Perspectives

N°26/081 – 8 avril 2026

Technologies – Record triennal dans la cybersécurité

2025 a été une année exceptionnelle pour les investissements dans les start-up de cybersécurité, atteignant leur niveau le plus élevé depuis trois ans. Cette dynamique est stimulée par d'importantes levées de fonds pour les entreprises spécialisées en IA dans ce secteur.

La cybersécurité entre dans sa période de transformation la plus rapide et la plus déterminante. Les avancées technologiques accélèrent l'innovation, mais élargissent parallèlement la surface d'attaque numérique, imposant ainsi le développement de nouveaux paradigmes défensifs adaptés aux nombreuses menaces ascendantes.

L'IA a désormais évolué d'une technologie émergente à une couche fondamentale des opérations d'entreprise, amplifiant les opportunités d'attaques et poussant les entreprises à repenser la conception, la gouvernance et l'exécution de la sécurité des systèmes, désormais devenue une priorité stratégique.

Les chiffres M&A

400 opérations de fusions-acquisitions ont été enregistrées en 2025 sur le secteur de la cybersécurité. Le volume total atteint 119 milliards de dollars, marquant une année record portée par des méga-deals comme l'acquisition de Wiz, start-up de sécurisation pour le cloud, par Google pour 32 milliards de dollars et de CyberArk, entreprise spécialisée dans la gestion de la sécurité des identités, par Palo Alto pour 25 milliards de dollars.

Les plus belles progressions du secteur de la cybersécurité en 2025 ont été Cloudflare avec une croissance de +83%, CrowdStrike avec +37% et Zscaler avec +25%.

Ces trois entreprises s'imposent comme les références de la « plateformisation » de la cybersécurité, une stratégie qui consiste à regrouper l'ensemble des solutions de cybersécurité dans un environnement unifié.

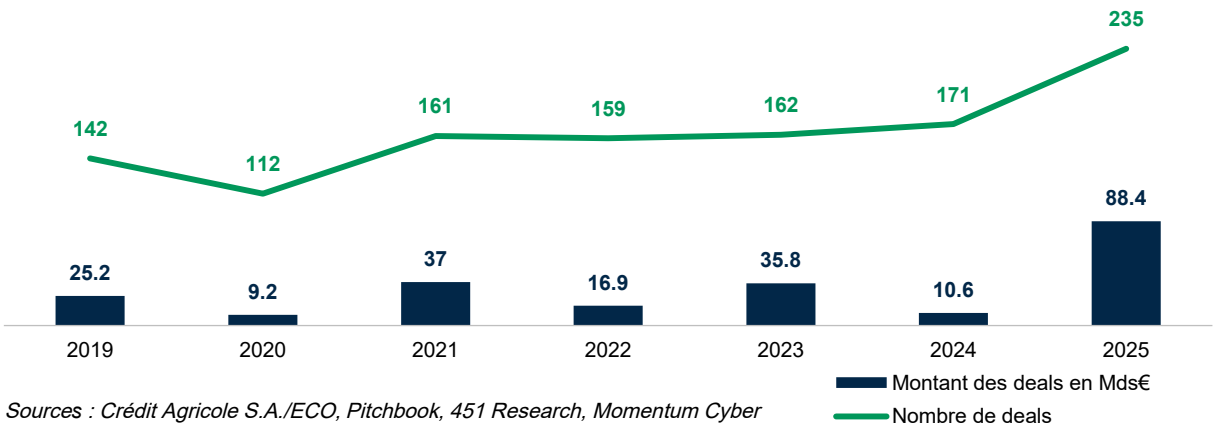
Étant en hyper-croissance, Cloudflare est sorti de la catégorie des « acteurs du web » pour devenir le nouveau géant de la sécurité réseau et a aspiré les parts de marché des acteurs traditionnels du matériel (pare-feu physiques) en proposant une sécurité 100% cloud. Cloudflare détient environ 39% de parts de marché dans le secteur des CDN (réseaux de distribution de contenu).

D'autres acteurs comme Cisco, Palo Alto, Accenture figurent parmi les principaux acquéreurs stratégiques, avec respectivement 28, 22 et 21 deals depuis 2010. Check Point intensifie ses acquisitions ces sept dernières années, Lakera étant notamment l'acquisition phare pour l'entreprise en 2025. Deloitte, Fortinet et Zscaler sont également relativement actifs sur les activités M&A.

En parallèle, les firmes de *private equity* (PE) développent des portefeuilles cybersécurité de plus grande envergure.

Menna SALIM
menna.salim@credit-agricole-sa.fr

Montants et nombre de deals M&A Cyber



Sources : Crédit Agricole S.A./ECO, Pitchbook, 451 Research, Momentum Cyber

+270% de croissance de la valeur des opérations de fusions-acquisitions entre 2024-2025
+22% de croissance du nombre d'opérations de fusions-acquisitions entre 2024-2025

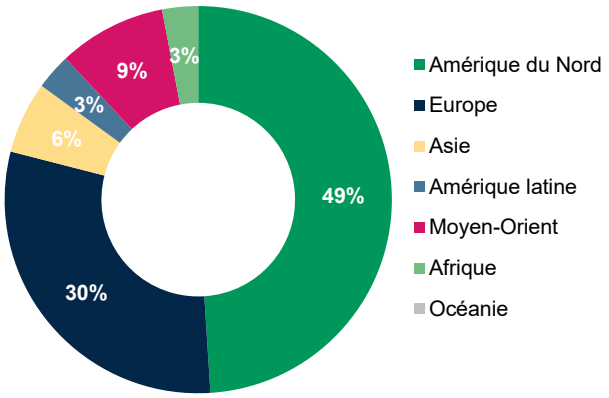
Des transactions dynamiques et internationales

Les opérations internationales se sont multipliées de manière régulière sur les quatre dernières années, reflétant la stratégie d'expansion géographique des acteurs du secteur de la cybersécurité.

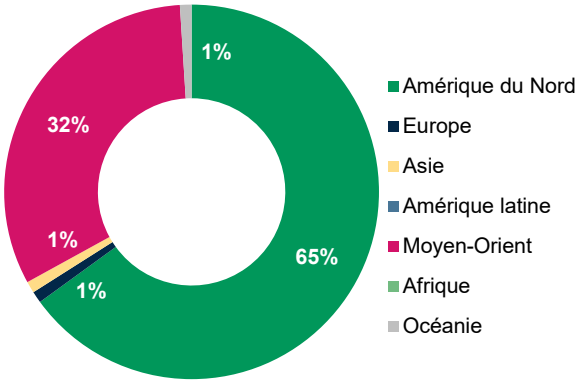
L'Amérique du Nord demeure le leader mondial dans le domaine des opérations M&A cyber, tant par le volume que par la valeur des transactions.

L'Europe se positionne en deuxième place pour le nombre d'opérations réalisées, tandis que le Moyen-Orient occupe le deuxième rang en termes de montants investis, reflétant ainsi des dynamiques régionales distinctes dans le financement de la cybersécurité.

Part dans le nombre total des deals en 2025



Part dans le montant total des deals en 2025



Sources : Crédit Agricole S.A./ECO, Pitchbook, 451 Research, Momentum Cyber

Les segments qui dominent les investissements

La gestion des risques et de la conformité ainsi que la sécurisation des canaux numériques demeurent les deux catégories les plus actives et les mieux financées dans les opérations de fusions-acquisitions en cybersécurité. Cette tendance illustre la priorité accordée par les organisations à la maîtrise des risques et au respect des obligations réglementaires.

L'acquisition de Calypso AI par F5 pour 180 millions de dollars en est une illustration emblématique : cette opération permet aux grandes entreprises de déployer l'IA avec des garde-fous en temps réel pour la gestion des risques et la conformité.

Le segment des services de sécurité enregistre le plus grand nombre de transactions avec 126 deals, tandis que la sécurité de l'IA s'impose désormais comme le secteur le plus financé en termes de montants investis, avec 144 financements. Cette

Menna SALIM
menna.salim@credit-agricole-sa.fr

dichotomie témoigne de la transformation profonde du paysage de la cybersécurité et met en évidence le décalage entre la fragmentation du marché traditionnel et la concentration des capitaux sur les technologies émergentes.

Cette dynamique se reflète dans les stratégies d'acquisition des acteurs majeurs, qui cherchent à renforcer leurs capacités en matière de sécurité de l'IA. SentinelOne s'empare de Prompt Security, une start-up qui donne la possibilité aux salariés de sécuriser leurs propres applications d'IA.

D'autres segments, bien que moins actifs, conservent leur importance stratégique et restent dynamiques, notamment la sécurité de l'Internet des objets (IoT) et la sécurité applicative.

Les catalyseurs d'un marché plus que jamais primordial

Les cybermenaces progressent à un rythme sans précédent, alimentées par la sophistication croissante des attaquants et la multiplication exponentielle des appareils connectés à l'échelle mondiale. Les dernières données de FIRST (*Forum of Incident Response and Security Teams*) révèlent que plus de 30 000 vulnérabilités ont été identifiées l'année dernière. Avec une hausse de 17% comparée aux années antérieures, cette évolution témoigne de l'intensification constante des risques cyber et prévoient le dépassement d'un niveau jamais atteint de 50 000 CVE[1] (*Common Vulnerabilities and Exposures*).

Cette tendance s'accentue avec l'adoption massive du cloud computing, qui transforme les terminaux et les flux de données en cibles privilégiées pour les attaquants. Cette fragmentation de l'infrastructure informatique crée des points d'exposition multiples et complexes à sécuriser.

L'intelligence artificielle : l'arme à double tranchant

L'utilisation croissante de l'IA agentique par les employés et les équipes de développement crée des vulnérabilités inédites. Cette tendance s'intensifie avec la démocratisation des plateformes *low-code no-code* et du développement assisté par IA, favorisant ainsi une multiplication non maîtrisée d'agents autonomes et la production de code insuffisamment sécurisé.

L'IA transforme la cybersécurité en permettant d'analyser d'énormes volumes de données en temps réel pour détecter plus vite les menaces et réduire les faux positifs, d'automatiser certaines réponses et de passer d'une posture réactive à une posture plus prédictive, en anticipant les attaques à partir de tendances observées. En revanche, les cybercriminels exploitent eux aussi les mêmes outils d'IA pour industrialiser et sophistiquer leurs attaques (*phishing* ciblé, contournement des défenses, automatisation de la recherche de failles).

L'un des principaux défis auxquels sont confrontés les acteurs de la cybersécurité concerne la contextualisation et la priorisation du traitement des vulnérabilités. Ces activités requièrent une étude humaine et poussent les entreprises à adopter des approches de « plateformisation » pour accéder à différentes couches d'informations et construire un contexte plus complet.

Avec l'entrée en vigueur complète de la directive NIS2[2] et du *Cyber Resilience Act* de l'UE, les fournisseurs américains devraient intensifier leurs acquisitions d'entreprises européennes. La NIS2 concerne environ 15 000 entités françaises. Cette stratégie leur permettra d'obtenir des infrastructures d'hébergement et de support locales conformes aux exigences de souveraineté numérique imposées par l'UE. Toutefois, les décisions budgétaires restent principalement guidées par des logiques de performance et de coûts, le critère de la souveraineté peine encore à s'imposer comme facteur déterminant, mais suscite clairement une prise de conscience au sein de l'écosystème.

Tendances 2026 : IA, consolidation et nouvelles opportunités

Nous anticipons davantage d'acquisitions liées à l'IA en 2026. Les entreprises de sécurité informatique et les *hackers* informatiques devraient intensifier leur utilisation des outils d'IA. L'IA continuera de rendre certaines cyberattaques plus efficaces et plus rapides, ce qui entraînera une multiplication du nombre total d'attaques, avec déjà une augmentation de 89% en 2025.

Par ailleurs, l'IA générative devrait automatiser un nombre croissant de fonctions dans les centres d'opérations de sécurité, permettant aux entreprises de faire face à la pénurie d'ingénieurs. La demande en cybersécurité devrait rester soutenue en 2026, avec une croissance alignée sur les budgets informatiques globaux.

Sans changements significatifs dans les stratégies d'atténuation, les systèmes critiques deviendront plus vulnérables aux acteurs malveillants avancés d'ici 2027. Il sera donc essentiel de maintenir le

[1] Identifiants uniques attribués aux vulnérabilités de sécurité informatique découvertes dans les logiciels, systèmes d'exploitation et matériels.

[2] *Network and Information Security 2*, directive européenne pour la réglementation européenne en matière de cybersécurité.

Menna SALIM
menna.salim@credit-agricole-sa.fr

rythme des développements liés à l'IA pour assurer des défenses solides.

Avec plus de 5 000 entreprises de cybersécurité à travers le monde, les opportunités de croissance par acquisitions sont considérables pour les acteurs cherchant à enrichir leur portefeuille de solutions. Les domaines prioritaires pour 2026 incluront notamment les solutions de sécurisation de l'IA (générative et agentique) ainsi que la protection des systèmes de technologie opérationnelle (OT).

Crédit Agricole S.A. — Direction des Études Économiques
12 place des États-Unis – 92127 Montrouge Cedex

Directeur de la Publication : Isabelle Job-Bazille

Rédacteur en chef : Romain Liquard

Documentation : Laurent Carret – **Statistiques :** Datalab ECO

Secrétariat de rédaction : Fabienne Pesty

Contact : *publication.eco@credit-agricole-sa.fr*

Consultez les Études Économiques et abonnez-vous gratuitement à nos publications sur :
Internet : https://etudes-economiques.credit-agricole.com/
iPad : application Etudes ECO disponible sur App store
Android : application Etudes ECO disponible sur Google Play