mapping is intended as a general resource for understanding the European cybersecurity landscape. It should not be considered as professional advice, endorsement, or validation of the companies listed.

LIABILITY

Our organization accepts no liability for any errors, omissions, or inaccuracies in this mapping, nor for any decisions made based on the information provided herein. Users are encouraged to conduct their own research and verification before relying on any information from this document.

THIRD-PARTY SOURCES

Third-party sources are quoted where appropriate. The European Champions Alliance is not responsible or liable for the content of external sources, including external websites referenced in this publication.

FUTURE UPDATES

The European Champions Alliance reserves the right to alter, update, or remove this publication or any of its content. This mapping is a dynamic project and will be periodically updated. However, we cannot commit to real-time corrections or immediate updates.

By accessing and using this mapping, you acknowledge and agree to this disclaimer. For any inquiries or corrections, please contact us at cybermapping@european-champions.org.



No Sponsors, no Mapping! *Thank you for your help!*

We extend our deepest gratitude to all our sponsors who have supported us financially and through their willingness to foster the growth of this ecosystem. Your contributions are not just investments in an initiative but in a vision — a strong, interconnected European network capable of facing the challenges of today and tomorrow.

The work we do is vital, and we take pride in building something meaningful. But to ensure its quality and reach, we need continued support. Building an ecosystem is not about lead generation or immediate returns. It's about investing in the foundation of a deeply rooted network — a network that empowers innovation, collaboration, and shared progress across Europe.

We encourage everyone who shares this vision to join us in building this ecosystem. Together, we can create a Europe where ideas flourish, connections strengthen, and opportunities abound for all.

Thank you for believing in and contributing to this mission.

Let's keep building, together.



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.

redalertlabs.com
cyberpass.com



AD FONTES

AD FONTES

Ad Fontes is a law firm based in Berlin and Paris, specialized in international business, labour, and corporate law. Founding partner Grit Karg is a renowned expert in data privacy, compliance, and digital regulation. Ad Fontes stands out by offering an integrated approach to cybersecurity with Sven Zehl, a recognized expert with extensive knowledge in cybersecurity and compliance. Core services include the CyberRiskCheck and PrivacyCheck.

adfontes.law



GOLD
SPONSORS



START-UP
SPONSORS



G+D VENTURES is an early-stage VC focusing on Cyber Security and TrustTech in Europe. The fund is driven by financial returns and backed by the European Investment Bank and the G+D Group, a Security-Tech company.

HI NOV is a European B2B fund made by entrepreneurs for entrepreneurs and based in Paris, Lyon and Munich. Hi inov supports outstanding hyper-growth companies that transform the ever-changing services and industrial landscape with their innovative digital deep-tech technologies.



UBCOM is a cybersecurity consultancy with a unique focus on sovereignty. Based in Switzerland, it benefits from constitutional protections, secrecy, and encryption capacities free from extraterritorial laws. UBCOM ensures top-tier cyber protection via sovereign solutions, securing sensitive data against economic intelligence and industrial espionage threats.

ECLECTICIQ is a global provider of threat intelligence technology and services that empower customers to neutralize critical cyber threats. Guided by our values — being curious, bold, accountable, and collaborative — we help security teams make smarter, faster decisions with dynamic solutions that reduce complexity and streamline threat detection and response.



ATEMPO is a leading independent European-based software vendor with an established global presence providing data resilience and management platforms. Atempo offers a complete range of solutions to protect, store, move and recover all mission-critical data sets for thousands of companies worldwide.



NYMIZ AI-powered B2B SaaS platform for data masking. Nymiz identifies and masks sensitive data in various formats using tokenisation and synthetic replacement techniques.



HARFANGLAB is an EU cybersecurity expert, providing cutting-edge endpoint security solutions to shield organizations from cyber-threats while preserving strategic autonomy.

A heartfelt Thank You to our partners

We want to extend our deepest gratitude to all of our partners, especially the cybersecurity associations across Europe, for their invaluable contributions to the 2025 European Cybersecurity Mapping. Your expertise, insights, and support in identifying start-ups and shaping the ecosystems have been instrumental in creating this comprehensive resource.

Together, we are not just mapping the landscape but fostering collaboration, innovation, and resilience in Europe's cybersecurity sector. Thank you for being an essential part of this journey and for your unwavering commitment to strengthening Europe's digital future.

Special thanks to our contributors who helped us map their ecosystems

- **SPAIN:** Marco Eckardt, member of the ECA volunteer group
- **FINLAND:** Lauri Ylä-Mononen, member of the ECA volunteer group
- **POLAND:** Ignacio Sbampato, member of the European Champions Alliance
- **GREECE:** Georgios Kotsougianis, Member of the ECA Supervisory Board

Special thanks also to Patrick Hollenbeck, member of the ECA Volunteer Group for the support in reaching out to the ecosystem and animating the community.

Do you want to become a volunteer at the ECA? Reach out to us at cybermapping@european-champions.org



SILVER
SPONSORS



European Cybersecurity Mapping 2025

European Cybersecurity Excellence
START-UP AND SCALE-UP EDITION

EMPOWERING THE EUROPEAN CYBERSECURITY ECOSYSTEM

Cybersecurity is not just a technology challenge; it's a cornerstone of Europe's digital sovereignty, political and economical resilience. With cyber threats escalating and innovation accelerating, understanding the ecosystem of start-ups and scaleups is critical for fostering collaboration, driving investment, and building a secure digital future.

The **2025 European Cybersecurity Mapping** is designed to provide a clear, comprehensive, and actionable overview of the players shaping the European cybersecurity landscape—empowering decision-makers, innovators, and investors alike.

METHODOLOGY

How to Make the Mapping Work for You

1. STRATEGY

The Mapping helps business leaders, policymakers, and investors identify key trends, emerging technologies, and untapped opportunities in cybersecurity to shape informed strategic decisions.

2. NETWORKING

Discover and connect with over 828 cybersecurity start-ups and scaleups across 20+ countries. The Mapping serves as a gateway to building meaningful partnerships and collaborations across the ecosystem. So important as customers tend to prefer integrated, functionally rich solutions

3. INVESTMENT

For VCs and investors, the Mapping highlights promising companies by category, size, and specialization, making it easier to identify the next big opportunities in European cybersecurity.

4. BENCHMARKING

Gain insights into how cybersecurity start-ups and scaleups compare across Europe. The Mapping enables companies to assess their position relative to peers in the industry.

5. HIRING

Talent managers and HR professionals can use the Mapping to identify companies driving innovation in cybersecurity, potentially unlocking new talent pools and partnership opportunities.

6. MARKET RESEARCH

Understand the competitive landscape, product categories, and regional ecosystems to support product development, go-to-market strategies, and expansion into new markets.

7. ECOSYSTEM ANALYSIS

Industry organizations and clusters can use the Mapping to assess the maturity and competitiveness of their regional or national cybersecurity ecosystems, identifying opportunities for growth and collaboration.

8. PARTNERSHIP BUILDING

At a time when customers seek solutions with wider functional range, corporations and cybersecurity vendors can identify potential technology partners or acquisition targets to enhance their product offerings and market reach.

9. EDUCATION AND TRAINING

Universities and training organizations can use the Mapping to identify leading companies and technology trends, shaping their curriculum to better prepare the next generation of cybersecurity professionals.

10. TECHNOLOGY SCOUTING

R&D teams and technology scouts can use the Mapping to discover innovative solutions and technologies addressing specific cybersecurity challenges.

11. COMPETITIVE INTELLIGENCE

Businesses can analyze their competitors' positioning and offerings through the Mapping to refine their strategies and stay ahead in the market.

12. POLICY DEVELOPMENT

Governments and policymakers can leverage the Mapping to understand the strengths and gaps in their national cybersecurity ecosystems, guiding the development of supportive policies and regulations.

Interview Ecosystem Supporter

AD FONTES



We see in our practice that EU-providers can in fact carve out a strong market position by offering tangible compliance evidence with concrete and GDPR based explanations of data flows and relevant certifications. Choosing a trusted cybersecurity provider strengthens customers' trust in the company and is a building block for an approach that integrates data privacy compliance and cybersecurity in the long term.



You operate at the interface between cybersecurity and law. How are both interrelated?

Cybersecurity focuses on preventing unauthorized access and protecting systems, while data privacy ensures personal data is handled

lawfully and ethically. Even though the scope is different - cybersecurity protects all data and systems, while privacy focuses on individuals' rights over personal data - both are strongly interconnected: Privacy regulations, like GDPR, or the various new EU regulations, drive cybersecurity priorities by defining protection requirements. Strong cybersecurity measures are vital for asset protection but also for achieving data privacy, as breaches compromise personal information. Due to this interconnection, it is so important for us to create a holistic approach allowing our clients to address both topics at the same time.

How can companies effectively manage both the risks posed by cyber threats and those arising from non-compliance with European and national legal rules?

In both domains - cyber threat landscape and EU/national regulation - complexity is growing at a fast pace. The EU has recently adopted several key measures, as the NIS2 directive or the Cyber Resilience Act, which aim to constitute a comprehensive approach to bolstering cybersecurity. Those regulations impose significantly stricter cybersecurity obligations on companies and increase C-level liabilities. Also the AI Act requires AI systems to comply with cybersecurity standards. In fact, cybersecurity is becoming law. We think this is a positive development in today's digital landscape, where cyber threats are increasingly sophisticated and pervasive. Our value is to help our clients operate in good balance between more or less flexible regulatory mechanisms and innovation and security needs.

What first steps would you recommend for a EU based medium-sized company that doesn't yet have a comprehensive technical and regulatory cybersecurity strategy?

The first crucial step is for the management to acknowledge cybersecurity as a strategic priority. This requires understanding the potential financial, operational, and reputational risks posed by cyber threats and regulatory non-compliance. For this purpose we conduct for our clients leadership briefings or workshops, emphasizing the impor-

tance of a comprehensive strategy. Operational kick-off is typically a risk assessment identifying assets to protect, risks and gaps. Such assessment is for example the CyberRiskCheck developed by the German BSI, ideally in combination with a Privacy Check. This is a standardized risk check, specifically developed for middle-sized companies. After an interview session, the company receives a report containing the score and concrete recommendations, structured according to urgency. The CyberRiskCheck enables a company to determine its own IT security level, highly relevant for cybersecurity insurability or funding rounds. It is a method recommended by German BSI to approach the NIS2 cybersecurity requirements.

Many U.S.-based cybersecurity providers seem often less transparent about their data processing while European providers tend to prioritize privacy. What criteria should companies use when choosing a cybersecurity service provider?

Outsourcing cybersecurity to a provider is a strategic choice. It gives access to advanced tools and technologies and allows the company to focus on its core business. The choice of providers should follow a structured process. Security capabilities, adaptability, scalability and pricing are essential procurement criteria but shall be completed by clear compliance requirements as companies are responsible for GDPR compliant processing of their providers. Compliance criteria are in particular minimization principles, data privacy policies, data sharing with third parties, auditability and transparency on encryption standards. We see in our practice that EU-providers can in fact carve out a strong market position by offering tangible compliance evidence with concrete and GDPR based explanations of data flows and relevant certifications. Choosing a trusted cybersecurity provider strengthens customers' trust in the company and is a building block for an approach that integrates data privacy compliance and cybersecurity in the long term.



Ad Fontes is a law firm based in Berlin and Paris, specialized in international business, labour, and corporate law. Founding partner Grit Karg is a renowned expert in data privacy, compliance, and digital regulation. Ad Fontes stands out by offering an integrated approach to cybersecurity with Sven Zehl, a recognized expert with extensive knowledge in cybersecurity and compliance. Core services include the CyberRiskCheck and PrivacyCheck.

adfontes.law



Grit KARG
Partner

Ad Fontes



Sven ZEHL
Cybersecurity Expert

Ad Fontes

Interview Scale-up

RED ALERT LABS



European consolidation is indeed necessary to strengthen the region's cybersecurity landscape. I believe institutions play a vital role in creating the policy framework that encourages consolidation. However, large users and integrators also have an incentive—they drive demand for unified solutions, and their active push would accelerate this process.



In a few words, what is your domain?

Red Alert Labs specializes in IoT cybersecurity. We help businesses manage risk and achieve compliance for their connected products through consulting, evaluation, and our AI-driven platform, CyberPass.

In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027 in technology and in customer's behaviour?

Since 2020, there's been a major evolution in how cybersecurity standards and regulations, like RED Directive, Cyber Resilience Act, ETSI EN 303 645 and EN 18031, have impacted IoT manufacturers and suppliers, creating pressure to comply with standard practices. We've also seen an increased reliance on connected devices, which has amplified cybersecurity threats. By 2027, I anticipate a shift toward more integrated cybersecurity compliance solutions, driven by AI and automation. Customer behaviour will lean toward demanding greater transparency in how vendors protect their products, pushing companies to provide proactive, end-to-end compliance management.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

European vendors can meet this challenge by embracing shared platforms that allow collaboration on core R&D efforts, which helps cut costs. Initiatives like CyberPass provide a standardized way to manage compliance, enabling vendors to leverage collective knowledge and streamlined certification processes, ultimately reducing the burden of separate investments.

Some say customers, especially in Europe, are fed up with scattered cybersecurity offerings and would prefer to find already integrated solutions. Do you agree? If yes, how do you meet or prepare to meet such a trend?

Yes, we agree. Customers are increasingly seeking simplicity and prefer integrated solutions to fragmented services that require multiple vendors. To meet this trend, we created CyberPass—an AI-powered platform that consolidates various aspects of compliance management into one unified solution. This allows us to offer an end-to-end approach that's easy to deploy and reduces the complexity customers often face.

Is European consolidation an actual perspective according to you? If yes, who should push the move: the institutions? The large users? Some large integrators? Vendors themselves?

European consolidation is indeed necessary to strengthen the region's cybersecurity landscape. I believe institutions play a vital role in creating the policy framework that encourages consolidation. However, large users and integrators also have an incentive—they drive demand for unified solutions, and their active push would accelerate this process. Vendors themselves should not wait; proactive engagement helps position them as early leaders in a consolidated market.

The EU has set up cybersecurity regulations; does that help? More generally, what do you expect from EU Authorities?

Yes, EU regulations such as the Cyber Resilience Act and RED Directive have helped by creating a clearer path for security expectations and compliance. However, we expect EU Authorities to provide more incentives for compliance, such as funding for SMEs to meet standards or establishing trust marks that reward secure practices. In addition, more uniformity across member states would help create a true single market for cybersecurity compliance services.



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.

redalertlabs.com
cyberpass.com



Roland ATOUI
Managing Director

Red Alert Labs

MAPPING SYSTEM & CRITERIA

The analyses conducted reveal that the scope of cybersecurity has significantly expanded since our 2022 mapping. For the 2025 edition, we have included 828 companies, which is 444 more than in 2022 (when the mapping featured 388 companies)—more than doubling the entries. This significant growth is attributable to two main factors:

- 1. A Broader and More Comprehensive Mapping:** The 2025 mapping covers more countries and incorporates additional data points, making it the most exhaustive version to date.
- 2. A Rapidly Growing Sector:** The cybersecurity field continues to evolve at an extraordinary pace, with many new companies founded over the past two years, reflecting its dynamic and prolific nature.

In this mapping, companies have been categorized based on their primary product focus to reflect their main area of expertise. Furthermore, we distinguish between two classifications: **Start-ups & Scale-ups**.

ADDITIONAL NOTES

In some cases, we applied minor waivers to the scale-up criteria for companies operating in transformative spaces. Companies with insufficient information were generally placed in the Start-up category.

If your company should be in a different category, contact us at cybermapping@euro-pean-champions.org. We will review your request and update it in the 2026 edition.

This classification aims to provide clarity and showcase the diversity of Europe's cybersecurity ecosystem. Let's continue building it together!



Start-ups

Start-ups are emerging companies or frontrunners in new technologies, showing strong potential for innovation and growth.

Definition: Early-stage companies to watch, focusing on breakthrough or pioneering technologies.

SELECTION CRITERIA:

Market presence: **1–10 years**

Turnover: **Around €1M**

Full-Time Employees (FTE): **15–40**

VC Funding: **≥ €1–5M**



Scale-Ups

Scale-ups are more established companies that have achieved significant growth milestones and market traction.

Definition: Companies in the growth stage or SMEs in active expansion.

SELECTION CRITERIA:

Market presence: **5–15 years**

Turnover: **€5 and above**

Full-Time Employees (FTE): **40 and above**

VC Funding: **≥ €5 and above**

OVERVIEW AND ANALYSIS OF CATEGORIES IN THE CYBERSECURITY MAPPING

Master category	Start-up	Scale-up	TOTAL
Threat management	116	36	152
Cloud & Data protection	107	38	145
Identity & Access Management	97	32	129
OT Security	39	19	58
Vulnerability assessment platform	47	10	57
Endpoint Security	38	7	45
Network Security	32	12	44
Application Security	29	11	40
Cyber Governance	27	3	30
Secure communication Platform	23	4	27
Fraud prevention & detection	23	4	27
Cryptography	15	6	21
Sensibilisation platform	14	3	17
Email Security	10	6	16
Code Checking	10	2	12
AI security & Integrity	6	1	7
TOTAL	633	194	828

LOOKING AHEAD

While every effort has been made to provide a comprehensive overview of the cybersecurity landscape, we acknowledge that the mapping is a work in progress. We are aware that it is not yet complete, but we have made our best effort to collect as many companies as possible, leveraging a wide variety of data sources to ensure diversity and representation.

Feedback and insights from stakeholders are invaluable as we strive to refine this project. Collaboration will be key in closing data gaps and enhancing the accuracy of future editions.

In our effort to showcase the European cybersecurity ecosystem, we categorized the 828 companies across 16 key segments, representing the most critical areas of cybersecurity innovation and activity. This classification highlights the diversity of solutions and services essential to addressing today's evolving threats while enabling stakeholders to identify trends, key players, and areas of opportunity.

The mapping reveals a landscape dominated by start-ups (633 companies, 77%) and complemented by scale-ups (194 companies, 23%), illustrating the dynamic nature of the European cybersecurity market.

Certain categories stand out for their concentration of companies, underscoring their importance in the current market:

- **Threat Management** leads the way with **152 companies (18,3%)**
- **Cloud & Data Protection** follows closely with **145 companies (17,5%)**
- **Identity & Access Management (IAM)** rounds out the top three with **130 companies (15,6%)**

Together, these top three categories account for **426 companies (51,4%)**, demonstrating their central role in addressing today's cybersecurity challenges. The remaining categories collectively host **400 companies (48%)**, indicating a somewhat diversified but uneven distribution across other segments.

NICHE AND EMERGING AREAS

While some domains like Threat Management and Cloud & Data Protection are heavily represented, others like OT Security (58 companies, 7%) and Cryptography (21 companies, 2,6%) are less populated, reflecting more niche areas of activity. Notably, AI Security and Integrity (6 companies) and Code Checking (11 companies) reveal critical gaps where the ecosystem may require further development and investment.

This categorization serves as a guide to understanding the structure of the cybersecurity ecosystem and its priorities. It highlights key domains driving innovation while identifying underrepresented areas that could present future growth opportunities.

ANALYSIS OF COMPANY SIZES IN THE CYBERSECURITY MAPPING

The dataset also categorizes the 828 companies by their employee size, offering insights into the distribution of start-ups and scale-ups based on workforce size.

Number of employees	Number of companies
2 - 10	120
11 - 50	268
51 - 200	92
201 - 500	32
501 - 1.000	11
1.001 - 5.000	14
5.001 - 10.000	2
10.001 +	5
NO DATA	284
TOTAL	828

KEY OBSERVATIONS

- Small Companies Dominate:**
 - The majority of companies (47%) fall into the **11–50 employees** range, with **268 companies**
 - An additional **120 companies** (15%) are even smaller, with just **2–10 employees**
 - Together, these two smallest categories account for **47% of the total mapped companies** (389 out of 828)
- Mid-sized Companies:**
 - Companies with **51–200 employees** represent the next significant category, comprising **92 companies (11%)**
 - **32 companies (3.7%)** have **201–500 employees**, showing fewer players in this mid-tier size range
- Large Companies:**
 - Only **32 companies (3.8%)** exceed **500 employees**, with the largest size range (**10,001+ employees**) including just **5 companies**. However, it should be clear that these big companies are mostly in Services, the activity as vendor being just one part of their scope
- Unreported Data:**
 - Due to resource constraints, we were unable to retrieve this missing data for this edition (284 or 34.6%). However, we plan to address this in the 2026 mapping to provide a more comprehensive overview.

The data highlights that the cybersecurity sector is largely composed of small to medium-sized enterprises (SMEs), which are driving much of the innovation. Larger companies are relatively rare, reflecting the fragmented and start-up-centric nature of the industry. Future mappings will aim to close the data gaps for even greater accuracy and insight.

ANALYSIS OF THE CYBERSECURITY LANDSCAPE BY COUNTRY

KEY INSIGHTS

- Dominance of France:**
 - France leads the cybersecurity mapping, with **311 companies**, representing 37.6% of the total mapped entities.
 - It hosts 70 scale-ups (35.9% of total scale-ups) and 241 start-ups, underlining its status as a hub for cybersecurity innovation and growth in Europe. This dominance could partly reflect the historical strength of our data collection from France.
- The Netherlands and Germany:**
 - The Netherlands follows with **148 companies** (17.6%), driven largely by its 132 start-ups and relatively smaller number of 16 scale-ups, highlighting it as an emerging start-up hotspot.
 - Germany ranks third with **96 companies (12%)**, featuring a more balanced mix of 50 scale-ups and 46 start-ups, suggesting a more mature and stable ecosystem compared to the Netherlands.
- Switzerland and Regional Leaders:**
 - Switzerland stands out with **78 companies (9.2%)**, led by 21 scale-ups and 57 start-ups, positioning itself as another robust player in the European cybersecurity market.
 - Other noteworthy contributors include:
 - **Estonia (46 companies)**, showcasing its strength as a digital and cybersecurity pioneer in the Baltics.
 - **Poland (32 companies)** and the **United Kingdom (25 companies)**, both contributing to the growing cybersecurity landscape in Eastern and Western Europe.
- Smaller but Active Players:**
 - Countries like **Greece (13 companies)**, **Spain (12 companies)**, and **Finland (12 companies)** are making steady progress, contributing innovation in niche cybersecurity domains.
 - **Denmark, Belgium**, and the **Czech Republic** each host **10 or fewer companies**, showcasing their smaller, more concentrated ecosystems.
- Sparse Representation:**
 - Several countries, such as **Ireland, Romania, Slovakia, Norway, Lithuania** and **Hungary**, each have **3 or fewer companies**, reflecting nascent ecosystems or lower activity in cybersecurity.

This geographical breakdown of the cybersecurity ecosystem reveals significant insights into the distribution of start-ups and scale-ups across Europe. However, it's important to note that the data may reflect some bias, as historically, we have had the most accurate data from France. Efforts are underway to improve this for the 2026 edition with the support of the broader ecosystem.

ACTION PLAN FOR STRENGTHENING THE EUROPEAN CYBERSECURITY ECOSYSTEM

OBSERVATIONS ON SCALE-UP VS. START-UP DISTRIBUTION

- Most countries show a higher concentration of **start-ups**, reflecting the overall dynamism of the cybersecurity market and its potential for growth.
- Scale-ups are concentrated in more mature markets like **France, Germany** and **Switzerland**, which benefit from stronger investment ecosystems and established innovation hubs.

GEOGRAPHICAL TRENDS AND INSIGHTS

- **In terms of number of vendors, Western Europe** dominates the cybersecurity landscape, driven by powerhouses like France, the Netherlands, and Germany. In terms of revenue size, while Switzerland hosts one of the main European cybersecurity vendor, France counts only one company with revenues >75 M€, Germany only two with revenues >75 M€ but has a bunch of entities in the range of 30-50 M€.
- **Central and Eastern Europe (e.g., Poland, Estonia, Czech Republic)** show promising activity, with Estonia standing out, likely benefiting from its national focus on digital resilience and e-government systems. On the other hand, Eastern Europe is home of the biggest European vendors (ESET from Slovakia, Avast from the Czech Republic and BitDefender from Romania and NORDIC SECURITY from Lithuania).
- **In the Nordics** the number of companies is small, but their size can be remarkable, with two vendors with revenues >= 100 M€ (Signicat from Norway and WithSecure from Finland).
- **Southern Europe (e.g., Spain, Italy, Greece)** lags slightly in the number of companies but shows potential for growth in targeted sectors.

Data Gaps and Future Improvements

- While this mapping provides valuable insights, we acknowledge a potential bias in the data due to historically stronger coverage from France. This could partially explain the high representation of French companies. For the 2026 edition, we will work closely with the broader cybersecurity ecosystem to enhance data accuracy and achieve more comprehensive geographical coverage.

Conclusion

- The cybersecurity landscape in Europe is highly diverse, with clear regional leaders like France, the Netherlands, and Germany driving the sector. While Western Europe dominates, growth opportunities are evident in Central and Eastern Europe. Closing data gaps and improving representation will further enrich future mappings, ensuring a more balanced and holistic view of the European cybersecurity ecosystem.
- To ensure this mapping was as comprehensive as possible, we reached out to numerous **industry associations** and stakeholders across Europe to collect accurate and up-to-date information. While we believe this mapping provides a robust snapshot of the ecosystem, we acknowledge that some regions may still be underrepresented.
- Looking ahead to the **2026 edition**, we aim to enhance the geographical coverage even further. If your country, region, or organization should be included or if you wish to collaborate with us, please do not hesitate to contact us at cybermapping@european-champions.org.
- Together, we can continue to build a more inclusive and representative map of Europe's cybersecurity ecosystem.

The Early Ecosystem: Between 1980 and 2000, the number of companies founded remains relatively low, reflecting the nascent stage of the cybersecurity market at that time. Few players existed, and the focus on cybersecurity as a standalone industry was minimal.

Growth After 2000: The majority of companies were founded **in the 2000s and 2010s**, reflecting the rise of digital technologies and the growing importance of cybersecurity in response to emerging threats.

Notably, there is a marked increase in company formation **starting in 2010**, with a consistent upward trend in the following years.

Peak Founding Period: The most active period for company creation was between **2015 and 2019**, with the highest number of companies founded in **2018 (42)** and **2017 (40)**. This surge aligns with the increasing digitization of economies, the rise of cloud computing, and a heightened awareness of cybersecurity risks.

Recent Activity: While company formation has slowed slightly in the most recent years (2022–2023), this could be due to reporting delays or economic uncertainties, such as those caused by the COVID-19 pandemic. However, **2021 (20 companies)** still saw significant activity, indicating sustained interest in the sector. Moreover, during 2023 - 2024, while cybersecurity has continued to grow, it has been at a lower pace. The breeding pond of young companies triggers less scale ups through organic natural growth. Which suggests that the strategic issue of consolidation should be considered, as many stakeholders see it as a necessary step in the building of true European champions.

In total, out of 828 vendors, only half a dozen or so can pretend to be an unicorn by valutation.

INTERPRETATION OF THE DATA

While the dataset is incomplete and should be viewed as indicative rather than definitive, the available data highlights key trends:

- The cybersecurity ecosystem has seen exponential growth over the past two decades, driven by the digital transformation of businesses and the increasing need to protect sensitive data.
- The peak in company formation around 2015–2019 suggests a wave of innovation during this period, fueled by emerging technologies like AI, IoT, and cloud computing.

The founding year data provides valuable insights into the evolution of the European cybersecurity ecosystem. While we acknowledge that we do not have founding year data for a large portion of the companies—this information can be challenging to retrieve—our dataset covers nearly half of the mapped companies. This serves as an indicative snapshot of trends and historical developments in the sector.

CHALLENGES AND FUTURE IMPROVEMENTS

- We are aware that founding year data is missing for a large number of companies in our mapping. This information can be difficult to retrieve due to variations in data availability across regions and company types. However, for the 2026 edition, we aim to collaborate with the ecosystem to enhance the completeness of this dataset, providing a more comprehensive view of the sector's evolution.
- Despite the limitations, the data we have gathered sheds light on the dynamic and rapidly evolving nature of the European cybersecurity market, offering valuable insights for stakeholders. This historical perspective is crucial for understanding the industry's growth trajectory and identifying future opportunities.

Interview Ecosystem Supporter

HI INOV



Europe needs to focus on creating ecosystems that integrate cybersecurity solutions directly into infrastructure development. Start-ups specializing in cyber-resilience for critical sectors like healthcare, energy, and finance will play a central role in this transformation. Collaboration between governments, large enterprises, and innovative start-ups is critical to addressing these challenges holistically.



What are the most pressing challenges Europe faces in achieving data sovereignty, and how do you see start-ups contributing to this goal?

Europe is at a critical juncture in defining its digital sovereignty. The challenge lies in building and securing infrastructure that aligns with our regulations while avoiding dependencies on non-European technologies. Start-ups play a pivotal role here, as they are agile enough to develop tailored solutions in areas like secure cloud services, encryption, and sovereign AI platforms. Supporting these start-ups through funding and scaling opportunities will be key to safeguarding Europe's digital independence.

How do you envision the development of resilient infrastructures to address emerging cybersecurity threats?

Resilient infrastructure is the backbone of a secure Europe. We need systems that are not only robust but adaptive to ever-evolving threats. This includes fostering innovation in areas like zero-trust architectures, AI-driven anomaly detection, and next-gen cybersecurity tools. Start-ups can be frontrunners by introducing fresh perspectives and cutting-edge technologies. Investments in such innovations will bolster both defence mechanisms and business continuity strategies across sectors.

With the explosive growth of data, particularly driven by large language models (LLMs) and AI, what technological innovations do you foresee as essential?

The data explosion fuelled by AI models like LLMs creates an urgent need for scalable and efficient data management. Technologies such as advanced data compression algorithms, high-performance computing, and edge processing will become indispensable. Moreover, we'll see a rise in privacy-preserving AI models and secure data sharing frameworks. This creates immense opportunities for start-ups working on infrastructure technologies that can handle these growing data demands while ensuring compliance and security.

You mentioned we are entering a new era of IT infrastructure. What impact do you foresee this will have on cybersecurity and defence strategies?

The shift to a new IT infrastructure era will redefine cybersecurity and defence. Increased data flow, interconnected systems, and AI-driven operations demand a proactive approach to cybersecurity. Europe needs to focus on creating ecosystems that integrate cybersecurity solutions directly into infrastructure development. Start-ups specializing in cyber-resilience for critical sectors like healthcare, energy, and finance will play a central role in this transformation. Collaboration between governments, large enterprises, and innovative start-ups is critical to addressing these challenges holistically.

Finally, how can venture capital contribute to fostering this wave of European innovation?

Venture capital must act as both a catalyst and a guide. Beyond funding, VCs should provide start-ups with access to networks, expertise, and strategic guidance to navigate regulatory landscapes and scale across Europe. Identifying and supporting the right teams early will ensure Europe maintains its competitive edge in infrastructure technology. We must also encourage cross-border collaboration, ensuring that innovations benefit the entire continent rather than just localized markets.

Hi inov is a European B2B early-stage VC fund made by entrepreneurs for entrepreneurs and based in Paris, Lyon and Munich. Hi inov supports outstanding hypergrowth companies that transform the ever-changing services and

industrial landscape with innovative digital deep-tech technologies. Their highly experienced investment and venture team guides their start-ups from humble beginnings to becoming tomorrow's industry category leaders.

Backed by a strong network of potential clients, partners, and experienced advisors, they will support them in becoming champions in their home market, quickly opening the doors to the French, German, and European markets and supporting their global expansion.

hiinov.com



**Dr. Wolfgang
KRAUSE**
Managing Partner

HI INOV

European Cybersecurity Mapping 2025

AI SECURITY AND INTEGRITY



BY COUNTRY

Legend

TYPE:

 SCALE-UP

 START-UP

OTHERS:

 MULTI-SECTOR COMPANY

Short Pitch: Safeguards AI systems and data integrity, preventing adversarial attacks, biases, and unauthorized manipulation.

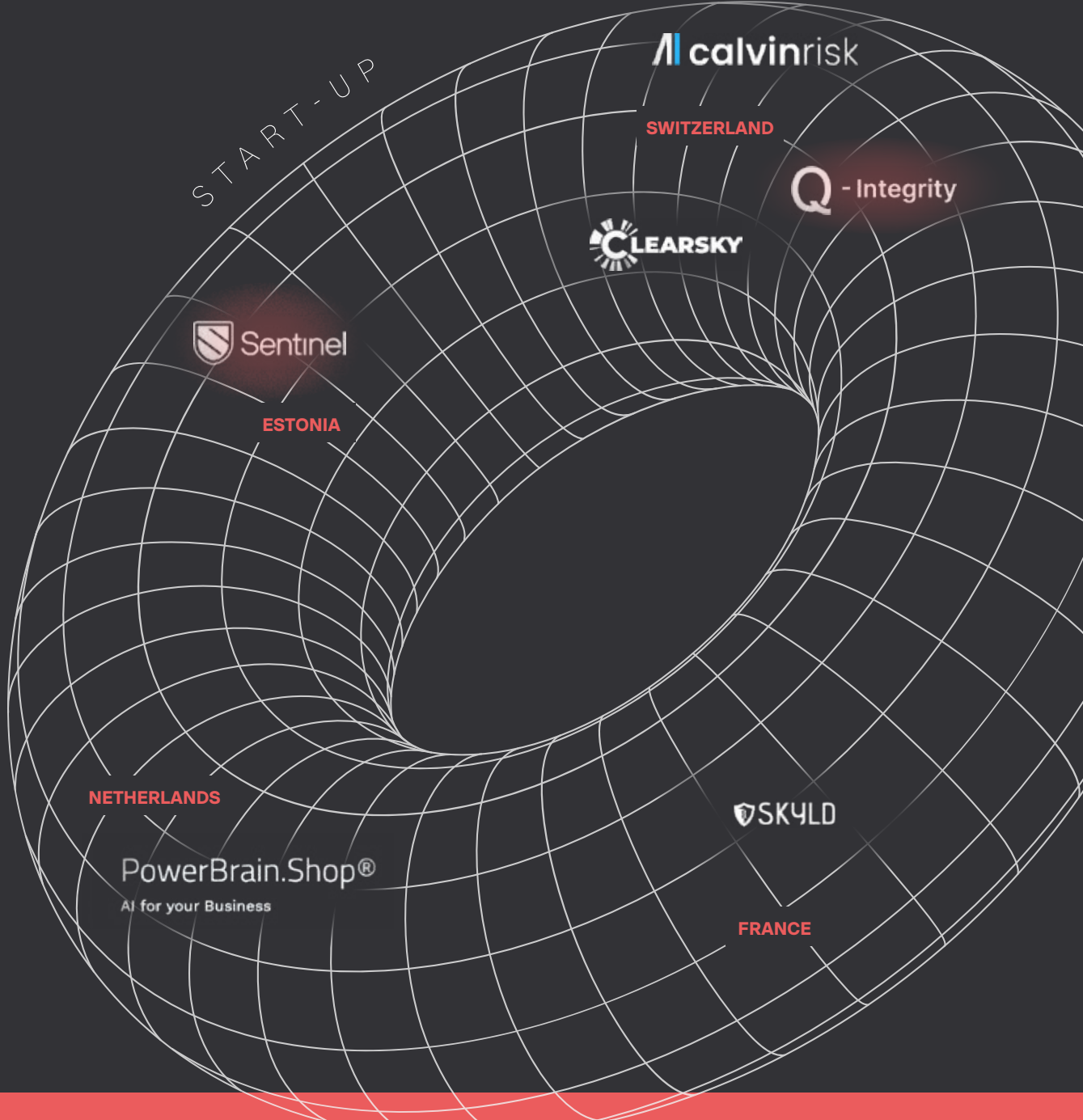
Why Choose European Technology: European providers prioritize ethical AI aligned with EU principles, avoiding dependency on foreign technologies that might introduce vulnerabilities or ethical concerns. Supporting them ensures Europe's leadership in AI innovation and compliance with strict privacy laws.

Importance for European sovereignty: 9/10

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



SWITZERLAND



6

START-UPS

1

SCALE-UP

European Cybersecurity Mapping 2025

APPLICATION SECURITY



BY COUNTRY

Legend

TYPE:

SCALE-UP

START-UP

OTHERS:

MULTI-SECTOR COMPANY

Short Pitch: Protects applications from vulnerabilities during development and deployment, ensuring secure functionality. Avoids breaches coming from compromised websites or APIs, filters unauthorized Internet connections.

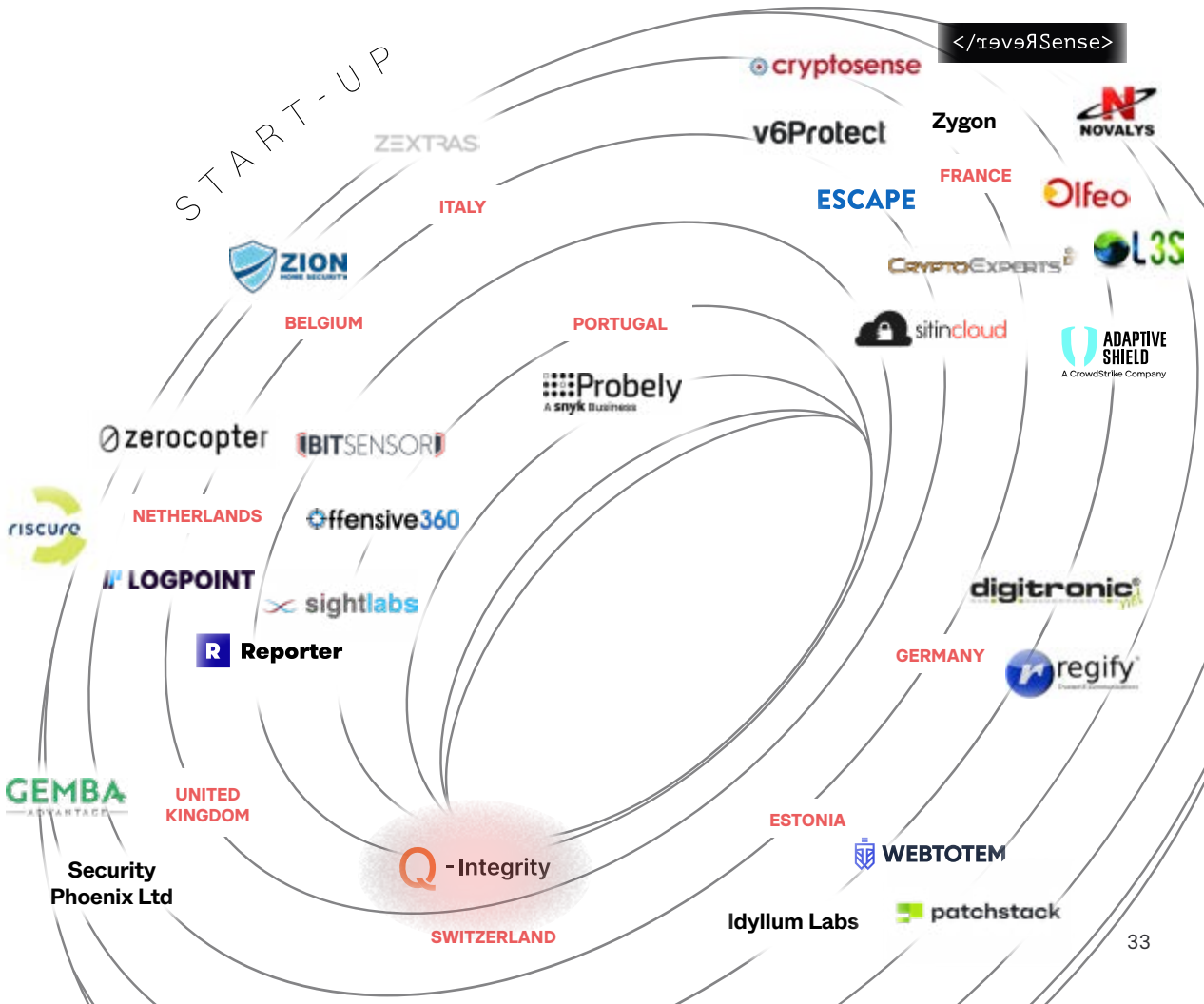
Why Choose European Technology: European companies provide localized solutions that align with EU standards. They ensure no data leaks to non-compliant jurisdictions, reinforcing Europe's strategic autonomy and promoting trust in secure application development.

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.

29
START-UPS

11
SCALE-UPS



Interview Scale-up

ECLECTICIQ



Real consolidation would have to be pushed by the market, à la “Cybus” concept, wherein European-native leaders consolidate (like Airbus) to face off against incumbents. But more thought is required to determine the desired outcomes for the European and global ecosystem. First, establish that this is a good idea – European consolidation to offset intra-European competition in favour of global competition. Then, determine what it should look like – based on outcomes.



In a few words, what is your domain?

Eclectiq is a global provider of threat intelligence technology and services that empower organizations to neutralize critical cyber threats to their business in an ever-evolving landscape.

We help security teams make smarter, faster decisions with dynamic solutions that reduce complexity and streamline threat detection and response. From our AI-embedded threat intelligence platform to our browser extension, our products improve workflows, reduce analyst fatigue, and mitigate cyber risk.

Our customers rely on our expertise and unique technology to integrate their security solutions, automate data processing, retrieve actionable intelligence that's most relevant to them, and safeguard operations and help them stay ahead of the latest cybersecurity threats.

In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027, in technology and in customer's behaviour?

Since 2020, cybersecurity has evolved significantly, driven by technological advancements and shifting attack strategies. At Eclectiq, we've observed the widespread adoption of cloud technologies, the rise and increasing sophistication of ransomware attacks, and the growing role of AI in strengthening cyber defences.

Firstly, cloud-first adoption has surged due to the shift to remote work and the growing reliance on cloud-based services. Organizations have moved critical infrastructure, applications, and data to the cloud, leading to the development of new cloud-native security models.

Ransomware attacks have also evolved to become more sophisticated, and we now have Ransomware as a Service (RaaS) which has democratized the ability to launch ransomware attacks.

AI in cybersecurity is becoming more commonplace with machine learning algorithms being used for detecting anomalous patterns, predicting cyber

threats, and automating incident response incorporating AI to improve real-time threat detection.

Looking ahead, I anticipate deeper integration of AI and automation in Security Operation Centres (SOCs), enabling smarter, more efficient decision-making. Quantum computing's arrival will challenge current encryption, prompting a shift to post-quantum cryptography designed to withstand quantum decryption.

I also think Zero Trust is likely to evolve from a best practice to a standard approach, addressing access, device health, identity, behaviour, and network segmentation for organizations of all sizes.

It may sound cliché, but the cybersecurity landscape will continue to rapidly evolve as new threats emerge and technology advances. Organizations will need to stay ahead of these developments by adopting more advanced defence mechanisms, embracing new technologies like AI, quantum computing, and Zero Trust, and ensuring compliance with growing privacy regulations.

Customers will become more aware and discerning, which means they will increasingly demand better security practices, driving organizations to prioritize cybersecurity more than ever before.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

European vendors must be proactive and strategic in how they fund, develop, and scale their cybersecurity innovations.

We often talk in European circles about the growth capital gap, but there is also a value creation gap. European vendors need to work with Member State policymakers to drive toward a unified capital market; streamlined or reduced regulatory burdens for start-ups; and looser labour laws for a special category devoted to start-ups.

More traditionally, vendors can form partnerships and prioritize emerging technologies – starting with building for what the world's largest markets want and expect, regardless of their presence in the market. Typically, European markets and buyers follow.

Eclectiq is a global provider of threat intelligence technology and services that empower customers to neutralize critical cyber threats. Guided by our values – being curious, bold, accountable, and collaborative – we help security teams make smarter, faster decisions with dynamic solutions that reduce complexity and streamline threat detection and response.

eclectiq.com



Cody BARROW
CEO

Eclectiq

Interview Scale-up

ECLECTICIQ



SILVER
SPONSOR

Customers are fed up with scattered cybersecurity offerings and would prefer to find already integrated solutions? Do you agree?

I do agree with the sentiment that European customers are likely to prefer integrated cybersecurity solutions. The increasing complexity of the cybersecurity landscape, along with regulatory and operational pressures, is driving a preference for integrated solutions and rationalization of vendors. While certain organizations may still opt for specialized point solutions where necessary, the demand for simplicity, cost-effectiveness, and comprehensive protection is pushing many toward integrated offerings.

However, while an integrated cybersecurity solution can streamline security operations and offer many benefits, the challenges related to complexity, cost, data management, and skill shortages need to be addressed carefully. Organizations must plan carefully, invest in the right tools, ensure proper training, and consider scalability and flexibility when adopting such solutions.

**Is European consolidation an actual perspective according to you?
If Yes, who should push the move:
the institutions? The large users?
Some large integrators? Investors?
Vendors themselves?**

While all these players have roles to play in driving consolidation, it is likely that a combination of large users, integrators, and investors would drive this shift, supported by EU institutions that create a conducive regulatory environment.

Currently, smaller vendors in Europe are competing against each other with vastly fewer resources than American competitors. Real consolidation would have to be pushed by the market, à la “Cybus” concept, wherein European-native leaders consolidate (like Airbus) to face off against incumbents. But more thought is required to determine the desired outcomes for the European and global ecosystem. First, establish that this is a good idea – European consolidation to offset intra-European competition in favour of global competition. Then, determine what it should look like – based on outcomes.

Ultimately, EU institutions may facilitate the process with supportive policies, but the market absolutely must take the lead.




European Cybersecurity Mapping 2025


CLOUD & DATA PROTECTION




Legend

TYPE:

 SCALE-UP

 START-UP

OTHERS:

 MULTI-SECTOR COMPANY

107

START-UPS

38

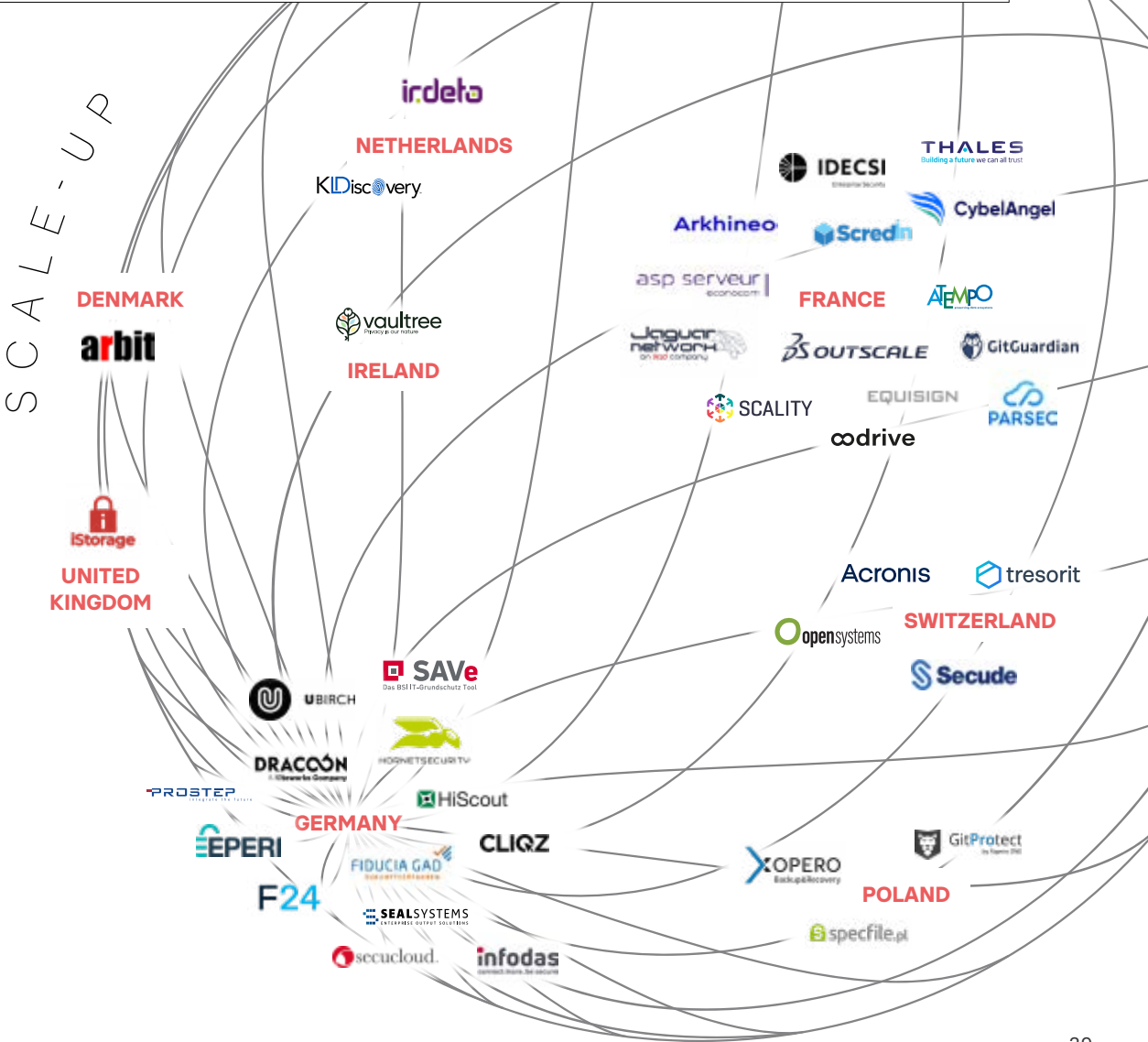
SCALE-UPS

When it comes to data protection, two words soon come in: NIS2, and cloud. NIS2, the EU regulation, recommends users make sure their data are protected against robbery, illicit copy, corruption, and of course crashes. Cloud has changed the game : inhouse systems could be seen as secure, at least as secure as the means used to globally protect the organization IT system warrant it. In the Cloud ... "where are my data?", am I sure it's correctly protected ? and that access is granted to regular users only?

It should be made clear that the trend to massively move IT systems and data to the cloud does not relieve users from protecting their data. Cloud providers usually make sure their system is protected, both from physical and logical hacking, but their cannot for instance decide who has access to the data, who can modify them. That remains on user's side. Which, by the way, explains why the Category "IAM – Identity and Access management" has also a lot of occurrences in this mapping.

That being said, data protection includes several subdomains, among which : make sure only authorized users have access and have proportionate rights (the companies focusing on IAM are classified under this IAM category better than in Cloud and Data Protection) – be able to recover your data in case of crash of ransomware attack – make sure your data stored in a cloud cannot be captured without your consent, which has some legal implication, but also triggers technical evolutions such as resorting to encryption – finally, even if you are confident, be quickly informed of any leak. European offers exist in all these areas, some of the companies which bear them being already largely international.

We have hereinabove mentioned encryption. This is an area by itself, in particular because the looming quantum computers will make classical means of encryption obsolete and inefficient. While the US NIST has published some families of algorithms which are so far said to resist to quantum computing deciphering, the European industry is definitely not lagging behind. Companies proposing systems to protect data by encryption and to store and retrieve them are classified under the Category Cloud and Data Protection, while those specifically focusing on searching and creating new encryption technologies are in the Encryption Category. There again, the border is often blurred as the members of this last family, while having strong roots in R&D, of course propose to implement their solution in the real users' world.



CLOUD & DATA PROTECTION

Legend

TYPE:


START-UP

OTHERS:

 MULTI-SECTOR COMPANY

Short Pitch: Secures cloud environments and sensitive data through secure storage and backup, air gap, encryption, access control, and compliance measures.

Why Choose European Technology: European vendors ensure that sensitive data remains within EU jurisdictions, providing robust protection without exposure to foreign surveillance laws. This enables governments and businesses to maintain data control and align with sovereignty goals.

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.

107
START-UPS

38

SCALE-UPS

START-UP

4

Interview Start-up

UBCOM



We leave 95% of our public markets accessible to companies outside Europe, while Europe only has access to 5% of the Chinese and American public markets. Since 2014, Europe has been building a strategy that consists of financing innovation with public money, then letting the excellent idea go to the United States or the MEA zone without forgetting the talent that goes with it. Europe produces free innovation for our competitors. It's as simple as that.



In a few words, what is your domain?

Ubcom is a cybersecurity consultancy specializing in the detection of digital solutions of a sovereign nature, whether political, legal, financial, or social, and we are specialists in secrecy protection. In other words, we help organizations of all sizes to identify tactical and strategic information and protect it against the various channels of possible or known threats, such as state, economic, or mafia espionage.

In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027 on technology and customer behaviour?

Since COVID-19, we have yet to see any breakthroughs in threat management. Whether in terms of technology or policy, developments have been linear and expected. Of course, the advent of AI and its analytical capabilities is the death knell for many vendors of vulnerability scanning solutions, for example, or of standard and regulatory governance solutions.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

I love this question. I'm a cybersecurity solutions entrepreneur attached to the sovereignty of ideas and their economy, and therefore, I'm a European activist. I've decided to stop using the consensual reserve when talking about politics. Mrs. von der Leyen being very Atlanticist, and even more so since her re-election, European politics has never ceased to preserve American and Chinese interests to the detriment of European genius and innovation. While we can be proud of the 14–20 plan's investment funds, for example, the latter represent only 10% of the amount the Chinese have put on the table for a period half as long. We leave 95% of our public markets accessible to companies outside Europe, while Europe only has access to 5% of the Chinese and American public markets. Since 2014, Europe has been building a strategy that consists of financing innovation with public money, then letting the excellent idea

go to the United States or the MEA zone without forgetting the talent that goes with it. Europe produces free innovation for our competitors. It's as simple as that. Thierry Breton will have done part of the job, but not everything. Those who want to defend a sovereign digital Europe have no power, and being a deputy or a Commissioner is not power. And those who do have power, for various reasons, get carried away by the value propositions of Google, Microsoft, AWS, Oracle, and others.

Some say customers, especially in Europe, are fed up with scattered cybersecurity offerings and would prefer to find integrated solutions. Do you agree?

No, I don't think so. The market is still immature enough to determine this. But it's true that this growing market leaves room for opportunists, resulting in fragmented offerings that know how to make coffee and toast. It's enough to confuse the customer. We sometimes find it hard to get our bearings because every day, there's a new offer, a new product. Of course, most of them serve no purpose at all or are just the same product presented with a different marketing focus that suggests it's new or different.

If yes to the above question, how do you meet or prepare to meet such a trend? Some vendors pledge to build interoperability between systems, so users can benefit from easily integrated offers while keeping their freedom of choice. What is your view on that?

With the advent of AI in cybersecurity, there will be many products to choose from, and it will be hell in the early days. Within two years, natural selection will give way to tangible products, and innovation will focus on the risks of the moment. But cybersecurity is not immune to the effects of fashion. It's a trend with its currents and movements.

UBCOM
CYBER PROTECTION & SOVEREIGNTY

UBCOM is a strategic consulting and secrecy protection agency created in 2014. It acts in cyber risk prevention and protects tactical and strategic information assets against economic intelligence and industrial espionage. Its experts advise and propose concrete solutions in cybersecurity, secrecy protection and digital sovereignty. Its objective: that all your exchanges (video, email, telephone) and your sensitive data are protected from any compromise and that the culture of secrecy is instilled at all levels of your organization.

ubcom.eu



Frans Imbert-Vier
CEO

UBCOM

Interview Start-up

UBCOM



SILVER
SPONSOR

At one time, we were in the Cloud, then in SD-ONE, and now we're doing NDR, tomorrow we'll be offering auto diag, and by 2025, mobility will no doubt be taken into account, with operators getting involved. But there's one trend that has stayed the same since the iPhone. It's free-mium or free. The trend towards free consumption is still on the rise, even if we'll never stop repeating that when it's free, the product is you.

Is European consolidation an actual perspective for you? If Yes, who should push the move: the institutions? The large users? Some large integrators? Investors? Vendors themselves?

There is no consolidation. It's a ruthless economic war in a divided Europe, with the dominant market being the USA, fuelled by Israeli innovation. Only those who claim to defend a so-called sovereign offer and are committed to this principle beyond the rhetoric manage to work together. There are very few of them. Less than 50 have been identified on the continent. For the others, there is too much competition for the trend to be reversed, and politicians have no interest in seeing this change. Divide and conquer remains a fundamental principle of public action.

The EU has set up cybersecurity regulations; does that help? More generally, what do you expect from EU Authorities?

Here's another great question. Since November 5, we've known what the Americans are going to eat out of European regulations. First, there's the agreement between Nvidia and Elon Musk. This is the technological base that will literally kill us in the regulatory sense. Trump's policy will wisely ignore our regulations, including the DSA. Musk promised to serve him European data on a platter to feed his unified AI base. The GAFAMs will feed him; he's already feeding himself with his Starlink telecom offering, and he'll become the leader in less than 5 years, with the Chinese almost ready. In Europe, we don't process any American data. In the U.S., we process just over 80% of data from EU countries. And if we think that ChatGPT, for example, is still a must-have, it's going to be smothered by Musk's power, which is guaranteed to secure its GPU supply before anyone else. You can have the best AI in the world, but without a GPU and data, it isn't very worthy. I've no words to add.



European Cybersecurity Mapping 2025

CODE CHECKING



Legend

TYPE:



SCALE-UP



START-UP

OTHERS:



MULTI-SECTOR COMPANY

Short Pitch: Analyzes source code for vulnerabilities, bugs, and compliance issues, enabling secure development.

Why Choose European Technology: European providers build tools with a focus on transparency and compliance, ensuring that security remains aligned with EU norms. Supporting them reduces risks tied to international dependency and boosts Europe's cybersecurity independence.

Importance for European sovereignty: 8/10

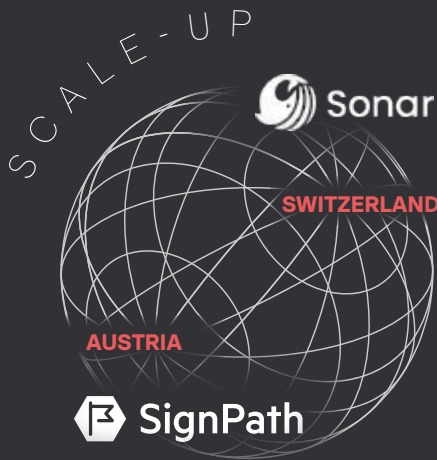
Secure software development is vital for ensuring no hidden backdoors or vulnerabilities are introduced, particularly for critical applications in sensitive industries.

10

START-UPS

2

SCALE-UPS



Interview

CESIN



CESIN's Role in Advancing Cybersecurity Maturity:

How does CESIN help elevate the cybersecurity maturity of organizations across different sectors in France? Are there particular challenges or focus areas that CESIN prioritizes to support its members in strengthening their cybersecurity efforts?

CESIN, with its +1200 members, all CISOs or equivalent, represents a major part of the French economy where all sizes of companies are present in all sectors of activity, including administrations. CESIN is able to address the most specialized subjects for very mature companies to the basic ones for the most modest.

What are the primary funding challenges your members face when trying to enhance their cybersecurity capabilities? How can CESIN and its network support organizations in securing more resources for cybersecurity, especially in a competitive funding landscape?

Through the benchmarks it conducts with its members (several per year), CESIN is able to provide them with sector-specific comparisons on the different components of cyber budgets. In addition, CESIN, rich in the varied profiles of its members, offers a Job Exchange Platform which allows some to offer positions and others to find new professional opportunities

Impact of Regulatory Changes on Investment in Cybersecurity:

With regulatory changes like the NIS2 Directive, how do you see the landscape for cybersecurity funding evolving among CESIN's members? Are these regulations creating new pressures or opportunities for organizations to invest more heavily in cybersecurity?

The regulation aims to deal with a problem that could not be addressed naturally. CESIN welcomes these new regulations with benevolence because we know that it is now the only way to make progress for thousands of small entities who discover cyber issues the day they are victims of a cyber-attack. CESIN intends to focus on mutual aid so that the largest companies help the most modest to increase their cyber maturity. This is how supply chain security will improve in the long term

Future Vision and Emerging Focus Areas for Cybersecurity:

Looking ahead, what are CESIN's strategic objectives for advancing cybersecurity across French organizations? Are there specific emerging threats, technologies, or areas where CESIN believes additional funding and focus will be crucial to enhancing resilience?

Having achieved the goal of indisputable recognition within the digital ecosystem, CESIN has decided to focus more on influence, especially in the political world, both at national and European level. Indeed, it seems essential to us that the voice of users and therefore their needs and difficulties be brought to the attention of the policies that will ultimately decide on the major orientations in terms of security, trust and sovereignty for our country.

It's now commonplace to say that users are a little upset about having to face some many niche player vendors, and would prefer to get integrated systems with a functional wider scope – some speak of the necessity of “plaformization” of the cybersecurity offering: do you agree? what advice would you give to European vendors?

CESIN does not necessarily look very favourably on the idea of “all-in-one” platforms in terms of cybersecurity. Indeed, when we see the way in which companies have locked themselves in by choosing single solutions for entire sections of their digitalization from which they can hardly get out in the event of a problem, we do not want to reproduce this model in cybersecurity. Without of course multiplying the solutions infinitely, we recommend the use of a few integrated solutions while having the possibility of covering residual risks with innovative solutions that are easy to integrate and just as easy to decommission. Cybersecurity requires agility in terms of solutions to respond to the ever-evolving threat and it is not the digital giants that will respond to this challenge.

CESIN (Club of Information and Digital Security Experts) is a 1901 law association, created in July 2012, with the objectives of professionalization, promotion and sharing around cybersecurity. A place for exchange and sharing of knowledge and experience, the CESIN allows cooperation between experts in information and digital security and between these experts and public authorities. He participates in national initiatives and is a force for proposals on regulatory texts, guides and other standards. CESIN has more than 1,000 members from all sectors, industries, ministries and companies, including CAC40 and SBF120.

cesin.fr



Alain BOUILLÉ
General Delegate

CESIN

European Cybersecurity Mapping 2025

CRYPTOGRAPHY



Legend

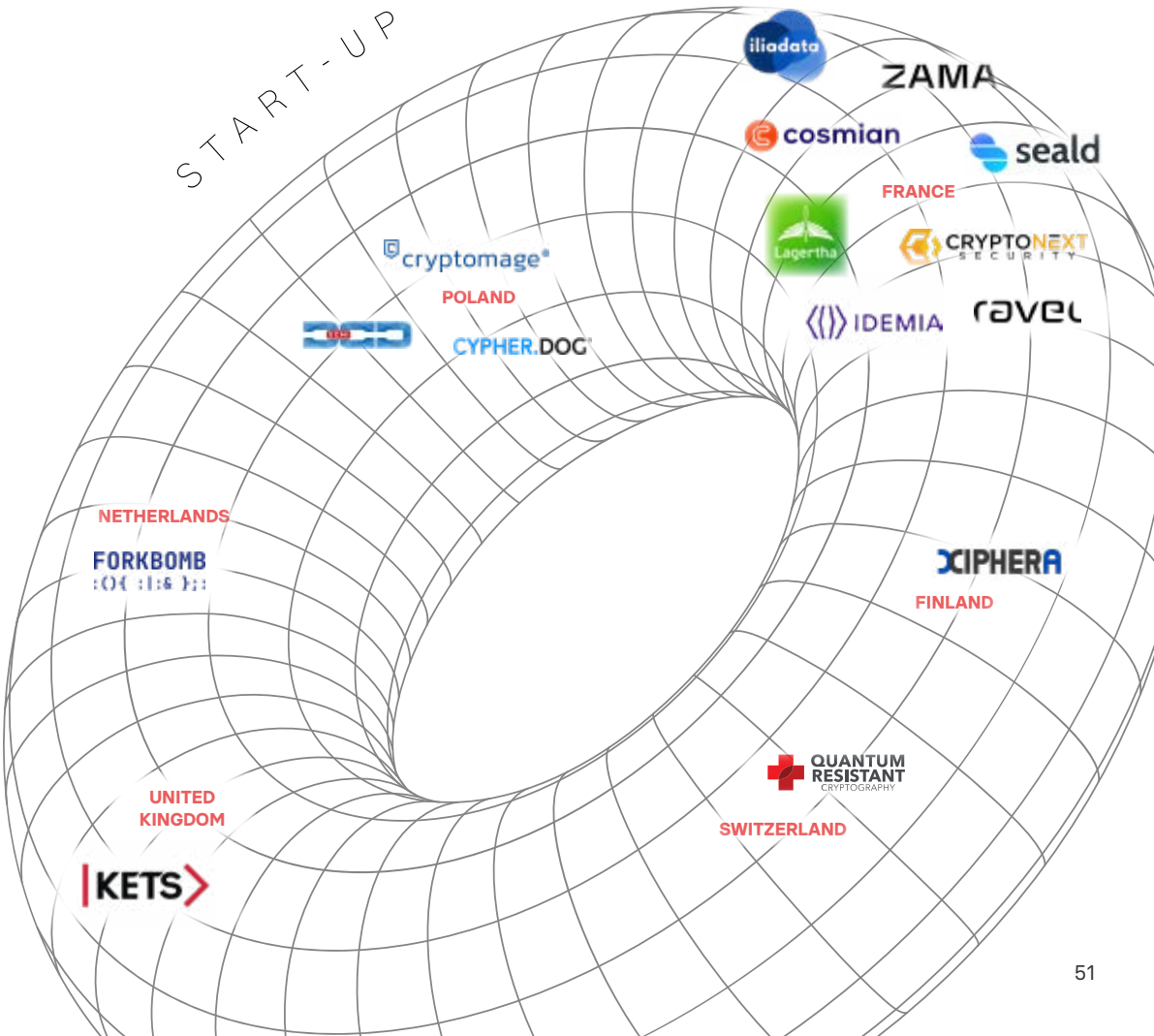
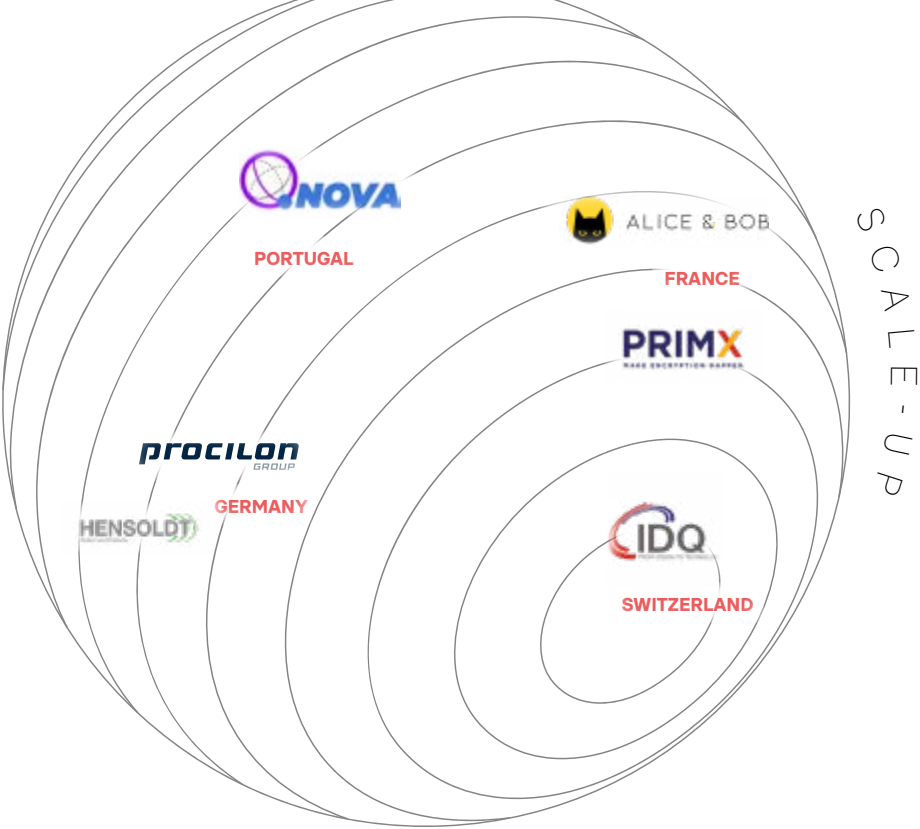
- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Provides encryption solutions to ensure secure and confidential digital communication. Quantum proof cryptography (QPC) is already necessary as quantum computers will rather soon be able to decipher classical encryption and files encrypted in such a way.

Why Choose European Technology: EU-based cryptographic solutions adhere to strict privacy standards, avoiding vulnerabilities linked to foreign jurisdictions. Using European vendors reinforces trust, ensures GDPR compliance, and strengthens Europe's autonomy in critical security infrastructure. European have a remarkable expertise in 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.



Interview Ecosystem Supporter

G+D VENTURES



The European start-up ecosystem in cyber is probably a decade behind Israel and the US from a founder experience, funding and success stories perspective. This may be true for many other start-up categories, but cyber in particular requires founders with hands-on experience in defensive and offensive cyber operations, and that is particularly more difficult to find across the European continent, as many practitioners prefer the long term stability of government or corporate employment contract. Contrast this with the thousands of young Israeli practitioners coming each year out of the Israeli military cyber units to make their first steps in the business world.



Cybersecurity Industry Evolution: How do you see the evolution of the cybersecurity industry? What are the main trends shaping it?

Cybersecurity will continue to evolve as long as technological innovation keeps moving forward. Looking 30 years back, the internet, 3G networks, cloud computing and blockchain have all opened new attack surfaces that required new cybersecurity tooling in response. The current innovations in GenAI and DefenseTech follow a similar path of triggering new cybersecurity solutions.

In parallel, these technological changes are creating a challenge for CISOs and IT Teams, having to purchase and utilize a large and complex spectrum of point solutions, that are increasingly costly and difficult to manage. We therefore expect not only further consolidation among existing vendors in more established categories, but also an increased level of automation to operate these tools more efficiently.

European Vendors and Competition: How do you view the competition between European and US/Israeli vendors? Are European vendors catching up?

The European start-up ecosystem in cyber is probably a decade behind Israel and the US from a founder experience, funding and success stories perspective. This may be true for many other start-up categories, but cyber in particular requires founders with hands-on experience in defensive and offensive cyber operations, and that is particularly more difficult to find across the European continent, as many practitioners prefer the long term stability of government or corporate employment contract. Contrast this with the thousands of young Israeli practitioners coming each year out of the Israeli military cyber units to make their first steps in the business world.

Another major challenge is the fragmented nature of the European market, making it very difficult to scale sales across different countries, cultures and languages. We see a lot of examples of great start-up teams focusing on a single country or region within Europe, but unable to expand from there. These are good businesses but poor investment opportunities for VC investors, whose business model is fundamentally based on high growth.

Lastly, European buyers tend to be less experimental with new technologies and generally have lower IT budgets to purchase new tools, as the economic fabric in Europe is still heavily reliant on lower-margin industries compared to the US.

Despite all these challenges, early success stories and the emergence of European VCs focused on cyber security help the European cyber ecosystem to rapidly mature and catch up with its competitors in other regions.

G+D Ventures is active since 2018 and founded by experienced Venture Capitalists. We are a theme-driven investor focusing on growth-oriented companies, whose innovations promote and protect trust in our society. With this goal in mind, we established a €50m co-investment vehicle with the European Investment Bank and G+D, dedicated to investing in early-stage European TrustTech start-ups. We designed this fund to move quickly, driven by financial returns while leveraging the support of G+D's business units. With the G+D Group's backing and decades of venture capital investing experience in both financial and corporate settings, we leverage our unique, global trust network to open doors for our portfolio companies.

gi-de.com/en/ventures



Assaf SHAMIA
G+D Ventures

Partner

Interview Ecosystem Supporter

G+D VENTURES



SILVER
SPONSOR

What strategies should start-up founders adopt to compete effectively in the global cyber markets?

Start-up founders should consider the following strategies and key approaches to compete effectively in the global cyber markets:

- European cyber founders should focus less on trying to create me-too versions of existing innovations from the US or Israel in Europe, and instead try to innovate globally with their own ideas.
- Adopt a global, not local, mindset from day one: the language you use in internal and external communication should be English, the early hires in sales, marketing and product management should have an international background and the business plan should be ambitious enough to consider global outreach and expansion.
- Partner with Europe-wide resellers, distributors and OEMs as a key element of the go-to-market strategy to enable quicker and more efficient scaling across the continent.
- Leverage upcoming regulatory requirements in Europe to better position the product towards European buyers.
- Tailor the product to address buyers with lower budgets or more conservative purchasing processes by offering lighter product versions or quick value demonstration capabilities.

Bigger Funds in Europe: Do you believe Europe needs larger funds to support cybersecurity vendors? Could this prevent scale-ups from seeking US shareholders?

I do not think funding is the main problem for cyber start-ups in Europe, to be honest. There is plenty of funding available in Europe across stages already, and I believe that getting US investors at the scale-up stage is actually helpful for start-ups looking to expand in the North American market with a local partner on their cap table.

The current state of the European cyber sector is still heavily tilted towards early-stage start-ups rather than scale-ups, and what is more urgently needed is expertise and value-adding capabilities of investors to support these early stage start-ups get to product market fit. In the past few years, we see several cyber-focused funds emerging in Europe and believe that this is a major step towards a more mature and globally-competitive European cybersecurity ecosystem.

European Cybersecurity Mapping 2025

CYBER GOVERNANCE



BY COUNTRY

Legend

TYPE:



SCALE-UP



START-UP

OTHERS:



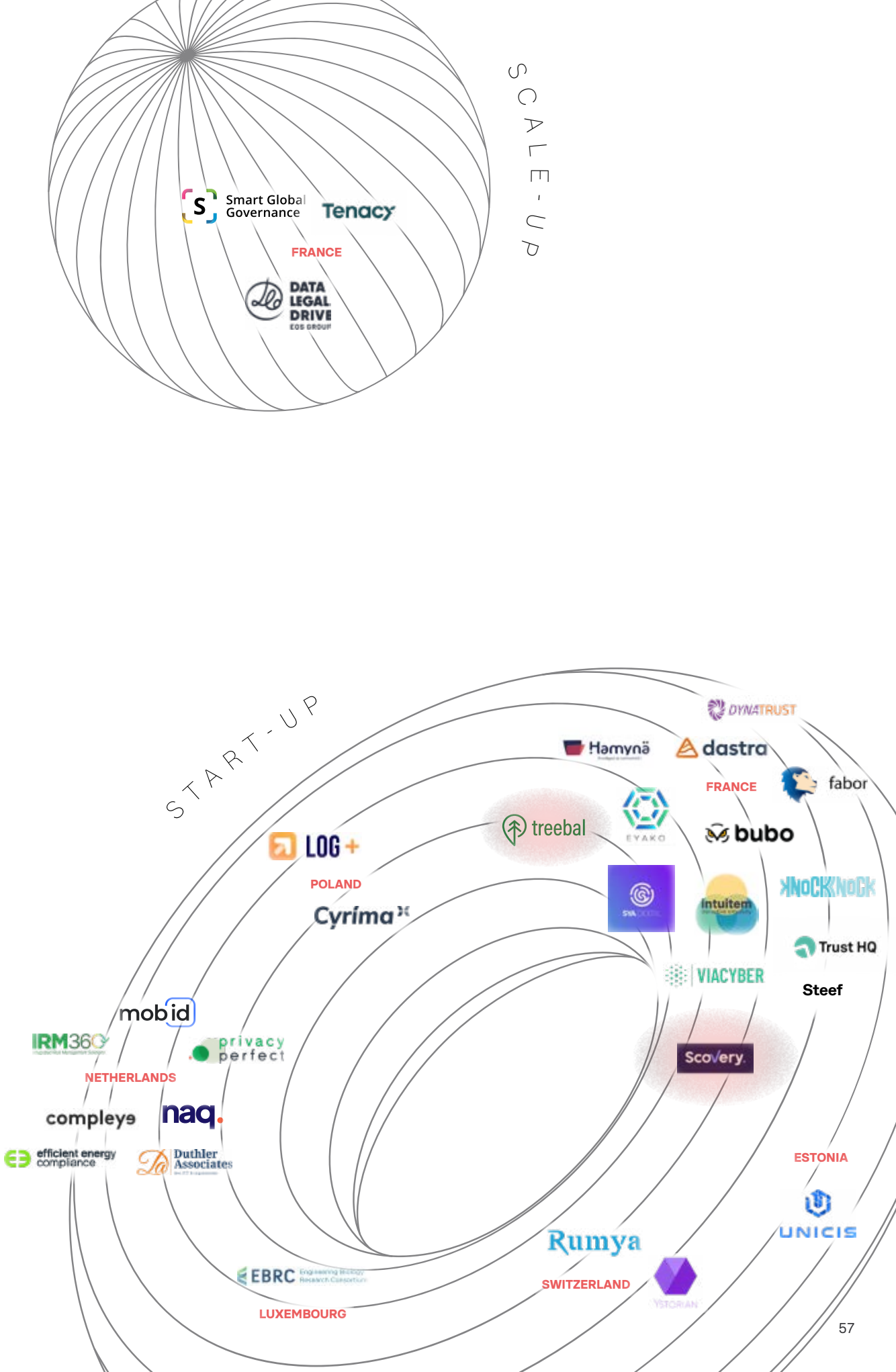
MULTI-SECTOR COMPANY

Short Pitch: Manages cybersecurity policies, compliance, risk assessments, and strategic decision-making.

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

Importance for European sovereignty: 9/10

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



Interview Scale-up

ATEMPO



European consolidation in cybersecurity is not just a possibility, but a vital step to enhance the region's resilience and competitiveness in a rapidly evolving threat landscape. Consolidation would enable pooling resources, expertise, and R&D to deliver more robust, integrated, and scalable solutions. Multiple stakeholders should drive this effort.



In a few words, what is your domain?

Atempo specializes in data resilience and cybersecurity, offering comprehensive solutions for protecting, securing, and recovering critical business data across workstations, servers, and enterprise applications. With seamless integration into diverse storage environments, Atempo defends against cyber threats like ransomware, ensures data immutability, and provides rapid recovery capabilities, enabling organizations to maintain continuity and safeguard their most valuable assets from loss or breach.

In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027, in technology and in customer's behaviour?

Since 2020, the data protection and cybersecurity landscape has evolved significantly, driven by the rise of ransomware attacks, the shift to hybrid and multi-cloud environments, and growing concerns around data sovereignty and compliance. Organizations have increasingly adopted AI-driven threat detection, immutable storage, and automated recovery to counter sophisticated cyber threats. Looking ahead to 2027, advancements in AI and ML, Zero Trust security, and edge computing will further transform the industry. Customers will demand more tailored, sustainable, and proactive solutions that integrate seamlessly into decentralized infrastructures while ensuring compliance with evolving regulations. This shift underscores the growing importance of cyber resilience as a cornerstone of business continuity.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

European vendors can tackle the R&D challenges in cybersecurity by leveraging strategic public and private initiatives to drive innovation and competitiveness. Accessing EU funding programs can provide essential financial support for advanced research while fostering public-private partnerships. Emphasizing data sovereignty and compliance with strict European regulations allows vendors to differentiate themselves from global competitors and attract customers seeking secure and sovereign solutions. Collaborating within ecosystems of academic institutions, research centres, and technology companies can help share R&D costs and accelerate innovation. European vendors can position themselves at the forefront of the industry by focusing on emerging technologies such as AI-driven threat detection, quantum-resilient cryptography, and secure edge computing. Additionally, targeting the growing MSP market with scalable SaaS-based offerings can generate revenue to reinvest in R&D. Through these strategies, European vendors can balance the financial demands of cybersecurity innovation and maintain global competitiveness.

Some say customers, especially in Europe, are fed up with scattered cybersecurity offering and would prefer to find already integrated solutions? Do you agree?

Yes, it's true that many customers, particularly in Europe, are seeking more integrated solutions to address their cybersecurity needs. The increasing complexity of the threat landscape, combined with the proliferation of niche tools, often leaves organizations overwhelmed and struggling to manage multiple, disconnected solutions. This fragmentation can lead to inefficiencies, gaps in security, and increased operational costs.

If yes to the above question, how do you meet or prepare to meet such trend? Some vendors pledge for building interoperability between systems, so that users can benefit of easily integrated offers while keeping their freedom of choice. What is your view on that?

At Atempo, we understand this challenge and believe in delivering holistic data resilience solutions that combine advanced cybersecurity capabilities with seamless integration across diverse infrastructures. By providing solutions that protect, secure, and ensure data recoverability within a unified platform, we help our customers reduce complexity while maintaining robust protection. Moreover, our focus on sovereignty and compliance aligns with European priorities, offering peace of mind for businesses navigating strict data regulations.

We believe the future lies in striking the right balance, offering comprehensive, integrated solutions that address real customer needs without sacrificing the flexibility to integrate with other tools or adapt to unique business environments.



Atempo is a leading independent European-based software vendor with an established global presence providing data resilience and management platforms.

Atempo offers a complete range of solutions to protect, store, move and recover all mission-critical data sets for thousands of companies worldwide.

atempo.com



Luc D'URSO
CEO

ATEMPO

Interview Scale-up

ATEMPO



Is European consolidation an actual perspective according to you? If yes, who should push the move: the institutions? The large users? Some large integrators? Investors? Vendors themselves?

European consolidation in cybersecurity is not just a possibility, but a vital step to enhance the region's resilience and competitiveness in a rapidly evolving threat landscape. Consolidation would enable pooling resources, expertise, and R&D to deliver more robust, integrated, and scalable solutions. Multiple stakeholders should drive this effort:

- European institutions can provide funding and policy incentives.
- Large private companies and public organizations can prioritize sovereign solutions, creating demand for collaboration.
- Investors can accelerate mergers and acquisitions among complementary players.
- Vendors themselves can initiate strategic partnerships to enhance their capabilities.

A unified approach will strengthen Europe's cybersecurity ecosystem and ensure it remains innovative, sovereign, and competitive on a global scale.

The EU has set up cybersecurity regulations, does that help? More generally, what do you expect from EU Authorities?

From Atempo's perspective, the EU's cybersecurity regulations, such as the NIS2 directive and GDPR, are essential steps toward creating a more secure digital ecosystem. These regulations raise the baseline for cybersecurity practices, ensuring organizations across sectors take the necessary measures to protect critical data and infrastructure. They also emphasize data sovereignty, a key priority for Atempo, as we specialize in providing solutions that comply with strict European regulations and ensure the security and recoverability of data within sovereign boundaries.

However, regulations alone are not enough. We expect EU authorities to continue fostering a supportive environment for European cybersecurity vendors through initiatives such as funding for R&D, promoting collaboration within the European tech ecosystem, and facilitating market access. Additionally, more transparent and consistent implementation guidelines for regulations would help organizations of all sizes comply more effectively, driving the adoption of best practices and secure solutions.

For vendors like Atempo, having EU-backed frameworks that encourage innovation, standardization, and market consolidation would strengthen Europe's position as a global cybersecurity and data protection leader.



European Cybersecurity Mapping 2025

EMAIL SECURITY



Legend

TYPE:

SCALE-UP

START-UP

OTHERS:

MULTI-SECTOR COMPANY

Short Pitch: Protects email systems from phishing, spam, malware, and unauthorized access.

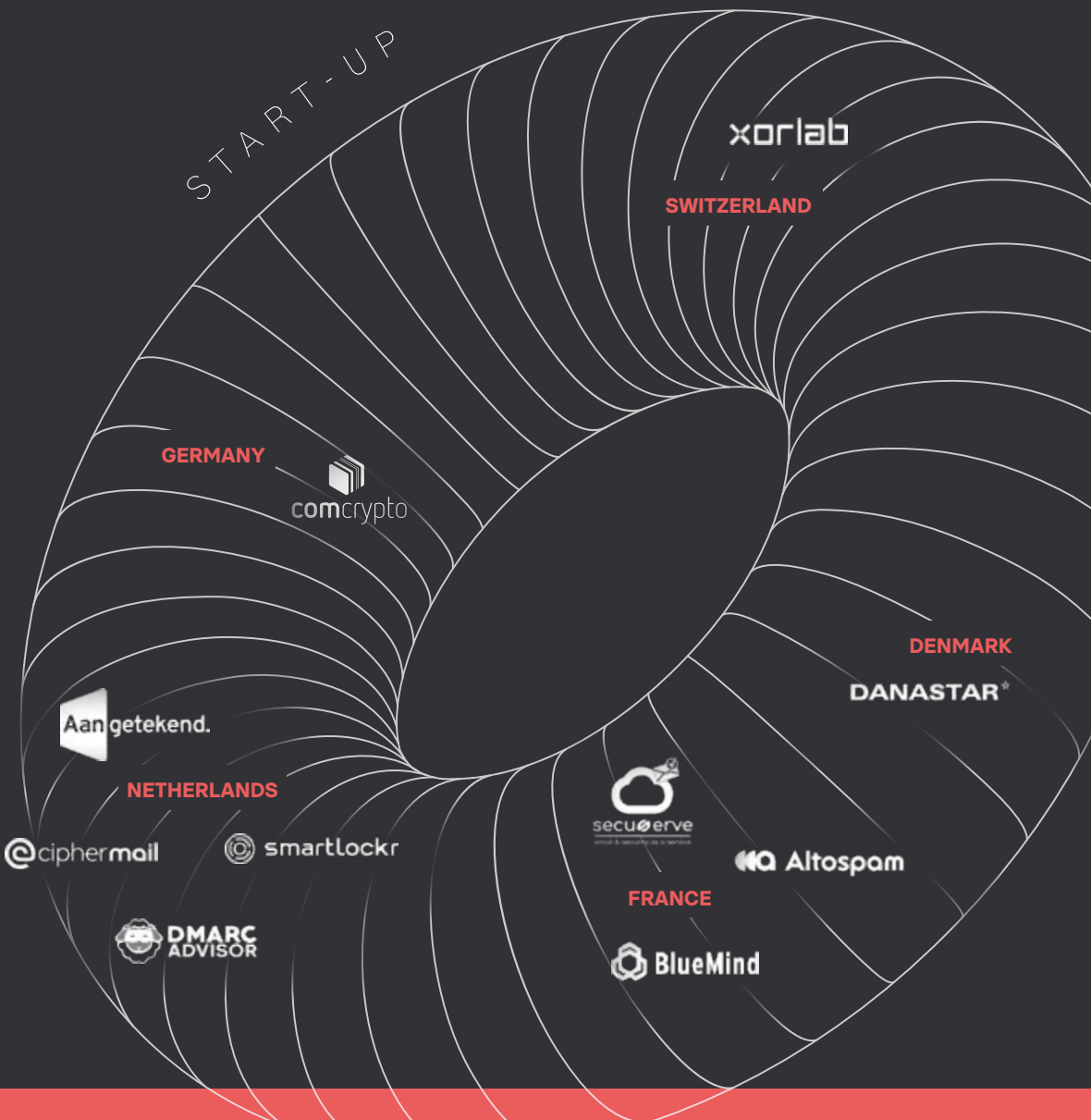
Why Choose European Technology: European providers prioritize privacy and sovereignty by operating within GDPR-compliant frameworks. Supporting them ensures secure communication free from risks associated with third-country laws, strengthening Europe's control over its digital communication channels.

Importance for European sovereignty: 8/10

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

10
START-UPS

6
SCALE-UPS



Interview Scale-up

HARFANGLAB



Cybersecurity ought to be accessible for everyone.

This means that while some mature customers will prefer choosing their cybersecurity tools independently and creating their own cybersecurity stack, others will want to find integrated solutions as they do not wish to lose time on building their cybersecurity stack themselves. And lately, it is true that the second category of customers has been more vocal.



In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027, in technology and in customer behaviour?

2020 was a key turning point in the field of cybersecurity. Indeed, with the pandemic, many businesses relied on digital tools to continue their operations, to interact with customers and employees and to share sensitive information. At the same time, cybercrime also accelerated and displayed more and more sophisticated attacks methods, targeting mostly SMBs, hospitals and local authorities across Europe. At the same time, but unfortunately quite a bit slower, EU organisations started to strengthen their cybersecurity measures. Regulations as well as cyberattacks with media coverage and direct consequences have generated a rise in the level of cybersecurity since 2020.

For the period up to 2027, I expect that this increase in cybersecurity will continue quite slowly, finally reaching the smaller entities with a democratization of cybersecurity tools and services with customers looking for a one-stop shop for all their cybersecurity needs. AI as a mean to assist stretched-out cybersecurity professionals will also factor pretty heavily on the market. Finally, as most of the current focus is on AI and Cloud, as they bring tremendous benefits, on-premises technologies will remain a key part of our digital environment and being able to efficiently secure them will continue to be a challenge.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

Luckily, this is also a critical area, with some ongoing investments, helping businesses to keep innovating as they grow. Although, this illustrates the need of consolidating the ecosystem, to join forces to build a strong cybersecurity actor that will be innovative and attractive enough to catch the attention of investors. There's also a need for more public support, from government to support local technologies and economy, like the United States are doing well.

Some say, customers, especially in Europe, are fed up with scattered cybersecurity offerings and would prefer to find already integrated solutions. Do you agree?

Cybersecurity ought to be accessible for everyone. This means that while some mature customers will prefer choosing their cybersecurity tools independently and creating their own cybersecurity stack, others will want to find integrated solutions as they do not wish to lose time on building their cybersecurity stack themselves. And lately, it is true that the second category of customers has been more vocal.

As a cybersecurity provider, keeping those customers needs as they change over time and across the EU is essential. Having an open architecture, using standardized formats and allowing easy connection to other cybersecurity tools : those are all technology features that should be required as they allow for an integrated approach. Especially, they allow MSSP partners to manage a complete suite of cybersecurity tools that match the customers' needs.

Is European consolidation an actual perspective?

Consolidation is absolutely necessary to increase European competitiveness at the international level and to address EU customers' needs for integrated offers in a timely manner. There are different ways to achieve this. Partnering with like-minded EU players is one of them : a concrete example is the OpenXDR platform that we launched in 2021 with gathered several market players around the promise of easy technical integrations. More recently, HarfangLab and IKARUS Security Software joined forces to create a shared offer of an EPP & EDR made in Europe, hosted in Europe and operated in Europe. Those are first steps in the right direction and we are hopefully confident that more will come.

HarfangLab is a French cybersecurity company specializing in endpoint protection. HarfangLab builds technologies that anticipate and neutralize cyberattacks on devices and servers, while also providing a better understanding of your IT infrastructure for improved security. HarfangLab's EDR software was the first EDR to be certified by ANSSI, and today protects hundreds of customers worldwide, including administrations, companies, and international organizations operating in highly sensitive sectors. HarfangLab's solutions are distinguished by their openness, with solutions that integrate natively with all other security bricks; their transparency, as the data collected by the tools remains fully accessible; and the strategic autonomy they offer, as customers are free to choose their hosting mode: cloud, public, private, SecNumCloud, or their own infrastructure.

harfanglab.io



Anouck TEILLER
Chief Strategy Officer

HarfangLab

Interview Scale-up

HARFANGLAB

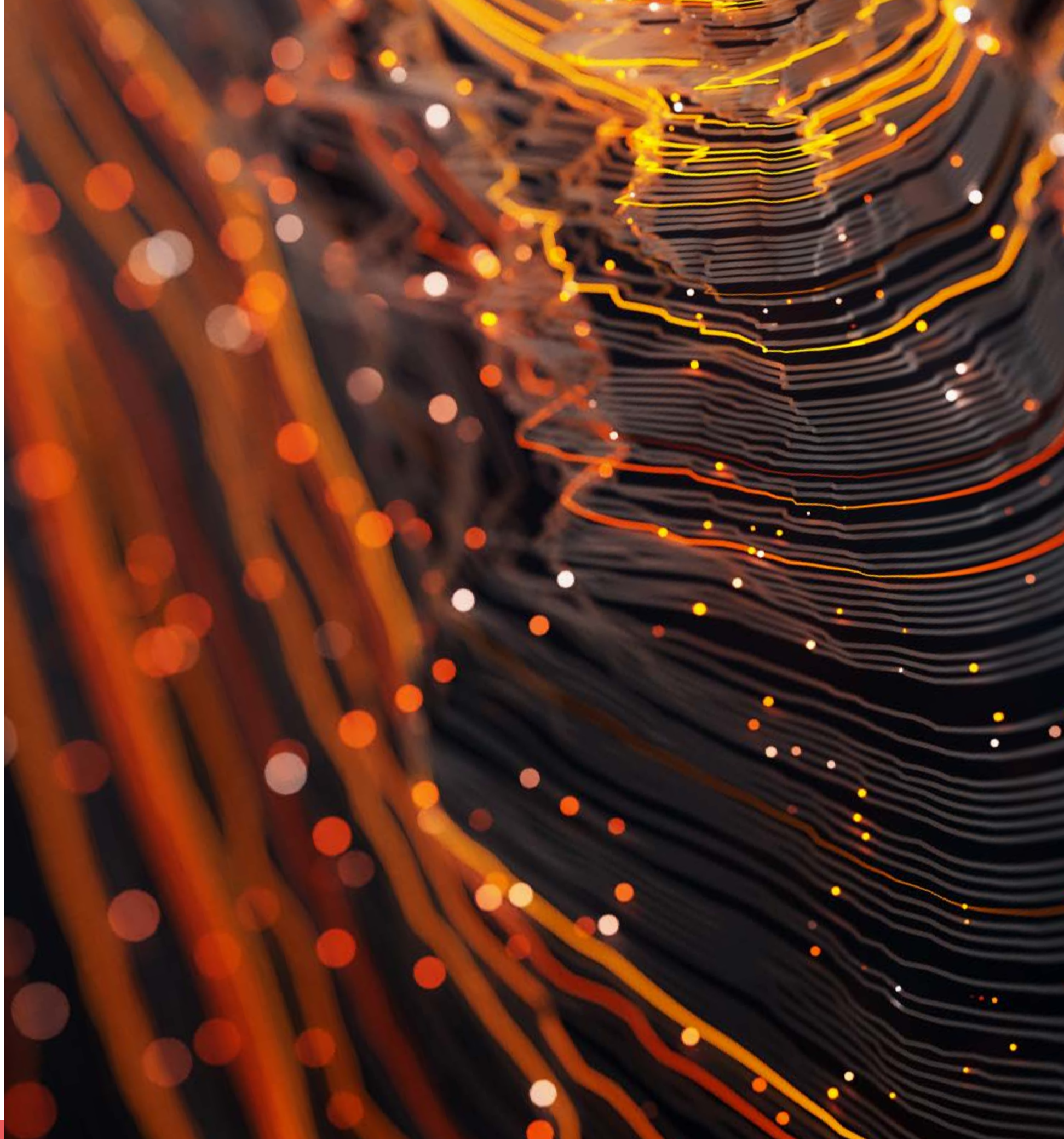


The EU has set up cybersecurity regulations; does that help?

Regulations, even when they are difficult to grasp, have the extremely positive effect of making people care about the topic. This was a big help in the field of cybersecurity that was too long observed as a purely technical matter.

More concretely, we recently surveyed 750 SMEs across Europe to understand how they felt regarding the upcoming regulations in Europe. And although many of them agree that it's more work and a challenge to achieve compliance, they also mostly believe that the high expectation from Europe is also turning into a competitive advantage on the market as it sets up a quality framework.

As cyberthreats are not diminishing in numbers or in complexity and as the world is increasingly polarized, cybersecurity regulations are one of the tools at our disposal to increase EU resilience. However, regulation for regulation is an empty shell and only when proper cybersecurity measures will be implemented in every EU entity will there be a significant change.



European Cybersecurity Mapping 2025

ENDPOINT SECURITY



BY COUNTRY

Legend

TYPE:

 SCALE-UP

 START-UP

OTHERS:

 MULTI-SECTOR COMPANY

Short Pitch: Secures user devices from cyber threats, ensuring safe network access. More and more relies on AI and automatized processes to detect malicious attempts, including not yet referenced attacks.

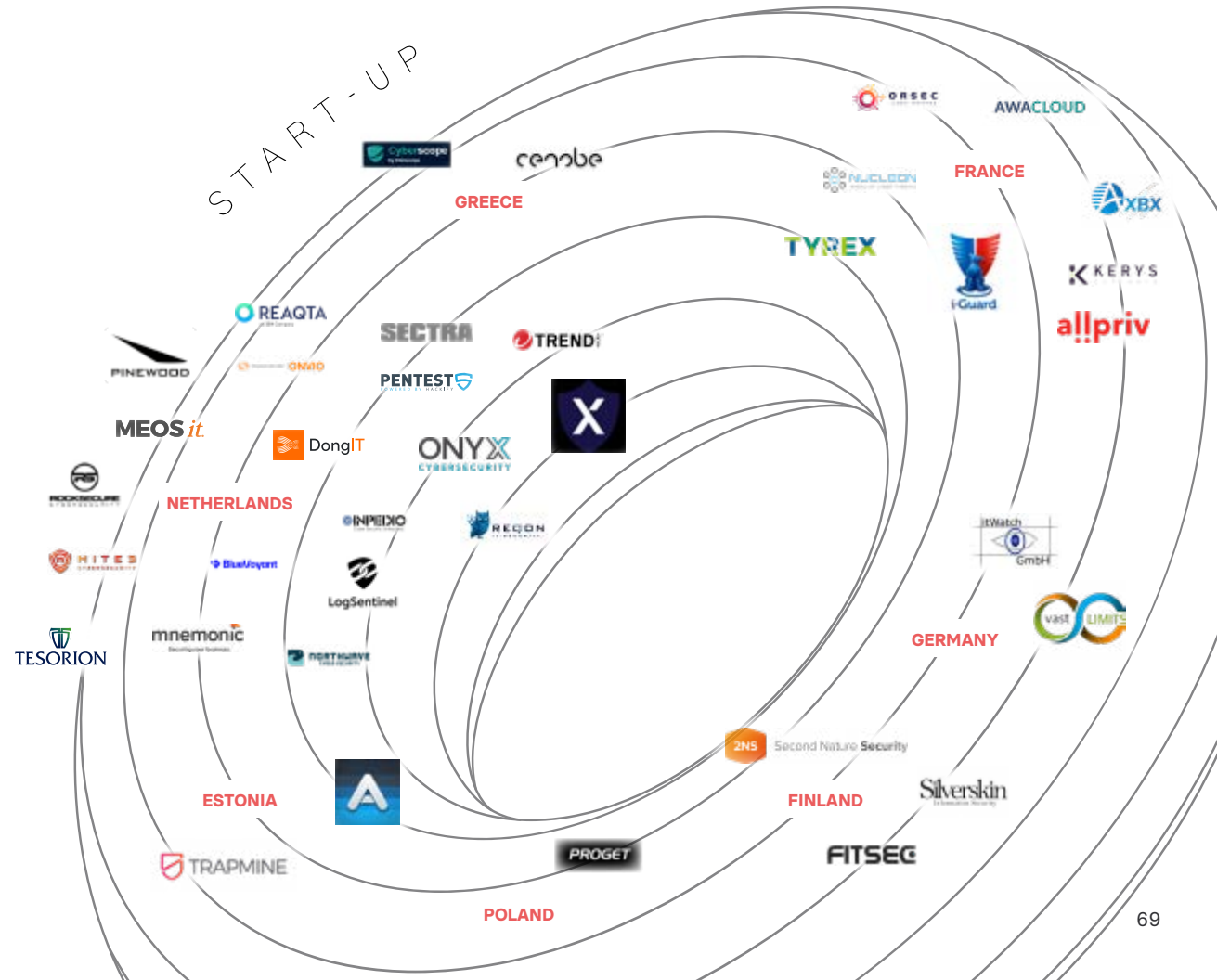
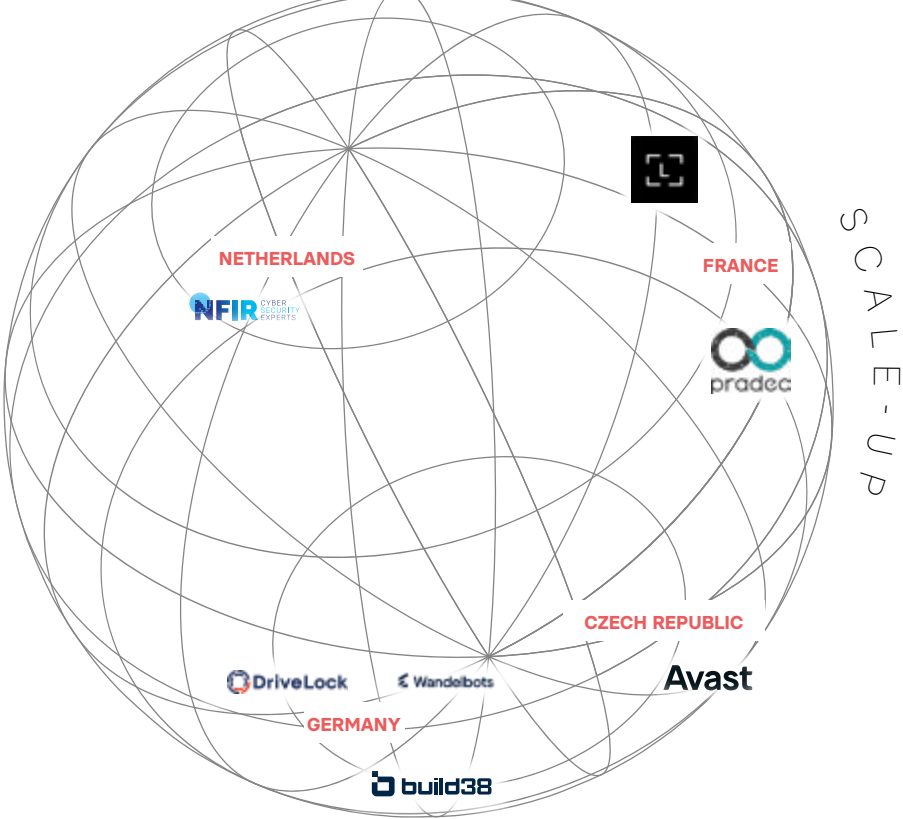
Why Choose European Technology: European vendors offer solutions tailored to local privacy regulations and sovereignty concerns, ensuring safe, compliant, and independent endpoint protection for businesses and governments.

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.

38
START-UPS

7
SCALE-UPS



Value Chain in Cybersecurity

Solution Providers

ADDED VALUE:

- Ensures R&D
- Provides turnkey solutions

Value-Added Distributors (VAD)

ADDED VALUE:

- Offers a catalog of complementary solutions
- Ensures training
- Configures and customizes products
- Integrates systems
- Provides technical support

Consultants

ADDED VALUE:

- Evaluates risks and analyzes vulnerabilities
- Conducts penetration tests and audits
- Designs and implements security policies
- Develops and implements security strategies
- Responds to incidents
- Develops a governance framework
- Provides regulatory assistance
- Advises on long-term security strategy

MSSP (Managed Security Services Provider)

ADDED VALUE:

- Monitors security on behalf of the end client
- Detects vulnerabilities and proposes corrective measures
- Manages identities and access
- Detects and responds to incidents
- Organizes awareness training
- Ensures compliance with regulations

Integrators (ESN and Value Added Resellers)

ADDED VALUE:

- Evaluates needs
- Designs and manages projects
- Defines architecture
- Installs and configures solutions
- Integrates complex systems
- Provides training
- Manages maintenance

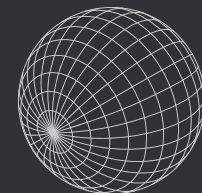
Resellers

ADDED VALUE:

- Understands the needs of end clients
- Ensures the availability of solutions
- Purchases from VADs and sells solutions to end clients
- Sometimes provides customization and integration based on their expertise but at a less complex level than VADs
- Occasionally provides basic support and after-sales service

END CLIENT

European vendors across Europe



COUNTRY	SCALE UP	START-UP	TOTAL
FRANCE	70	240	310
NETHERLANDS	16	130	146
GERMANY	51	45	96
SWITZERLAND	21	58	79
ESTONIA	6	40	46
POLAND	5	27	32
UNITED KINGDOM	5	20	25
GREECE		13	13
SPAIN	1	11	12
FINLAND	2	10	12
DENMARK	3	7	10
CZECH REPUBLIC	2	5	7
PORTUGAL	2	4	6
ITALY	1	5	6
BELGIUM	2	4	5
LUXEMBOURG		5	6
AUSTRIA	1	4	5
IRELAND	1	2	5
SWEDEN		2	3
SLOVAKIA	2		2
ROMANIA	1	1	2
NORWAY	1		1
LITHUANIA	1		1
HUNGARY		1	1
TOTAL	194	634	828



Interview

DCYPHER

The key lies in advancing and adopting technical standards that enable interoperability between components. Such standards would support a modular approach, allowing organizations to integrate best-in-class solutions while maintaining flexibility and fostering innovation.



Trends

The last couple of years, we see as main trend the shifting of attention from putting the responsibility mostly in the hands of the individual citizen or organization, towards a focus on the whole public and private ecosystem. Resulting in putting significantly more efforts in supply chain-, IT/OT- and Cloud security. We also see this wider attention in the new EU legislation on cyber, the changing role of CIO's and CISO's, technological focus on SOC automation, AI for autonomous cyber systems and more attention towards state actors with offensive cyber programs. Also, in both low and high classified information security, there will be much attention to the advancements in (post-quantum) crypto.

For the next years, it goes without saying that the influence of AI will be enormous. There will be a significant scale-up in both defence and attack with AI, as well as on AI. As dcypher, we stimulate R&D that leads to future-proof cybersecurity systems that are inherently secure. Amongst others, this is an ambition achieved by rethinking software development and stimulate "cybersecurity by design" in new products, systems and infrastructures. This is to be combined with autonomous systems that defend, repair and prevent during the whole lifecycle, also to be implemented in already existing legacy.

R&D investments

The constant sophistication and scale of attacks, as well as the trends and ambition described above, require significant investments in R&D. Far beyond the possibilities of separate organizations, industrial sectors and even national governments. From the point of strategic digital autonomy, it is to be hoped that the EU will develop policies to actively combine national investments and prevent fragmentation. National organizations such as dcypher aimed at public-private collaboration as well as EU organizations such as ECCC who is responsible for cybersecurity in Horizon Europe program and Digital European Program, should be able to combine knowledge, solutions and budgets to scale up significantly. This is in line with the recent Draghi Report on European competitiveness.

Relevance of integrative solutions

Another aspect of fragmentation is technology. Offerings on for example the annual InCyber Forum conference demonstrate clearly an extremely wide arrange of cyber products and services. For the average buyer and CISOs, this creates a bewildering level of complexity, requiring the management of contracts with dozens of vendors. An alternative approach—developing or purchasing integrated solutions—can significantly simplify this aspect. However, this also easily leads to vendor lock-in and may slow innovation on separate components of these integrated solutions. Technical standards that provide interoperability between components should allow for a more modular approach, but these standards are

in the relatively young field of cybersecurity not mature yet, and easily outdated given the rapid changes in technology induced amongst others by new threats. To address this challenge, as dcypher we believe the key lies in advancing and adopting technical standards that enable interoperability between components. Such standards would support a modular approach, allowing organizations to integrate best-in-class solutions while maintaining flexibility and fostering innovation. However, given the rapid evolution of cybersecurity threats, these standards must be dynamic and adaptive. At dcypher, we see a critical role for ourselves in driving collaboration amongst stakeholders to address this issue and build a more resilient and adaptable cybersecurity ecosystem.

Cyber industry developments

Consolidation in the industry is inevitable. The enormous growth potential of the global cybersecurity market is such that the larger players in the cybersecurity industry and investors will strive towards increasing market share and higher margins. Amongst others, by buying start ups and cyber businesses to claim national presence in a wide range of countries. Procurement of products and services related to national security often require this national presence. Though governments are observing this development and sometimes limit acquisitions based on national security motives, in general they appear not to have much influence. Despite the disadvantages from a national point of view, consolidation may lead to global leaders that are able to increase the volume of investments in R&D, which may be an advantage for the whole ecosystem of cybersecurity.

Consequences of legislation

The EU is currently setting up a large framework of cybersecurity legislation, amongst other concerned with supply chains and responsibilities (NIS2), digital product security (CRA) or specific sectors (DORA, financial sector). Generally, such law's stimulate innovation, so this is to be encouraged as long as we focus on innovating processes, value propositions, development methods and so on, and not take refuge to only compliancy and legal structures.

dcypher is the Dutch platform for public private collaboration on cybersecurity innovation. Established by the national government, it serves as a catalyst for connecting demand, supply, and means (such as investments and subsidiaries) to drive knowledge development and translation into actual applications of cybersecurity solutions. Therefore, we work closely with education, research, industry and government, setting research agenda's and defining development program's. From our perspective, hereby some observations on the future of cybersecurity.

dcypher.nl



Eddy BOOT
Director

dcypher

European Cybersecurity Mapping 2025

FRAUD PREVENTION & DETECTION



BY COUNTRY

Legend

TYPE:



SCALE-UP



START-UP

OTHERS:



MULTI-SECTOR COMPANY

Short Pitch: Detects, prevents, and responds to fraudulent activities using behavioral analytics and machine learning.

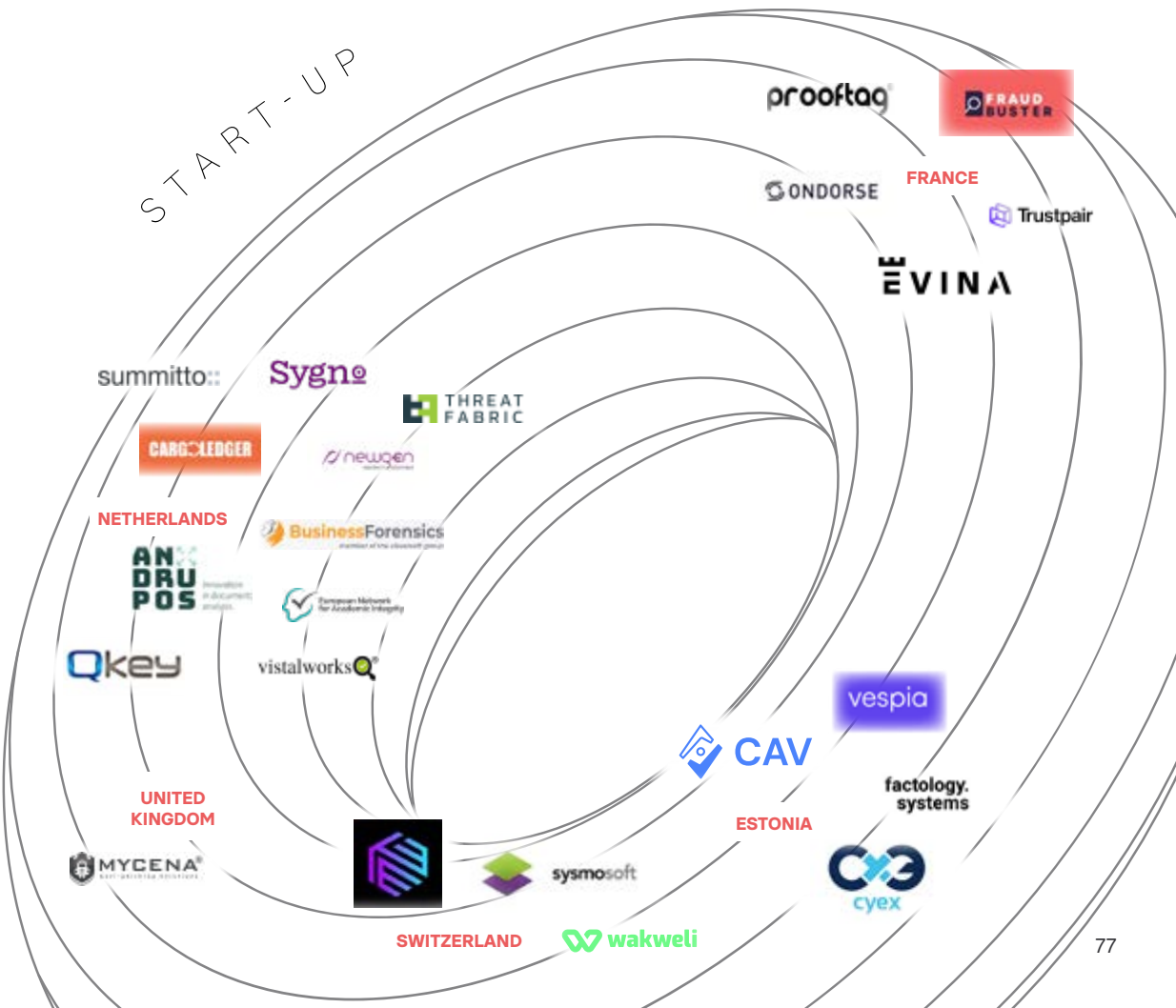
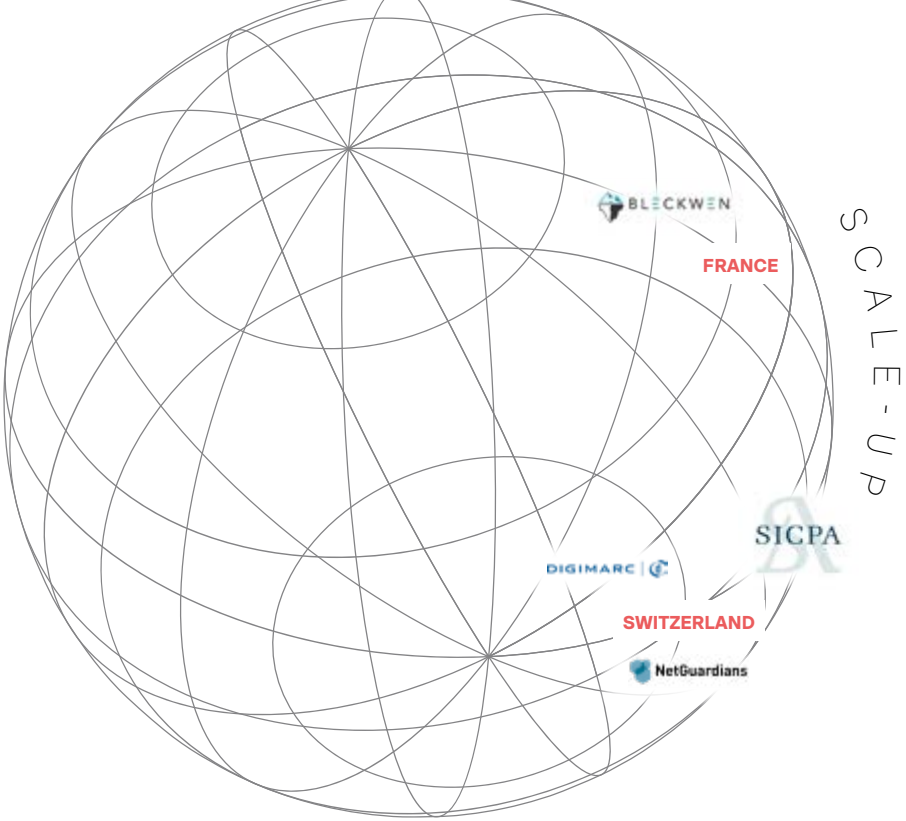
Why Choose European Technology: European providers offer fraud detection solutions tailored to EU-specific challenges and regulations. Their localized expertise enhances trust and compliance, enabling businesses to securely handle sensitive financial and personal data.

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.

23
START-UPS

4
SCALE-UPS



Interview

TELETRUST

Mapping the European cybersecurity vendors is essential in fostering a cohesive and resilient cybersecurity ecosystem across Europe. Frequently, vendors are unaware of each other's capabilities and offerings across national borders, which can limit opportunities for collaboration and innovation.



TELETRUST is the leading organization representing German cybersecurity actors, including private companies, government agencies, and academic institutions. Our objectives are to promote cybersecurity expertise, facilitate collaboration among German and European cybersecurity stakeholders, and support a secure digital ecosystem for businesses and citizens. Additionally, we advocate for strong regulatory frameworks and best practices to protect against evolving cyber threats.

To achieve these objectives, we foster dialogue among stakeholders, organize conferences and workshops, and collaborate on research and development initiatives. We also work to standardize cybersecurity practices across sectors, promote awareness, and encourage investment in cybersecurity innovation.

Mapping the European cybersecurity vendors is essential in fostering a cohesive and resilient cybersecurity ecosystem across Europe. Frequently, vendors are unaware of each other's capabilities and offerings across national borders, which can limit opportunities for collaboration and innovation. Additionally, CISOs and cybersecurity professionals are under constant pressure to stay updated on the rapidly evolving landscape of cybersecurity solutions.

We believe this mapping will be a valuable resource, enhancing mutual understanding and enabling the European cybersecurity industry to connect as a community. By promoting visibility and accessibility of European vendors, this initiative will encourage collaboration, facilitate the sharing of best practices, and support the development of strategic partnerships. Collaboration at the European level is crucial to address cross-border threats, strengthen Europe's digital autonomy, and ensure a united front against global cybersecurity challenges. Through this effort, we aim to build a stronger, more integrated European cybersecurity industry that is better equipped to protect our shared digital future.

To share a perspective on the German cybersecurity landscape, we see three major trends:

- **Increased Focus on Industrial Cybersecurity:** With Germany's strong industrial base, protecting critical infrastructure from cyber threats has become a top priority. Cybersecurity solutions tailored to manufacturing, logistics, and energy sectors are rapidly evolving.
- **Emphasis on Data Sovereignty and Compliance:** As data privacy regulations tighten, there is a growing emphasis on developing solutions that ensure compliance with both national and EU-level data protection standards, such as the GDPR.
- **Adoption of Artificial Intelligence and Automation:** German cybersecurity firms are increasingly integrating AI and automation into their solutions, enabling faster threat detection and response, and helping organizations mitigate the impact of attacks in real-time.

The IT Security Association Germany (TeleTrust) is a wide-ranging competence network for IT security with members from industry, administration, consulting and research as well as national and international partner organisations with similar objectives.

teletrust.de



**Dr. Holger
MÜHLBAUER**
Managing Director

TeleTrust

Interview Ecosystem Supporter

SOPRA STERIA

European cybersecurity start-ups excel in innovation, agility and niche expertise but face gaps in scaling and global competitiveness. With Sopra Steria Ventures, Sopra Steria fosters growth by providing strategic investments, market access and partnerships. As deglobalization rises, we aim to strengthen European resilience by promoting local innovation, reducing external dependencies and maintaining balanced global collaboration.



Strategic Role of Cybersecurity in Integration Services: As an integrator, how does Sopra Steria view the role of cybersecurity within digital transformation projects? What are the main cybersecurity challenges you encounter when integrating solutions across diverse client environments, and how do these shape Sopra Steria's strategic priorities?

At Sopra Steria, cybersecurity is a fundamental requirement for a successful digital transformation that ensures trust and resilience in solutions. Key challenges include adapting diverse client infrastructures, managing legacy systems and mitigating evolving threats. This complexity drives our strategic focus on proactive risk management, tailored security solutions and fostering a culture of continuous improvement.

Investment Focus in the Cybersecurity Start-up Ecosystem: From the perspective of Sopra Steria Ventures, what criteria do you prioritize when evaluating cybersecurity start-ups for potential partnerships or investments? Are there specific technology areas or capabilities that you believe hold the most promise for enhancing Sopra Steria's offerings in cybersecurity?

Sopra Steria Ventures prioritizes start-ups with innovative, scalable solutions addressing emerging threats, strong technical capabilities and a proven market fit. Key focus areas include AI-driven threat detection, zero-trust architectures and cloud security. Start-ups aligning with our vision of proactive, integrated cybersecurity strengthen our offerings and help clients stay ahead of evolving risks.

Collaborating with European Cybersecurity Start-ups and Vendors: Given Sopra Steria's commitment to supporting the European technology ecosystem, how do you assess the current strengths and gaps of European cybersecurity start-ups and vendors? What role does Sopra Steria Ventures play in supporting and scaling these start-ups, and how do you see this collaboration evolving over the next few years?

European cybersecurity start-ups excel in innovation, agility and niche expertise but face gaps in scaling and global competitiveness. Sopra Steria Ventures fosters growth by providing strategic investments, market access and partnerships. As deglobalization rises, we aim to strengthen European resilience by promoting local innovation, reducing external dependencies and maintaining balanced global collaboration.

Navigating Regulatory Compliance Through Partnerships: With increasing regulatory requirements, such as NIS2 and the Cyber Resilience Act, how does Sopra Steria integrate compliance into its cybersecurity strategy, particularly when partnering with start-ups? Do these regulations influence your investment or partnership decisions, and how do you see them impacting the cybersecurity landscape for integrators?

Sopra Steria embeds compliance with regulations like NIS2 and the Cyber Resilience Act into its cybersecurity strategy by prioritizing start-ups with robust, regulation-ready solutions. These frameworks shape investment decisions, ensuring alignment with evolving standards. They drive innovation, demand proactive risk management and position integrators as critical enablers of secure, compliant digital ecosystems.

Vision for the Future of Cybersecurity in Integration Services: Looking ahead, what strategic trends or emerging technologies do you believe will shape the future of cybersecurity within integration services? How is Sopra Steria Ventures positioning itself to remain at the forefront of these developments, and what impact do you foresee this having on the European cybersecurity market?

Future cybersecurity trends in integration include AI-driven defenses, quantum resilience and zero-trust architectures. Sopra Steria Ventures stays ahead by investing in start-ups advancing these technologies and fostering innovation within Europe. This approach strengthens regional expertise, boosts competitiveness and supports a robust European cybersecurity ecosystem aligned with emerging threats and global challenges.

Sopra Steria, a major Tech player in Europe, recognised for its consulting, digital services and software development, helps its clients drive their digital transformation to obtain tangible and sustainable benefits. It provides end-to-end solutions to make large companies more competitive by combining in-depth knowledge and innovative technologies with a fully collaborative approach. With 56,000 employees in nearly 30 countries, the Group generated revenue of €5.8 billion in 2023.

soprasteria.com



Olaf JANSSEN
Head of Cyber Security

Sopra Steria Germany

European Cybersecurity Mapping 2025

IDENTITY & ACCESS MANAGEMENT



BY COUNTRY

Legend

TYPE:

SCALE-UP

START-UP

OTHERS:

MULTI-SECTOR COMPANY

Short Pitch: Manages user identities and access permissions to ensure secure and authorized access. Crucial as many IT systems are moved to the Cloud.

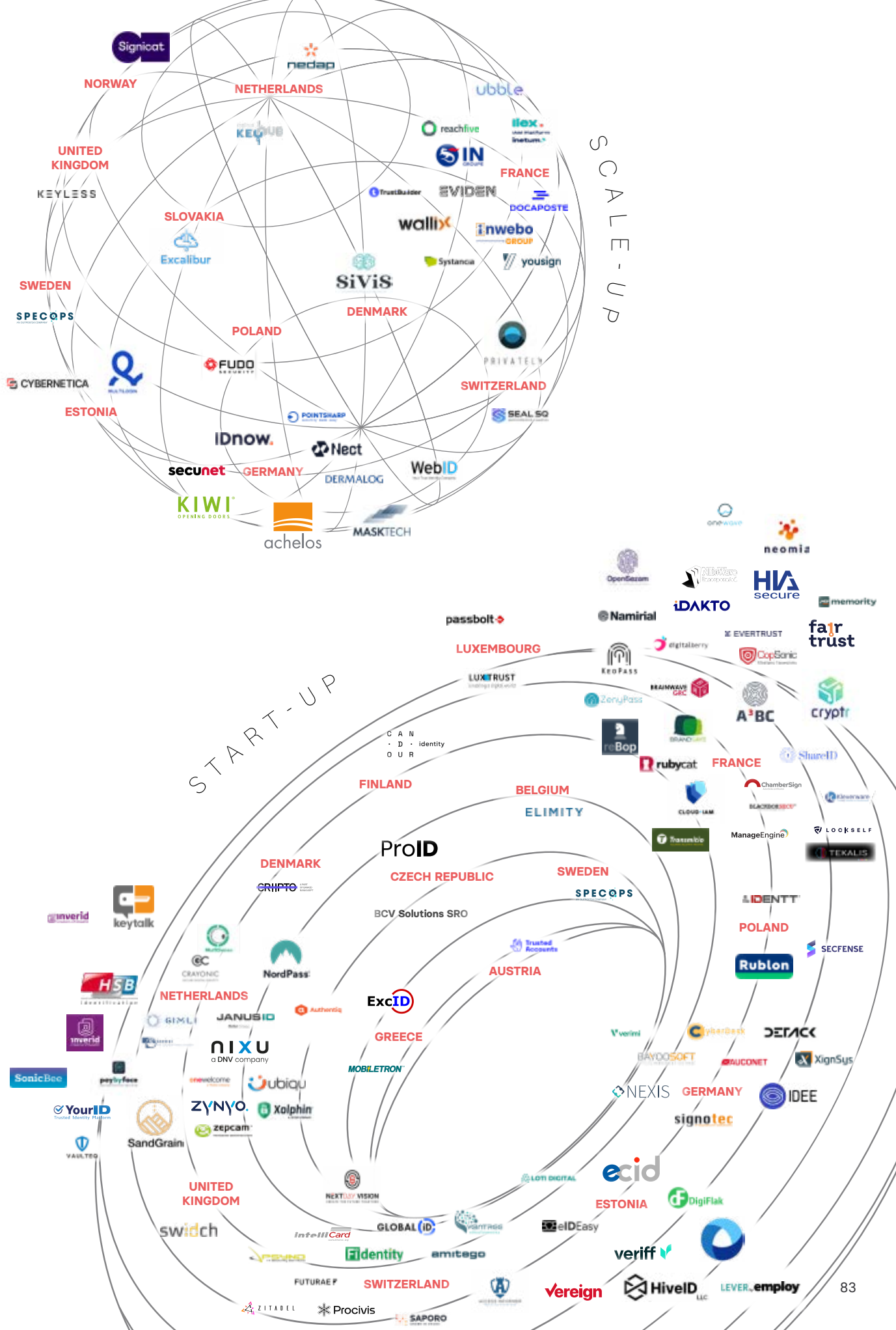
Why Choose European Technology: European IAM providers ensure that sensitive access credentials remain secure and compliant with EU regulations. Supporting these technologies reduces dependency on external solutions and enhances trust in digital identity frameworks.

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.

97
START-UPS

32
SCALE-UPS



Interview Start-Up

NYMIZ



By focusing on collaboration, regulatory harmonization, and investment in talent and technology, Europe can build a thriving cybersecurity ecosystem that competes globally while safeguarding its digital sovereignty.



What is the issue your product solves?

Nymiz can help companies meet GDPR, CCPA, HIPAA, and NIS 2 requirements to comply with Privacy Regulations, with the Protection Against Cyber Attacks reducing the value of sensitive data to attackers by anonymising it and securing Testing Environments preserving referential integrity. Protecting sensitive data in generative AI models to ensure privacy and reduce risks. Also, being Cost Effective and Optimizing Processes by replacing manual anonymisation methods with automated and efficient solutions. Useful for Data Utility Preservation by maintaining data usability for analytics and operations with synthetic data and masking techniques and, last but not least, by educating businesses on data privacy's importance and offering accessible, scalable solutions to them.

How do you see Spain's cybersecurity ecosystem? What are the main trends you see?

Spain's cybersecurity ecosystem is dynamic and growing, supported by a robust regulatory framework, a thriving innovation landscape, and an increasing emphasis on data privacy. At Nymiz, we see this as an exciting opportunity to contribute to the ecosystem with advanced solutions that not only address current challenges but also anticipate future needs, enabling organizations to stay secure and compliant while unlocking the value of their data not only in Spain but in Europe.

The role of the ECA is to help build cybersecurity champions at the European scale. In your opinion, what would help achieve this goal?

The ECA has the potential to transform the European cybersecurity landscape by fostering champions that embody innovation, trust, and resilience.

By focusing on collaboration, regulatory harmonization, and investment in talent and technology, Europe can build a thriving cybersecurity ecosystem that competes globally while safeguarding its digital sovereignty. At Nymiz, we are committed to being part of this journey, contributing to Europe's leadership in data privacy and cybersecurity solutions.

Does this cyber solution really deserve our trust?

Cyber solutions are indispensable but come with risks. Installed on our devices and servers, they access all our data and exchanges, even before encryption. While discussions around trusted cloud services are common, trust in cyber solutions often escapes scrutiny.

In a complex geopolitical context, risks abound. For instance, U.S. products are subject to extraterritorial laws, potentially requiring data collection or backdoors at the request of authorities. Beyond this, factors like solution security, third-party components, and encryption methods matter. To choose wisely, businesses must evaluate solutions with a tailored risk assessment framework, asking targeted providers clear questions and expecting transparent answers.

42k.io: A European repository for cyber solutions

In October 2023, a group of CISOs, consultants, software publishers, and associations developed a grid of 150 questions to guide customers in evaluating and selecting cyber solutions. This effort evolved into a collaborative initiative: a European repository where vendors register their solutions to demonstrate transparency, showcase relevance, and save time by answering common client queries in one click.

Interview Start-Up

42K.IO

With 80 contributors, this tool not only fosters trust and transparency but also breaks down national barriers in Europe's cyber market, encouraging new business relationships and a more interconnected ecosystem.

Join the movement!

Absolute measures of "sovereignty" or "trust" are subjective and vary by project. The 42k.io repository empowers users to weigh responses against their own criteria while offering a transparency score that penalizes incomplete answers.

For vendors, this tool demonstrates the relevance of their solutions, allows European users to discover each solution in detail, and generates new leads. It also saves time for their sales staff, who no longer need to respond to lengthy questionnaires, as decision-makers can get answers to almost all their queries with just one click.

Launched at the InCyber Forum (2024) with the support of Admiral Coustillière, 42k.io is accessible on its website. Born from the Cyberun media initiative, it's an associative project relying on contributions from clients, consultants, and vendors. Join today to help strengthen the European cyber ecosystem!

42k.io

42k.io



Oscar VILLANUEVA
CEO and Co-Founder

Nymiz



B2B SaaS Platform based on AI for data masking. With our Proprietary NLP model we can understand the context to automatically find sensitive data and mask it, managing documents, PDF, images, emails as long as databases in several languages while using different techniques such as masking, token or synthetic data replacement for Legal, Healthcare and Government

nymiz.com

European Cybersecurity Mapping 2025

NETWORK SECURITY



Legend

TYPE:



OTHERS:



Short Pitch: Protects networks from unauthorized access, attacks, and breaches.

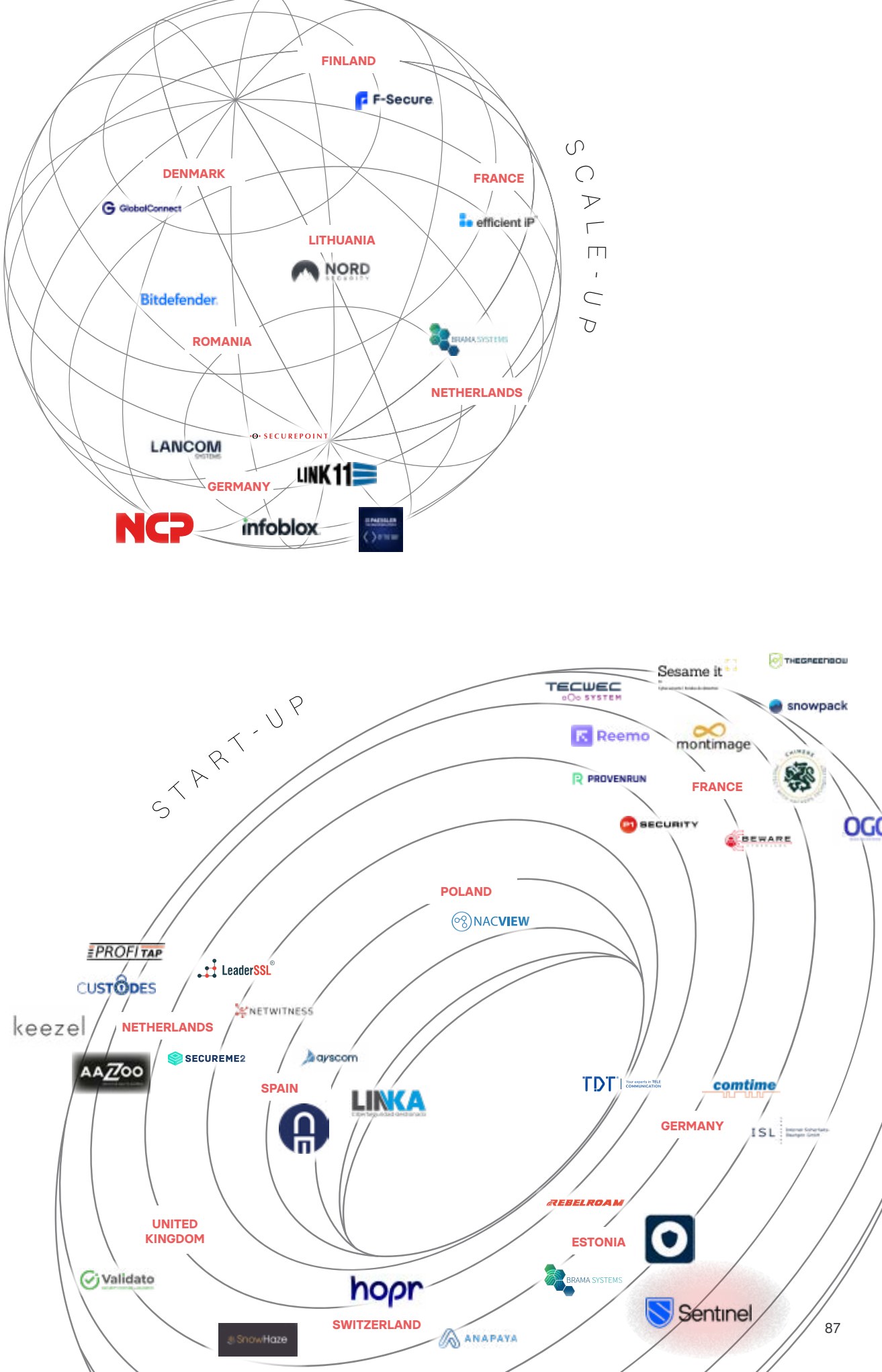
Why Choose European Technology: European network security providers focus on GDPR compliance and EU-specific threat landscapes. Their localized expertise and alignment with regional regulations ensure secure and sovereign network operations.

Importance for European sovereignty: 9/10

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

32
START-UPS

12
SCALE-UPS



Interview Scale-Up

HORNETSECURITY

EU regulations like NIS2 are vital in strengthening security standards across the region and ensuring consistency. From EU authorities, we expect clear frameworks, support for cybersecurity innovation, and efforts to strengthen the European cybersecurity market, enabling European vendors like Hornetsecurity to be competitive globally.



In a few words, what is your domain?

Hornetsecurity is the leading European cybersecurity vendor, specializing in next-gen email security, backup, security awareness and GRC solutions, with a special focus on solutions for Microsoft 365.

Some say customers, especially in Europe, are fed up with scattered cybersecurity offering and would prefer to find already integrated solutions? Do you agree?

Absolutely. At Hornetsecurity, it has been our vision for years to provide customers with seamless, integrated solutions that simplify cybersecurity management. We are delivering on this vision by offering a single platform that encompasses a wide range of cybersecurity products.

Is European consolidation an actual perspective according to you? If Yes, who should push the move: the institutions? The large users? Some large integrators? Investors? Vendors themselves?

For us, it is primarily a reality. As a vendor, many of our acquisitions have been of companies headquartered in Europe, in line with our ambition to be the European cybersecurity Champion with a global reach.

If yes to the above question, how do you meet or prepare to meet such trend? Some vendors pledge for building interoperability between systems, so that users can benefit of easily integrated offers while keeping their freedom of choice. What is your view on that?

What we hear from our customers and partners is a clear push towards vendor rationalization, driven by both economic and operational needs. In response, we focus on a "single platform approach" that delivers the best-of-breed cybersecurity services in a streamlined, unified way. This allows us to meet the demand for simplicity and integration while still providing a range of top-tier, AI-powered solutions within one central platform, reducing the complexity of managing multiple vendors.

In your domain, what have been the main evolutions since 2020? And what evolutions do you anticipate for the period up to 2027, in technology and in customer's behaviour?

Threats have become more sophisticated, with attackers leveraging AI to bypass traditional defences. Microsoft 365 security has become a critical focus due to its vast adoption, making it a prime target. The use of generative AI has revolutionized threat content generation, enabling hyperrealistic phishing attempts at scale. Recently, the rise of Copilot has introduced new vectors for exploitation. These two trends will likely continue to shape the threat and risk landscape for the next 2–3 years, driving the need for adaptive, AI-informed security strategies.

Cybersecurity means R&D, hence money. How can European vendors meet this challenge?

Hornetsecurity is a highly successful cybersecurity vendor, which has enabled us to sustain significant investments in innovation. This includes hiring top-tier talent—Europe is rich in expertise, particularly in AI and cybersecurity—and acquiring trailblazing vendors to expand and enhance our portfolio.

The EU has set up cybersecurity regulations, does that help? More generally, what do you expect from EU Authorities?

Yes, EU regulations like NIS2 are vital in strengthening security standards across the region and ensuring consistency. From EU authorities, we expect clear frameworks, support for cybersecurity innovation, and efforts to strengthen the European cybersecurity market, enabling European vendors like Hornetsecurity to be competitive globally.



Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, & security awareness solutions that help companies of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Its premium services are used by more than 75,000 customers.

hornetsecurity.com



Daniel HOFMANN
CEO

Hornetsecurity

European Cybersecurity Mapping 2025

OT SECURITY



Legend

- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Protects industrial and critical infrastructure systems from cyber threats. Included Sensors, communication and data processing administration and security.

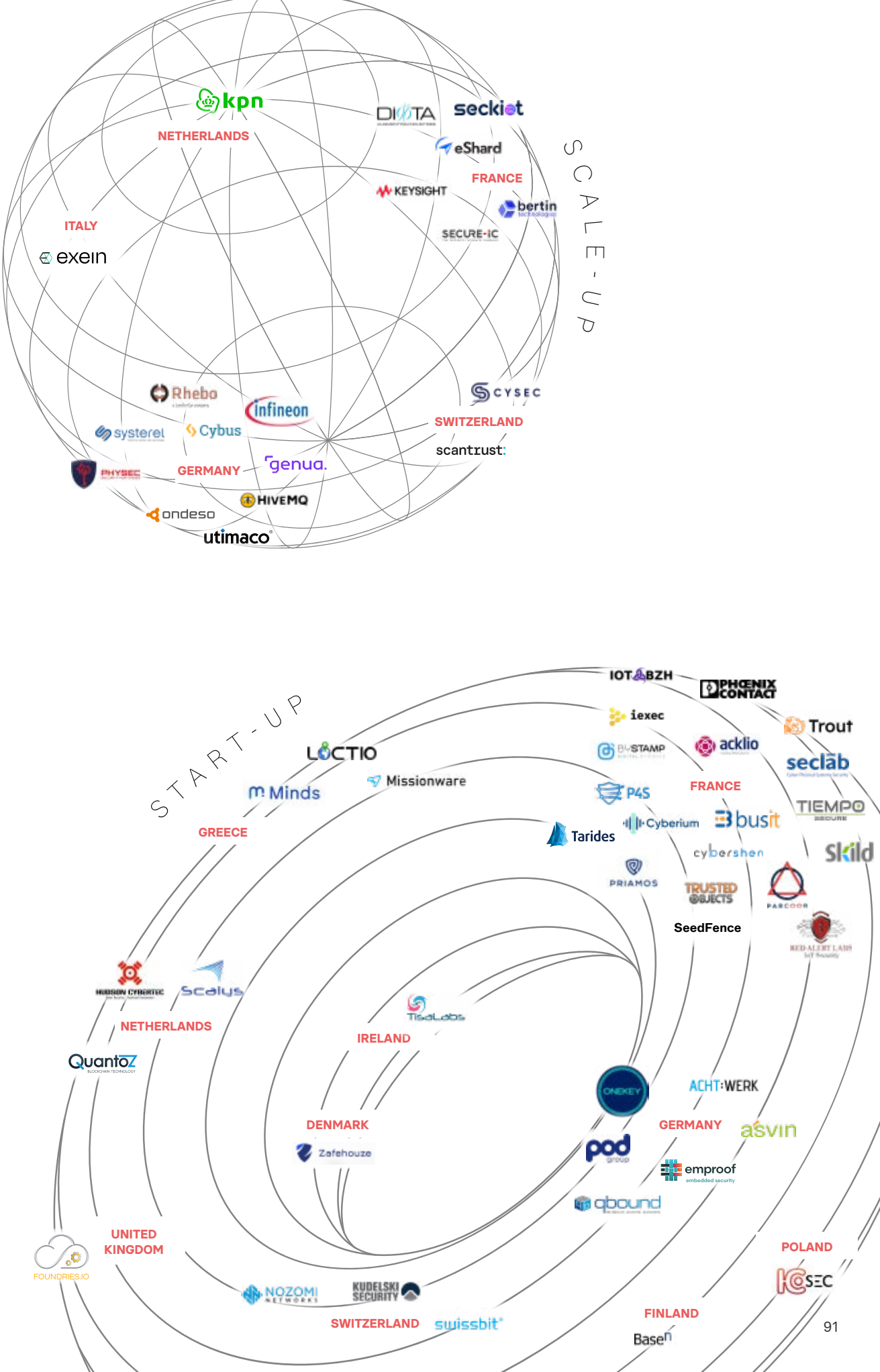
Why Choose European Technology: European providers understand the unique needs of regional industrial environments and ensure compliance with EU safety and security standards. Their expertise strengthens Europe's ability to secure its critical infrastructure independently.

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.

39
START-UPS

19
SCALE-UPS



Interview Scale-Up

SEKOIA.IO

By focusing on collaboration, regulatory harmonization, and investment in talent and technology, Europe can build a thriving cybersecurity ecosystem that competes globally while safeguarding its digital sovereignty.



Scaling European champions through an open XDR approach in cybersecurity

Sekoia.io is a SOC platform, that means a cybersecurity platform which is dedicated to detection and response. We operate in a competitive and evolving market, and customer organizations willing to strengthen their security posture first ask for efficiency and fast time-to-value. It's all about budget concern and ROI coming from top management, which must become real in cybersecurity choices.

From a business perspective, the EU cybersecurity market is not mature and is currently marked by consolidations- a trend that is likely to continue. Our European champions should be able to benefit from EU market access to develop their international expansions and make sure they will be able to compete with US & Israeli tech giants. While some initiatives like the NIS2 directive are key to improve European cyber-resilience, the EU should find the balance between regulation and openness.

Rather than platformization - which in the end favours tech giants - we believe the solution lies in interoperability between security technology solutions - an initiative promoted for instance within the Open XDR approach. It is also the European DNA to favour collaboration and openness, instead of vendor lock-in. We are stronger together!

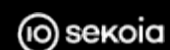
Sekoia.io is the European expert in extended detection and response solutions boosted By AI and Cyber Threat Intelligence. By combining threat anticipation through knowledge of attackers with automation of detection and response, the Sekoia SOC platform provides security teams a unified view and total control over their information systems.

sekoia.io



**David
BIZEUL**
Co-founder and CSO

Sekoia.io



European Cybersecurity Mapping 2025

SECURE COMMUNICATION PLATFORM



Legend

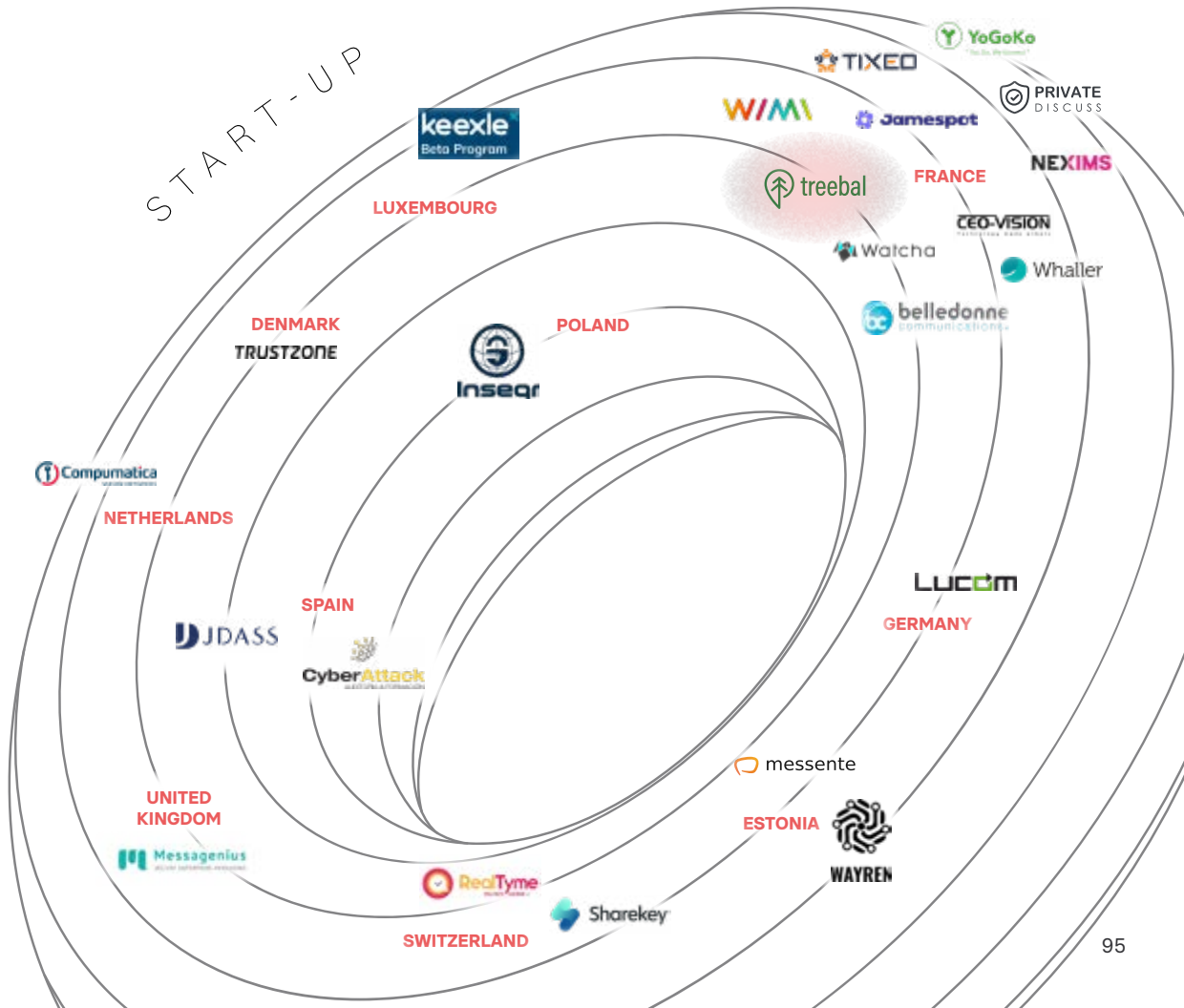
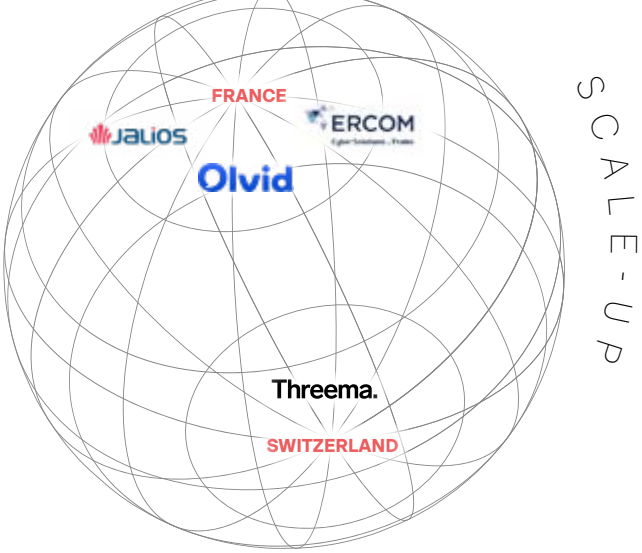
- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Provides encrypted communication channels for secure messaging, data exchange, collaborative and videoconference systems.

Why Choose European Technology: European vendors design platforms 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.



23
START-UPS

4
SCALE-UPS

Interview Scale-Up

SIGNICAT

While our primary push is always on organic growth, we have used M&A as a strategic lever to expand into new markets. ... Our end-goal is to build the most comprehensive and advanced digital identity and fraud platform globally. On the back of this the goal is to consolidate our European position further and establish a global position.



Strategic Acquisitions: Signicat has made several acquisitions across Europe. What strategic goals have these acquisitions achieved, and how have they enhanced your service offerings?

We've made 7 bolt-on acquisitions in the past 5 years, all of them serve two purposes. They are contributing to our goal of building a Scalable, Pan-European platform that supports the whole digital identity lifecycle, and secondly they are bringing in industry-leading talent.

Each of the acquisitions enhances our offerings in unique ways. One example is our UK based acquisition Sphonic. They are a market leader in Risk Orchestration technology operating on 200+ partner sources to solve for KYC, KYB and AML use-cases. Another example is Lithuanian-based Dokobit, which is a leader in Signing and Portals.

Integration Challenges: What challenges have you encountered during the integration of these acquired companies, and how have you addressed them to maintain service continuity and innovation?

All acquisitions are different and come with different integration pain-points, but typical challenges would fall in three areas. One is integrating teams across different locations and cultural preferences, another is enabling product and tech integration to enable cross-selling synergies and the third is resolving back-office processes, systems to ensure one unified way of working.

To enable a straightforward path to technology integration, all acquisition candidates are put through a rigorous DD process. Moreover, Signicat has developed and fine-tuned our integration playbook with clearly defined activities to be executed at various phases of the integration process.

Our goal is to ensure that existing customers of both entities remain undisturbed during integration processes, while making sure that over time they get the benefit of being able to use the complete product platform. This usually involves a fair amount of work to ensure service redundancy, a clear rationale around replacing any duplicate services for a clearly

better service, carefully developed decommission plans with clear and frequent communication.

Over the past years, we have also built our state-of-the-art next gen. Digital Trust Platform that is built on best-in-class tech principles around containerization and microservices driven architecture. This further enables easier integration of services from acquired entities.

Market Expansion: How have these acquisitions influenced Signicat's expansion into new European markets, and what impact have they had on your customer base and partnerships?

While our primary push is always on organic growth, we have used M&A as a strategic lever to expand into new markets. An example of this would be Sphonic's acquisition, which strengthened our presence in the UK, and ElectronicID which strengthened our presence in Iberia and Latam.

There hasn't been a big shift in customer base or partnerships through acquisitions, as all acquisitions largely serve similar customers in similar verticals to Signicat. That said, most acquisitions tend to serve customers in their core market. Cross-selling products from the complete platform gives us an opportunity to expand both the number of markets we serve these customers in and the range of services they use from us. Based on that, over time we have steadily built up more and more Pan-European relationships across the base.

Technological Synergies: Can you discuss any technological synergies realized from these acquisitions that have improved your digital identity and cybersecurity solutions?

The technologies acquired add to the toolbox of Signicat, broadening and deepening the coverage of the digital identity lifecycle. Having these building blocks in the toolbox enables us to combine solutions and develop new products like our leading Identity Document and Biometric Verification products, or our best-in-class Orchestration suite.



Signicat is a pioneering, pan-European digital identity company with an unrivalled track record in the world's most advanced digital identity markets. Founded in 2006, Signicat's mission is to build technology for people to trust each other in a digital world. Its Digital Identity Platform incorporates the most extensive suite of identity-proofing and authentication systems in the world, all easily accessible through a single integration point. The platform supports and orchestrates seamlessly the full identity journey, from recognition and onboarding, through login and consent, to making legally binding business agreements which stand the test of time. In 2019, Signicat was acquired by leading European private equity investor Nordic Capital. Today, Signicat boasts a workforce of over 450 dedicated professionals across 17 European offices.

signicat.com



Pinar ALPAY
Chief Product
& Marketing Officer

Signicat

Interview Scale-Up

SIGNICAT

In addition to this, Signicat has developed a best-in-class next-gen Tech platform including a state-of-the-art internal developer platform.

The infrastructure and the related experience from building it is very useful to accelerate the technological evolution journey for the acquired entities.

In addition, Signicat has a number of leading certifications essential to be able to serve the strictest customers requiring the highest level of assurance e.g., in Banking and Financial services. Acquiring these certifications can be a long and arduous process, but our in-house Information Security team is able to guide the incoming organizations through these processes.

All of this is in addition to typical operational synergies that you'd encounter e.g., from consolidating tech. stacks, cloud and other supplier contracts, etc.

Future Outlook: Looking ahead, what are Signicat's plans for further growth and innovation in the digital identity and cybersecurity landscape?

Our end-goal is to build the most comprehensive and advanced digital identity and fraud platform globally. On the back of this the goal is to consolidate our European position further and establish a global position.

Our innovative product team and strong commercial organization would drive a large part of the journey organically. Where needed, we plan to continue leveraging successful M&A to accelerate time to market.



European Cybersecurity Mapping 2025

SENSIBILISATION PLATFORM



Legend

- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Raises cybersecurity awareness and trains employees to recognize and respond to threats.

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

Importance for European sovereignty: 7/10

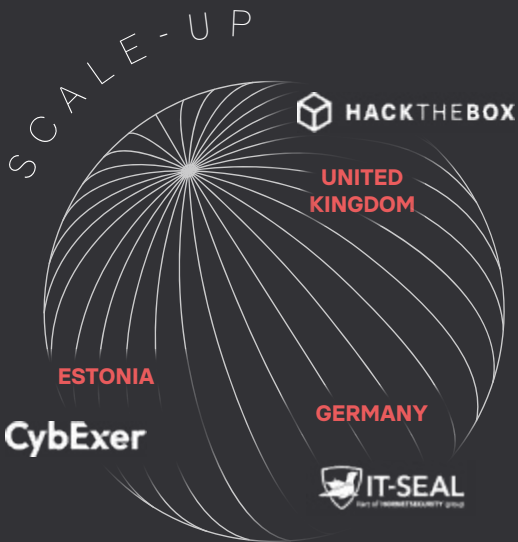
Awareness and training are essential for resilience but have a lower direct impact on sovereignty compared to technologies securing infrastructure or data.

14

START-UPS

3

SCALE-UPS



Interview Scale-Up

CYSEC

As the industry evolves, the question of European consolidation is becoming more pressing. We believe that institutions, large users, and vendors must collaborate to create a more unified cybersecurity ecosystem. Strategic investments and cooperative efforts will be essential to drive this change, with institutions playing a leading role in fostering partnerships and incentivizing collaboration.



As there is a rapid expansion of the space sector, cybersecurity has become a major challenge, requiring robust and scalable solutions to address the vulnerabilities of space applications. CYSEC, a leader in this field, is at the forefront of providing security solutions tailored to the needs of mission-critical systems and satellite communications. Since 2020, there have been significant advances in the field of cybersecurity. For mission-critical systems, the emphasis is increasingly on integrating security measures right from the start of the design process. This evolution takes into account the growing complexity of threats and the need for resilience. At the same time, satellite communication has embraced innovations such as software-defined satellites, which offer flexibility but introduce new vulnerabilities. By 2027, CYSEC foresees the adoption of secure-by-design architectures, where encryption and authentication are seamlessly integrated to create robust and adaptable communication systems.

However, innovation in cybersecurity requires substantial investment especially in research and development. In Europe, this poses a particular challenge, as quick and efficient funding is crucial for execution. Public-private partnerships and programs like Horizon Europe provide critical support, but vendors must also work to streamline financial flows and maximize the impact of these investments.

Another key trend is the demand for integrated cybersecurity solutions. European customers are increasingly dissatisfied with fragmented offerings and seek cohesive, interoperable systems that simplify deployment and management. CYSEC has embraced this trend by prioritizing interoperability, enabling users to integrate various systems seamlessly while maintaining the freedom to select solutions that best meet their needs. As the industry evolves, the question of European consolidation is becoming more pressing. CYSEC believes that institutions, large users, and vendors must collaborate to create a more unified cybersecurity ecosystem.

Strategic investments and cooperative efforts will be essential to drive this change, with institutions playing a leading role in fostering partnerships and incentivizing collaboration.

Finally, EU regulations have provided a much-needed framework to raise the security baseline across the industry. While imposing interoperability could help create a cohesive cybersecurity landscape, it is essential to balance standardization with innovation. Beyond regulation, CYSEC sees a clear need for continued support for R&D and collaboration, ensuring Europe remains competitive in securing the future of space.

Thanks to its proactive approach and commitment to innovation, CYSEC is helping to build a safe and resilient space sector that meets the demands of an ever-changing media environment.



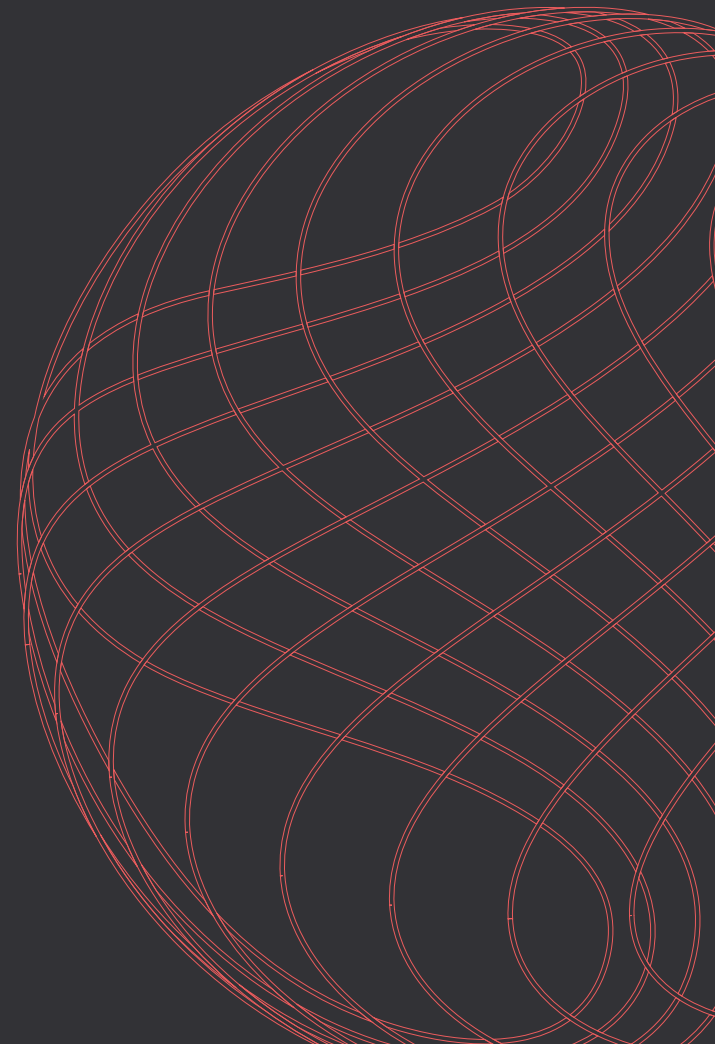
A sovereign and encrypted solution that integrates an enhanced authentication system, verifying the identity and reliability of callers in both audio and video.

cysec.com



Patrick TRINKLER
Co-Founder & CEO

CYSEC



European Cybersecurity Mapping 2025

THREAT MANAGEMENT



Legend

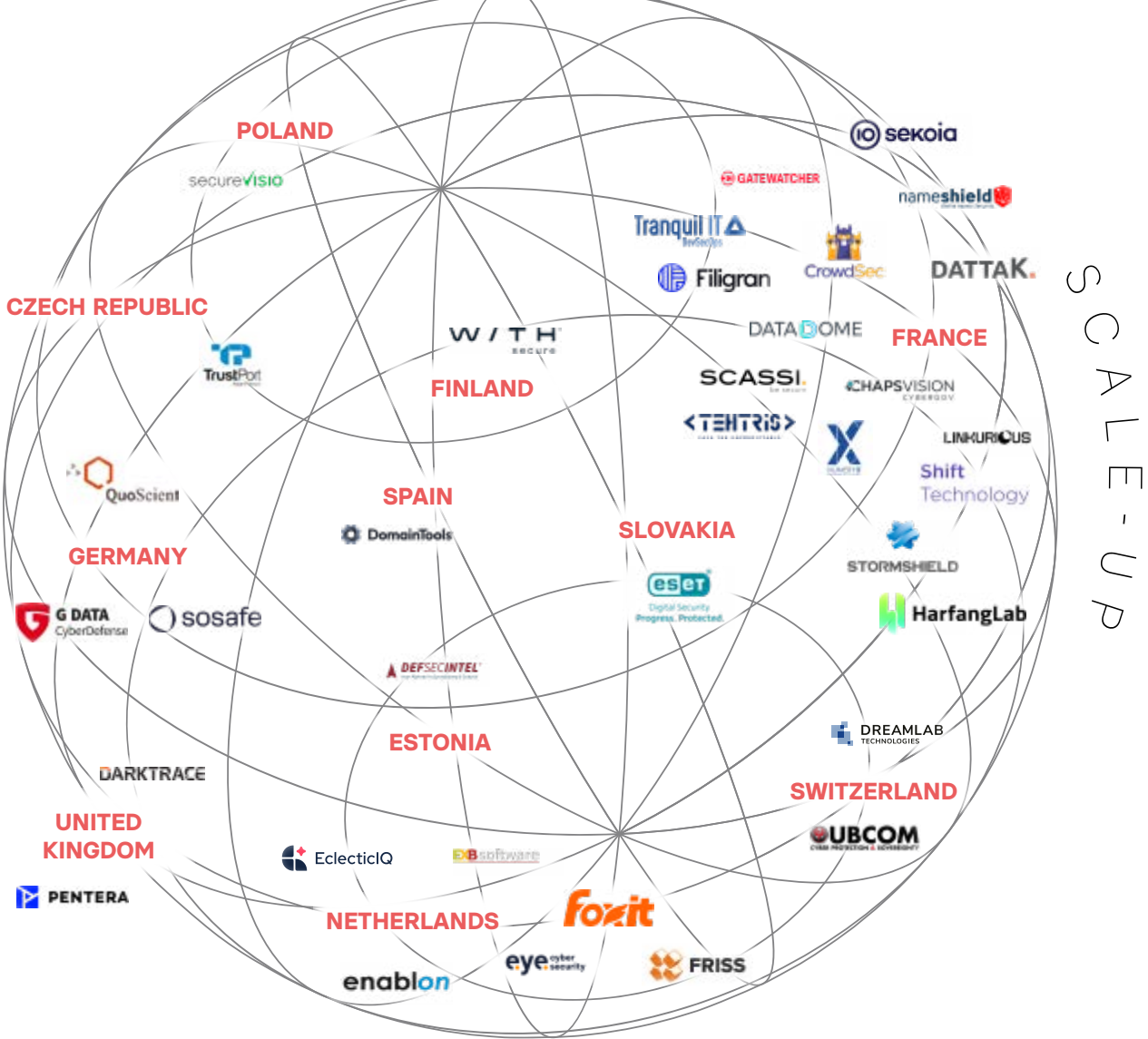
- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Identifies, analyzes, and mitigates cyber threats with proactive and reactive strategies. More and more AI based and automatized, it allows cybersecurity teams to avoid wasting time and focus on key issues.

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

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.



SCALE-UP

European Cybersecurity Mapping 2025

THREAT MANAGEMENT



Legend

- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Identifies, analyzes, and mitigates cyber threats with proactive and reactive strategies. More and more AI based and automatized, it allows cybersecurity teams to avoid wasting time and focus on key issues.

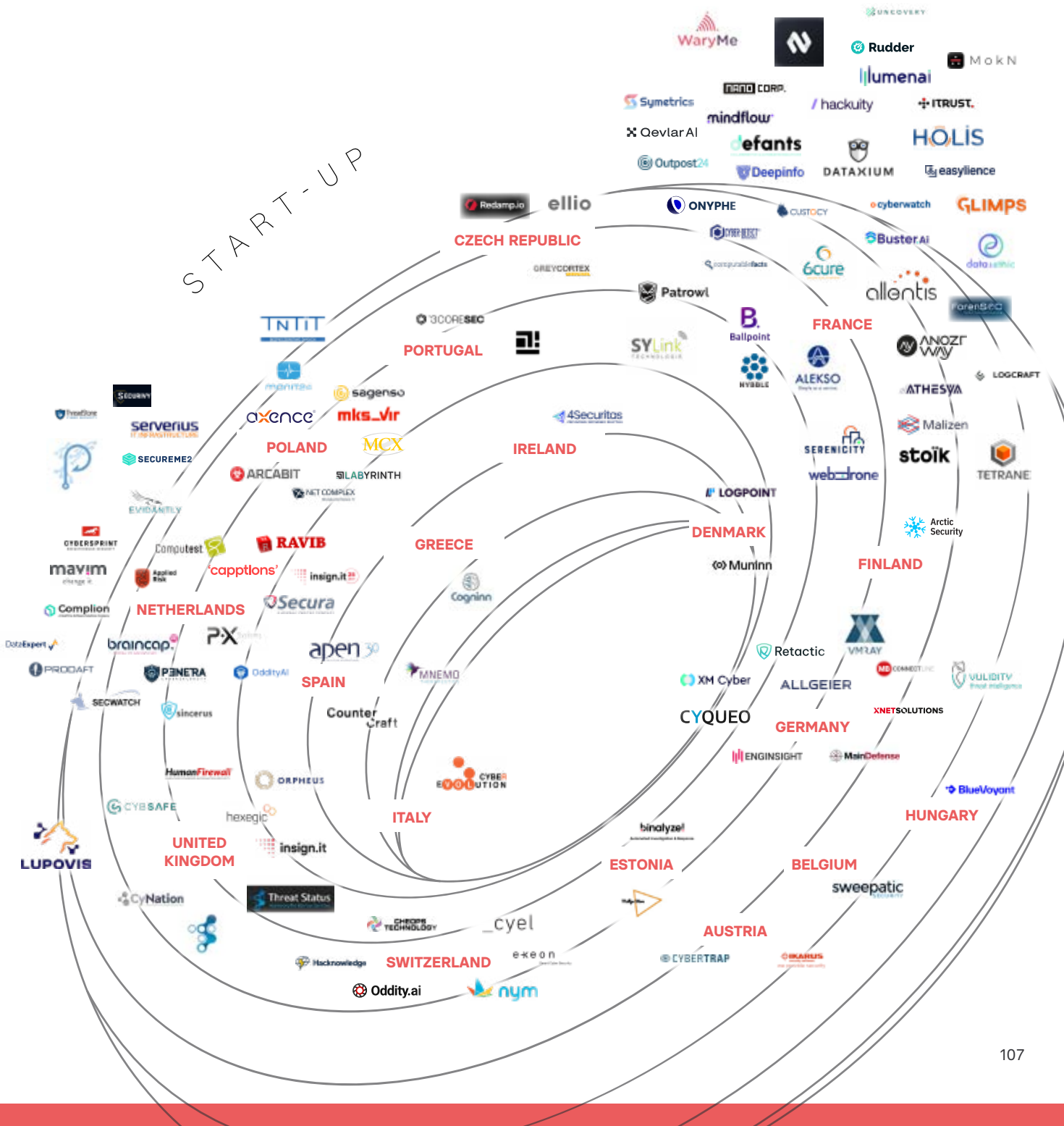
Why Choose European Technology: European providers deliver solutions tailored to local regulatory frameworks and threat landscapes, ensuring trusted and sovereign management of cybersecurity risks.

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.

116
START-UPS

36
SCALE-UPS



Interview Academia Supporter

ÉCOLE POLYTECHNIQUE

European vendors have a rich and diverse offer. One may see the amount of European regulations as a weakness hindering innovation, but it also ensures that European vendors all offer products with reasonable security guarantee leading to a very healthy ecosystem, making it one of its main strengths.



As a responsible for Research and High Education programs, what the biggest challenges you see regarding cyber resilience, and what are the key trends in technology you see at present or coming?

Cyber resilience should be central to a company's digital strategy, encompassing three key areas: anticipation, detection, and reaction. Anticipation involves choosing robust technologies and securing data in storage and transit, including preparing for post-quantum migration as per NIST and ANSSI deadlines. Detection requires prompt analysis of irregular behaviours, where AI can enhance log and behaviour analysis. Reaction goes beyond solving technical issues to include effective crisis communication to reassure clients, an often-overlooked aspect. Academia should focus on advancing security technologies while training individuals to stay calm, make sound decisions, and communicate effectively during crises.

How do you see the European cybersecurity vendors' offering? Which are its good points, and where are the weaknesses?

European vendors have a rich and diverse offer. One may see the amount of European regulations as a weakness hindering innovation, but it also ensures that European vendors all offer products with reasonable security guarantee leading to a very healthy ecosystem, making it one of its main strengths, quite like Oulipo did for literature.

What do you see as the most important areas where students should be trained?

Cybersecurity is becoming so vast that it gets harder to be trained in everything. To my eyes, students should be trained to be curious, and learn to pick which new technology to study next. That being said, clearly some trends are emerging:

- Secure Programming, being able to develop sound programs running in constant time without memory leak will always be an important cybersecurity skill, whatever languages are used in the future.
- Core building blocks like cryptography will always be useful, probably with post-quantum consideration.
- Learning how AI and cyber can interact for better and worse

Risk and crisis managements are very important skills to develop, remembering to integrate the human element in cybersecurity, and how to behave when even the best defence fails.

Do we have enough cooperation across Europe regarding cybersecurity? Between academics and between academics and the industry?

Cybersecurity is really a field where cooperation is important, as a defence is as strong as its weakest link. In academia, conferences and horizon programs are great occasions to foster this cooperation across Europe. However, the gap is bigger between academics and companies, partly due to a different work culture and trade secrets, but also simply because they don't know each other well enough, and I genuinely believe specific events to promote this kind of action can be excellent.



Since its creation in 1794, École Polytechnique has been producing and sharing multidisciplinary knowledge at the highest level, for its students, for companies and for society, by developing an entrepreneurial spirit, boldness and a sense of general interest in its three fundamental missions of education, research and innovation.

polytechnique.edu



Olivier BLAZY
Professor

École Polytechnique

European Cybersecurity Mapping 2025

VULNERABILITY ASSESSMENT PLATFORM



Legend

- TYPE:
- SCALE-UP
 - START-UP
- OTHERS:
- MULTI-SECTOR COMPANY

Short Pitch: Identifies and prioritizes system vulnerabilities to provide a sound basis to IT systems protection and resilience policy.

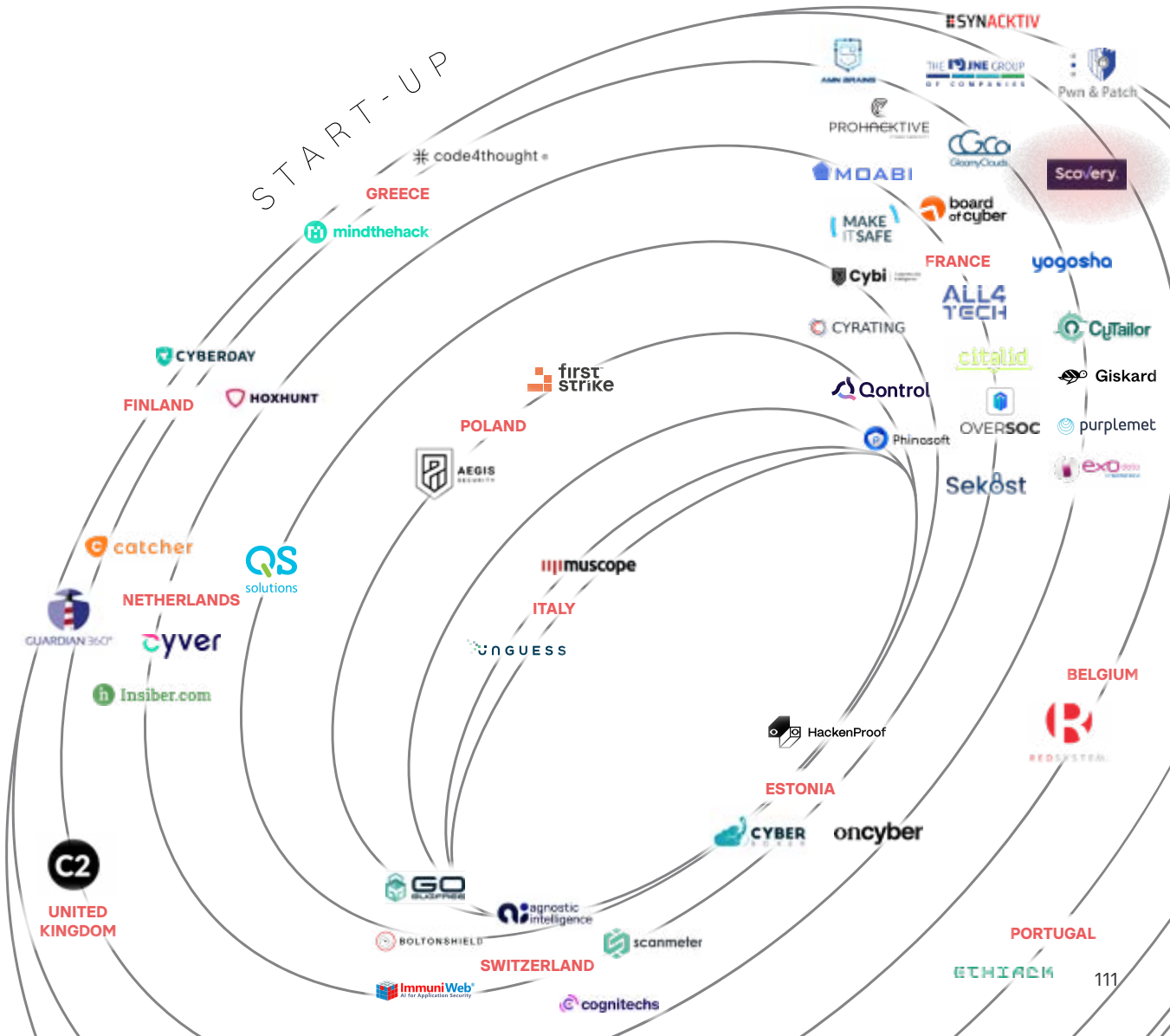
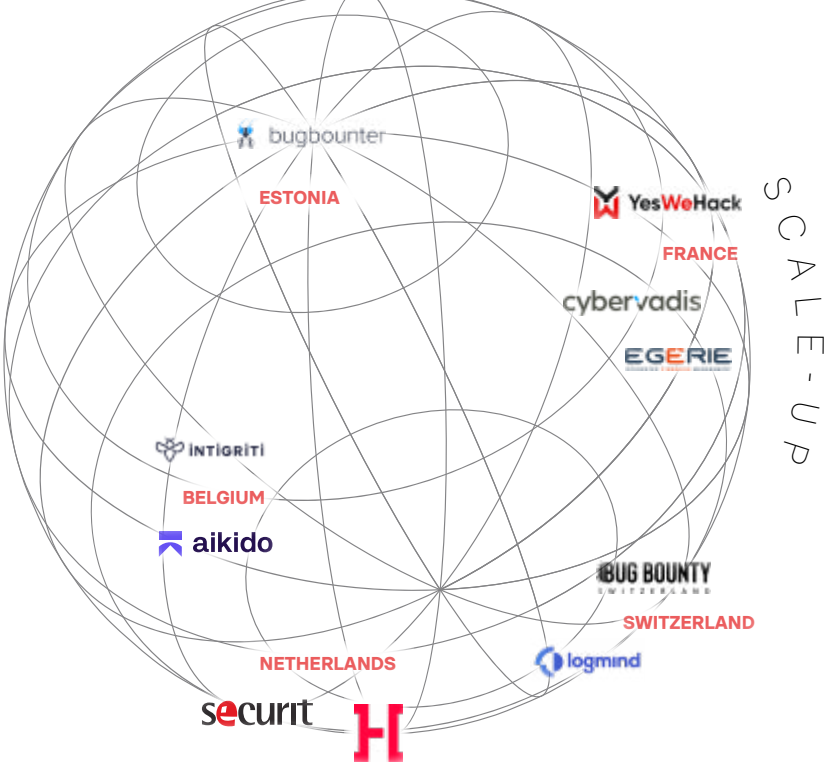
Why Choose European Technology: European platforms ensure that sensitive assessment data remains within EU jurisdictions, aligning with privacy and sovereignty goals. This promotes trust and transparency in securing organizational systems.

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.

47
START-UPS

10
SCALE-UPS



The key lies in advancing and adopting technical standards that enable interoperability between components. Such standards would support a modular approach, allowing organizations to integrate best-in-class solutions while maintaining flexibility and fostering innovation.

French excellence at the service of European digital sovereignty

Founded in 2013, Hexatrust is the leading association of French and European champions in cybersecurity, trusted cloud and the digital workplace. Bringing together more than 140 software publishers and integrators, this trade association embodies French technological excellence in the service of European digital sovereignty.

Hexatrust's mission is based on three fundamental pillars: to promote the expertise and innovation of its members, while defending their interests with institutions; to encourage the development of digital SMEs/ETIs; and to build a coherent national industrial offering. To this end, the association plays a key role in helping its members to access public and private markets, while stimulating collaborative innovation.

Committed to European digital sovereignty, Hexatrust is particularly active in the debates surrounding the introduction of new regulations impacting the industry and helping its members and companies in the sector to cope with them (NIS 2, SREN, etc.).

Its vision for the future of the European cybersecurity industry revolves around three major axes:

- Strengthening Europe's strategic autonomy through trusted sovereign solutions
- Accelerating collaborative innovation between European players
- Developing an industry of excellence capable of competing internationally.

Hexatrust embodies the dynamics of an innovative, sovereign French cybersecurity industry, resolutely turned towards Europe, to build together a digital world of trust.

Jean-Noël de Galzain,
Chairman of Hexatrust



European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP AND SCALE-UP EDITION

CONCLUSIONS OF THE EUROPEAN CYBERSECURITY MAPPING

The European Cybersecurity Mapping highlights the dynamic and rapidly evolving landscape of cybersecurity in Europe. Through comprehensive research, interviews, and collaboration with industry leaders, this mapping underscores several key findings:

CONCLUSION

DIVERSITY OF PLAYERS

The European cybersecurity ecosystem is rich in diversity, comprising start-ups, scale-ups, established companies, and public institutions. These players bring a wide range of innovative solutions across AI security, application security, OT security, and more, addressing both emerging and established threats.

FRAGMENTATION AND GAPS

While diversity is a strength, fragmentation remains a challenge. Many promising start-ups lack visibility, and industry associations are not yet fully interconnected. Additionally, certain regions and sectors are underrepresented, reflecting a need for broader inclusion and outreach. The move towards consolidation between vendors that we see emerging should be highlighted and supported.

THE IMPORTANCE OF SOVEREIGNTY

European cybersecurity sovereignty is crucial for protecting critical infrastructure, ensuring compliance with GDPR, CRA, NIS2 and other regulations, and reducing dependence on foreign technologies. This mapping demonstrates that Europe has the talent and solutions to lead in cybersecurity but requires greater collaboration and investment to realize its potential.

NEED FOR ECOSYSTEM INVESTMENT

Building and maintaining a robust cybersecurity ecosystem requires significant resources. Sponsors, industry associations, and stakeholders must continue to invest in initiatives like this mapping to ensure the ecosystem's growth and sustainability.

COLLABORATION IS KEY

Collaboration among start-ups, corporates, industry associations, and governments is essential for addressing Europe's cybersecurity challenges. A shared vision and commitment to strengthening the ecosystem can drive innovation, improve resilience, and ensure Europe's global competitiveness.

ACTION PLAN FOR STRENGTHENING THE EUROPEAN CYBERSECURITY ECOSYSTEM

To address these findings and create a stronger, more unified cybersecurity ecosystem in Europe, we propose the following action plan:

1. Foster Collaboration Across Stakeholders

— Create Regional Hubs:

Establish regional cybersecurity hubs to connect local players and bridge gaps between regions.

— Strengthen Public-Private Partnerships:

Facilitate joint initiatives between governments, corporates, and start-ups to tackle large-scale cybersecurity challenges.

— Enhance Cross-Sector Engagement:

Encourage participation from non-tech sectors (e.g., finance, healthcare) to ensure comprehensive cybersecurity coverage.
2. Promote European Sovereignty in Cybersecurity

— Prioritize European Solutions:

Advocate for the use of European vendors in critical infrastructure projects to reduce dependency on non-EU technologies. Our American friends are good at leveraging Public orders, as well as having private Corps adopting innovation and purchasing it from local actors. European decision-makers should privilege really open competition and give better chances to local vendors.

— Help vendors to cooperate and make their offers interoperable,

so that customers which demand solutions with a wider and fully integrated functional scope easily find them among the European offerings.

— Support Strategic Standards:

Align cybersecurity efforts with EU regulations and policies to ensure uniformity and compliance.

— Invest in Critical Technologies:

Focus on areas like cryptography, AI security, and OT security to strengthen Europe's autonomy.
3. Increase Investment in the Ecosystem

— Secure More Sponsors:

Attract sponsors to fund research, mapping, and innovation projects that enhance the ecosystem's quality and visibility.

— Boost R&D Funding:

Advocate for increased European funding for cybersecurity research and development, particularly for start-ups and scale-ups.

— Encourage Venture Capital Participation:

Highlight the business potential in cybersecurity to draw more private investment. So far, despite some progress compared to the years before 2020, the European capacity to finance cybersecurity vendors 'development is yet by far too small. As a result, a number of European vendors which have succeeded to exceed some threshold and/or have developed a unique technology, have many chances to end up taken over by a US fund. It's time to consider unifying and strengthening the European financial market, so that innovative cybersecurity European industry can develop and remain European.
4. Enhance Ecosystem Representation and Visibility

— Expand Future Mapping Efforts:

Ensure the 2026 mapping includes a broader range of companies, regions, and associations to capture a more comprehensive picture.

— Encourage Submissions:

Invite start-ups, scale-ups, and industry associations to actively participate in mapping efforts by sharing insights and success stories.

— Showcase European Leadership:

Promote European cybersecurity achievements through conferences, publications, and international collaborations.
5. Strengthen Awareness and Skills Development

— Develop Awareness Campaigns:

Launch sensibilization platforms to train individuals and organizations on cybersecurity best practices.

— Promote Education and Training:

Invest in cybersecurity education at all levels, from primary schools to specialized university programs. Multiply the occasions for Public Research labs and High Education to connect to the industry, this at multi-national scale across Europe.

— Upskill the Workforce:

Support initiatives that provide cybersecurity training for professionals across industries.
6. Support Policy and Regulatory Development

— Advocate for Clear Policies:

Work with EU policymakers to create clear, actionable guidelines that support innovation while ensuring security.

— Streamline Compliance Efforts:

Develop tools to help companies navigate the complexities of cybersecurity compliance.

— Encourage Data Sharing for Threat Management:

Promote secure and GDPR-compliant data-sharing frameworks to improve threat intelligence and response.



Call to Action

The European cybersecurity ecosystem has incredible potential, but realizing it requires collective effort. We encourage all stakeholders to join us in this mission:

- **Sponsors:** Provide the financial support needed to sustain and grow initiatives like this mapping.
- **Start-ups and Scale-ups:** Share your stories, innovations, and insights to help us showcase the ecosystem's vibrancy.
- **Industry Associations:** Collaborate with us to ensure your members are represented and your expertise is included.
- **Governments and Policymakers:** Work with us to create the frameworks and funding mechanisms needed to secure Europe's digital future.

Together, we can build a cybersecurity ecosystem that not only protects Europe but also sets a global standard for collaboration, innovation, and sovereignty. Let's make Europe a global leader in cybersecurity.

For inquiries or to get involved, contact us at cybermapping@european-champions.org



ABOUT THE EUROPEAN CHAMPIONS ALLIANCE (ECA)

Building Europe's Future Together

The **European Champions Alliance (ECA)** is a dynamic, nonprofit organization dedicated to fostering collaboration and innovation within Europe's tech ecosystem. We bring together start-ups, scale-ups, corporates, investors, and institutions to create a unified network that strengthens Europe's position in the global technology landscape. Our mission is to empower European tech champions by promoting cross-border growth, knowledge sharing, and ecosystem development.

Why the Ecosystem Matters

The European tech ecosystem thrives on collaboration. No single organization, company, or country can address the challenges of a rapidly evolving digital world alone. By building strong networks, we can collectively:

- **Drive Innovation:** Foster the development of cutting-edge technologies that respond to Europe's unique needs and values.
- **Enhance Sovereignty:** Strengthen Europe's independence in key technological areas like cybersecurity, AI, and digital infrastructure.
- **Encourage Growth:** Create opportunities for start-ups and scale-ups to thrive, supported by an interconnected and supportive environment.

How Ecosystem Partners Can Support Us

To achieve these goals, we need the active involvement of all ecosystem partners. Here's how you can help:

1. **Sponsorship:**
Sponsors play a critical role in enabling our initiatives. Your financial support helps us conduct research, organize events, and produce valuable resources like the European Cybersecurity Mapping. In return, sponsors gain visibility, credibility, and recognition as key enablers of Europe's tech ecosystem.
2. **Collaboration:**
Partner with us on initiatives, share your expertise, or contribute to projects like the Cybersecurity Mapping. Your insights and involvement strengthen the value and relevance of our work.
3. **Amplification:**
Help us spread the word about ECA's mission and initiatives. By amplifying our message, you can inspire more organizations to join this collective effort.
4. **Engagement:**
Participate in our events, webinars, and workshops. Engage with our network to exchange ideas, build relationships, and create synergies that drive collective success.

Why This Is Important

Building a resilient, competitive, and collaborative tech ecosystem in Europe is not just important—it's essential. Supporting the ECA means investing in Europe's future:

- It's about securing technological sovereignty and reducing dependence on external players.
- It's about fostering an environment where European tech companies can grow and compete globally.
- It's about creating opportunities for innovation, jobs, and economic growth that benefit us all.

By supporting the ECA, you become part of a movement that drives progress, connects leaders, and shapes the future of European tech. Together, we can build the strong, unified ecosystem that Europe needs to thrive.

For more information on how to support us, please contact us at welcome@european-champions.org. Thank you for believing in our mission and for contributing to Europe's success.



European
Champions Alliance

European Cybersecurity Mapping 2025

European Cybersecurity Excellence

START-UP & SCALE-UP EDITION

powered by

IN CYBER
FORUM

gold sponsors

