MARS 2026

IN CYBER FORUM EUROPE

PANORAMA DE L'INNOVATION

Croissance, souveraineté et passage à l'échelle : les signaux du marché

PRIX DE LA STARTUP

LAURÉATS 2026

Prix du Président de la République	**VIRTUALBROWSER**
Prix de la Croissance	**QEVLAR AI**
Prix de l'Impact Opérationnel	**AVANOO**
Prix de la Croissance	**LABEL4.AI**
Prix Coup de Cœur	**LABEL4.AI**

Sommaire

Le mot du Président du jury

Vous êtes côté grand groupe, avec des contraintes d'intégration, de conformité et de continuité d'activité. Parmi les dossiers reçus, qu'est-ce qui vous a fait dire : « ça, je peux vraiment l'industrialiser dans un SI complexe » ?

Pour un grand groupe comme le Crédit Agricole, on a bien sûr des enjeux et des contraintes un peu spécifiques. Quand on considère une solution innovante, on se pose tout de suite des questions comme « est ce que je n'introduis pas un risque supplémentaire dans mon SI ? », « quelle est la pérennité de la solution ? », « est ce que je vais dégrader ma qualité de service ou ma continuité d'activité en positionnant un SPOF *(single point of failure)* ? ». Et c'est vrai que ça nous rend particulièrement prudents sur des solutions qui joueraient un rôle central sur le fonctionnement même de notre SI, dans des couches d'infrastructures par exemple. En revanche, on peut intégrer beaucoup plus facilement des solutions qui vont améliorer des processus (de détection par exemple, de gouvernance ou de sensibilisation) car on ne prend pas le même type de risque dans ce cas-là.

En tant que directeur cybersécurité et risques IT, qu'est-ce qui fait la différence entre une solution séduisante sur le papier et une solution qui réduit réellement le risque (de façon mesurable) dans une organisation comme le Crédit Agricole ?

Une solution qui réduit réellement les risques est une solution qu'on peut déployer à l'échelle sur un grand périmètre. Bien sûr, c'est important de pouvoir faire des expérimentations sur des « petits » périmètres pour confirmer la pertinence d'une solution, son apport de valeur ou de sécurisation, mais ce qui fait vraiment la différence, c'est quand on peut la déployer à grande échelle et de manière la plus homogènes possible dans la multitude d'environnements que l'on doit couvrir (technologies, géographies). Dans un grand groupe, on est trop souvent confrontés à une multitude de solutions disparates qui couvrent des fractions de périmètre.

On parle beaucoup de souveraineté, mais dans les faits, les critères sont souvent plus nuancés. Qu'est-ce que vous mettez derrière ce mot quand vous évaluez une start-up : localisation des données, gouvernance, dépendances technologiques, capacité d'audit, autre chose ?

C'est un bon sujet, et particulièrement d'actualité dans le contexte géopolitique actuel. Pour commencer, je ne suis pas très à l'aise avec le mot souveraineté, car c'est un terme normalement réservé à un État. Quand on est une entreprise internationale comme le Crédit Agricole, on doit prendre en compte l'ensemble des géographies dans lesquelles on est implantés, et ce qui est souverain en France ne l'est pas forcément dans un autre pays européen ou en Asie. Je préfère donc parler d'autonomie stratégique, qui consiste à ne pas dépendre d'un acteur tiers dans nos choix technologiques.

Nous disposons depuis quelques semaines d'un outil intéressant développé en France par un ensemble d'acteurs publics et privés : l'indice de résilience numérique (IRN). Cet IRN vise à évaluer et piloter les dépendances numériques critiques, en couvrant les dépendances business et stratégiques (augmentations tarifaires, modifications unilatérales de contrat), les dépendances sécuritaires (cybersécurité, autonomie opérationnelle), les dépendances technologiques (explicabilité des modèles d'IA, maîtrise de la chaîne d'approvisionnement technologique) mais aussi, comme vous l'avez évoqué à juste titre, les capacités de gouvernance et de maîtrise opérationnelle. L'utilisation de ce nouvel outil permet de bien adresser l'ensemble des dimensions à prendre en compte.

Si vous aviez un seul conseil à donner aux start-ups cyber qui candidatent : ce serait plutôt de renforcer la preuve (certifications, auditabilité), le *go-to-market* (canaux, partenaires), ou la maturité produit (déploiement, support, intégrations) ? Et quel « problème prioritaire » aimeriez-vous voir attaqué l'an prochain ?

Bien sûr les certifications et l'audibilité sont importantes, mais mon conseil pour les start-ups qui candidatent est double :

1. présenter un dossier de candidature qui met bien en avant le côté innovant de la solution, son potentiel de marché et sa viabilité technologique. C'est bien la combinaison de ces éléments qui permet de convaincre le jury.

2. préparer un pitch qui permet de confirmer ces éléments mais aussi de développer la stratégie de développement, qu'elle soit produit ou commerciale, et de mettre en avant des premiers cas d'utilisation chez des clients

L'an prochain, je serai curieux de voir des start ups qui proposent des solutions concrètes pour résoudre le problème de la cyber dans des plus petites structures (PME, ETI), car c'est très souvent un angle mort, pourtant fondamental à l'échelle française et européenne.

François DELZANT
Président du Jury
Directeur Cybersécurité et Risques IT Groupe
chez Groupe Crédit Agricole

Le regard de l'analyste

SEGMENT 1 : SecOps piloté par l'IA et automatisation de la sécurité offensive

Ce segment représente l'évolution de deux marchés établis et d'une catégorie en émergence rapide.

Premièrement, les plateformes de Security Operations évoluent des systèmes traditionnels de type SIEM et SOAR, reposant sur une orchestration fondée sur des règles, vers une automatisation du SOC nativement conçue autour de l'intelligence artificielle. L'objectif n'est plus simplement de soutenir des workflows, mais de permettre des investigations exécutées par la machine, un raisonnement contextuel et une priorisation à grande échelle.

Deuxièmement, la gestion des vulnérabilités et les tests d'intrusion évoluent également. Ils passent d'approches basées sur des scans statiques et des campagnes ponctuelles à des mécanismes continus et automatisés de validation de sécurité. L'accent se déplace de l'identification de failles théoriques vers la démonstration de leur exploitabilité réelle dans des chemins d'attaque crédibles.

À l'intersection de ces deux tendances apparaît une catégorie émergente : les opérations de sécurité autonomes. Ces solutions utilisent l'IA comme couche d'exécution centrale, et non comme simple fonctionnalité. Elles enquêtent, corrèlent, valident et, dans certains cas, déclenchent des actions de réponse avec une intervention humaine minimale. Les humains restent responsables des décisions, mais les machines opèrent à la vitesse et à l'échelle requises.

POURQUOI CES SOLUTIONS SONT ESSENTIELLES

L'intelligence artificielle accélère massivement les cybermenaces. Les attaquants utilisent désormais l'IA pour l'analyse automatisée de code, la découverte de vulnérabilités, l'adaptation d'exploits, la reconnaissance et la production d'ingénierie sociale extrêmement convaincante. La vitesse de développement et de mutation des attaques a considérablement augmenté. Des cycles de défense reposant principalement sur l'analyse humaine ne peuvent plus suivre ce rythme.

Les défenseurs doivent donc adopter l'IA comme capacité fondamentale. Il ne s'agit pas d'obtenir des gains marginaux d'efficacité, mais d'aligner les capacités défensives sur la vitesse des machines offensives. Sans automatisation ni raisonnement piloté par l'IA, les organisations seront dépassées en matière de détection, de validation et de réponse.

Dans le même temps, la surcharge des analystes SOC atteint des limites structurelles. Les volumes d'alertes continuent d'augmenter sous l'effet des architectures *Cloud* natives, des environnements hybrides, des systèmes centrés sur les API et de l'augmentation des sources de télémétrie. Ajouter simplement davantage d'analystes n'est pas une solution durable. Les organisations ont besoin de solutions capables de réduire réellement le bruit, éliminer les faux positifs et produire des résultats à forte confiance. Lorsqu'elle est correctement implémentée, l'IA peut effectuer un tri à grande échelle et permettre aux experts humains de se concentrer sur les risques critiques nécessitant un jugement.

Un autre défi provient de l'émergence d'environnements massifs et extrêmement volatils. Les identités non humaines, telles que les comptes de service, les API et les identifiants machine, sont désormais bien plus nombreuses que les utilisateurs humains. Les systèmes d'IA agentique introduisent par ailleurs des acteurs partiellement autonomes capables de créer et modifier dynamiquement les états opérationnels. Ces environnements sont élastiques et éphémères. Les modèles de contrôle centrés sur l'humain ne peuvent pas gérer cette vitesse ni cette complexité. Les systèmes de sécurité doivent donc fonctionner de manière autonome, continue et à grande échelle.

La convergence entre l'offensive pilotée par l'IA, les limites humaines opérationnelles et des infrastructures dynamiques rend l'innovation dans les opérations de sécurité autonomes indispensables.

CONTEXTE DES FOURNISSEURS

Qevlar AI illustre l'automatisation du SOC conçue nativement autour de l'IA. Son approche repose sur l'investigation autonome des alertes grâce à un raisonnement contextuel et basé sur des graphes. En réduisant les faux positifs et en standardisant les investigations à la vitesse de la machine, la solution répond directement à la surcharge des analystes et permet aux équipes humaines de se concentrer sur les incidents à fort impact.

XEOPS.AI représente l'évolution de la sécurité offensive vers une validation continue de l'exploitabilité pilotée par l'IA. En découvrant et en vérifiant automatiquement les vulnérabilités exploitables, la solution distingue les failles théoriques des risques réellement exploitables. Dans un contexte où les attaquants utilisent l'IA pour accélérer le développement d'exploits, cette capacité apporte une clarté et une priorisation critiques.

Ensemble, ces solutions illustrent la transition plus large d'outils assistés par l'humain vers des opérations de sécurité exécutées par des machines et supervisées par des experts.

SEGMENT 2 : Gouvernance, gestion du risque et de l'exposition

Ce segment regroupe des solutions centrées sur la gouvernance globale, la visibilité et la maîtrise du risque. Il répond à une réalité fondamentale : dans un environnement où les cybermenaces évoluent aussi rapidement que les nouveaux produits de sécurité apparaissent, la gouvernance devient la couche de contrôle principale.

Les organisations opèrent aujourd'hui avec des empilements fragmentés de solutions de sécurité spécialisées. Sans découverte complète des actifs et supervision coordonnée, ces contrôles restent partiels et incohérents.

Le socle établi de ce segment repose sur les marchés du GRC (Governance, Risk and Compliance), de la gestion du risque tiers et de la gestion de l'exposition. Ces marchés convergent progressivement. Les cadres traditionnels de gouvernance sont enrichis par des capacités de visibilité en temps réel et de découverte technique. La gestion du risque fournisseur ne repose plus seulement sur des questionnaires périodiques mais évolue vers des évaluations continues et fondées sur des preuves. La gestion de l'exposition élargit la perspective : il ne s'agit plus seulement de vulnérabilités, mais de risques systémiques liés aux actifs, aux identités, aux fournisseurs et aux services *Cloud*.

Un principe central s'impose : on ne peut pas protéger ce que l'on ne connaît pas. La découverte est le préalable à la gouvernance. Ce n'est qu'en comprenant leurs actifs, leurs dépendances, leurs identités, leurs fournisseurs et les composants émergents liés à l'IA que les organisations peuvent définir des politiques cohérentes et appliquer des mesures de protection efficaces.

POURQUOI CES SOLUTIONS SONT ESSENTIELLES

La prolifération de l'IA agentique représente un défi structurel de gouvernance. Grâce à des approches de développement à faible barrière, parfois qualifiées de vibe coding, les utilisateurs métiers et les développeurs déploient de plus en plus d'agents d'IA autonomes ou semi-autonomes en dehors des processus de contrôle formels. Cela génère un phénomène de *shadow AI,* dont l'ampleur et les risques dépassent largement ceux historiquement associés au *shadow IT* ou au *shadow SaaS*.

Les agents d'IA peuvent agir, interagir avec les systèmes et générer de nouveaux états opérationnels de manière autonome. Des erreurs de configuration, des privilèges excessifs ou des manipulations malveillantes peuvent donc produire des effets amplifiés. La gouvernance doit donc inclure la découverte et le contrôle de ces nouvelles entités.

Dans le même temps, les risques liés aux tiers et aux chaînes d'approvisionnement augmentent. Les écosystèmes numériques sont profondément interconnectés. Il devient plus facile pour des attaquants d'exploiter des fournisseurs plus petits ou moins matures pour atteindre une cible principale.

Les évaluations périodiques traditionnelles des fournisseurs ne suffisent plus. Il faut une visibilité continue et un scoring dynamique du risque pour comprendre et maîtriser cette surface d'attaque étendue.

Les phases de test et de validation exigent également des environnements strictement contrôlés. À mesure que les organisations expérimentent de nouveaux systèmes d'IA, de nouvelles applications et des intégrations complexes, des environnements sécurisés et isolés sont nécessaires pour évaluer les risques sans exposer les systèmes de production. La gouvernance doit donc intégrer des garde-fous architecturaux, en plus des politiques.

Enfin, l'exposition s'étend désormais aux services *Cloud*, aux API, aux identités machine et aux dépendances externes. La surface d'attaque est dynamique et souvent exposée à l'extérieur. Comprendre l'exposition en continu devient essentiel pour prioriser les contrôles et allouer efficacement les ressources.

Dans ce contexte, la gouvernance n'est pas une contrainte bureaucratique. Elle constitue le cadre stratégique permettant d'appliquer les mesures de protection de manière cohérente et proportionnée au risque réel.

CONTEXTE DES FOURNISSEURS

Avanoo répond au déficit de gouvernance généré par la prolifération d'outils d'IA et de services SaaS non contrôlés. En identifiant et en évaluant les outils d'IA non autorisés, la solution apporte la visibilité nécessaire pour définir et appliquer des politiques adaptées dans un environnement où les outils autonomes se multiplient rapidement.

Galink se concentre sur les risques cyber liés aux fournisseurs et aux partenaires. Sa plateforme permet une évaluation continue de la maturité des prestataires, aidant les organisations à comprendre et à réduire leur exposition dans des chaînes d'approvisionnement numériques de plus en plus interconnectées.

Noways intervient sur la dimension risque et résilience du *Cloud*. En cartographiant les dépendances et en évaluant les risques liés aux changements, la solution renforce la gouvernance dans des environnements *Cloud* complexes où les erreurs de configuration et les modifications non maîtrisées peuvent fortement accroître l'exposition.

SHINDAN s'inscrit également dans ce segment en offrant une visibilité sur l'intégrité et la posture de sécurité des appareils mobiles. Dans des contextes impliquant des dirigeants ou des profils à haut risque, comprendre l'état de compromission ou la configuration d'un appareil est essentiel pour appliquer des politiques de protection efficaces et réduire l'exposition.

Ensemble, ces solutions montrent que la cybersécurité efficace commence par une découverte exhaustive et une gouvernance solide. C'est sur cette base que les contrôles de protection peuvent être appliqués de manière durable.

Martin KUPPINGER
Founder and Principal Analyst responsible
KuppingerCole research

Présentation des lauréats 2026

Prix du Président de la République	**VIRTUALBROWSER**
Prix de la Croissance	**QEVLAR AI**
Prix de l'Impact Opérationnel	**AVANOO**
Prix de la Croissance	**LABEL4.AI**
Prix Coup de Cœur	**LABEL4.AI**

VIRTUALBROWSER

ANNÉE DE CRÉATION : 2024

SIÈGE SOCIAL : PARIS

EFFECTIF : 15

FONDATEUR :
EDOUARD DE RÉMUR

RÉFÉRENCES CLIENT :
THALES, FRAMATOME, ARQUUS, STUDIO TF1, MINISTÈRE DES AFFAIRES ÉTRANGÈRES

LE PRIX DU PRÉSIDENT DE LA RÉPUBLIQUE

TRANSFORMER LE WEB EN UNE ARMURE ÉTANCHE AVEC VIRTUALBROWSER

Plus de 80 % des cyberattaques exploitent aujourd'hui les failles des navigateurs web. Pour verrouiller cette porte d'entrée, VirtualBrowser a développé une technologie d'isolation qui exécute la navigation sur un serveur distant plutôt que sur le poste de travail. En isolant le web dans un conteneur virtuel, la start-up parisienne vise une isolation complète face aux menaces numériques.

VirtualBrowser neutralise les menaces web les plus sophistiquées, comme le phishing et les *ransomwares*, en isolant totalement la navigation du réseau de l'entreprise. Cette technologie permet aux collaborateurs d'accéder sereinement aux sites non catégorisés ou à leurs outils SaaS, même depuis des réseaux Wi-Fi publics ou des terminaux personnels (BYOD). En cas d'incident cyber sur le parc informatique, la solution garantit une continuité d'activité immédiate via un environnement virtuel sécurisé. La solution entend résoudre le dilemme entre une protection radicale et la liberté d'usage des employés.

La start-up propose la première solution de navigation isolée à avoir obtenu la certification CSPN de l'ANSSI, un gage de confiance pour les environnements critiques. Elle se caractérise aussi par sa flexibilité de déploiement (en SaaS ou On-Premise) permettant aux entreprises de garder une maîtrise souveraine de leurs données, s'adaptant ainsi aux contraintes de sécurité les plus strictes.

En misant sur la navigation isolée, encore peu déployée en Europe, VirtualBrowser se positionne sur un segment en forte croissance, porté par la généralisation du SaaS et du travail hybride.

Présentation des lauréats 2026

QEVLAR AI

ANNÉE DE CRÉATION : 2023

SIÈGE SOCIAL : ISSY-LES-MOULINEAUX

EFFECTIF : 40

FONDS LEVÉS DEPUIS LA CRÉATION : ENVIRON 17,5 MILLIONS D'EUROS

CO-FONDATEURS : AHMED ACHCHAK & HAMZA SAYAH

RÉFÉRENCES CLIENT : ORANGE CYBERDEFENSE, SODEXO, NOMIOS, ETC.

PRIX DE LA CROISSANCE

LIBÉRER LE TEMPS ET LA PRISE DE DÉCISION DES PROFESSIONNELS DE LA CYBERSÉCURITÉ AVEC QEVLAR AI

Face à l'explosion des attaques, les centres de sécurité (SOC) sont submergés par un volume important d'alertes. Trier les faux positifs des vrais incidents peut constituer une véritable perte de temps pour les analystes. Cette saturation génère une «fatigue des alertes» chronique, laissant ainsi le champ libre aux menaces critiques qui passent inaperçues faute d'une investigation immédiate. Dans ce contexte, les outils d'automatisation traditionnels ne suffisent plus car ils sont trop rigides pour contrer la vitesse et la complexité des cyberattaques modernes.

Là où la plupart des solutions se contentent d'assister l'humain, Qevlar AI ne se limite pas à assister l'analyste : la plateforme automatise l'investigation. Sa plateforme déploie des agents autonomes capables de mener des investigations cyber complètes en moins de trois minutes, sans nécessiter la maintenance complexe de scénarios pré-établis (playbooks). Grâce à un moteur de raisonnement par graphes, elle annonce une précision de 99,8 % en ancrant chaque décision dans des faits auditables, éliminant ainsi les risques d'hallucinations. Cette approche permet aux centres de sécurité de passer d'une posture réactive à une stratégie de chasse aux menaces, tout en s'intégrant de manière fluide via API à l'écosystème cyber existant.

L'expertise de Qevlar AI est particulièrement reconnue au sein de l'écosystème tech, puisque celle-ci a notamment été sélectionnée pour rejoindre le prestigieux Future 40 (qui regroupe les 40 start-ups les plus prometteuses parmi les 1 000 présentes sur le campus de Station F). Elle a aussi été citée dans le *Emerging Tech Impact Radar* de Gartner, spécifiquement dans la catégorie *Global Attack Surface Grid.*

Le positionnement illustre une tendance de fond : l'automatisation cognitive des SOC, dans un contexte de pénurie de talents.

PRIX DE L'IMPACT OPÉRATIONNEL

REPRENDRE LE CONTRÔLE DE SON PATRIMOINE NUMÉRIQUE GRÂCE À AVANOO

L'utilisation d'applications et outils d'IA n'est pas sans risque pour l'entreprise : environ 60 % d'entre eux sont utilisés par les employés à l'insu de la DSI, créant un phénomène massif de Shadow IT. Cette opacité expose l'organisation à des risques de fuites de données critiques et à des failles de sécurité majeures, tout en rendant quasi impossible la mise en conformité avec les réglementations européennes comme le RGPD ou NIS2. En parallèle, cette prolifération non contrôlée entraîne un gaspillage budgétaire considérable, les entreprises finissant par payer pour des licences inutilisées ou des logiciels redondants qu'elles ne parviennent plus à identifier.

Avanoo propose une technologie de collecte hybride combinant une intégration aux annuaires d'entreprise et une extension de navigateur légère.

Cette approche permet de cartographier en temps réel 100 % des usages, révélant ainsi les outils de Shadow IT et d'IA qui échappent habituellement aux radars de la DSI. La plateforme analyse ensuite chaque application pour évaluer sa conformité réglementaire et détecter les licences inutilisées, transformant ces données en leviers d'économies immédiats. Enfin, elle guide les collaborateurs vers un catalogue d'outils sécurisés, substituant ainsi une gouvernance proactive et pédagogique aux interdictions systématiques.

Cette capacité à cartographier le Shadow AI constitue un différenciateur clé. Contrairement aux leaders américains, cette solution française garantit un hébergement et un traitement conformes aux exigences européennes. Elle se distingue également par une approche pédagogique : elle ne se contente pas de surveiller, mais oriente activement les collaborateurs vers les outils déjà sécurisés par l'entreprise. En quelques jours, elle transforme ainsi une informatique subie en un parc applicatif maîtrisé, sûr et optimisé.

AVANOO

ANNÉE DE CRÉATION : 2024

SIÈGE SOCIAL : PARIS

EFFECTIF : ENTRE 11 ET 50

FONDS LEVÉS DEPUIS LA CRÉATION : NON COMMUNIQUÉ

CO-FONDATEURS : TANGUY DUTHION, ETIENNE DELOUVRIER, ALEXANDRE TOUZET

RÉFÉRENCES CLIENT : AIR LIQUIDE, LE MONDE, EY

Présentation des lauréats 2026

LABEL4.AI

ANNÉE DE CRÉATION : 2024

SIÈGE SOCIAL : PARIS

EFFECTIF : 7

FONDS LEVÉS DEPUIS LA CRÉATION : ENVIRON 1 MILLION D'EUROS

CO-FONDATEURS : NICOLAS BODIN, VIVIEN CHAPPELIER, ANTHONY LEVEL, RONY ABECIDAN, TEDDY FURON, MATHIEU DESOUBEAUX

PRIX DE LA RECHERCHE

PRIX COUP DE CŒUR

DÉTECTER LES CONTENUS MODIFIÉS PAR IA

L'essor de l'IA générative complexifie la distinction entre contenu authentique et contenu manipulé. Cette opacité favorise une explosion des deepfakes et des fraudes à l'identité, menaçant directement la sécurité des entreprises et l'intégrité de l'information. Les nouvelles régulations européennes comme l'AI Act imposent des exigences renforcées de transparence sur l'origine des contenus, créant un défi de conformité majeur pour les organisations.

Pour répondre à ces défis, Label4.ai déploie une technologie de pointe capable d'analyser et de certifier l'origine de tout contenu numérique, qu'il soit visuel, sonore ou textuel. Sa plateforme combine des algorithmes de détection de deepfakes ultra-précis pour repérer les manipulations, et un système de tatouage numérique (ou *watermarking*) invisible pour garantir l'authenticité d'un contenu dès sa création. En s'appuyant sur cette expertise *forensics*, la start-up permet aux organisations de tracer leurs actifs numériques et de prouver leur intégrité face aux tentatives de fraude. Cette double approche assure non seulement une protection de l'image de marque, mais contribue à répondre aux exigences de l'AI Act

Label4.ai se différencie par son approche multimodale capable d'authentifier simultanément le texte, l'audio et la vidéo, là où la plupart des solutions se limitent à un seul format. Son innovation réside dans la combinaison unique de la détection de deepfakes et du tatouage numérique (watermarking) invisible, garantissant une traçabilité des contenus même après compression ou modification. En tant qu'acteur souverain français, la start-up s'appuie sur une expertise de pointe en police scientifique numérique *(forensics)* pour offrir des preuves auditables et conformes aux exigences strictes de l'AI Act. Cette rigueur technologique permet de restaurer la confiance dans les contenus numériques en transformant la transparence en un standard de sécurité.

Ce que révèle le Prix : quand l'innovation devient exécution

Avec environ 60 candidatures, quel est votre sentiment sur la capacité d'innovation des start-ups françaises de la filière cybersécurité ?

L'écosystème est effervescent, mais surtout crédible. Nous ne sommes plus dans le « bricolage », mais dans la construction de produits prêts pour l'industrie.

Quel rôle jouent ces start-ups dans la construction d'une filière cyber souveraine en France et en Europe ?

Elles apportent des solutions sur des niches critiques (protection des API, sécurité du *Cloud*, gestion des identités) où nous étions dépendants de solutions américaines ou israéliennes.

Pour construire une filière souveraine, il ne suffit pas de dire « achetez français ». Il faut que la solution soit techniquement équivalente aux géants du marché.

Y a-t-il un domaine (ex: détection, réponse, gouvernance) où vous avez trouvé que l'innovation était particulièrement bluffante cette année ?

De manière générale, l'utilisation judicieuse de l'IA pour faire gagner du temps aux équipes opérationnelles de sécurité (des analystes, des développeurs, des administrateurs, etc.).

Quel message envoyez-vous à l'écosystème cyber en récompensant les lauréats de cette édition ?

Le message est double : « Ambition et passage à l'échelle ». La technologie ne suffit plus : les gagnants sont ceux qui ont une vision *go-to-market* claire. On ne récompense pas seulement le meilleur produit, mais la meilleure vision d'entreprise.

Visez l'Europe, tout de suite : le marché domestique français est un excellent terrain d'entraînement, mais il est trop petit pour la survie à long terme. Le message est d'oser l'exportation dès les premières années pour devenir des champions européens, et non rester des champions locaux.

Pour conclure, quel est le défi majeur que vous aimeriez voir une start-up relever lors de la prochaine édition du prix ?

La start-up qui proposera une solution *plug-and-play* pour sécuriser l'usage de ChatGPT ou Copilot en entreprise, avec une couche de souveraineté, aura un boulevard devant elle.

Olivier FRACHON
Responsable de la sécurité du groupe Air Liquide, membre du jury

Quel est le premier indicateur que vous regardez dans un dossier cyber : la technologie, l'équipe, ou la taille du marché adressable ?

Cela dépend surtout de la maturité : au tout début, l'équipe est déterminante ; plus on avance, plus la traction commerciale pèse. En cyber, une « bonne équipe » ne suffit pas sans capacité de *go-to-market* (vente enterprise, partenariats, canaux) et sans compréhension claire de l'acheteur (CISO, IT, produit). Sur le marché, au-delà de la taille, je regarde le CAGR, mais aussi le *pain point,* l'urgence réglementaire, l'existence d'un budget et la *willingness-to-pay*. Enfin, la techno en France est souvent robuste, mais on vérifie surtout la défendabilité : distinguer une tech solide d'un vrai *moat* (données propriétaires, intégrations, distribution, conformité, effets de réseau, switching costs).

Quelle est la valeur ajoutée d'une start-up cyber française face aux géants américains ou israéliens aujourd'hui ?

L'avantage clé, c'est l'agilité : cycles d'innovation plus courts et capacité à itérer vite. Elles sont souvent ouvertes à des *design partnerships* avec des *early adopters* pour répondre précisément au besoin terrain, et elles ont aussi une forte capacité d'intégration : s'insérer dans des stacks hétérogènes et co-construire avec les équipes client.

Quelle tendance technologique parmi les dossiers reçus vous semble la plus bankable pour les trois prochaines années ?

La sécurité de l'IA est aujourd'hui le thème le plus porteur, mais c'est un ensemble de sous-sujets où les budgets commencent à se structurer : gouvernance & conformité / *risk management,* protection des usages (prompt injection, data leakage, abuse), et *monitoring / red teaming /* évaluation continue. Le critère *bankable*, c'est quand il y a un acheteur clair, un budget identifié et un ROI mesurable.

Y a-t-il un segment de la cyber (ex: identité, *Cloud*, résilience) que vous jugez aujourd'hui sur-investi ou, au contraire, délaissé ?

La *cyber awareness* est très encombrée. La sécurité de l'IA attire beaucoup de monde, mais le sujet étant très vaste, c'est probablement seulement le début. À côté de ça, la sécurité de l'embarqué et du logiciel est plutôt sous-investie au regard de l'ampleur des enjeux : *drivers* très concrets (IoT, automotive, industriel, médical) et montée des exigences (SBOM, CRA, sécurisation du cycle de dev).

En quoi le label «Lauréat du Prix de la Start-Up du Forum INCYBER» est-il un signal positif pour de futurs investisseurs lors d'une levée de fonds ?

Parce que convaincre un jury aussi exigeant et diversifié est un signal crédible sur la qualité de l'équipe et la pertinence du besoin adressé.

William LECAT
Associé à Auriga Partners, membre du jury

Comment l'ANSSI perçoit-elle le dynamisme de l'écosystème cyber français par rapport à ses voisins européens cette année ?

Le Prix de la Start-up du Forum INCYBER est un précieux observatoire de l'écosystème de l'innovation en cybersécurité en France et en Europe. Cette année encore, le Jury a eu l'opportunité de découvrir et d'évaluer plusieurs dizaines de candidatures venues de France (80 %) et d'Europe (20 %).

Le territoire européen est particulièrement propice à l'innovation et au développement de solutions très technologiques pour la cybersécurité, du fait de l'excellence académique en France et en Europe, des multiples soutiens et outils d'accompagnement mis en place au niveau de l'UE et des États, mais aussi de l'intérêt croissant des clients pour les solutions nationales ou européennes, pour de nombreuses raisons.

L'ANSSI ne saurait trop recommander aux clients de faire confiance aux éditeurs français et européens, pas uniquement parce qu'ils sont européens, mais parce que leurs solutions sont compétitives, que ce soit en termes d'innovation, de robustesse, d'efficacité ou de valeur économique.

Le passage de « start-up prometteuse » à « fournisseur de confiance » est un saut difficile. Quel est le principal obstacle que vous avez identifié chez les candidats ?

Ce passage n'est difficile que pour les solutions qui n'arrivent pas à apporter une preuve de valeur. L'écosystème français, par exemple, permet aux jeunes pousses prometteuses de se développer assez naturellement : les structures d'incubation et d'accélération spécialisées en cybersécurité ainsi que le financement de l'innovation sont disponibles, accessibles et performants ; le marché atteignable depuis la France est très conséquent. Par ailleurs, le système d'évaluation des solutions est sans doute ici plus qu'ailleurs particulièrement bien rodé et efficace. Les Visas de Sécurité ANSSI sont reconnus, voire exigés, par des clients de plus en plus attentifs à la confiance qu'ils peuvent accorder aux solutions qu'ils installent au cœur de leurs systèmes d'information.

Avez-vous vu des solutions innovantes pour aider les PME et les collectivités, qui sont souvent les maillons faibles de la chaîne cyber ?

La prise en compte des menaces cyber par tous les acteurs économiques ou publics, quelle que soit leur taille, est une condition nécessaire à la résilience numérique globale. Les startups peuvent adresser tous types de clients, y compris ceux de taille intermédiaire, nombreux et de plus en plus conscients de la nécessité d'agir pour leur cybersécurité. Les startups doivent marketer leurs solutions pour qu'elles soient compréhensibles, intégrables et bien sûr pertinentes par rapport au contexte et aux besoins de ces clients non spécialistes.

Les lauréats du Prix de la Start-up cette année encore répondent parfaitement à ces exigences : des besoins adressés clairs et stratégiques, des solutions immédiatement opérationnelles, avec un apport immédiat et mesurable en termes de sécurisation du système d'information. Et, ce qui ne gâche rien, elles s'adressent à tout type d'acteurs, y compris les grands comptes.

Olivier GUÉRIN
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Membre du jury

Analyses des candidatures

SYNTHÈSE STRATÉGIQUE

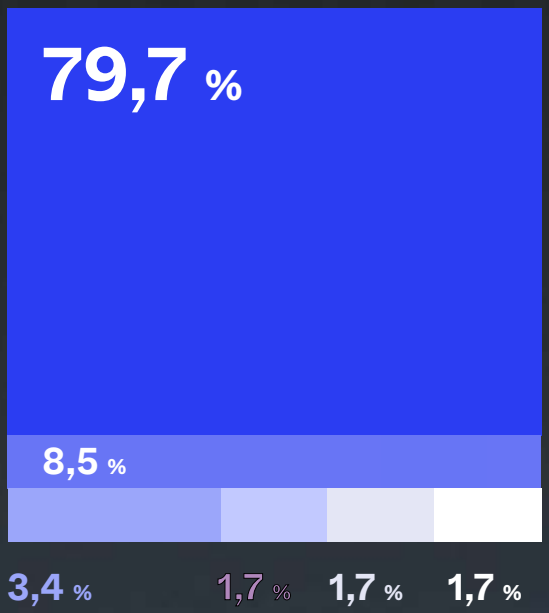
L'édition 2026 confirme une évolution notable de l'écosystème cyber français. L'innovation ne se limite plus à la démonstration technologique, elle s'inscrit dans une logique d'industrialisation et de passage à l'échelle.

Les candidatures analysées révèlent un secteur fortement investi en R&D, majoritairement orienté vers le *Cloud*, et structuré autour de cibles métiers clairement identifiées (RSSI, DSI, équipes SecOps).

Au-delà de la performance technique, les enjeux d'intégration, de conformité et de souveraineté deviennent des critères structurants dans l'adoption des solutions.

D'un autre côté, l'ambition internationale s'affirme nettement. Le développement commercial hors de France constitue désormais la priorité stratégique pour une majorité d'acteurs, soutenue par des intentions de levées de fonds significatives.

Ce panorama met ainsi en lumière un écosystème encore en phase d'amorçage financier, mais résolument tourné vers la consolidation européenne et l'industrialisation de ses offres.



ORIGINE GÉOGRAPHIQUE DES CANDIDATURES

Avec 79,7 % des candidatures issues de France, le panorama reste très majoritairement national. La Suisse (8,5 %) constitue le deuxième vivier. Le Royaume-Uni, les Pays-Bas et le Luxembourg (1,7 % chacun), ainsi que la Belgique (3,4 %), complètent marginalement l'échantillon.

Segments des solutions

QUELS SONT LES DIFFÉRENTS SEGMENTS DE LA CYBERSÉCURITÉ REPRÉSENTÉS DANS LES CANDIDATURES ?

Segment de la solution	Nombre de solutions	2025	2026	Évolution
Gouvernance, traçabilité et audit		**8**	**11**	**+37,5 %**
Gestion des identités et des accès		**5**	**8**	**+60 %**
Vulnérabilité		**6**	**7**	**+16,7 %**
Sécurisation des applications		5	5	0 %
Cyber Threat Intelligence		8	4	-50 %
DevOps / SecOps		1	4	+300 %
Sécurisation des données		9	3	-66,7 %
IOT / OT / Cybersécurité industrielle		2	3	+50 %
Détection et réponse à incident		6	3	-50 %
Sensibilisation		3	3	0 %
Prévention des fuites de données			3	
Inforensic			2	
Sécurisation des flux mobiles et web		2	2	0 %
Sécurité réseaux		5	1	-80 %

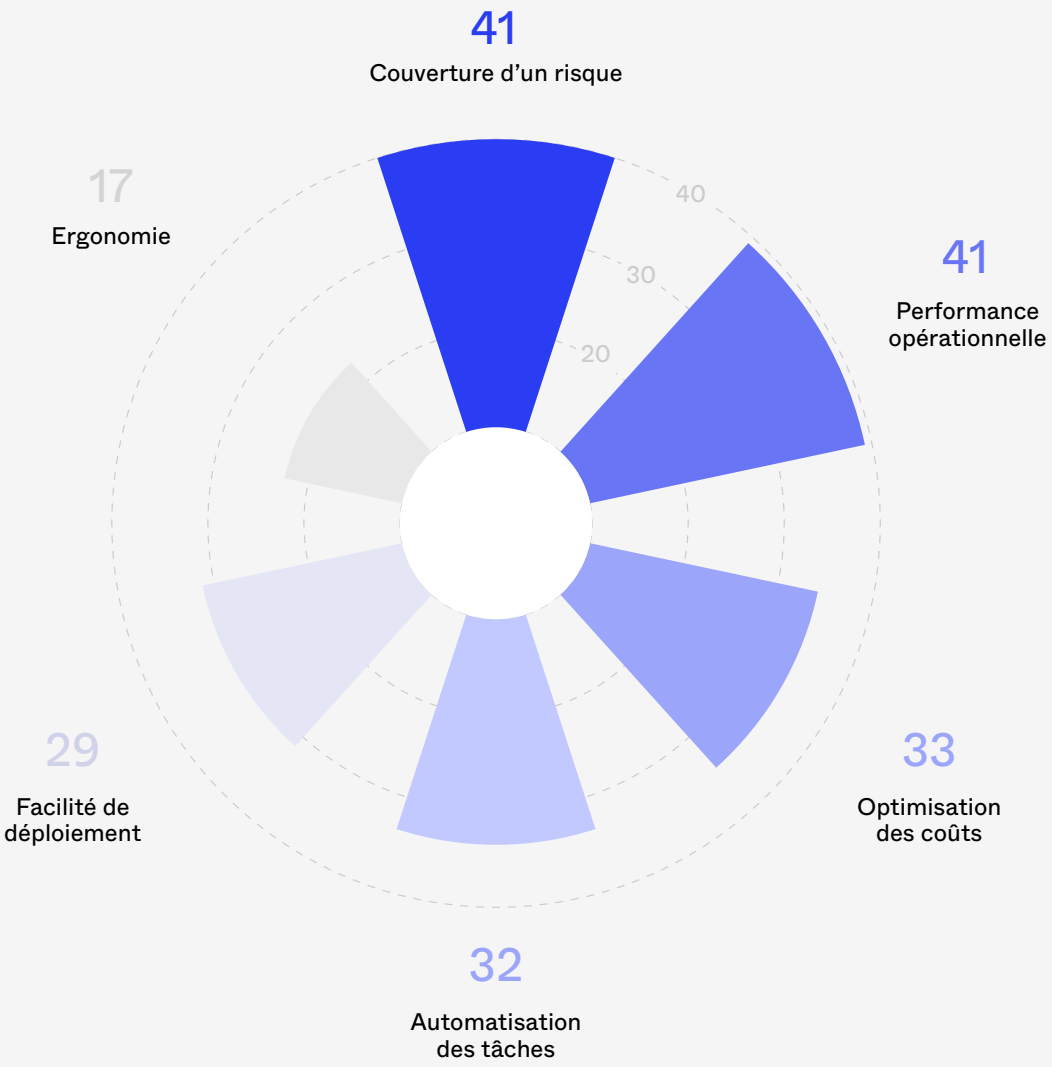
Les candidatures couvrent un large spectre de la cybersécurité, mais trois segments dominent nettement : la gouvernance, la traçabilité et l'audit (18,64 %), la gestion des identités et des accès (13,56 %) et la vulnérabilité (11,86 %).

La progression du segment gouvernance / traçabilité / audit n'est pas neutre. Elle s'inscrit directement dans le contexte réglementaire européen marqué par l'entrée en vigueur ou la montée en puissance de NIS2, DORA et du *Cyber Resilience Act*. Les solutions proposées ne se limitent plus à protéger : elles doivent désormais permettre de tracer les actions, documenter les décisions et démontrer la conformité.

Le marché évolue ainsi vers une logique de compliance opérationnelle. La capacité à produire des preuves, à structurer les processus de contrôle et à sécuriser la gouvernance devient un facteur différenciant au même titre que la performance technique.

Modèle économique et maturité

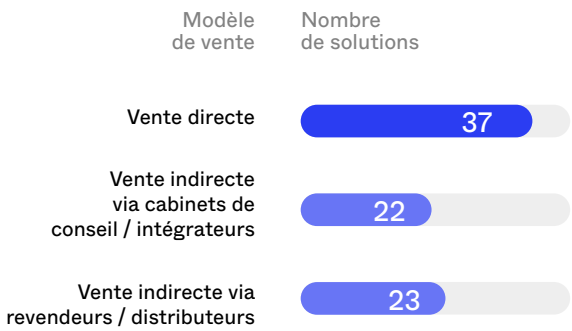
QUELLE EST LA VALEUR AJOUTÉE DES SOLUTIONS PRÉSENTÉES ?



Une quarantaine de candidats citent la couverture d'un risque jusqu'ici peu ou pas couvert et l'amélioration de la performance opérationnelle pour qualifier la valeur ajoutée de leur solution. Le marché privilégie les outils qui comblent des lacunes de sécurité critiques tout en apportant un bénéfice opérationnel direct et mesurable, notamment via l'optimisation des coûts et l'automatisation des tâches, citées par une trentaine de candidats. Enfin, l'importance accordée à la facilité de déploiement (29 mentions) confirme une attente forte : des solutions capables de s'intégrer rapidement, sans friction.

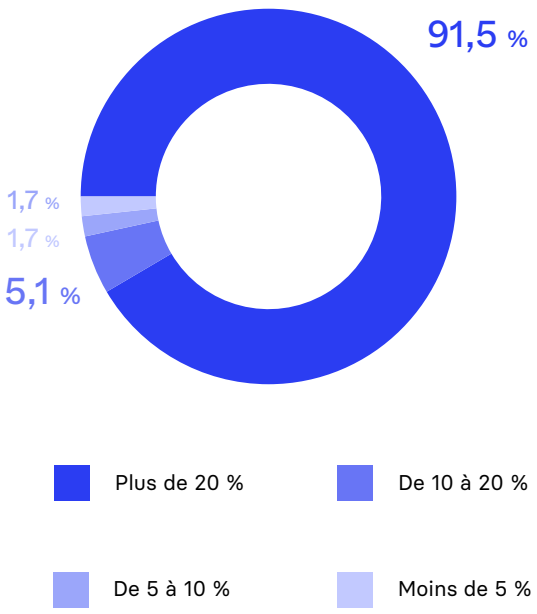
Modèle économique et maturité

QUELS MODÈLES DE VENTES SONT PRIVILÉGIÉS ?



Une majorité d'entreprises (37 solutions) privilégie un modèle hybride : licence et vente directe. Cette combinaison associe la récurrence du modèle de licence au contrôle de la relation client via la vente directe. La vente indirecte reste toutefois significative (via cabinets de conseil, intégrateurs, revendeurs ou distributeurs), signe d'une stratégie de couverture qui s'appuie sur les réseaux de partenaires.

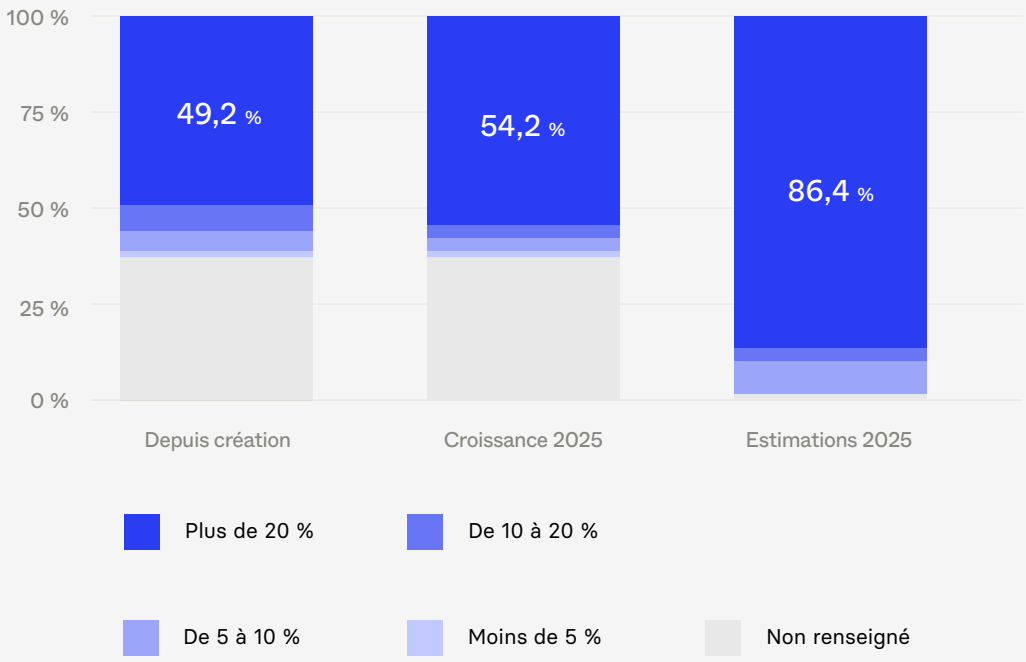
QUELLE PART INVESTIE EN R&D ?



La tendance est nette : 91,5 % des solutions investissent plus de 20 % de leur chiffre d'affaires en R&D VS 77,9 % en 2025, confirmant l'intensité de l'effort d'innovation dans le secteur. À l'inverse, seules deux entreprises (3,4 %) déclarent un investissement inférieur à 10 % du chiffre d'affaires.

Traction et croissance

CROISSANCE ANNUELLE



Près de la moitié des entreprises (49,2 %) déclarent une croissance annuelle moyenne supérieure à 20 % depuis leur création. À noter : 37,3 % des répondants n'ont pas renseigné cette donnée, ce qui limite la comparabilité.

Plus de la moitié des entreprises (54,2 %) déclarent une croissance supérieure à 20 % en 2025. Là encore, 37,3 % des réponses ne sont pas renseignées. Les croissances plus modérées (de « moins de 5 % » à « 10–20 % ») restent minoritaires.

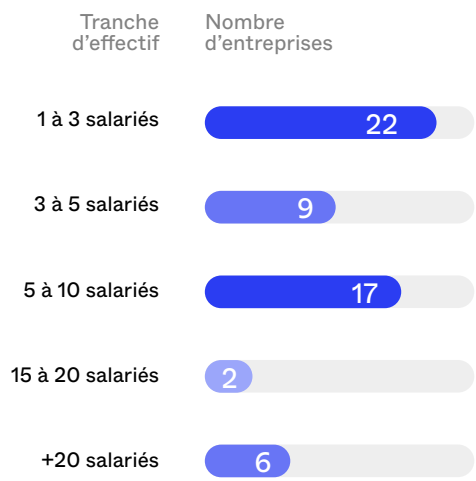
L'année 2026 est envisagée avec optimisme : 86,4 % des répondants anticipent une croissance supérieure à 20 %. Les trajectoires plus modérées (entre 5 % et 20 %) représentent 11,9 % de l'échantillon.

Typologie des solutions

LES SOLUTIONS PRÉSENTÉES SONT-ELLES *FULL CLOUD ?*

Option *Cloud*	Nombre de solutions	Évolution par rapport à 2025
Hybride	**27**	**+30,9 %**
Full *Cloud*	**22**	-17,1 %
Non	6	-23,3 %
Non concerné(e)	4	+1,5 %
Cloud total (hybride + full *Cloud*		+3,8 %

Le *Cloud* s'impose comme standard de déploiement : 49 solutions sur 59 (83 %) reposent sur une architecture *Cloud*. Ce chiffre confirme une normalisation du *Cloud* dans l'écosystème, mais la répartition interne révèle une évolution plus fine : le modèle hybride devient majoritaire (27 solutions), devant le full *Cloud* (22). Autrement dit, le débat ne porte plus sur l'adoption du *Cloud*, désormais acquise, mais sur son mode d'implémentation. Les start-up privilégient des architectures modulaires, capables de s'adapter aux contraintes d'intégration, de sécurité et de souveraineté, plutôt qu'un modèle SaaS exclusif.



80 % des entreprises comptent moins de 10 salariés, confirmant un écosystème encore largement composé de structures en phase d'amorçage.

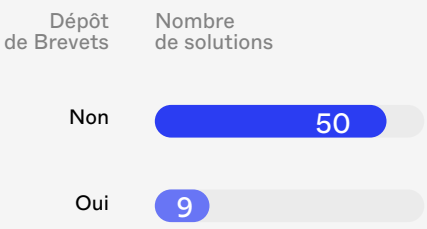
Si l'on observe l'émergence d'un noyau d'acteurs entre 10 et 15 salariés, signe d'un début de passage à l'échelle, les entreprises dépassant 20 salariés restent minoritaires. L'innovation est donc dynamique, mais encore portée par des équipes resserrées, où la capacité d'exécution repose sur des organisations agiles plutôt que sur des effectifs consolidés.

QUAND LA SOUVERAINETÉ ÉCONOMIQUE ET LA PROTECTION DES DONNÉES DEVIENNENT DES MOTIVATIONS D'ACHAT

Impact sur le choix des partenaires	Nombre de solutions	Évolution par rapport à 2025
Oui	**47**	**+12,2 %**
Non	10	
Non concerné(e)	3	

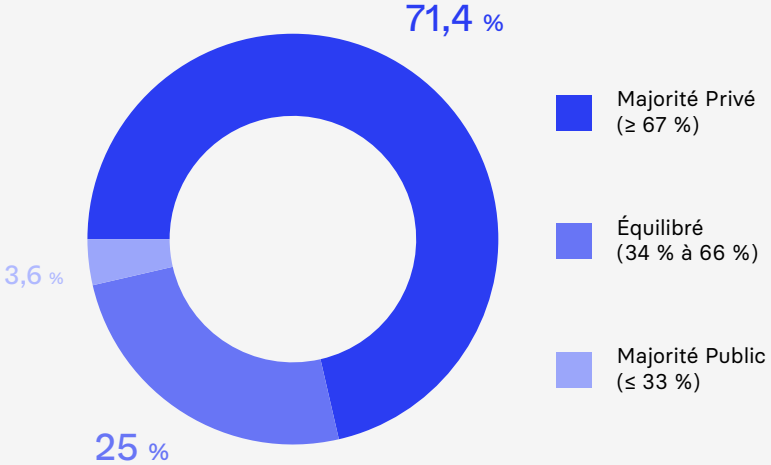
En 2026, 47 solutions sur 60 (78 %) déclarent que les enjeux de souveraineté numérique et de protection des données influencent le choix de leurs partenaires commerciaux, contre 69,5 % en 2025. Cette progression de 8,5 points confirme que la souveraineté n'est plus un argument secondaire mais un critère structurant dans les décisions d'achat, traduisant une montée en puissance des exigences de conformité, de maîtrise technologique et de confiance.

LES SOLUTIONS PRÉSENTÉES SONT-ELLES CONCERNÉES PAR LE DÉPÔT D'UN OU PLUSIEURS BREVETS ?



La protection par brevet reste minoritaire. 50 solutions sur 59 déclarent ne pas avoir déposé de brevet, contre 9 qui indiquent l'inverse. Cela reflète un écosystème encore en phase de construction produit et de montée en maturité.

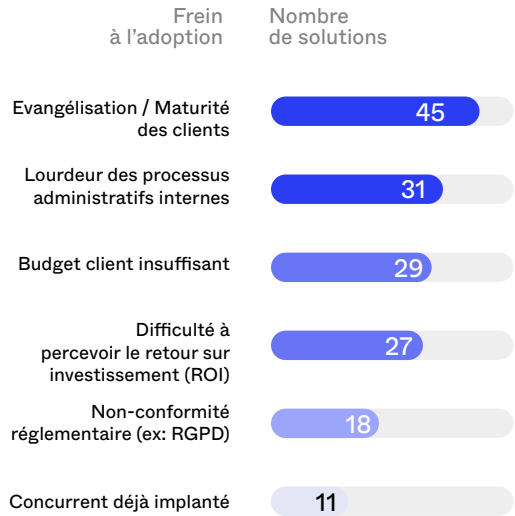
QUELLE EST LA PART DU PUBLIC ET DU PRIVÉ DANS LA CLIENTÈLE DES ENTREPRISES PRÉSENTÉES ?



Le secteur privé représente 71,4 % de la base clientèle moyenne. Un quart des entreprises (25 %) affichent un portefeuille équilibré entre public et privé, tandis que 3,6 % seulement déclarent une majorité de clients publics. L'accès au marché public apparaît donc plus difficile ou moins prioritaire que la traction B2B.

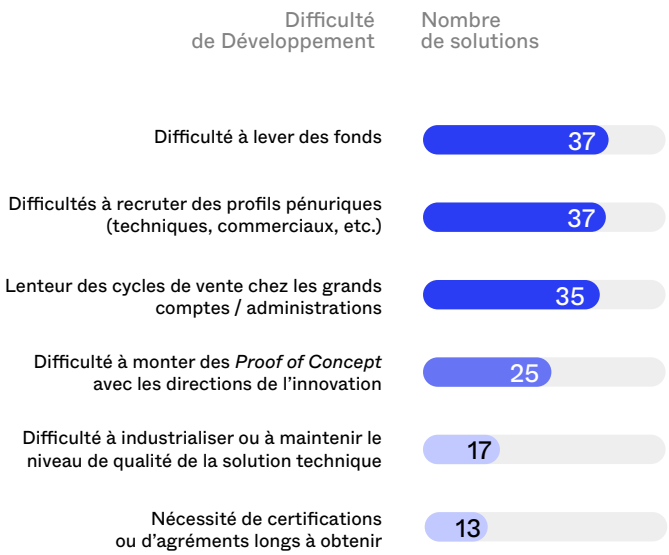
Freins et défis structurels

QUELS SONT LES FREINS À L'ADOPTION DES SOLUTIONS PRÉSENTÉES CHEZ LES CLIENTS ?



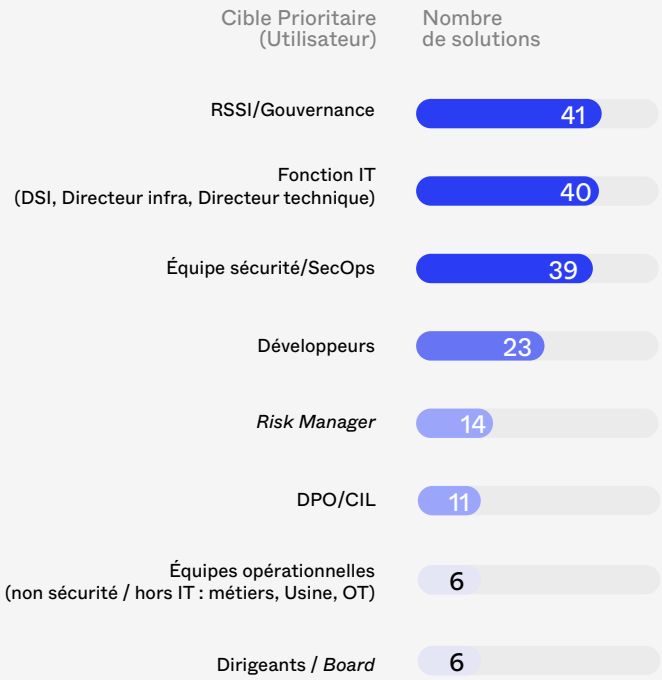
Le premier frein, cité par 45 solutions, tient à la maturité du marché : une forte part des offres suppose encore un effort d'évangélisation. Viennent ensuite des contraintes d'exécution côté clients : lourdeur des processus internes (31 mentions) et budgets insuffisants (29). Enfin, la décision d'achat repose sur deux conditions : démontrer un ROI lisible (27) et lever les doutes liés à la conformité réglementaire (18), notamment au regard du RGPD.

QUELLES SONT LES DIFFICULTÉS RENCONTRÉES POUR LE DÉVELOPPEMENT DE L'ENTREPRISE ?



La croissance des entreprises candidates se heurte à un double défi structurel que sont le financement et le recrutement (37 citations chacun). Ce besoin de capitaux et la tension sur le marché des talents soulignent les difficultés classiques de passage à l'échelle.
En parallèle, l'inertie commerciale reste un frein majeur pour 35 acteurs, confrontés à la lenteur des cycles de vente auprès des grands comptes et des administrations. Enfin, la phase critique de validation technique n'est pas épargnée : 25 solutions pointent du doigt la complexité de mise en œuvre des *Proof of Concept (PoC),* révélant des frictions persistantes dans les processus d'évaluation des clients.

QUELLES SONT LES CIBLES PRIORITAIRES EN TERMES D'UTILISATEURS ?



Ambitions sectorielles et géographiques

CIBLES PRIORITAIRES : LE TRIPTYQUE RSSI – DSI – SECOPS DOMINE

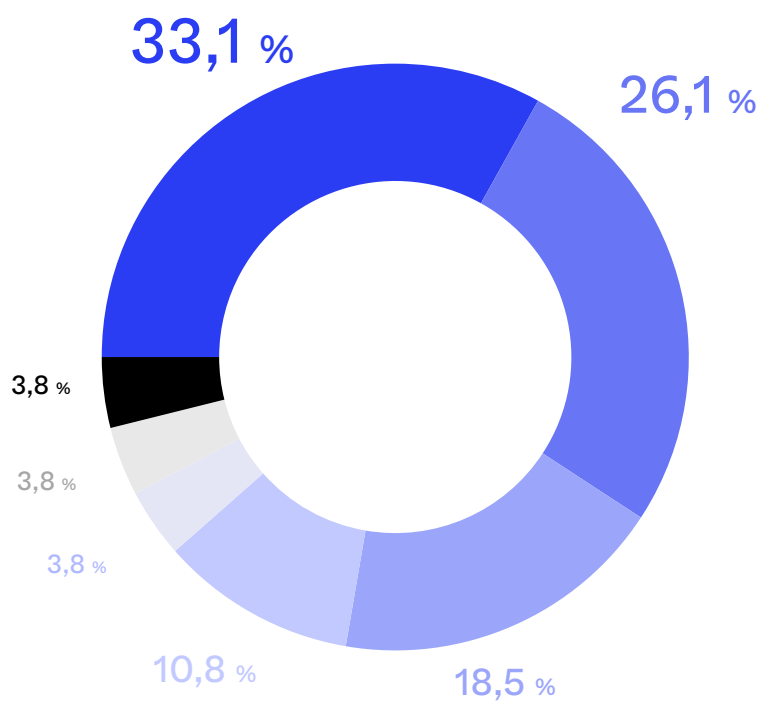
Les utilisateurs stratégiques se concentrent sur trois fonctions clés :

RSSI / Gouvernance : 33,1 %
Fonctions IT / DSI : 26,1 %
Équipes Sécurité / SecOps : 18,5 %

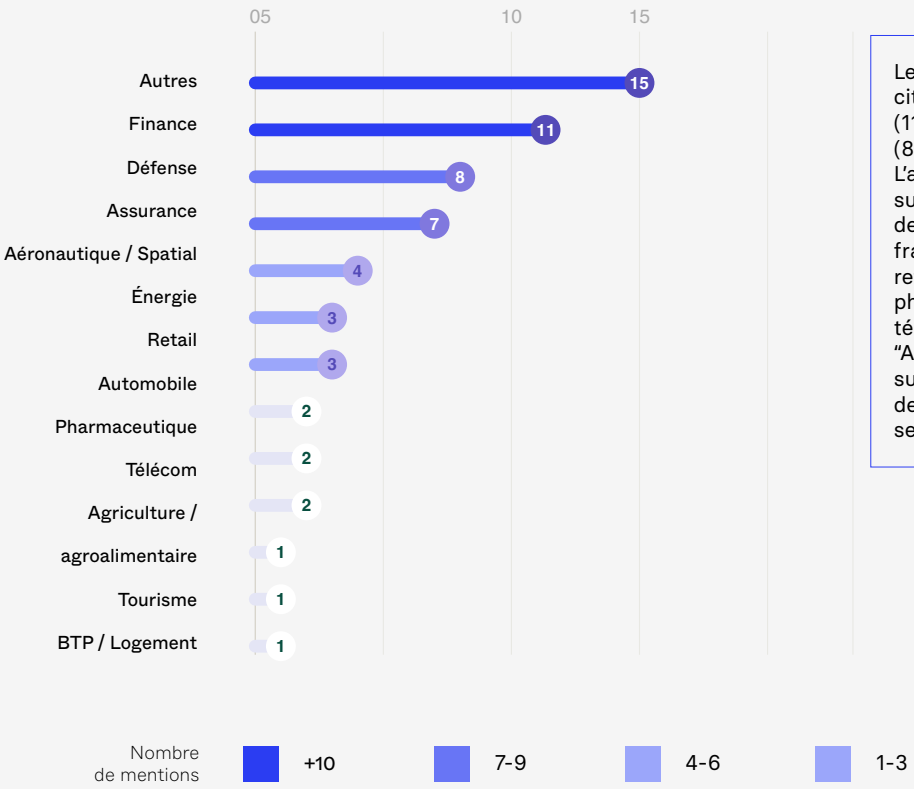
À elles seules, ces fonctions concentrent plus de 75 % des mentions.

Les développeurs (3,8 %), DPO/CIL (3,8 %) et directions juridiques (3,8 %) apparaissent comme des cibles secondaires. Les *Risk Managers* (10,8 %) complètent le dispositif côté gestion des risques.

La hiérarchie est claire : la décision reste pilotée par la gouvernance et l'infrastructure, avec une exécution sécuritaire opérationnelle.

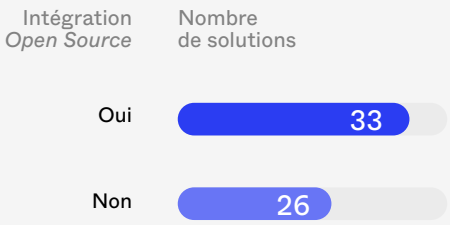


QUELS SONT LES SECTEURS D'ACTIVITÉ CIBLÉS ?



Les verticales les plus citées sont la finance (11 mentions), la défense (8) et l'assurance (7). L'aéronautique/spatial suit (4), puis un groupe de secteurs plus fragmentés (énergie, retail, automobile, pharmaceutique, télécom). La catégorie "Autres" (15) montre surtout l'hétérogénéité des positionnements sectoriels.

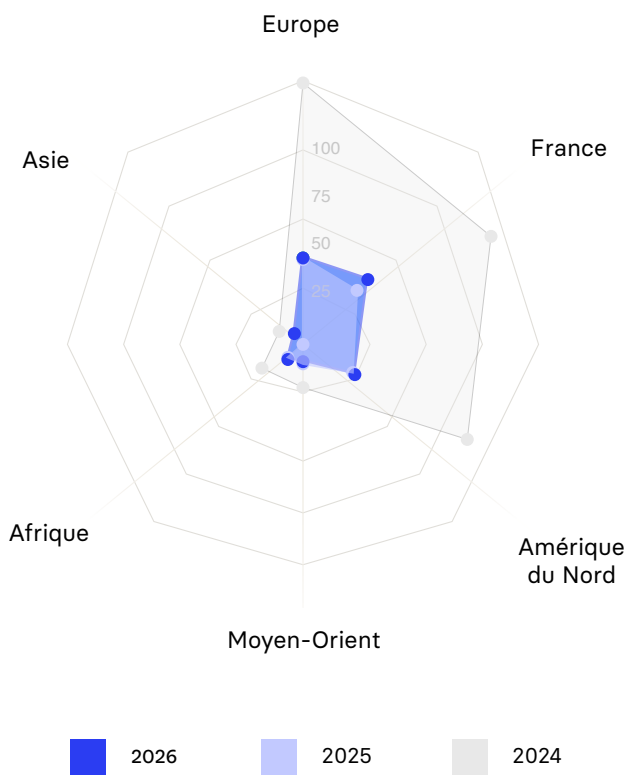
LES SOLUTIONS SE BASENT-ELLES OU INTÈGRENT-ELLES UNE PARTIE *OPEN SOURCE ?*



L'*open source* s'impose comme un pilier technologique pour une majorité du panel : 56 % des solutions (33 sur 59) l'intègrent nativement ou s'appuient sur ses briques logicielles. Dans le secteur de la cybersécurité, ce choix reflète une quête d'accélération du développement, mais aussi un besoin de transparence et d'auditabilité, gages de confiance pour les utilisateurs. Pour autant, le modèle propriétaire conserve une place significative, puisque seules 26 solutions ont fait le choix stratégique de s'en affranchir totalement.

Ambitions sectorielles et géographiques

QUELLES SONT LES PRIORITÉS DE DÉVELOPPEMENT GÉOGRAPHIQUE ?



Si l'attractivité nord-américaine ne recule pas en valeur absolue, elle ne progresse pas non plus. En revanche, sur deux ans, l'écart est significatif : citée par 71,8 % des répondants en 2024, l'Amérique du Nord ne représente plus que 22,6 % des mentions en 2026. Ce décalage ne traduit pas un abandon du marché américain, mais une hiérarchisation plus sélective des ambitions internationales.

La France, en revanche, gagne nettement en priorité et l'Europe demeure le premier objectif. Cela traduit un resserrement stratégique autour du marché européen, plutôt qu'un désengagement vis-à-vis des États-Unis.

Zone géographique	2024	2025	2026	Évolution 2026 vs 2025
Europe	**99 %**	**32,7 %**	**32,8 %**	**+0,3 %** *stable*
France	**82 %**	**23,8 %**	**28,8 %**	**+18,5 %**
Amérique du Nord	**71,8 %**	**22 %**	**22,6 %**	**+2,7 %** *quasi stable*
Moyen-Orient	16,6 %	7,1 %	6,2 %	-12,7 %
Afrique	17,9 %	6 %	6,2 %	+3,3 %
Asie	10,2 %	N.D.	4 %	*N.C.*

Les start-ups sondées pouvaient choisir plusieurs régions comme axe de développement

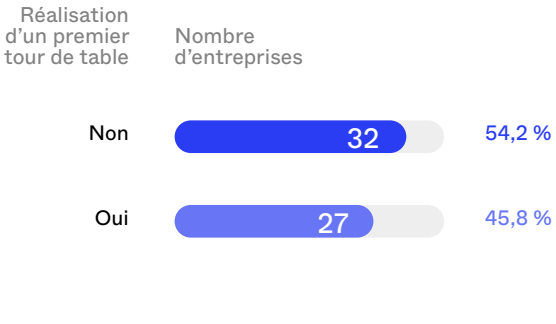
LA VISION DU DÉVELOPPEMENT DES ENTREPRISES DE L'ÉCHANTILLON

Vision de développement	Nombre d'entreprises	Pourcentage
S'imposer en tant que leader de votre segment de marché	27	45,8 %
Disrupter le marché / s'imposer comme technologie de rupture	22	37,3 %
Étoffer votre offre et diversifier les segments de marché	7	11,9 %
Réussir un Exit auprès d'un acteur de référence sur le marché	3	5,1 %

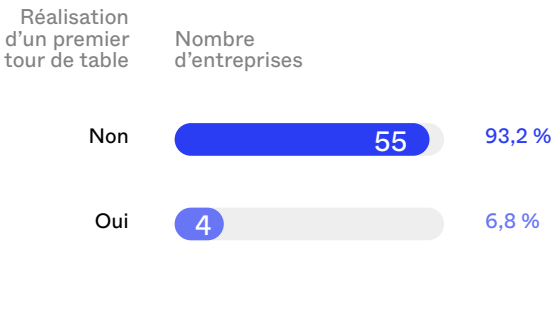
L'échantillon affiche une ambition de croissance marquée : 45,8 % visent le leadership sur leur segment, et 37,3 % se positionnent comme technologie de rupture. Les stratégies d'élargissement de l'offre restent minoritaires (11,9 %), et l'option d'un exit rapide est marginale (5,1 %).

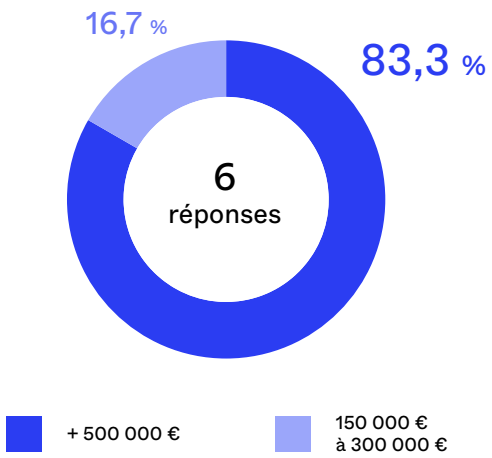
Financement et passage à l'échelle

PREMIER TOUR DE TABLE



DEUXIÈME TOUR DE TABLE





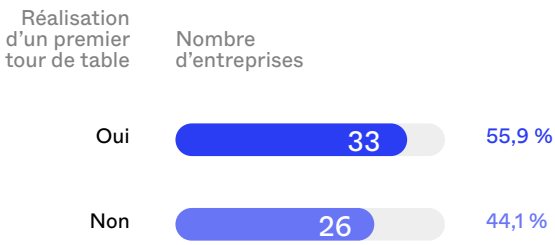
Premier tour de table : 45,8 % des entreprises déclarent en avoir réalisé un, contre 54,2 % qui ne l'ont pas encore fait. Parmi les premiers tours renseignés, une majorité se situe au-dessus de 500 000 €.

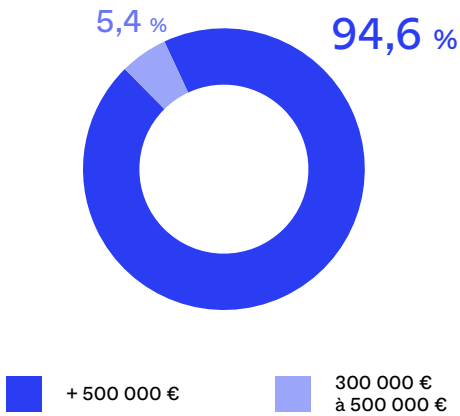
Le second tour reste rare : seules 6,8 % des entreprises déclarent en avoir réalisé un. Lorsqu'il est renseigné, le montant se situe le plus souvent dans la tranche la plus élevée.

Les intentions de levée sont élevées : 55,9 % envisagent une levée dans les six prochains mois. Parmi elles, la quasi-totalité vise plus de 500 000 €.

Le capital recherché est principalement orienté vers le développement commercial international (59,32 %), devant le développement produit/technologie (32,20 %).

LEVÉE DE FONDS





Plus de la moitié des entreprises (55,9 %) envisagent de lever des fonds dans les six prochains mois, contre 44,1 % qui n'envisagent pas de levée à court terme.

Cette proportion confirme une dynamique d'accélération : une part significative de l'écosystème cherche à renforcer ses moyens pour soutenir son développement commercial, technologique ou international.

La quasi-totalité des entreprises concernées (94,6 %) ciblent un montant supérieur à 500 000 €. Seules 5,4 % envisagent une levée comprise entre 300 000 € et 500 000 €.

Ce positionnement traduit des ambitions de passage à l'échelle assumées, avec des besoins en capital structurants plutôt qu'opportunistes.

FINANCEMENT : UN ÉCOSYSTÈME ENCORE JEUNE, MAIS AMBITIEUX

Objectif prioritaire de la levée	Nombre d'entreprises à avoir mentionné l'objectif	Pourcentage
Développement commercial international	35	59,32 %
Développement produit/ technologie	19	32,20 %
Croissance externe	3	5,08 %
Marketing / Communication	1	1,69 %
NSP	1	1,69 %

Premier tour de table :
45,8 % ont déjà levé
54,2 % n'ont pas encore réalisé de premier tour

Parmi les levées réalisées :
56 % ont levé plus de 500 000 €

Second tour :
93,2 % n'ont pas encore réalisé de second tour. Seules 6,8 % ont atteint ce stade

Intentions de levée :
55,9 % prévoient une levée dans les 6 mois
94,6 % de ces levées ciblent plus de 500 000 €

Objectif principal des fonds :
59,3 % : développement commercial international
32,2 % : développement produit

PANORAMA DE L'INNOVATION

Croissance, souveraineté et passage à l'échelle : les signaux du marché

PRIX DE LA STARTUP

MARS 2026

IN CYBER FORUM EUROPE