

2025

État des lieux de la sécurité du cloud

Perspectives et stratégies pour protéger
les environnements cloud



FORTINET®

Introduction

L'adoption du cloud nourrit la transformation des infrastructure IT et de la cybersécurité, en offrant des niveaux d'évolutivité et de flexibilité sans précédent. Si une stratégie multi-cloud renforce encore plus ces avantages, elle présente néanmoins des défis uniques, ce qui incite les entreprises à mettre en œuvre des solutions innovantes pour protéger efficacement leurs ressources critiques.

L'État des lieux 2025 de la sécurité du cloud, basé sur l'opinion et les perspectives de 873 professionnels de la cybersécurité, livre une analyse approfondie des évolutions de la sécurité du cloud. Ce rapport met en évidence les principales tendances, les défis et les priorités des entreprises qui évoluent dans des environnements de plus en plus complexes. Il vise à accompagner les professionnels de l'informatique et de la sécurité qui cherchent à renforcer la posture de sécurité de leurs environnements hybrides et multi-clouds, tout en continuant à innover.

Les temps forts de ce rapport sont les suivants :

- **Les stratégies hybrides et multi-clouds ont le vent en poupe** : plus de 78 % des personnes interrogées font appel à au moins deux fournisseurs cloud, ce qui souligne une nette progression des approches multi-clouds pour renforcer la résilience et tirer parti de capacités spécialisées. 54 % des entreprises ont adopté des modèles de cloud hybride qui associent environnements sur site et cloud public, afin de gagner en flexibilité et en contrôle.
- **La sécurité et la conformité sont des préoccupations essentielles** : les problématiques de sécurité et de conformité sont les principaux obstacles à l'adoption du cloud computing. Elles sont citées par 61 % des entreprises qui s'efforcent de répondre aux exigences réglementaires et de protéger leurs données sensibles.
- **Pénurie de compétences en matière de sécurité du cloud** : 76 % des entreprises pointent une pénurie de compétences en matière de sécurité du cloud, ce qui souligne un besoin pour davantage d'automatisation, des compétences plus ciblées et une optimisation des ressources.
- **Une faible confiance dans la détection en temps réel des menaces** : les données de l'enquête soulignent que 64 % des personnes interrogées ne sont pas totalement confiantes dans la capacité de leur entreprise à assurer une détection en temps réel des menaces.
- **Plateformes unifiées de sécurité cloud** : l'enquête indique que 97 % des personnes interrogées préfèrent les plateformes proposant des tableaux de bord centralisés, pour simplifier la configuration de politiques et améliorer la visibilité sur l'ensemble de l'empreinte cloud d'une entreprise.
- **Adoption rapide du CSPM (Cloud Security Posture Management) et du CNAPP (Cloud-Native Application Protection Platforms)** : pour restaurer les erreurs de configuration et les défauts de conformité, 67 % des personnes interrogées sollicitent des solutions CSPM et 62 % des solutions CNAPP afin de protéger les environnements cloud.



Ce rapport souligne l'importance des solutions unifiées de sécurité du cloud pour simplifier la mise en œuvre des politiques, automatiser la détection des menaces et offrir un même niveau de protection sur tous les environnements hybrides et multi-clouds. En tirant parti de ces informations et des meilleures pratiques, les entreprises instituent une posture de sécurité du cloud résiliente qui s'adapte à l'évolution des menaces et aux exigences des entreprises.

Nous exprimons nos sincères remerciements à [Fortinet](#), un leader mondial de la sécurité du cloud, pour sa contribution essentielle à cette étude. Son expertise et ses connaissances en matière de sécurisation des environnements hybrides et multi-clouds ont permis de considérablement étayer les conclusions et recommandations présentées dans ce rapport.

Nous espérons que ce rapport constituera une ressource précieuse pour les professionnels de l'informatique et de la cybersécurité qui s'efforcent de protéger leur entreprise à l'heure d'une expansion rapide du cloud computing.

Cordialement,

Holger Schulze

Fondateur, Cybersecurity Insiders

Faire évoluer les stratégies de déploiement cloud

Le choix de la stratégie de déploiement cloud d'une entreprise impacte directement ses besoins de sécurité, ses résultats opérationnels et ses exigences en matière d'infrastructure. Une telle décision est donc cruciale pour les environnements informatiques à multiples facettes d'aujourd'hui.

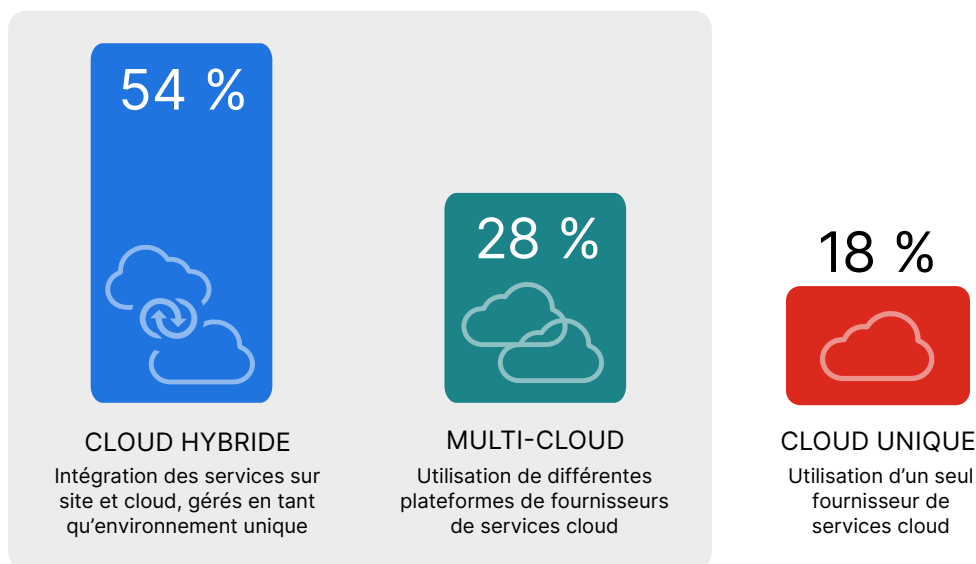
Les résultats de l'enquête en témoignent : le cloud hybride est la stratégie prédominante, choisie par 54 % des personnes interrogées, contre 43 % l'année dernière. Cette progression, reflète une tendance marquée, celle de l'abandon du cloud unique au profit d'une intégration de plusieurs services cloud avec des systèmes sur site, pour ainsi donner lieu à des environnements homogènes. Par exemple, un acteur de la grande distribution peut utiliser un cloud public pour héberger des applications liées à ses clients tout en conservant les données de paiement sensibles dans un système privé sur site, pour ainsi assurer la conformité à des réglementations comme PCI DSS. De telles stratégies hybrides permettent de bénéficier de l'évolutivité des clouds publics tout en gardant le contrôle sur les données critiques d'entreprise.

Le multi-cloud suit à 28 %. Ce type d'environnement est privilégié par les entreprises qui répartissent leurs instances entre plusieurs fournisseurs pour éviter une trop forte dépendance à l'un d'entre eux ou pour utiliser certaines fonctionnalités spécifiques. Par exemple, une entreprise technologique pourrait héberger ses applications gourmandes en ressources de traitement sur Amazon Web Services (AWS) tout en utilisant les services de Google Cloud pour un traitement analytique des données optimisé par IA. Cette entreprise renforce ainsi ses performances tout en évitant d'être dépendante d'un seul fournisseur.

L'utilisation d'un cloud unique est une pratique de moins en moins courante : seules 18 % des entreprises ne font appel qu'à un seul fournisseur, contre 22 % en 2024. Cette option reflète souvent une volonté de ses partisans de simplifier les tâches de gestion, mais potentiellement au prix d'une flexibilité moindre. Ce cloud unique est souvent le modèle préféré des petites entreprises, à l'instar d'un cabinet d'avocats qui utiliserait exclusivement Azure de Microsoft pour le stockage de ses documents et la gestion des workflows, dans l'idée de privilégier une simplicité de gestion par rapport à la diversification.

► Quelle est la principale stratégie principale de votre entreprise en matière d'environnement cloud ?

82 % des entreprises utilisent un environnement multi-cloud ou hybride

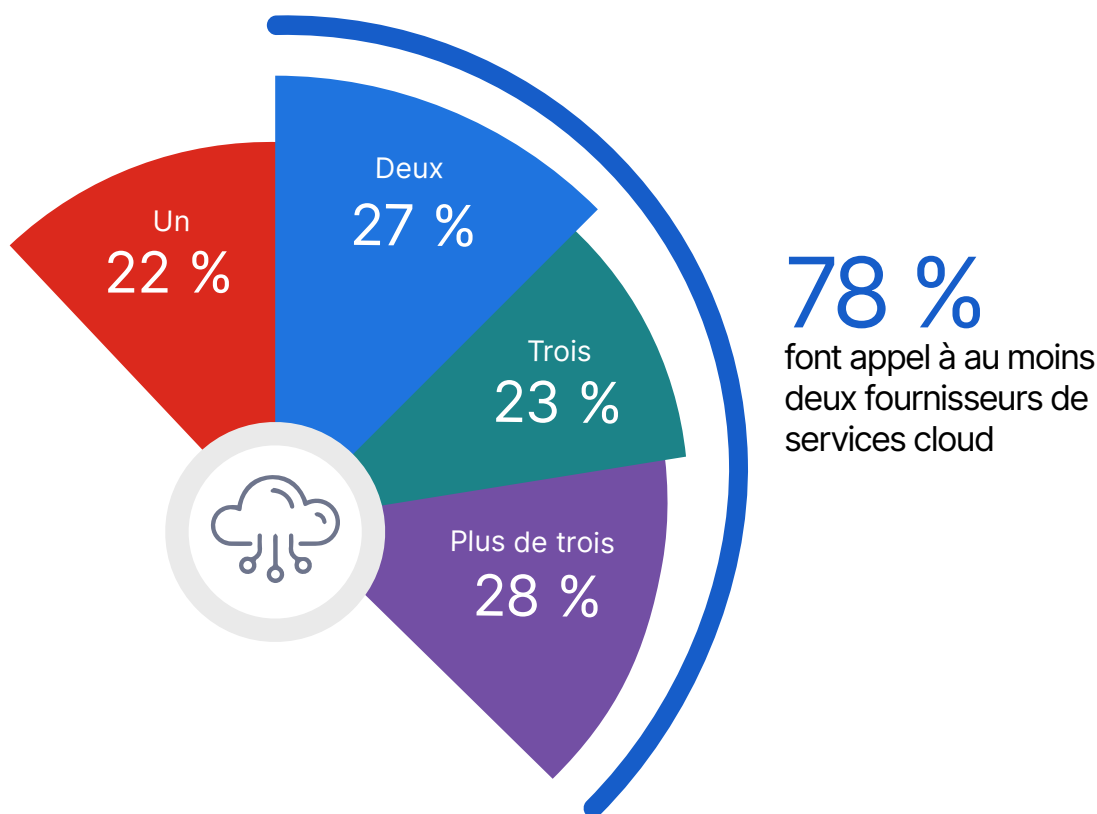


Renforcer l'adoption du multi-cloud

Le nombre croissant de fournisseurs cloud utilisés par les entreprises reflète une préférence pour les stratégies hybrides et multi-clouds, ainsi que la complexité opérationnelle qu'elles introduisent.

L'enquête révèle que 78 % des entreprises font appel à deux fournisseurs cloud ou plus, un chiffre qui progresse de 7 points en un an et qui témoigne de cette nouvelle orientation qu'est l'adoption du multi-cloud. Par exemple, une multinationale utilisera AWS pour son réseau mondial de fourniture de contenu, tout en faisant appel aux offres de Microsoft Azure dans les régions régies par une gouvernance stricte qui impose un hébergement en local des données. L'utilisation stratégique de différents fournisseurs permet aux entreprises de faire appel à des capacités spécialisées, à l'instar des services IA de Google Cloud ou de l'expertise sur les bases de données d'Oracle Cloud. La résilience est assurée grâce à la redondance.

► À combien de fournisseurs cloud votre entreprise fait-elle appel ?



Domination des fournisseurs majeurs de services cloud

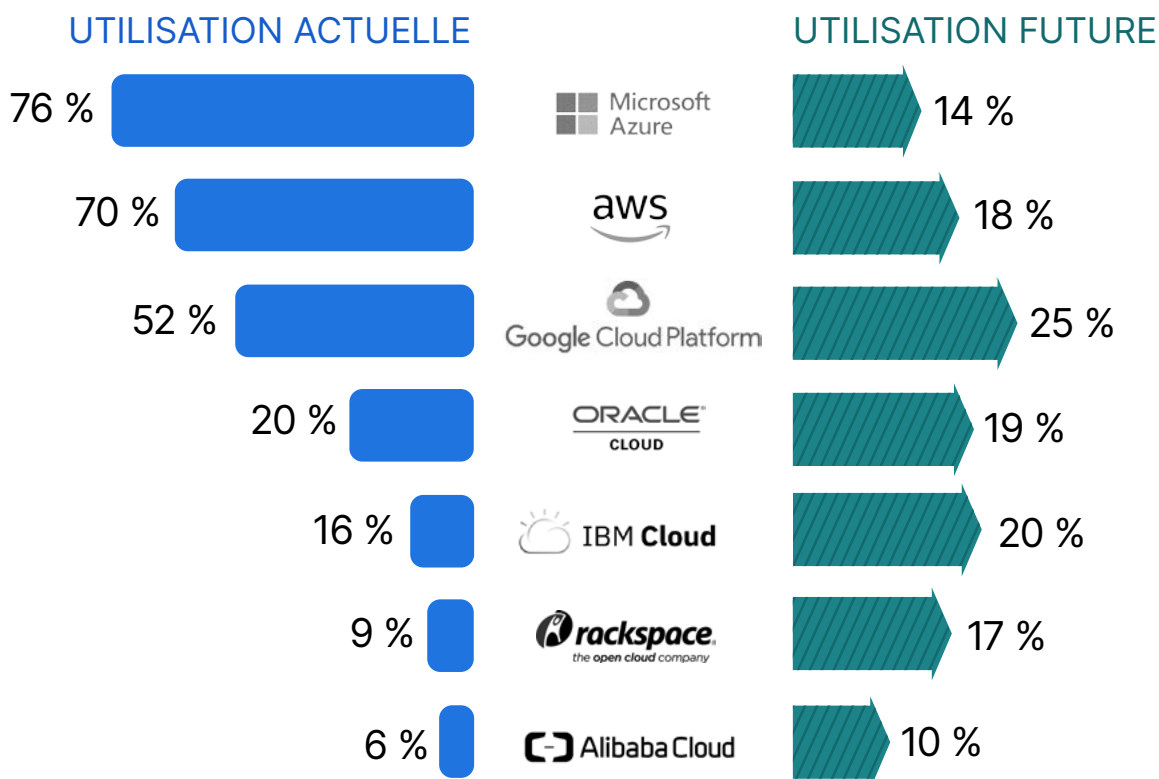
Déterminer les fournisseurs de services cloud auxquels les entreprises font appel, ou comptent le faire, permet d'identifier les préférences du marché et révèle comment les entreprises définissent leur stratégie cloud en fonction de l'évolution de leurs instances et de capacités spécialisées.

Les résultats confirment que Microsoft Azure et AWS sont des acteurs dominants, avec respectivement 76 % et 70 % des personnes interrogées qui déclarent les utiliser actuellement.

Adopté par 52 % des personnes interrogées, Google Cloud Platform suscite de plus en plus d'intérêt, comme en témoignent les 25 % de personnes interrogées qui prévoient d'y recourir à l'avenir.

Quant à Oracle Cloud et IBM Cloud, ils présentent des parts de marché plus modestes mais suscitent un intérêt notable pour l'avenir, probablement en raison de leur expertise en matière d'intégration avec les systèmes d'entreprise existants.

- Quel(s) fournisseur(s) d'IaaS utilisez-vous actuellement ou prévoyez-vous d'utiliser à l'avenir (sélectionnez toutes les réponses qui s'appliquent)?



Lever les barrières à l'adoption du cloud

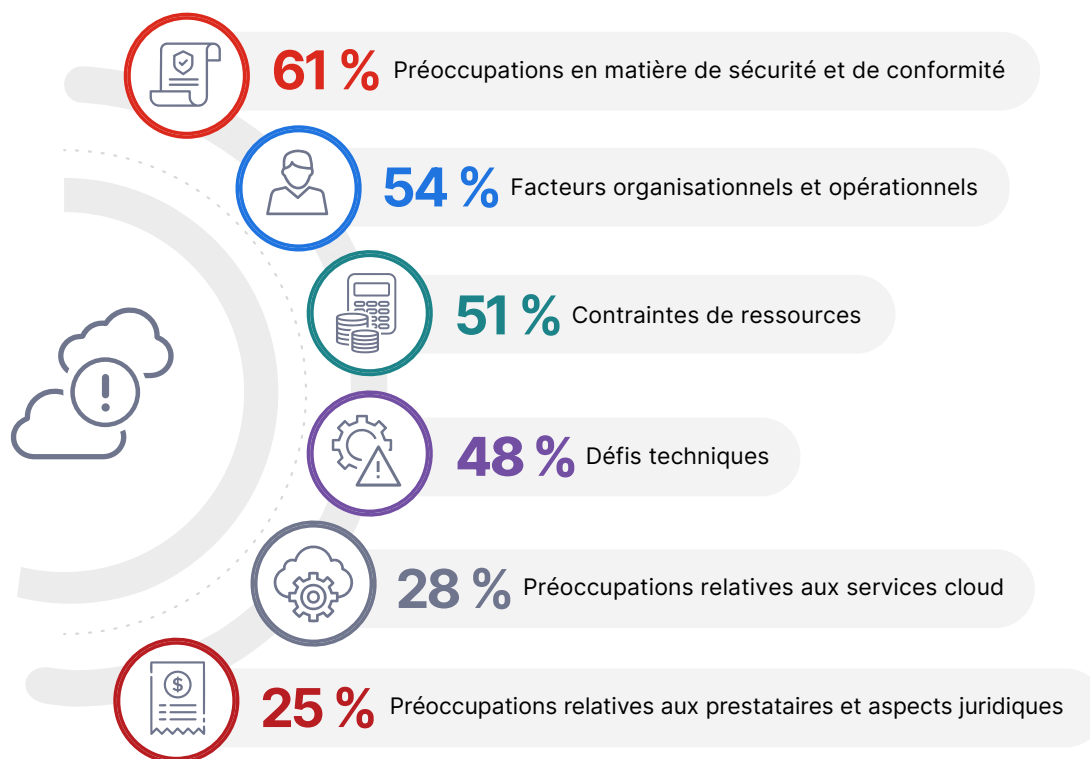
L'enquête révèle les principaux obstacles que rencontrent les entreprises qui adoptent des services cloud. Elle pointe les défis que les équipes informatiques et de sécurité doivent relever pour tirer le meilleur parti des environnements cloud.

Les problématiques de sécurité et de conformité restent le principal défi, cité par 61 % des personnes interrogées (contre 59 % dans l'enquête de l'année dernière). Ce chiffre reflète un intérêt plus marqué pour des sujets comme les fuites de données et la mise en conformité réglementaire. Par exemple, un acteur des soins de santé pourrait retarder la migration des dossiers sensibles de patients vers le cloud en raison d'une conformité incertaine avec HIPAA ou d'autres réglementations régionales de protection des données.

Les facteurs organisationnels et opérationnels suivent de près avec 54 % (contre 49 % l'année dernière). Ces facteurs portent sur la résistance au changement, sur des craintes de dépendance par rapport à des fournisseurs et sur des obstacles culturels. Ainsi, un industriel pourrait se montrer réticent à migrer ses systèmes existants vers le cloud par crainte de perdre le contrôle sur ses processus propriétaires.

Les contraintes de ressources (déficit d'expertise des équipes, restrictions budgétaires...) sont citées par 51 % (contre 49 % en 2024) du panel, soulignant la difficulté pour nombre d'entreprises de gérer et sécuriser leurs environnements cloud. Parallèlement, les défis techniques, bien que légèrement moins prééminents cette année (48 %), restent néanmoins un obstacle majeur, en particulier lors de l'intégration d'environnements cloud hybrides complexes.

► Quels sont les principaux obstacles à l'adoption du cloud par votre entreprise ?



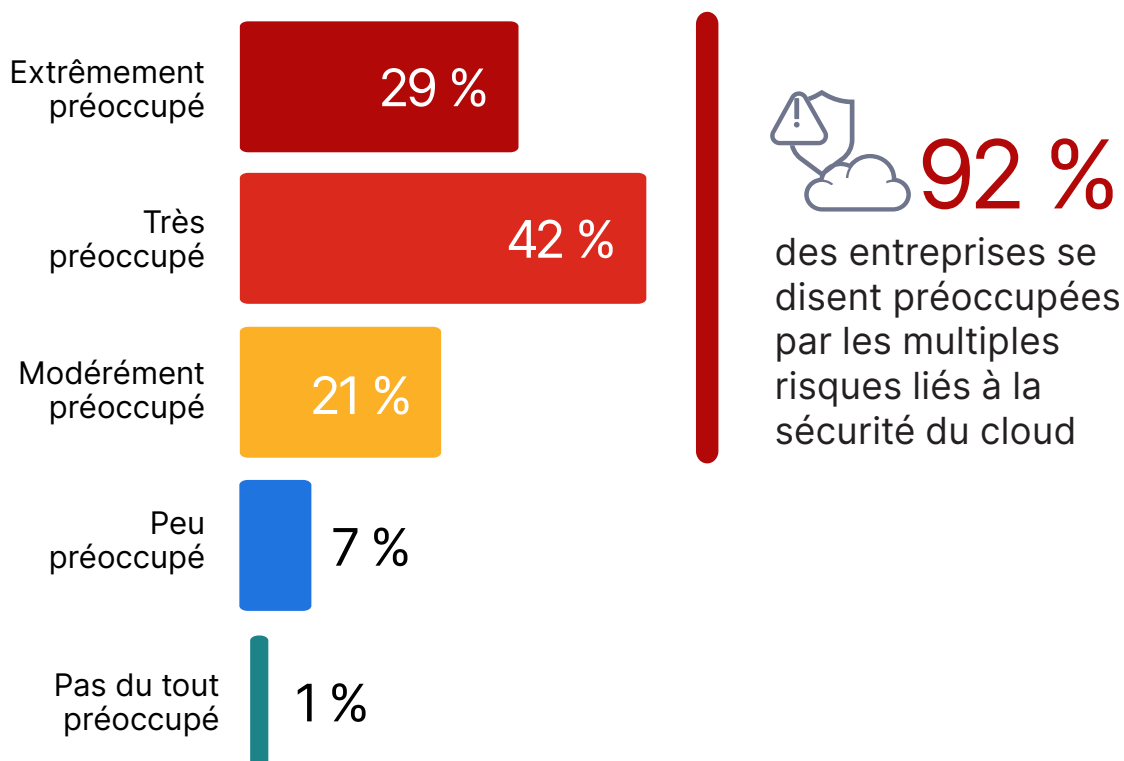
Préoccupations liées à la sécurité du cloud public

Les préoccupations persistantes concernant la sécurité des clouds publics reflètent la nécessité d'un équilibre entre les avantages de l'évolutivité et de l'agilité, d'une part, et la nécessité d'une protection solide, d'autre part.

Une part élevée des répondants (92 %) exprime des inquiétudes quant à la sécurité des clouds publics, soulignant qu'il s'agit d'un domaine critique pour les professionnels de l'informatique et de la cybersécurité.

Cette appréhension est dans le droit fil des résultats de cette enquête, avec 61 % des répondants qui font de la sécurité et de la conformité le principal obstacle à l'adoption du cloud computing. Prenons l'exemple d'un acteur des services financiers qui envisage de migrer les données transactionnelles de ses clients vers le cloud. Il pourrait hésiter par crainte d'une non-conformité réglementaire ou d'une exposition potentielle d'informations sensibles suite à une erreur de configuration. Ces préoccupations portent également sur des risques spécifiques : fuite de données, confusion sur le partage des responsabilités de sécurité et visibilité limitée sur les activités des fournisseurs cloud, ce qui complique davantage la décision de passer au cloud.

► À quel point êtes-vous préoccupé par la sécurité des clouds publics ?



Les défis opérationnels du cloud

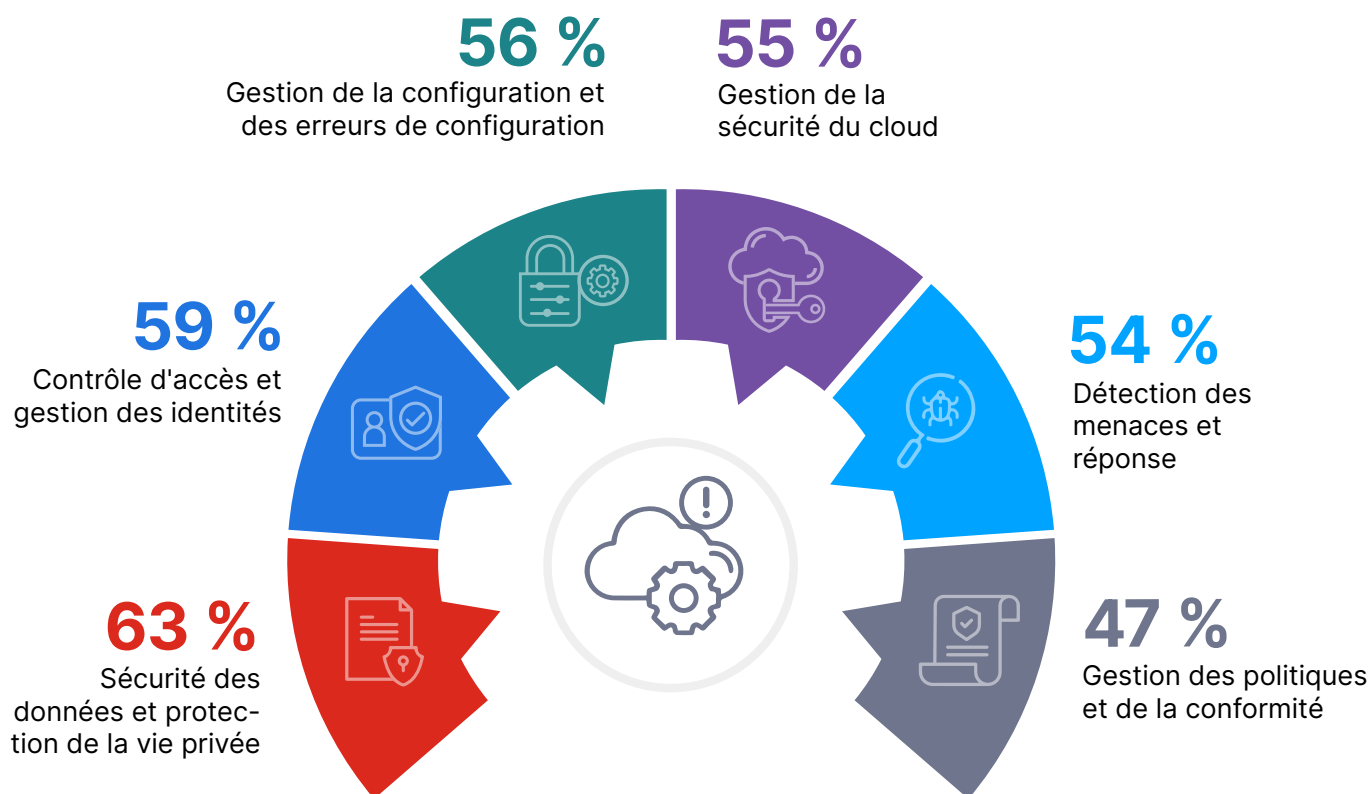
La gestion au quotidien des opérations de sécurité dans le cloud rencontre des obstacles complexes, en évolution, et qui pèsent sur la capacité des entreprises souhaitant sécuriser leurs environnements.

La sécurité et la confidentialité des données constituent une préoccupation majeure. Cette thématique, citée par 63 % des personnes interrogées, reflète les craintes actuelles portant sur la protection des informations sensibles et la prévention des fuites de données. Le contrôle d'accès et la gestion des identités suivent avec 59 %, soulignant la nécessité d'une authentification solide et d'une gestion des privilèges dans les environnements cloud distribués. Un cloud hybride, par exemple, peut être confronté à des soucis de synchronisation des politiques d'accès des utilisateurs qui s'appliquent tant aux systèmes sur site qu'aux plateformes cloud.

La gestion de la configuration, et notamment des erreurs de configuration, arrive en troisième position avec 56 %, illustrant la difficulté opérationnelle d'appliquer certaines pratiques essentielles, comme un monitoring de l'exposition publique involontaire des buckets de stockage dans le cloud, une vulnérabilité qui a permis nombre de piratages médiatisés dans le passé.

La gestion de la sécurité du cloud (55 %), la détection et la réponse aux menaces (54 %) et la gestion des politiques et de la conformité (47 %) soulignent collectivement le besoin pour des solutions pertinentes et évolutives de gestion les environnements multi-clouds.

► **Quels sont les principaux défis que vous rencontrez dans la gestion au quotidien des opérations de sécurité du cloud (sélectionnez toutes les réponses pertinentes)?**



Les autres réponses sont les suivantes :

Shadow IT et utilisation non autorisée d'applications 46 % | Intégration et automatisation du cloud 43 % | Sécurité des endpoints 40 % | Allocation des ressources 38 % | Pratiques DevSecOps 31 % | Agilité et complexité des opérations 25 %

Sécuriser les environnements cloud dynamiques

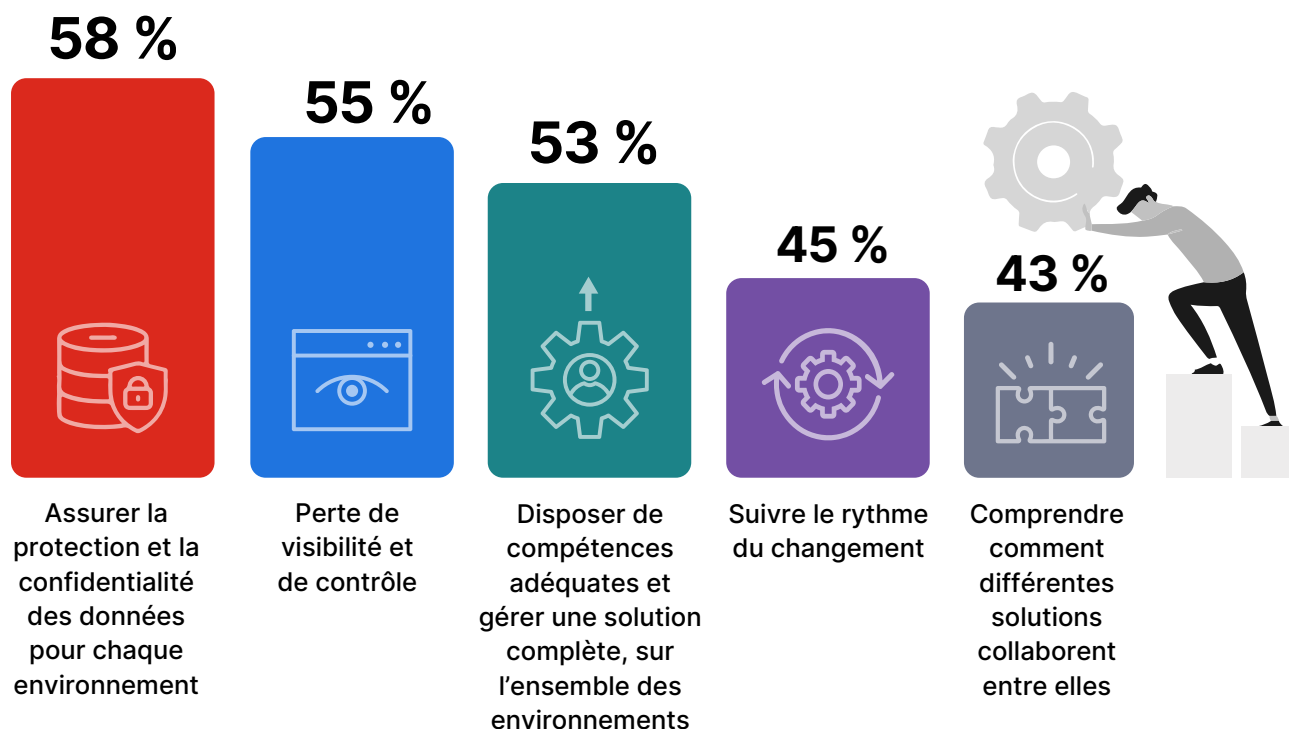
La sécurisation des environnements multi-clouds se confronte à des défis découlant de leur complexité, d'une absence de normalisation et de technologies qui évoluent rapidement. Ces problèmes ont un impact direct sur la capacité des organisations à protéger les données sensibles, à pérenniser l'efficacité opérationnelle et à gérer différents écosystèmes cloud.

Garantir la protection des données et la confidentialité pour chaque environnement constitue le principal défi, cité par 58 % des personnes interrogées, contre 55 % en 2024. Ce chiffre est dans le droit fil des résultats précédents de notre enquête, où la sécurité des données et la confidentialité ont été identifiées comme la principale préoccupation opérationnelle (63 %), soulignant la nécessité de mesures de protection cohérentes pour les infrastructures cloud fragmentées.

55 % du panel pointent la difficulté de disposer d'une visibilité pérenne sur le multi-cloud, ce qui fait écho aux 55 % des répondants qui indiquent que la gestion de la sécurité du cloud est un défi quotidien.

Le déficit de compétences pour déployer et gérer des solutions multi-clouds complètes est cité par 53 % du panel interrogé. La capacité à suivre le rythme du changement (45 %) et la compréhension de comment différentes solutions s'intègrent entre elles (43 %) reflètent les obstacles opérationnels et stratégiques résultant d'une évolution rapide des technologies cloud.

► Quels sont vos les défis le plus critiques pour la sécurisation des environnements multi-clouds (sélectionnez toutes les réponses pertinentes)?



Les autres réponses sont les suivantes :

Gérer les coûts des différentes solutions 41 % | Comprendre les possibilités d'intégration des services 40 % | Fournir un accès transparent aux utilisateurs en fonction de leurs informations d'identification 37 % | Sélectionner le bon mix de services 30 % | Autre 1 %

Faible confiance dans la détection en temps réel des menaces

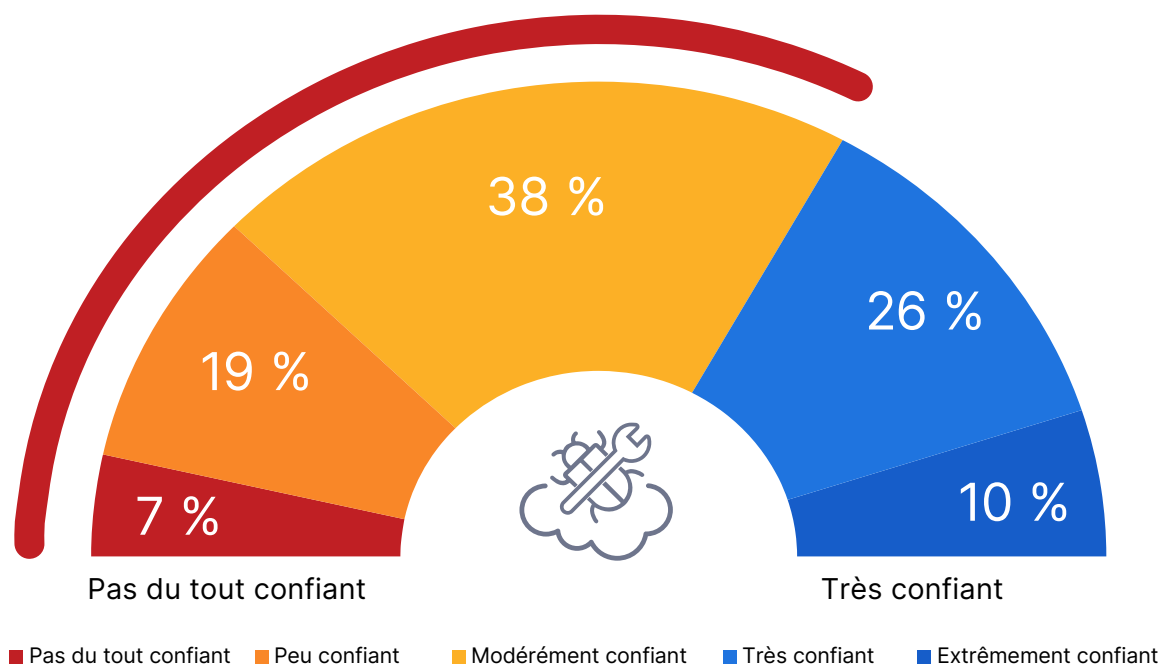
La capacité à détecter et à répondre en temps réel aux menaces dans les environnements cloud est essentielle compte tenu d'entreprises qui adoptent des stratégies multi-clouds et hybrides de plus en plus complexes. Avec ces architectures, il est difficile de disposer d'une visibilité transparente et d'assurer une réactivité rapide sur des plateformes diverses.

Les données de l'enquête mettent en évidence un déficit de confiance majeur, 64 % des personnes interrogées indiquant qu'elles n'ont pas confiance dans la capacité de leur entreprise à assurer la détection des menaces en temps réel. Par exemple, une entreprise peut ignorer comment faire le lien entre différents événements malveillants isolés, entraînant ainsi un retard dans l'identification et la prise en charge d'un incident potentiel. Ainsi, bien que de nombreuses entreprises disposent des mesures de sécurité fondamentales, la sophistication croissante des menaces liées au cloud et la gestion fastidieuse de multiples environnements rendent ceux-ci vulnérables aux attaques avancées et aux erreurs de configuration. Les résultats de l'enquête mentionnés précédemment vont dans le même sens, montrant que la perte de visibilité et de contrôle (55 %) et les défis liés à la détection et à la réponse aux menaces (54 %) constituent les principaux obstacles aux opérations de sécurité cloud.

Seules 10 % des personnes interrogées se déclarent extrêmement confiantes et 26 % très confiantes, ce qui signifie que moins de 40 % d'entre elles sont bien préparées aux exigences d'une gestion moderne des menaces liées au cloud.

- Quel est votre degré de confiance dans la capacité de votre entreprise à détecter les menaces et à y répondre en temps réel sur l'ensemble de vos environnements cloud ?

64 % ont peu ou pas confiance dans la capacité de leur entreprise à gérer les menaces liées au cloud



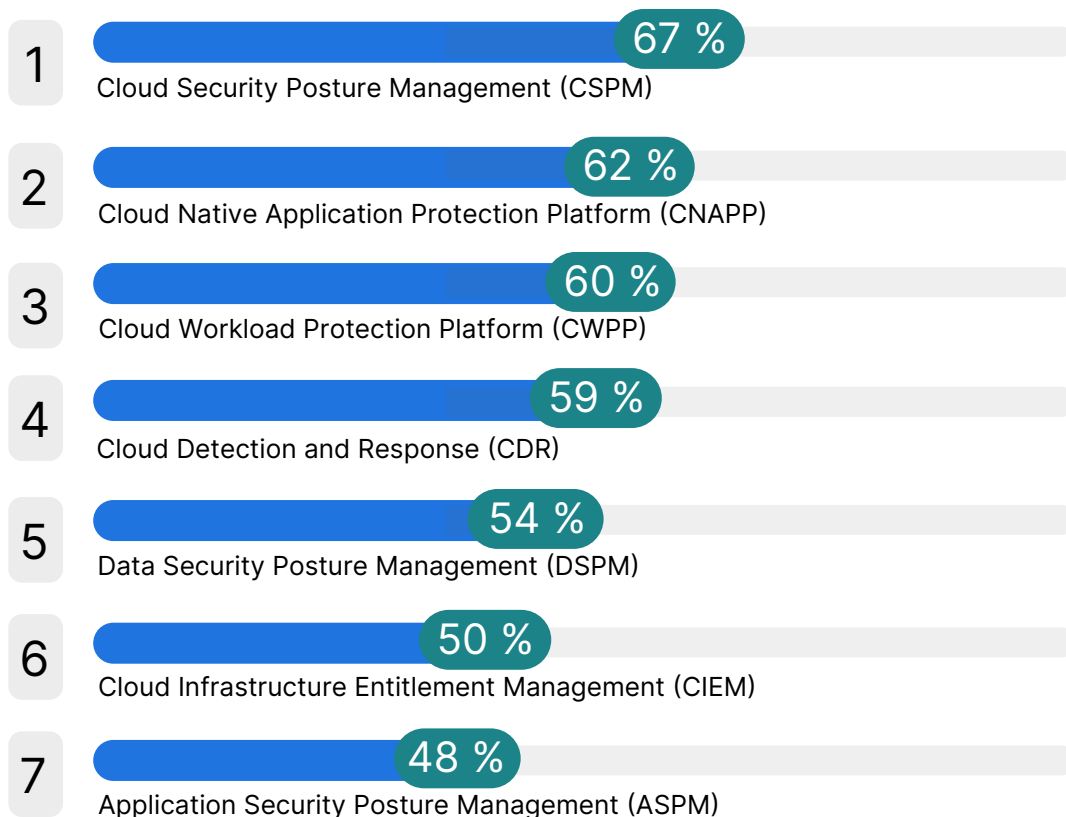
Priorités en matière de sécurité du cloud

À mesure que les entreprises étendent leur empreinte cloud, il devient essentiel de déployer le bon panel de fonctionnalités de sécurité, pour ainsi garantir la résilience, la conformité et l'efficacité opérationnelle face à des menaces toujours plus nombreuses.

En matière de priorités dans le choix d'outils critiques de sécurité cloud sur les 12 prochains mois, c'est la gestion de la posture de sécurité cloud (CSPM) qui ressort en tête avec 67 % des répondants, soulignant le rôle essentiel de cette technologie dans l'identification et la correction des erreurs de configuration dans le cloud. Par exemple, un outil CSPM peut alerter une entreprise sur les buckets de stockage exposés dans AWS, évitant ainsi un piratage de données particulièrement coûteux.

De même, les plateformes de protection des applications natives du cloud (CNAPP), mentionnées par 62 % du panel, indiquent qu'une sécurité active tout au long du cycle de vie des applications devient une priorité. Une plateforme CNAPP peut signaler de manière proactive les vulnérabilités d'instances conteneurisées exécutées dans Kubernetes, identifier les activités malveillantes et détecter une chaîne d'événements indiquant une compromission. Juste derrière, les plateformes de protection des charges de travail dans le cloud (CWPP), à 60 %, et la détection et la réponse dans le cloud (CDR), à 59 %, soulignent l'importance croissante accordée à la sécurité des instances et à la maîtrise des menaces, en particulier dans les environnements multi-clouds. L'adoption d'un outil de CIEM (gestion des habilitations dans l'infrastructure cloud), à 50 %, témoigne d'un besoin pour un contrôle robuste des accès et des privilèges sur diverses plateformes cloud et de la volonté de mettre en œuvre le principe du moindre privilège ou de supprimer les informations d'identification inutilisées.

► Parmi les fonctionnalités suivantes, lesquelles utilisez-vous ou prévoyez-vous d'utiliser au cours des 12 prochains mois (sélectionnez toutes les réponses pertinentes)?



Pallier la pénurie de compétences en cybersécurité

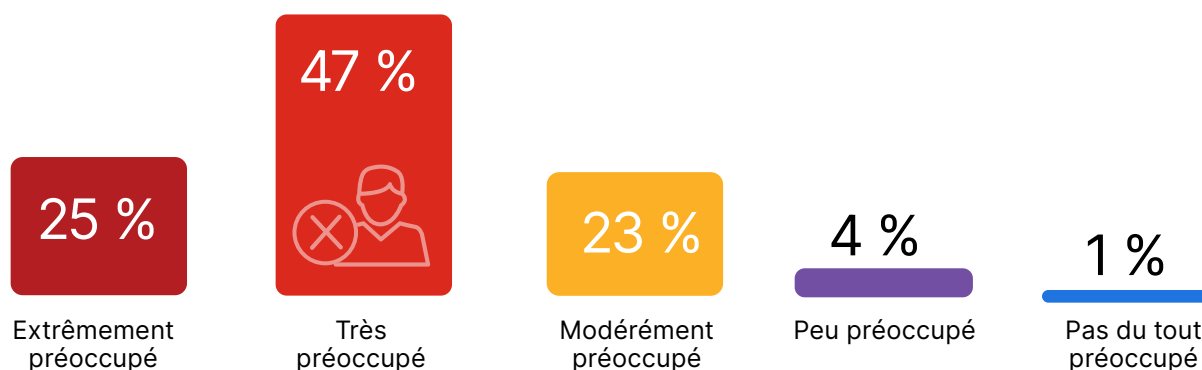
La pénurie de professionnels qualifiés reste une problématique critique dans tous les domaines de la cybersécurité, avec une incidence directe sur la capacité des entreprises à protéger leurs ressources et à répondre efficacement à l'évolution des menaces.

95 % des personnes interrogées affirment être modérément à extrêmement préoccupées par la pénurie actuelle de compétences en cybersécurité, soulignant une pression importante sur les entreprises qui s'efforcent de recruter et de retenir les talents nécessaires pour relever les défis de plus en plus complexes de la cybersécurité. Ainsi, un acteur des soins de santé qui s'efforce de mettre en œuvre des fonctions de sécurité dédiées au multi-cloud pourrait être ralenti dans son projet en raison d'un déficit de spécialistes dans des domaines spécifiques (gestion de la configuration cloud, CIEM...)

- Dans quelle mesure êtes-vous préoccupé par la pénurie de professionnels qualifiés dans le domaine de la cybersécurité, une réalité qui touche l'ensemble du secteur ?

95 %

des entreprises sont modérément à extrêmement préoccupées par la pénurie de professionnels qualifiés en cybersécurité, une réalité qui touche l'ensemble du secteur.



Cette préoccupation est confirmée par les données de l'enquête qui montrent que 76 % des entreprises accusent aujourd'hui une pénurie de talents en cybersécurité.

- Votre entreprise est-elle confrontée à une pénurie de talents en matière de cybersécurité ?



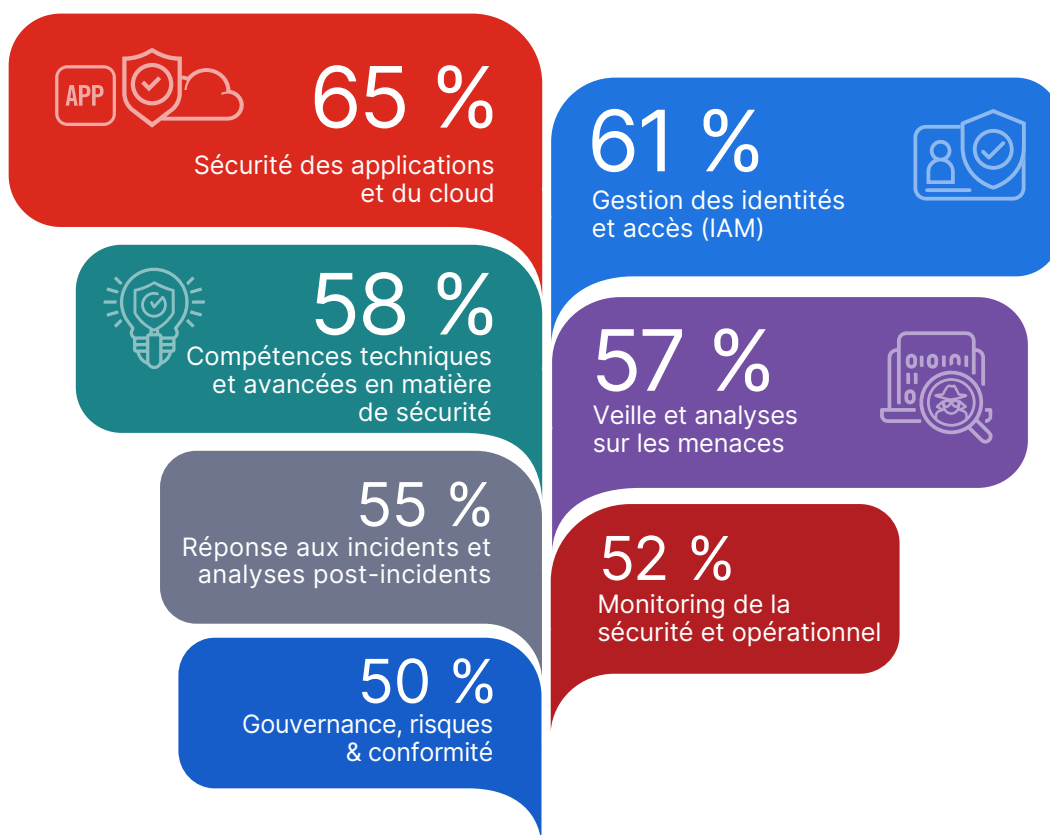
Compétences clés de sécurité pour contrer les menaces actuelles

Les résultats de l'enquête sur les compétences les plus importantes mettent en évidence la diversité et l'évolution de l'expertise dont les entreprises ont besoin pour relever des défis de plus en plus complexes en matière de sécurité du cloud.

Les compétences en matière de sécurité des applications et du cloud sont les plus citées (65 %), reflétant la priorité accordée par les entreprises à la sécurisation des plateformes et applications cloud. Par exemple, une expertise en matière de sécurité des plateformes cloud peut porter sur la création de garde-fous automatisés et de landing zones sécurisées et évolutives, tous disponibles sous forme de code afin d'automatiser leur déploiement.

La gestion des identités et des accès suit de près à 61 %, soulignant la nécessité pour des contrôles d'accès robustes, en particulier dans les environnements hybrides et multi-clouds où la gestion unifiée des privilèges utilisateurs est essentielle. Les compétences techniques et avancées en matière de sécurité (58 %), ainsi que la veille et l'analyse des menaces (57 %) indiquent une demande croissante pour des spécialistes capables d'exploiter l'IA et de comprendre les tactiques sophistiquées des adversaires, afin d'identifier et de déjouer rapidement les activités malveillantes, notamment en cas de compromission de comptes d'administrateur. Les compétences en matière de réponse aux incidents et d'expertise post-incident (55 %) restent essentielles pour maîtriser les incidents, tandis que le monitoring et les opérations de sécurité (52 %) mettent en évidence un besoin d'expertise pour détecter les anomalies et accélérer les risques.

- Quelles sont les compétences de sécurité les plus importantes demandées par votre entreprise ?
(indiquez toutes les réponses pertinentes)



Les autres réponses sont les suivantes :

Formation et sensibilisation 45 % | Communication et stratégie 39 % | Incertain 3 %

Tendances en matière d'investissement dans la sécurité du cloud

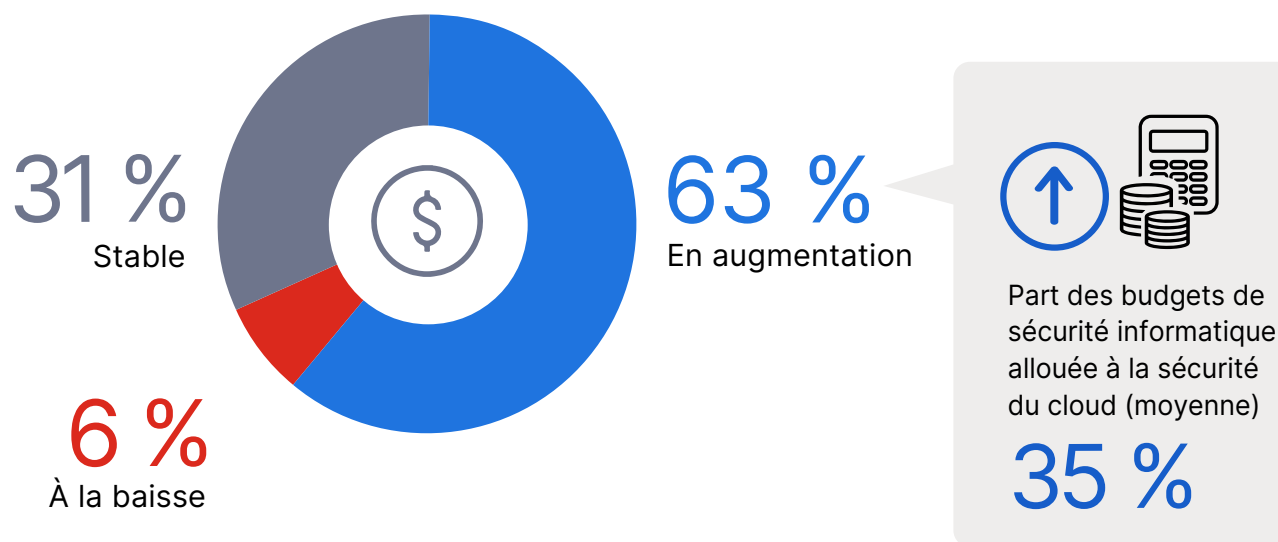
Les résultats de l'enquête révèlent de nouvelles perspectives sur la façon dont les organisations priorisent leurs ressources financières pour relever les défis de la sécurité du cloud. 63 % des personnes interrogées déclarent avoir l'intention d'augmenter leurs budgets de sécurité du cloud au cours des 12 prochains mois (contre 61 % l'année dernière), ce qui indique une reconnaissance de la nécessité de renforcer les défenses au sein des environnements hybrides et multi-clouds.

Parallèlement, 31 % indiquent des budgets inchangés (contre 32 % en 2024), ce qui indique sans doute que les entreprises ont déjà beaucoup investi ou qu'elles privilégient une bonne gestion des opérations. Seuls 6 % des répondants anticipent un repli budgétaire, une tendance rare alors que les menaces cloud et les exigences réglementaires s'intensifient.

En moyenne, 35 % des budgets de sécurité informatique sont alloués à la sécurité du cloud, ce qui montre que la protection du cloud est devenue un poste d'investissement important, notamment parce que l'adoption du est dynamique.

Les investissements plus importants dans la sécurité du cloud s'inscrivent dans une approche proactive visant à corriger les lacunes en matière de visibilité, de contrôle d'accès et de détection des menaces. Les entreprises qui prévoient d'augmenter leurs budgets devraient se concentrer sur des solutions comme le CNAPP qui intègrent efficacement différentes capacités clés afin de maximiser l'impact de l'investissement.

► Quelle sera l'évolution de votre budget consacré à la sécurité du cloud au cours des 12 prochains mois ?

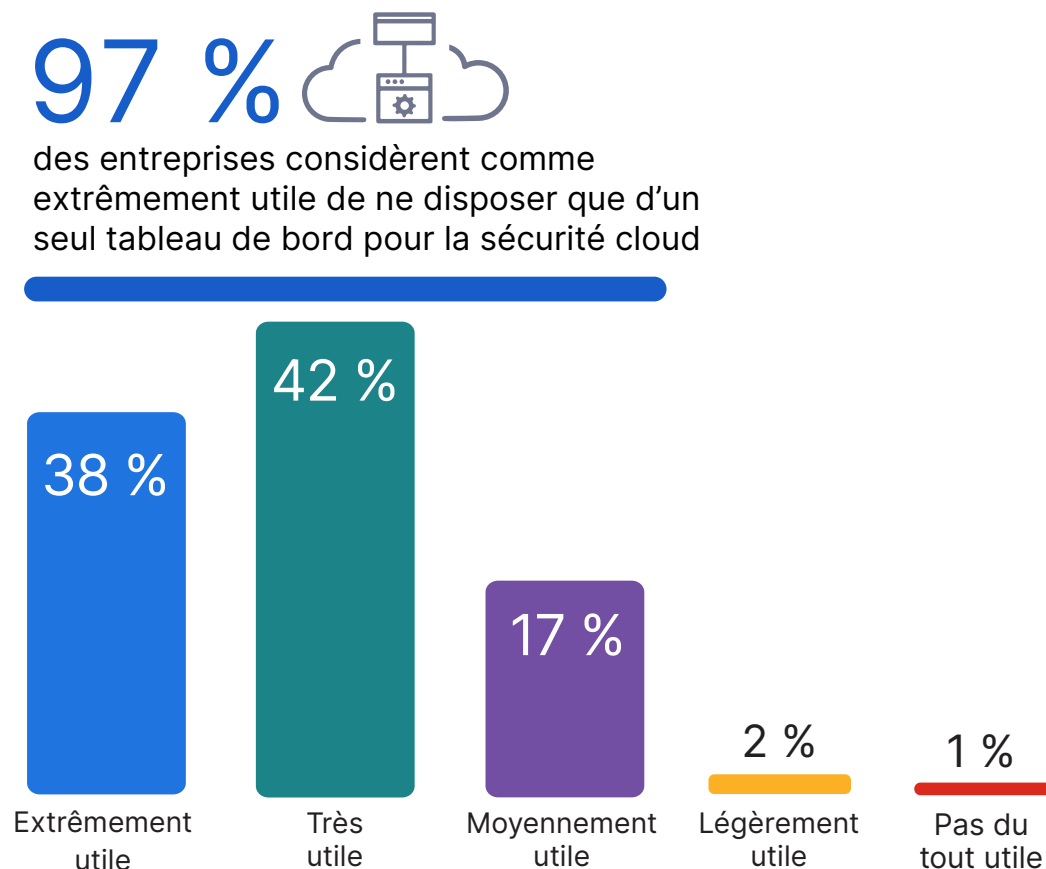


La valeur des plateformes unifiées de sécurité du cloud

L'intérêt d'une plateforme de sécurité unifiée, dotée d'un tableau de bord centralisé, est de simplifier la configuration des politiques, d'en garantir la cohérence et d'améliorer la visibilité sur l'ensemble de l'empreinte cloud d'une entreprise.

Notre enquête montre un intérêt massif pour ce concept, 97 % des personnes interrogées jugeant une telle plateforme modérément à extrêmement utile. Par exemple, un tableau de bord unique pourrait permettre à un acteur des services financiers d'appliquer des contrôles d'accès uniformes sur AWS, Azure et Google Cloud, réduisant ainsi la probabilité d'erreurs de configuration. Cet exemple est en phase avec les résultats précédents, quand 55 % des personnes interrogées citent l'absence de visibilité et de contrôle comme le principal défi des environnements multi-clouds et hybrides, soulignant la nécessité d'outils centralisés pour pallier ces lacunes.

- Quelle serait l'utilité d'une plateforme unifiée de sécurité cloud, avec un tableau de bord qui vous permettrait de configurer toutes les règles de protection des données de manière cohérente, sur l'ensemble de vos environnements cloud ?



Meilleures pratiques pour renforcer la sécurité hybride et multi-cloud

Les entreprises adoptent de plus en plus des environnements hybrides et multi-clouds, ce qui induit une gestion complexe de multiples fournisseurs et peut fragiliser la sécurité. Pour relever efficacement ces défis, il est essentiel de mettre en œuvre les meilleures pratiques stratégiques, celles en phase avec les perspectives du secteur et qui tirent parti de solutions de sécurité avancées.

Les recommandations suivantes proposent des mesures concrètes pour améliorer votre posture de sécurité du multi-cloud.

1

AUTOMATISER LA DÉTECTION ET LA REMÉDIATION DES RISQUES LIÉS AU CLOUD

Les erreurs de configuration constituent des vulnérabilités courantes, et 67 % des personnes interrogées utilisent ou prévoient d'adopter des outils automatisés pour traiter cette problématique. Les solutions de monitoring continu et de remédiation en temps réel peuvent identifier de manière proactive les risques, à l'instar d'un espace de stockage mal configuré ou d'autorisations excessives, et les corriger efficacement. Ces outils simplifient également la mise en conformité avec les réglementations en vigueur.

2

PROTÉGER LES FLUX DE DONNÉES DANS LES ENVIRONNEMENTS CLOUD

Lorsque les données circulent entre les environnements cloud, leur sécurité et leur intégrité doivent être assurées. Pour 58 % des personnes interrogées, la protection et la confidentialité des données est une préoccupation majeure. Les outils offrant une visibilité complète sur les flux de données aident les entreprises à protéger les données pendant leur transit. Ces outils surveillent les risques potentiels, empêchent les accès non autorisés et facilitent la conformité à des cadres réglementaires tels que le RGPD, améliorant ainsi les efforts de protection des données.

3

UNIFIER LES MÉCANISMES DE DÉTECTION DES MENACES

54 % des personnes interrogées font état de difficultés à détecter et à répondre aux menaces dans les environnements multi-clouds. Les solutions de détection unifiée des menaces proposent une visibilité centralisée, ce qui permet aux équipes d'identifier et de traiter rapidement les anomalies. Ces outils peuvent corréler les données entre les différents environnements cloud afin d'accélérer la détection des menaces et affiner la réponse à celles-ci.

4

DES FORMATIONS SPÉCIFIQUES AU CLOUD POUR LES ÉQUIPES DE SÉCURITÉ

La pénurie de compétences touche 76 % des entreprises, obérant leur capacité à déployer et à gérer efficacement des solutions cloud natives. La formation continue des collaborateurs dans des domaines tels que DevSecOps et la sécurité des conteneurs permet aux équipes de relever les nouveaux défis de sécurité.

5

FAVORISER LE POLICY-AS-CODE POUR UNE MISE EN ŒUVRE COHÉRENTE DE LA SÉCURITÉ

Puisque 43 % des personnes interrogées déclarent avoir des difficultés à comprendre comment les différentes solutions s'intègrent, l'utilisation d'approches de type policy-as-code garantit une application cohérente des règles de sécurité sur toutes les plateformes. L'approche policy-as-code simplifie les audits et permet une gestion automatisée de la configuration. Les fonctionnalités de sécurité sont ainsi en phase avec les exigences métier de l'entreprise.

6

ADAPTER LES INVESTISSEMENTS EN SÉCURITÉ AUX BESOINS DES INSTANCES APPLICATIVES

La sécurité des applications est une priorité, 62 % des personnes interrogées prévoyant d'adopter des plateformes de protection intégrale. La sécurité de bout en bout des applications, de leur phase de conception à leur mise en production, garantit une protection adaptée aux instances et assure la cohérence des politiques sur tous les environnements. Les solutions qui s'intègrent aux environnements de conteneurs et à la sécurité des environnements de production répondent efficacement à ce besoin.

7

NORMALISER LES CONTRÔLES D'ACCÈS POUR TOUS LES ENVIRONNEMENTS CLOUD

Le contrôle d'accès et la gestion des identités demeurent un défi majeur pour 59 % des entreprises, en particulier dans le cloud distribué. Les solutions de contrôle d'accès centralisé simplifient la gestion des privilèges des utilisateurs et appliquent des politiques de sécurité cohérentes au sein des environnements hybrides et multi-clouds. La mise en œuvre d'une plateforme unifiée de gestion des identités garantit une application transparente des politiques tout en minimisant le risque d'accès non autorisé.

8

OPTER POUR DES OUTILS DE SÉCURITÉ DANS LE CLOUD ET GAGNER EN ÉVOLUTIVITÉ

Avec 54 % du panel qui privilégie le cloud hybride en tant que modèle principal de déploiement, les outils de sécurité fournis depuis le cloud doivent faire preuve d'évolutivité. Ces solutions assurent un même niveau de protection pour les environnements, qu'ils soient sur site ou dans le cloud public, ce qui permet aux entreprises d'étendre leur empreinte cloud sans grever leur productivité opérationnelle.

Conclusion

Ce rapport souligne l'importance d'un investissement stratégique dans des outils unifiés, dans la formation et dans des processus adaptés aux exigences d'une sécurité du cloud hybride et du multi-cloud. En relevant nombre de défis (erreurs de configuration, pénurie de compétences et manque de visibilité), les entreprises peuvent assurer une posture de sécurité résiliente.

La mise en œuvre des meilleures pratiques fournies dans ce rapport permet aux entreprises de réussir dans des environnements cloud complexes, en protégeant leurs ressources critiques tout en favorisant leur agilité et leur conformité réglementaire. Des avantages essentiels à l'heure d'une transformation digitale rapide.

Glossaire de la sécurité du cloud

Ce glossaire livre un aperçu des technologies de sécurité du cloud présentées dans ce rapport, en mettant l'accent sur leur fonction, les problématiques de sécurité qu'elles traitent et la raison pour laquelle elles s'imposent pour protéger les environnements cloud complexes d'aujourd'hui.

Application Security Posture Management (ASPM) - L'ASPM (ou gestion de la posture de sécurité des applications) offre une visibilité sur les vulnérabilités applicatives et les problématiques de configuration tout au long du cycle de développement logiciel. Cette approche fait appel à des pratiques de codage sécurisé et intègre la sécurité dans les workflows DevSecOps. L'ASPM sécurise les applications, de leur conception à leur mise en production.

Cloud Detection and Response (CDR) - Le CDR est une technologie experte qui identifie et neutralise les menaces dans les environnements cloud. Elle offre une visibilité en temps réel sur les activités cloud, ce qui identifie rapidement les anomalies et permet de réagir rapidement aux incidents. Le CDR est la pièce maîtresse d'une ligne de défense robuste contre les menaces sophistiquées qui ciblent les environnements cloud distribués.

Cloud Infrastructure Entitlement Management (CIEM) - Le CIEM s'intéresse à la gestion des autorisations et du contrôle d'accès dans les environnements cloud. Cette technologie identifie les autorisations excessives, applique le principe du moindre privilège et réduit le risque d'abus de privilèges. Le CIEM contribue à des politiques d'accès sûres et conformes au sein des architectures multi-clouds.

Cloud Native Application Protection Platform (CNAPP) - Une plateforme de protection des applications cloud-natives fédère plusieurs fonctionnalités de sécurité pour protéger ces applications tout au long de leur cycle de vie. Elle associe une protection des instances, une gestion de la configuration et une protection des applications en production, pour ainsi sécuriser les conteneurs, les fonctions serverless et d'autres instances cloud-natives. Le CNAPP est essentiel pour les entreprises qui font appel à des pratiques de développement modernes telles que DevOps et les microservices.

Cloud Security Posture Management (CSPM) - Le CSPM vise à automatiser la détection des erreurs de configuration au sein des environnements cloud. L'infrastructure cloud est surveillée en permanence pour détecter les risques de sécurité (buckets de stockage exposés, contrôles d'accès laxistes...), garantissant ainsi la conformité réglementaire. Le CSPM est essentiel à une visibilité étendue et à la prise en charge des vulnérabilités dans les environnements multi-clouds et hybrides.

Cloud Workload Protection Platform (CWPP) - Le CWPP sécurise les instances présentes dans les environnements cloud, y compris les machines virtuelles, les conteneurs et les architectures serverless. Cette technologie offre une visibilité sur les vulnérabilités, assure la cohérence des politiques de sécurité et protège les instances contre les menaces avancées. Cette plateforme s'impose pour les entreprises qui gèrent des instances déployées au sein de différents clouds.

Data Security Posture Management (DSPM) - Cette technologie orientée données répertorie, classifie et sécurise les informations sensibles dans les environnements cloud. Elle garantit que les données sont correctement protégées et répond aux exigences réglementaires en matière de protection et de confidentialité, comme ceux du RGPD. Le DSPM s'impose pour protéger les informations sensibles dans les écosystèmes complexes du cloud.

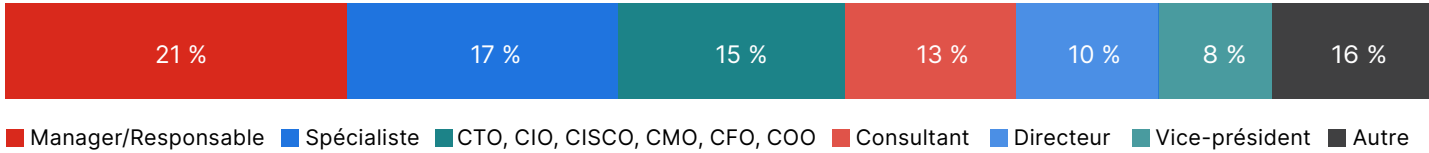
Méthodologie et données démographiques

Le rapport 2025 sur la sécurité du cloud est basé sur une enquête menée fin 2024, pour recueillir l'opinion et les perspectives de 873 professionnels de l'informatique et de la cybersécurité, issus de différents pays et évoluant dans différents secteurs d'activité (technologies, services financiers, soins de santé et administrations). Les personnes interrogées sont représentatives d'organisations de tailles différentes, de petites entreprises aux multinationales. Ces professionnels occupent des postes allant de spécialiste à cadre dirigeant.

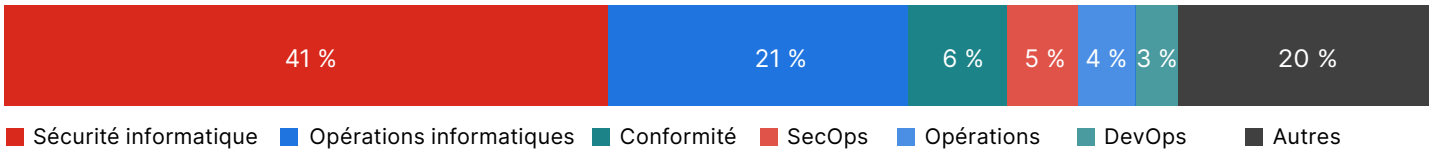
L'enquête, réalisée en ligne, s'est penchée sur les tendances, défis et priorités en matière de sécurité cloud. Les résultats fournissent une perspective d'ensemble de la façon dont les entreprises gèrent la complexité des environnements cloud et des technologies de sécurité nécessaire pour contrer les menaces émergentes.

Pour les questions qui permettent aux répondants de choisir plusieurs réponses, le cumul des résultats peut être supérieur à 100 %.

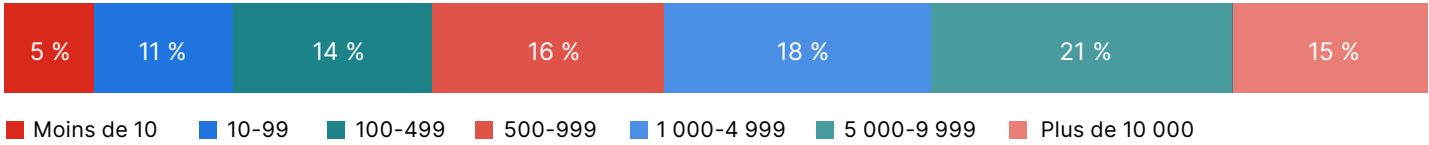
NIVEAU FONCTIONNEL



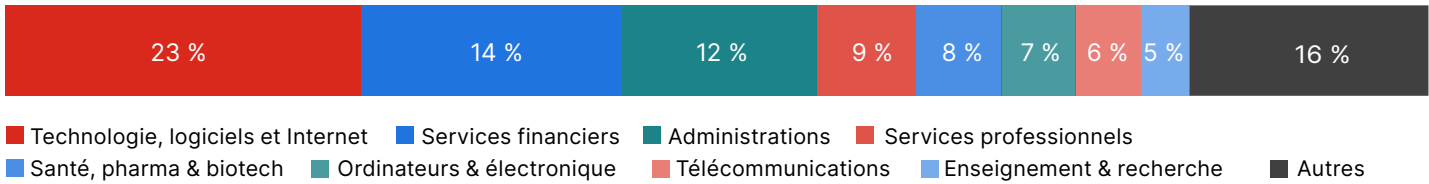
SERVICE



EFFECTIF DE L'ENTREPRISE



SECTEUR D'ACTIVITÉ



Réutilisation du contenu

Nous encourageons la réutilisation des données, des graphiques et des textes de ce rapport selon les termes de cette [Licence internationale Creative Commons Attribution 4.0](#). Vous êtes libre de partager et d'utiliser ce travail à des fins commerciales, à condition de citer le rapport comme stipulé dans les termes de la licence. Exemple : « État des lieux 2025 de la sécurité du cloud par Cybersecurity Insiders et Fortinet »



Fortinet (NASDAQ : FTNT) assure la sécurité des entreprises, fournisseurs de services et administrations parmi les plus importantes au monde. Fortinet offre à ses clients une visibilité et un contrôle complets sur leur surface d'attaque en expansion, et la possibilité de répondre à des exigences de performances toujours plus élevées, aujourd'hui comme demain. La plateforme Fortinet Security Fabric peut relever les défis de sécurité les plus critiques et protéger les données sur l'ensemble de l'infrastructure, que ce soit dans des environnements réseau, applicatifs, multi-clouds ou edge. Fortinet se classe au premier rang des appliances de sécurité commercialisées dans le monde. Plus de 800 000 clients font confiance à Fortinet pour protéger leurs activités.

[**www.fortinet.com/fr**](http://www.fortinet.com/fr)

Cybersecurity

I N S I D E R S

Cybersecurity Insiders fédère plus de 600 000 professionnels de la sécurité informatique et des fournisseurs de technologies de premier plan afin de favoriser une résolution intelligente des problématiques et la collaboration, et ainsi relever les défis actuels les plus critiques en matière de cybersécurité.

Notre approche privilégie la création de contenus pertinents qui informent et sensibilisent les professionnels sur les nouvelles tendances de la cybersécurité, les solutions et les meilleures pratiques. Qu'il s'agisse d'études approfondies, d'évaluations impartiales de produits, de guides pratiques, de webinaires pertinents ou d'articles de sensibilisation, nous nous engageons à fournir des ressources qui apportent des réponses éprouvées aux défis complexes de la cybersécurité d'aujourd'hui.

Contactez-nous dès aujourd'hui pour découvrir comment Cybersecurity Insiders peut vous aider à vous démarquer sur un marché concurrentiel, pour encourager la demande, la visibilité de votre marque et votre statut de leader d'opinion.

Envoyez-nous un courriel sur info@cybersecurity-insiders.com ou visitez cybersecurity-insiders.com