THALES
Building a future we can all trust

#ÉtudeSécuritéCloud2025

2025

ÉTUDE SUR LA SÉCURITÉ DU CLOUD

Sécuriser un univers hybride et multicloud

cpl.thalesgroup.com

Sommaire

Résumé

Les services cloud sont devenus un socle incontournable de l'infrastructure des entreprises, mais leur sécurisation reste un défi majeur. Cette nouvelle édition de l'**Étude Thales sur la sécurité du cloud** dresse un état des lieux des enjeux, priorités et réussites des organisations dans la protection de leurs environnements et de leurs données. Si l'intégration du cloud est désormais généralisée, la maturité en matière de sécurité reste inégale. Et avec la montée en puissance des initiatives d'intelligence artificielle, fortement dépendantes du cloud, la nécessité d'une protection des données efficace et maîtrisée devient plus urgente que jamais.

Réalisée auprès de près de 3200 sondés dans 20 pays, cette étude rassemble les points de vue de dirigeants, responsables et praticiens sur l'évolution du paysage de la sécurité cloud. Elle révèle une réalité persistante : malgré des investissements en hausse, la complexité des environnements hybrides et multicloud met les équipes de sécurité sous forte pression. De plus en plus d'entreprises peinent à sécuriser leurs actifs cloud — un défi accentué par les besoins massifs en données des projets d'intelligence artificielle. La cybercriminalité suit cette tendance : quatre des cinq principaux actifs ciblés par les attaques sont désormais hébergés dans le cloud. Dans ce contexte, renforcer la sécurité et rationaliser les opérations apparaissent comme deux leviers essentiels pour accroître la résilience et l'efficacité globale des dispositifs de protection.

S&P Global
Market Intelligence

Source : Enquête personnalisée 2025 sur la sécurité du cloud
S&P Global Market Intelligence 451 Research, réalisée pour le compte de Thales.

Parrainé par

EXCLUSIVE NETWORKS

Remarque : Tous les graphiques présentés dans ce document proviennent des enquêtes personnalisées sur la sécurité du cloud réalisées par S&P Global Market Intelligence 451 Research entre 2021 et 2025.

Principaux enseignements

Le cloud, toujours au cœur des préoccupations en matière de sécurité

64% considèrent la sécurité du cloud comme une priorité incontournable.

52% ont déclaré que leur budget « sécurité et IA » empiète sur les ressources dédiées à la cybersécurité.

Seulement **8%** protègent au moins 80 % de leurs données cloud par chiffrement.

54% des données stockées dans le cloud sont aujourd'hui considérées comme sensibles, contre 47 % l'an passé.

Les attaques visent en priorité les ressources cloud

54% citent une augmentation des attaques directes visant à compromettre leur infrastructure.

L'humain : le maillon faible de la sécurité

68% considèrent le vol d'identifiants/secrets comme la méthode d'attaque d'infrastructure cloud connaissant la plus forte progression.

La complexité, véritable obstacle à la sécurité du cloud

85 Le nombre moyen d'applications SaaS utilisées, en hausse de 6 %.

2,1 Le nombre moyen de fournisseurs de cloud public sollicités par une entreprise.

55% estiment que la sécurisation des environnements cloud est plus complexe que celle des infrastructures hébergées on premise, contre 51 % l'année précédente.

57% utilisent au moins cinq systèmes de gestion, contre 53% l'an dernier.

Souveraineté numérique dans un monde hybride

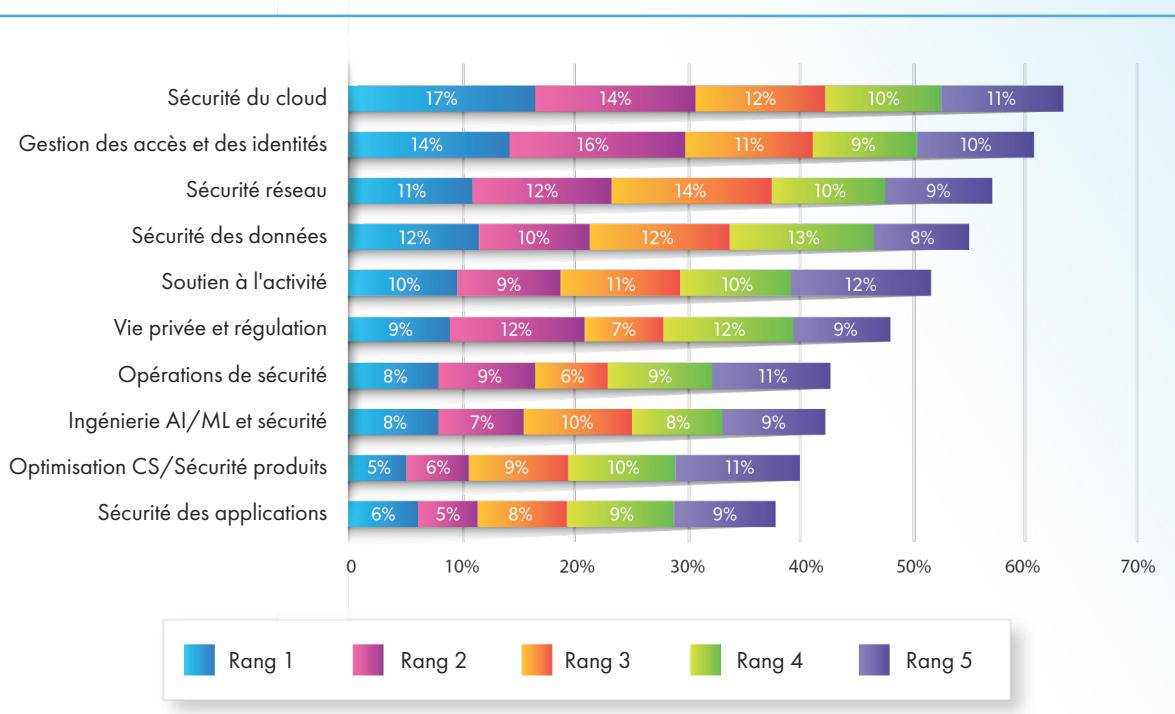
42% considèrent que le chiffrement et la gestion des clés suffisent à atteindre les objectifs de souveraineté, quel que soit l'emplacement physique des données.

33% considèrent que la pérennité et la portabilité des charges de travail et des données constituent les principaux moteurs de la souveraineté numérique.

Sécurité : le cloud reste au cœur des préoccupations

L'infrastructure informatique des entreprises a profondément évolué : le cloud est désormais au cœur des environnements numériques modernes, bien au-delà d'une simple option technologique. Si son adoption est quasi généralisée, de nombreuses organisations renforcent encore leurs compétences et leurs pratiques opérationnelles pour en tirer pleinement parti. La sécurisation des données et des infrastructures cloud exige une approche spécifique, reposant sur des méthodes et outils adaptés à cet écosystème en constante mutation. Cependant, la diversité des mécanismes de contrôle et de protection proposés par les fournisseurs rend la gestion de la sécurité particulièrement complexe. Les équipes de cybersécurité, déjà sous pression, doivent composer avec des environnements hétérogènes tout en assurant une protection continue et homogène des actifs. L'essor des initiatives en intelligence artificielle, qui mobilisent des volumes croissants de données hébergées dans le cloud, accentue encore ces défis et renforce la nécessité d'une sécurité intégrée, cohérente et évolutive.

Les principaux domaines de la sécurité

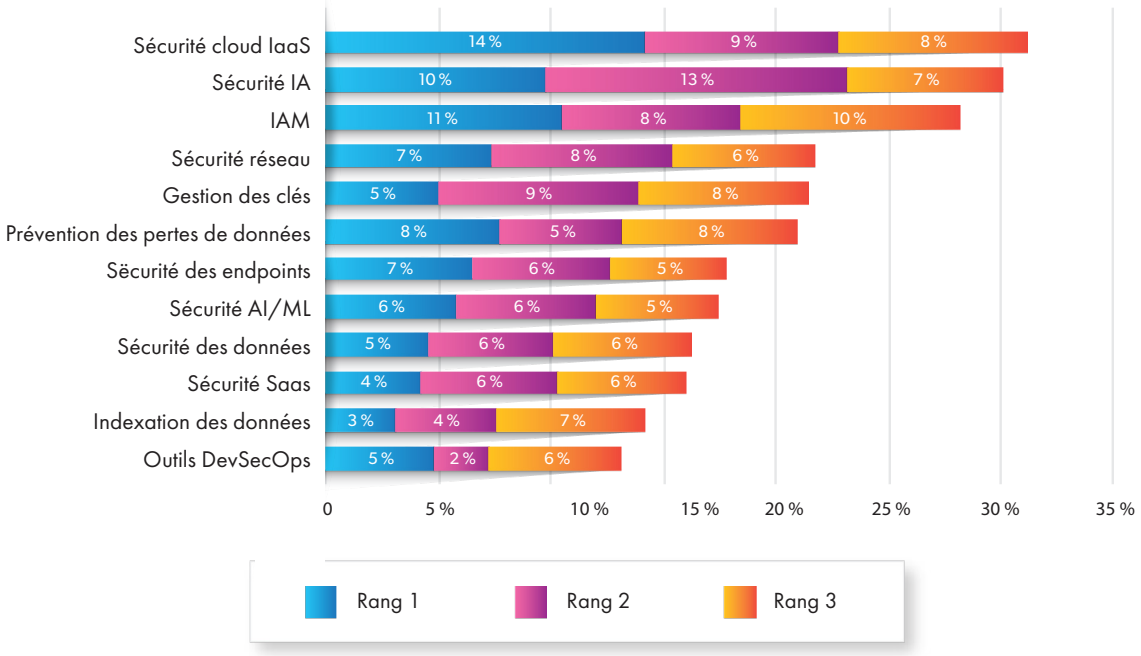


La sécurité du cloud demeure cette année encore la principale source de préoccupation pour les organisations. Les enjeux ne se limitent plus à la protection technique des environnements cloud : ils concernent aussi la disponibilité des compétences nécessaires pour les gérer efficacement. Près des deux tiers des sondés (64 %) citent la sécurité du cloud parmi leurs cinq priorités majeures, et 17 % la placent même en tête. Le fait qu'elle occupe cette position depuis plusieurs années, malgré des investissements importants, souligne à quel point il s'agit d'un défi complexe et durable, à la fois technologique, organisationnel et humain.

52 %, soit plus de la moitié, affirment que les dépenses dédiées à la sécurité IA empiètent sur le budget alloué à la sécurité existante.

Les dépenses dédiées à la sécurité du cloud restent soutenues, confirmant son statut de priorité d'investissement absolue. Mais l'évolution rapide des technologies et services cloud contraint les entreprises à un effort permanent d'adaptation : elles doivent sans cesse renforcer leurs compétences internes et leurs capacités opérationnelles pour rester à niveau dans un environnement en mutation constante. L'essor de l'intelligence artificielle vient accentuer cette pression. La sécurité liée à l'IA, nouvel élément du classement cette année, se hisse directement à la deuxième place des priorités budgétaires, signe de son importance croissante. Cependant, plus de la moitié des organisations (52 %) indiquent que ces nouveaux budgets sont ponctionnés sur les investissements existants en cybersécurité, ce qui soulève des questions sur la cohérence stratégique et la répartition efficace des ressources. Dans la mesure où une grande partie des projets IA reposent sur le cloud, cette redéfinition budgétaire pourrait affecter les efforts de protection des environnements cloud eux-mêmes.

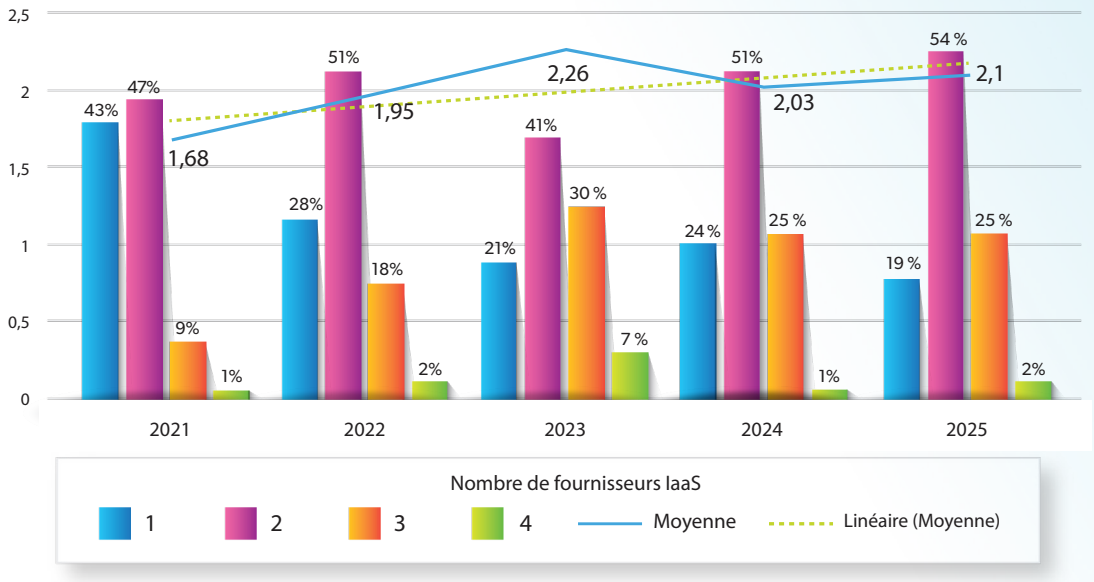
Principales technologies de sécurité selon le niveau d'investissement



La complexité, obstacle majeur à la sécurité du cloud

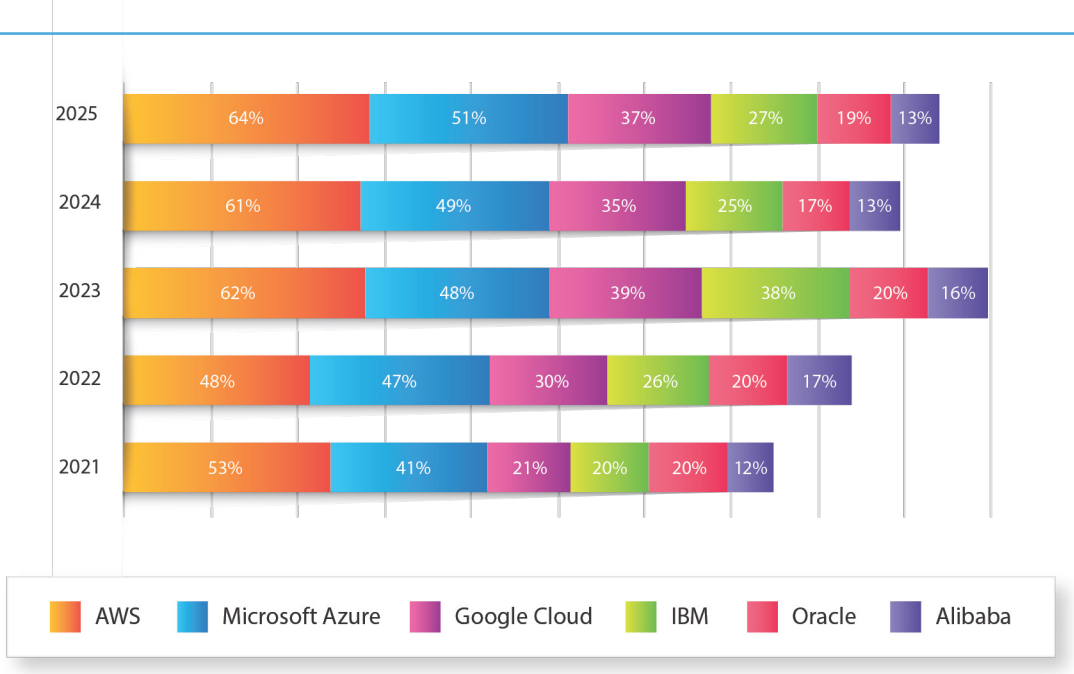
La sécurité du cloud continue de mobiliser des investissements soutenus, en grande partie à cause de la complexité croissante des environnements informatiques actuels. La majorité des entreprises opèrent désormais dans une infrastructure hybride et multicloud, combinant plusieurs environnements IT internes et plusieurs fournisseurs de services cloud. Cette année, les organisations utilisent en moyenne 2,1 fournisseurs de cloud public, en parallèle de leurs systèmes on premise. Cette diversification, source de flexibilité et d'innovation, rend aussi la sécurité plus complexe. Ainsi, 55 % des sondés estiment que sécuriser le cloud est plus complexe que de protéger une infrastructure interne. Ce chiffre marque une hausse de 4% par rapport à l'année précédente. La multiplication des environnements et des acteurs rend donc la sécurité cloud plus stratégique et plus exigeante que jamais.

Adoption du modèle multicloud Infrastructure-as-a-Service (IaaS)



L'adoption de plusieurs fournisseurs IaaS (Infrastructure as a Service) est désormais la norme. Comme l'illustre le graphique ci-dessous, l'usage de ces services progresse chez presque tous les prestataires. La plupart des organisations prévoient d'intégrer de nouveaux fournisseurs, que ce soit par croissance interne ou à la suite de fusions et acquisitions. Cette diversification oblige les équipes de sécurité à adapter leurs contrôles aux spécificités de chaque environnement cloud.

Tendances d'adoption du cloud chez les différents fournisseurs

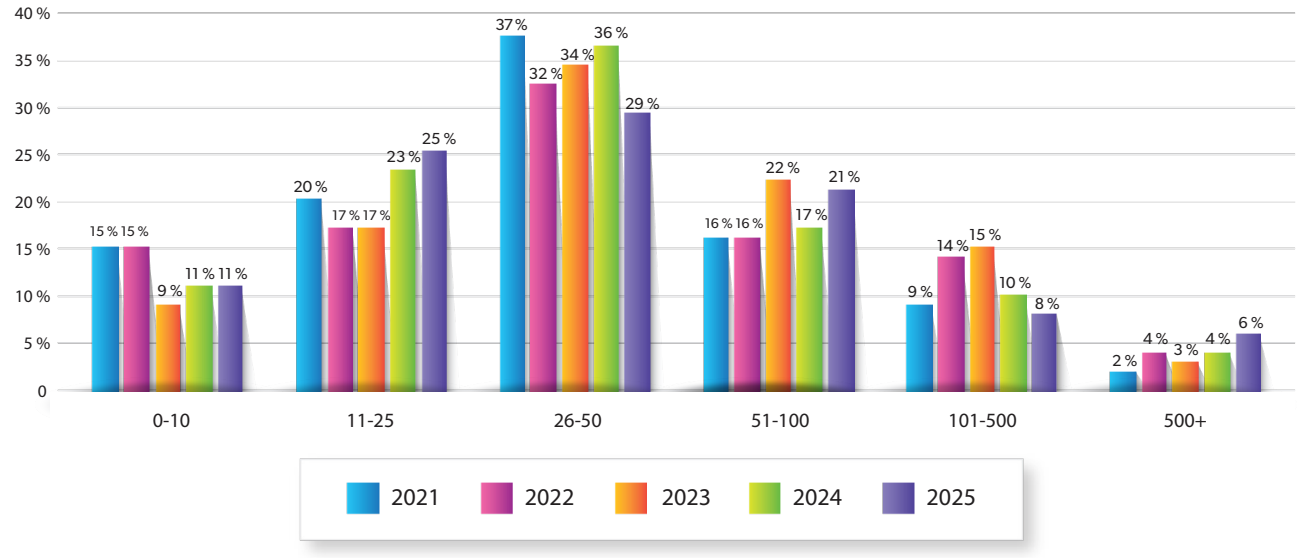


Parallèlement, le nombre d'applications SaaS utilisées par les entreprises ne cesse d'augmenter. Si ces solutions peuvent simplifier certains aspects opérationnels, elles introduisent également de nouveaux défis de sécurité. Les contrôles d'accès et la protection des données y sont souvent moins transparents et plus difficiles à maîtriser, tandis que la visibilité sur les flux et le stockage des données demeure limitée. Ces contraintes soulèvent par ailleurs des questions croissantes de souveraineté des données

En moyenne, les organisations interrogées déclarent utiliser 85 applications SaaS, soit une hausse de 6 % en un an. Dans un écosystème désormais composé de plusieurs clouds et d'un grand nombre d'applications SaaS, les niveaux de contrôle et de visibilité varient fortement d'un service à l'autre. Les équipes de sécurité peinent dès lors à harmoniser leurs pratiques avec les politiques internes, notamment en matière de gestion des identités, des accès et des données.

En moyenne, les entreprises sondées déclarent utiliser 85 applications SaaS, soit une augmentation de 6 % par rapport à l'année dernière.

Nombre d'applications SaaS (Software-as-a-Service)



La prolifération des outils de sécurité

Le nombre croissant d'outils de sécurité — un phénomène souvent qualifié de tool sprawl — complexifie encore davantage la sécurité dans le cloud. L'adage selon lequel « la complexité est l'ennemie de la sécurité » s'applique ici plus que jamais, comme le montrent les résultats de l'étude. Près des deux tiers des répondants (61 %) déclarent utiliser au moins cinq outils différents pour la découverte, la surveillance ou la classification des données. De même, 57 % utilisent cinq gestionnaires de clés ou plus pour assurer le chiffrement de leurs données. Cette multiplication d'outils accroît les risques d'erreurs de configuration et d'incidents opérationnels.

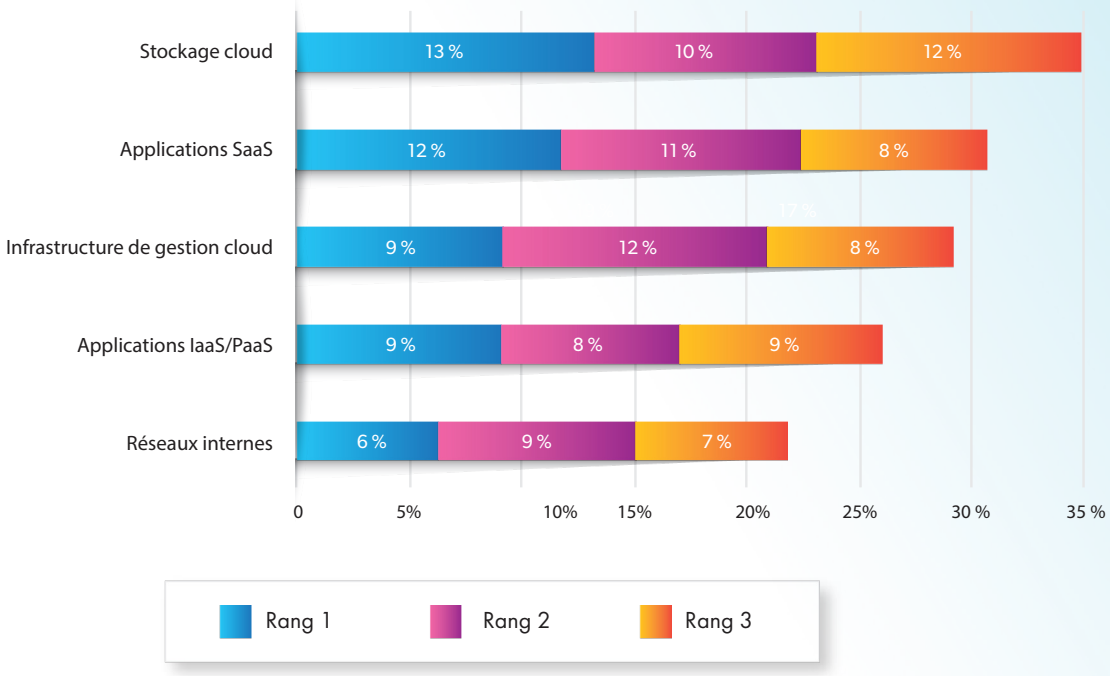
Avec la diversité des fournisseurs cloud, il peut être tentant d'utiliser un système de gestion des clés distinct pour chaque environnement. Les outils natifs proposés par chaque fournisseur sont généralement propres à leur écosystème, difficiles à étendre à d'autres clouds et complexes à intégrer avec les solutions on-premise (sur site). Comme les entreprises utilisent en moyenne plus de deux fournisseurs cloud, cette approche entraîne une fragmentation qui complique le suivi et le contrôle du chiffrement à l'échelle de l'entreprise.

Pour simplifier la protection des données, la gestion des clés doit être intégrée à l'ensemble de l'infrastructure et extensible aux nouveaux clouds à mesure qu'ils sont adoptés. Une plateforme unifiée de gestion des clés permet non seulement de rationaliser les opérations, mais aussi d'améliorer l'efficacité et la cohérence de la protection des données.

Cybercriminalité et ressources cloud

L'adoption massive de ces technologies, combinée aux difficultés persistantes que rencontrent les organisations pour en assurer la sécurité, a ouvert la voie à de nouvelles opportunités pour les cybercriminels. Si bien que le cloud s'impose désormais comme l'une des principales cibles de la cybercriminalité. Selon les résultats de cette étude, quatre des cinq types d'actifs les plus touchés par des attaques sont hébergés dans le cloud. À mesure que la valeur des données augmente, les hackers se concentrent logiquement sur les environnements où elles sont les plus nombreuses et les plus sensibles. Les plateformes cloud offrent en outre une surface d'exposition plus large, ce qui accroît le risque de compromission lorsqu'elles ne sont pas protégées de manière adéquate.

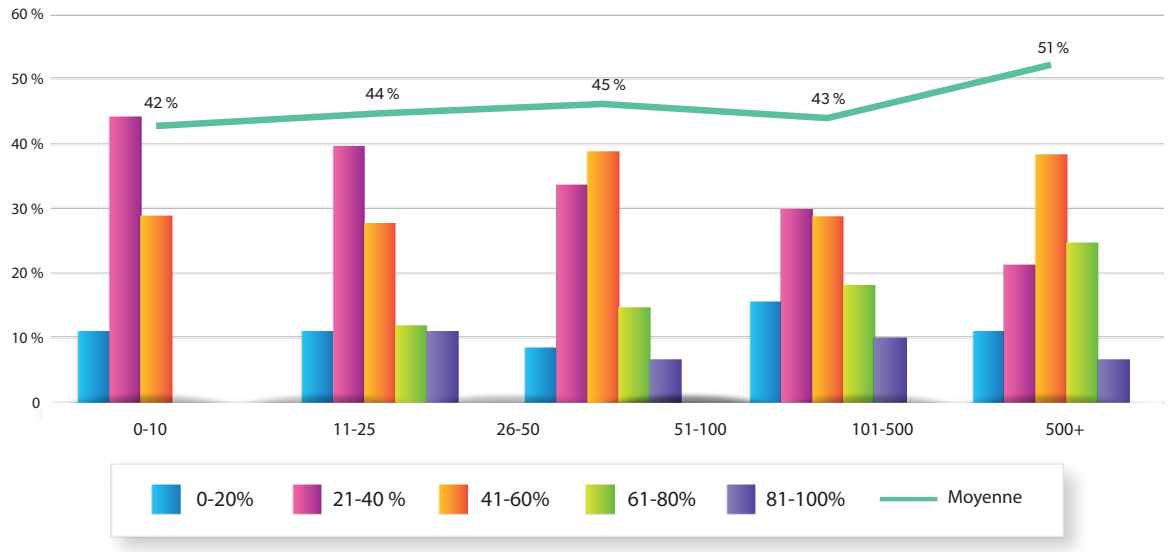
Principales cibles de la sécurité cloud



Les modes d'attaque contre le cloud évoluent rapidement. Près d'une organisation sur deux (54 %) constate une hausse des attaques directes ciblant les infrastructures elles-mêmes et plus des deux tiers (68 %) observent une augmentation des attaques d'accès (vol d'identifiants ou secrets). C'est un risque critique : lorsque le contrôle d'accès constitue la seule barrière de protection, la moindre compromission peut exposer des volumes massifs de données sensibles. Parallèlement, les entreprises hébergent toujours plus d'informations critiques dans le cloud : 85 % indiquent que 40% ou plus de leurs données cloud revêtent un caractère sensible, contre 61 % seulement l'an passé. Si la proportion de données sensibles chiffrées continue de progresser, elle reste encore insuffisante face à l'ampleur des risques actuels. Dans un contexte où les attaques par vol d'identifiants se multiplient, le chiffrement s'impose comme une mesure indispensable pour contrer les intrusions qui franchissent les mécanismes d'authentification. Il devient un pilier de la résilience des organisations et un prérequis pour une stratégie cloud véritablement sécurisée.

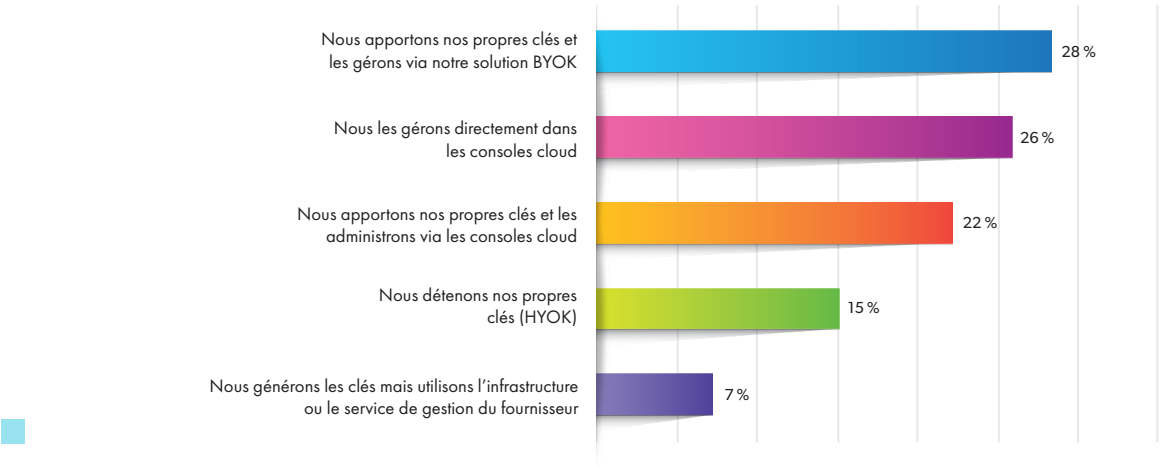
Pour autant, la protection des accès doit encore progresser. Alors que l'utilisation de méthodes d'authentification avancées augmente, seulement 65 % déclarent avoir mis en place une authentification multifacteurs (MFA) pour sécuriser l'accès au cloud. La combinaison authentification faible + données sensibles non chiffrées devient donc un risque majeur pour les entreprises.

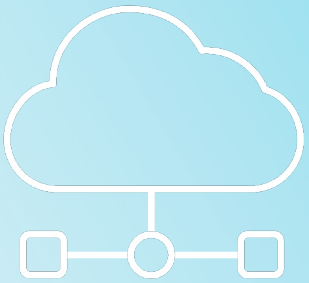
Chiffrement des données cloud à caractère sensible



Les entreprises font des progrès encourageants dans leur gestion des clés. Selon l'étude de cette année, l'adoption de la stratégie « Bring You Own Key» (BYOK) est en hausse : 28 % utilisent cette méthode (contre 25 % l'an dernier). Cependant, 48 % continuent à gérer les clés de chiffrement via les consoles des fournisseurs cloud, ce qui complexifie les opérations en environnement multicloud. Pour simplifier la gestion et alléger la charge opérationnelle, la mise en place d'un système unifié de gestion des clés devient incontournable.

Méthodes de gestion des clés de chiffrement



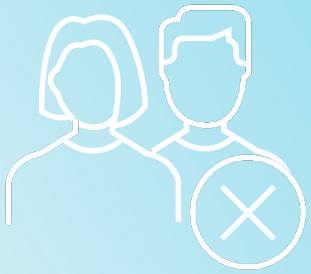


La souveraineté numérique dans un monde hybride

L'utilisation croissante des services cloud soulève de plus en plus de préoccupations liées à la souveraineté des données. À l'origine, l'un des principaux avantages du cloud résidait dans la possibilité d'héberger et de gérer les données sans se soucier de leur localisation. Aujourd'hui, cet atout est devenu une contrainte : les réglementations nationales et régionales exigent souvent que les données soient stockées et traitées dans des zones géographiques précises. Pour se conformer à ces exigences, les organisations doivent mettre en place des capacités robustes de gestion et de contrôle des données, afin de garantir à tout moment la maîtrise de leur localisation, de leur accès et de leur protection. Le chiffrement apparaît comme une réponse essentielle à ces nouveaux besoins : 42 % des organisations le considèrent comme le moyen le plus efficace pour limiter les risques associés à la localisation des données.

16 % des entreprises citent la conformité locale et 21 % la conformité internationale comme principaux moteurs de leurs démarches de souveraineté des données. Pourtant, la motivation la plus fréquente demeure la portabilité des données et des charges de travail (33 %). Ces résultats, en ligne avec ceux de l'an dernier, confirment une tendance nette : les organisations privilégient avant tout la flexibilité et le contrôle de leurs environnements cloud.

Le chiffrement (42 %) est largement reconnu comme moyen efficace de réduire les risques liés à la localisation des données.



Le facteur humain, maillon faible du processus

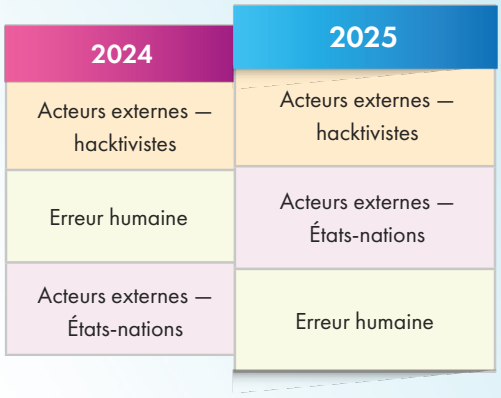
Face à l'essor de l'IA, le monde appelle à maintenir une supervision humaine alors même que, dans le domaine de la sécurité, l'humain demeure le maillon faible. De la même manière, les résultats de cette étude révèlent un écart entre les préoccupations des entreprises et les causes réelles des incidents : les attaques externes restent la principale source d'inquiétude mais c'est bien l'erreur humaine qui demeure la première cause des failles de sécurité.

Bien que les erreurs humaines ne soient citées qu'au troisième rang des menaces identifiées, elles demeurent la principale cause réelle des brèches de sécurité. Cet écart entre la perception du risque et la réalité illustre une mauvaise priorisation des efforts de protection, particulièrement marquée dans les environnements cloud. Cette situation s'explique en partie par le manque de compétences spécialisées au sein des équipes et par la complexité croissante des opérations de sécurité cloud, qui rendent les erreurs plus probables et plus coûteuses. Dans ce contexte, les attaques exploitant des identifiants volés ou des secrets compromis apparaissent comme les tactiques qui progressent le plus rapidement (68 %).

Une seule compromission d'identité peut suffire à exposer des données sensibles non protégées. Pour y remédier, les organisations cherchent à réduire la probabilité d'erreur humaine en renforçant les contrôles d'authentification. Les résultats de l'étude montrent des avancées encourageantes : l'authentification multifacteur (MFA) reste la mesure la plus répandue pour sécuriser l'accès au cloud (65 %), même si elle n'est pas encore généralisée. L'introduction de méthodes résistantes au phishing, telles que la biométrie et les solutions sans mot de passe, témoigne d'une évolution vers des approches plus robustes.

En revanche, la gestion des accès à privilèges (PAM) — pourtant déterminante pour limiter les erreurs et contenir les abus dans les environnements cloud — reste encore peu déployée (38 %). Au-delà des technologies, la complexité est une source majeure d'erreurs : les entreprises doivent chercher à simplifier les opérations de sécurité en misant sur la consolidation et l'intégration des outils.

Principales préoccupations liées aux attaques

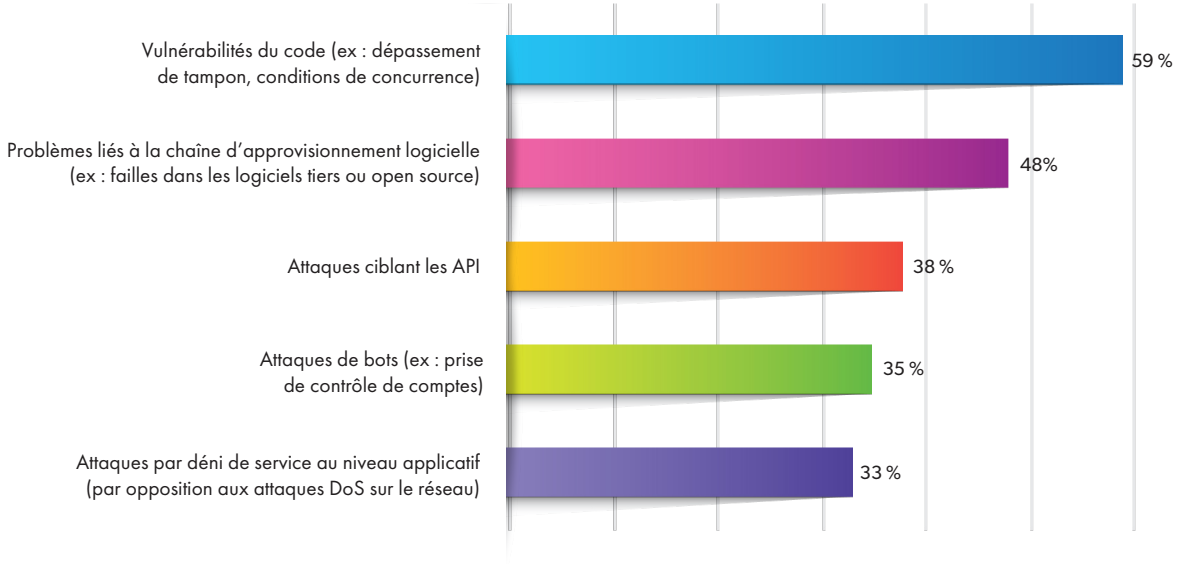


Les attaques ciblant les identifiants ou secrets volés sont reconnues comme les tactiques de piratage de l'infrastructure cloud qui progressent le plus rapidement (68 %).

Sécurité AppSec et DevOps dans le cloud

Les grandes avancées AppSec et DevOps ont lieu désormais dans le cloud. Les approches cloud-native et les pratiques d'Infrastructure as Code (IaC) permettent d'accélérer la mise en production des applications et de les rendre plus flexibles. Cependant, cette évolution impose de nouvelles exigences en matière de sécurité. Parmi ces exigences, la sécurisation des API occupe une place centrale. Les API constituent aujourd'hui la colonne vertébrale des opérations cloud : elles orchestrent les flux, automatisent les processus et assurent la communication entre services. Plus d'un tiers des organisations déclarent en exploiter plus de 500, un volume qui multiplie mécaniquement les points d'exposition potentiels. Les environnements intégrant des services d'IA s'appuient eux aussi massivement sur les API. Protéger ces interfaces devient donc indispensable pour garantir la fiabilité et la sécurité des projets IA, qui dépendent souvent de données sensibles et de connexions multiples à des services externes. Les attaques ciblant les API (38 % des préoccupations) demeurent encore sous-estimées par rapport aux vulnérabilités de code (59 %) ou aux risques de la chaîne d'approvisionnement logicielle (48 %) : il semble pourtant important de rappeler que les API elles-mêmes peuvent présenter des vulnérabilités de code et devenir des vecteurs d'accès en cas de compromission de la chaîne d'approvisionnement logicielle.

Principales préoccupations en matière de sécurité applicative

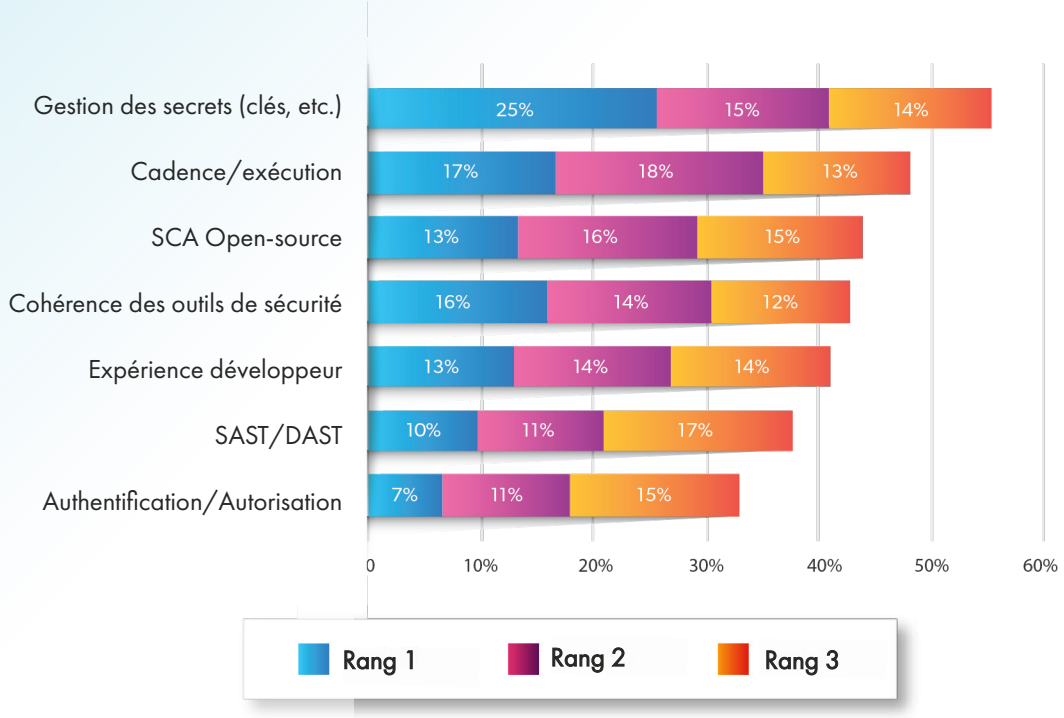


La gestion des secrets (clés, tokens, etc.) est aujourd'hui identifiée comme étant le principal défi de sécurité dans le développement applicatif. Cette préoccupation est pleinement justifiée : les secrets compromis figurent en tête des vecteurs d'attaque des infrastructures cloud. Pour autant, la gestion de ces identifiants et secrets d'accès au cloud reste complexe. Les équipes de développement peinent à maîtriser leur implémentation et les équipes de sécurité ont des difficultés à évaluer la robustesse réelle des environnements applicatifs.

Des approches comme le platform engineering, où les chaînes de développement s'appuient sur des outils et pipelines validés, offrent une voie prometteuse pour renforcer la sécurité. Pourtant, seuls 16 % citent les outils DevSecOps dédiés à la gestion des secrets parmi les technologies les plus efficaces pour protéger les données. Ce manque d'attention à la gestion des secrets est d'autant plus préoccupant que le chiffrement des données sensibles dans le cloud reste insuffisant. En l'absence de pratiques solides de gestion et de protection des secrets, la compromission d'identifiants ou de clés d'accès peut permettre à un cybercriminel de contourner les contrôles existants et d'accéder directement à des données non chiffrées.

Protéger les applications cloud implique d'assurer une maîtrise complète du cycle de vie des données. Localisation, classification, chiffrement et contrôle d'accès doivent fonctionner en synergie pour garantir une sécurité homogène.

Principaux défis DevSecOps



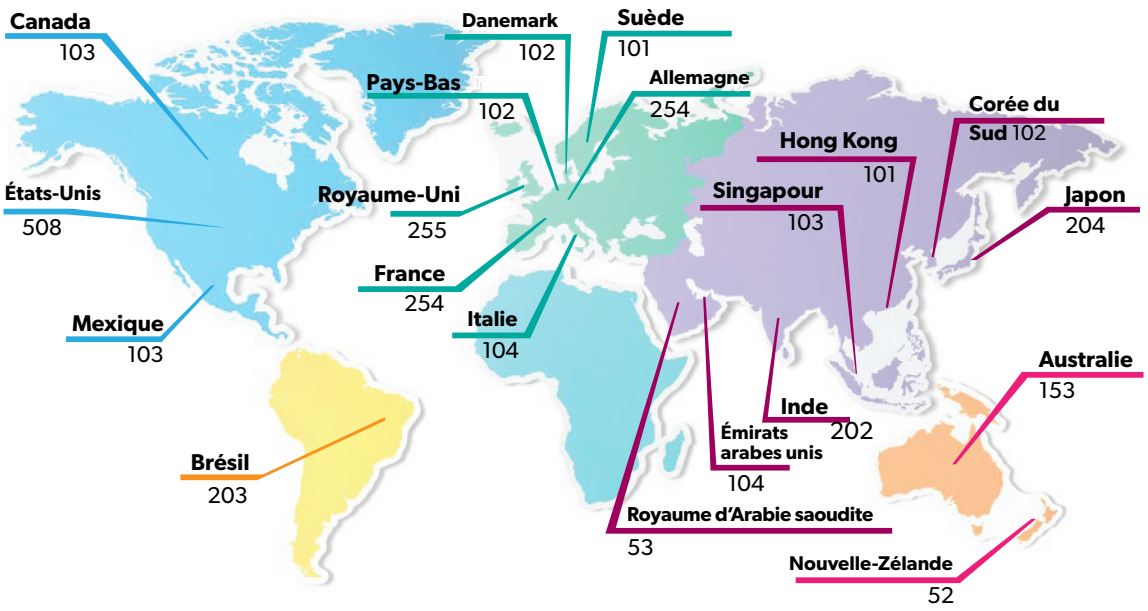
Vers un cloud plus sûr

Le cloud est devenu un pilier incontournable de l'infrastructure des entreprises actuelles. Pour préserver la confiance des clients et rester compétitives, les organisations doivent en garantir un usage sûr et maîtrisé. L'adoption du chiffrement progresse comme moyen de protection des données, mais des lacunes importantes subsistent. La part encore élevée de données sensibles non chiffrées dans le cloud représente un risque significatif que les entreprises doivent traiter en priorité. La simplification de la gestion de la sécurité cloud est également essentielle. Avec un système de gestion de la sécurité centralisé, couvrant à la fois les environnements on-premise et cloud, les équipes de sécurité peuvent mieux coordonner leurs actions, réduire la charge opérationnelle et s'adapter plus facilement aux évolutions ou aux changements de fournisseurs cloud. L'essor de l'intelligence artificielle illustre parfaitement les transformations profondes qui affectent la cybersécurité : augmentation des budgets, exigences accrues en matière d'infrastructures et besoins croissants de disponibilité des données. Face à ces évolutions, la sécurité doit devenir un moteur d'adaptation et d'innovation, et non un frein aux ambitions de l'entreprise. Les organisations s'appuient désormais sur des infrastructures hybrides et la sécurité doit refléter cette réalité en assurant une vision unifiée et cohérente de la protection des données et des accès. Améliorer la productivité et l'efficacité des équipes de sécurité doit aussi constituer une priorité, car la fatigue opérationnelle et l'erreur humaine demeurent les principales causes de compromission dans le cloud. En mettant en place un environnement de sécurité moins fragmenté et plus intégré, les entreprises permettent à leurs équipes de se concentrer sur des initiatives à plus forte valeur stratégique. Une sécurité cloud efficace devient ainsi la base d'une innovation maîtrisée : elle offre aux entreprises la confiance nécessaire pour exploiter pleinement les opportunités des technologies émergentes comme l'intelligence artificielle, pour avancer vers l'avenir en toute sérénité.

Les organisations doivent simplifier la gestion de leur sécurité cloud en améliorant l'intégration des outils et en utilisant des plateformes unifiées.

À propos de cette étude

Cette étude repose sur une enquête mondiale réalisée auprès de 3 163 participants au moyen d'un questionnaire en ligne. L'échantillon regroupe des professionnels de la sécurité et de la gestion IT, sélectionnés dans chaque pays en fonction de leur rôle et de leur niveau d'expertise sur le sujet. Les critères de participation ont exclu les répondants issus d'organisations dont le chiffre d'affaires annuel est inférieur à 100 millions de $ US, ainsi que certaines entreprises situées dans la tranche de 100 à 250 millions de $ US, selon les pays concernés. Il convient de noter que cette recherche est de nature observationnelle : elle vise à identifier des tendances et des corrélations, pas à établir de relation de causalité entre les variables étudiées.



Chiffre d'affaires	Nombre de répondants
100m$ à 249,9m$	187
250m$ à 499,9m$	802
500m$ à 749,9m$	842
750m$ à 999,9,$	770
1 à 1,49 milliard $	226
1,5 à 1,99 milliard $	111
2 milliards $ ou plus	225
Total	3 163

Secteur d'activité	Nombre de répondants	Secteur d'activité	Nombre de répondants
Distribution	301	Autre	170
Industrie manufacturière	291	Voyage / Hôtellerie	166
Santé	274	Pharmaceutique	164
Services financiers	258	Commerce en ligne	149
Gouvernement	255	Automobile	144
Technologies	217	Éducation	137
Énergie & Services publics	198	Télécommunications	128
Transports	187	Biotechnologie	124
Total			3 163

THALES

Building a future we can all trust

Pour nous contacter, rendez-vous sur :
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/recherche-securite-cloud