

2024

Sécurité du cloud : Rapport



FORTINET®

Introduction

La stratégie cloud-first a le vent en poupe. C'est un fait. Les entreprises tendent de plus en plus à développer et à déployer des applications pensées pour le cloud. C'est ainsi que la majorité d'entre elles recourent à une approche hybride ou multicloud pour répondre à différents cas d'usage et modèles de travail. Résultat : la surface d'attaque s'est considérablement élargie, tandis que la sécurisation des environnements cloud est devenue à la fois plus essentielle et plus complexe que jamais.

Fruit d'une étude mondiale menée auprès de 927 professionnels de la cybersécurité, notre rapport 2024 sur la sécurité du cloud vous livre un éclairage sur les grandes tendances actuelles. Au sommaire : les principaux défis que pose la protection de ces environnements dématérialisés d'une grande complexité, les solutions et stratégies prioritaires des professionnels de la cybersécurité, leurs choix budgétaires et leurs bonnes pratiques de sécurité des workloads cloud.

Principales conclusions :

- **Préférence pour le multicloud** – Les entreprises misent majoritairement (78 %) sur des stratégies hybrides et multicloud pour conjuguer flexibilité, contrôle et avantages propres à chacun des fournisseurs.
- **Obstacles à l'adoption du cloud** – En tête, les problèmes de sécurité et de conformité du cloud (59 %) freinent considérablement la mise en œuvre de stratégies multicloud. Puis viennent les problématiques techniques (52 %) et le manque de ressources (49 %), deux facteurs qui limitent la visibilité et le contrôle des politiques au sein des infrastructures multicloud et accentuent la nécessité d'une expertise solide en sécurité du cloud.
- **Pénurie de compétences en cybersécurité** – Les entreprises se heurtent à un manque criant d'expertise en cybersécurité. Pour preuve, 93 % des sondés s'inquiètent de ne pas trouver des professionnels qualifiés pour protéger leurs environnements multicloud complexes. Or cette incapacité à recruter met à mal leur posture de sécurité et leurs efforts stratégiques. De plus, ce déficit chronique de compétences en sécurité du cloud entrave à la fois la portée et le rythme d'adoption du multicloud.
- **Préférence pour une plateforme de sécurité cloud unifiée** – 95 % des répondants plaident en faveur d'une plateforme unique pour rationaliser la sécurité sur l'ensemble des environnements cloud et en finir avec la gestion de systèmes disparates qui impactent leur efficacité. Le but : simplifier et automatiser la gestion de la sécurité, pallier la pénurie de talents et renforcer la sécurité grâce à une meilleure visibilité et à des politiques homogènes.

Nous tenons à remercier [Fortinet](#) pour son précieux soutien à cette vaste étude sectorielle. Nous espérons que ce rapport apportera aux professionnels de la cybersécurité – managers et exécutants – une grille de lecture essentielle pour renforcer la sécurité de leur transformation digitale en général, et de leurs environnements cloud en particulier, face à une menace en perpétuelle mutation.

Cordialement,

Holger Schulze

Fondateur, Cybersecurity Insiders

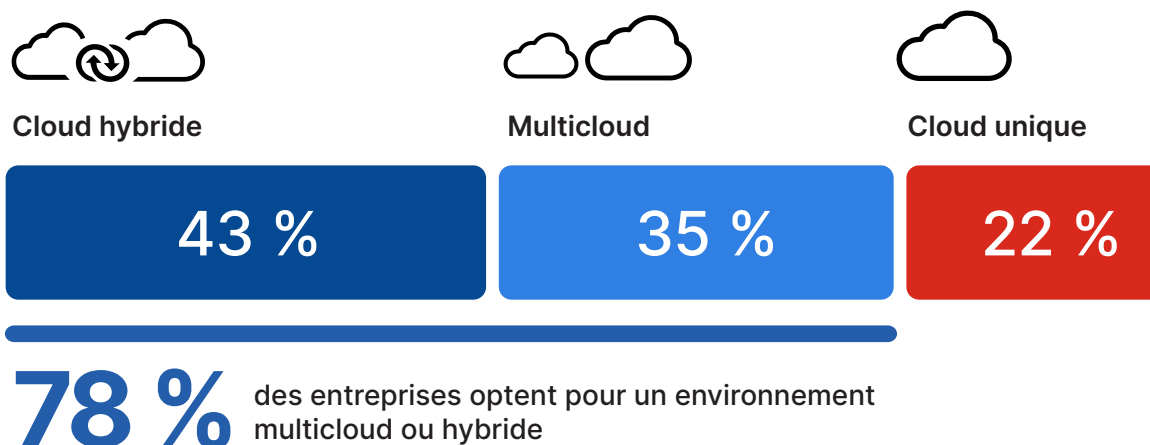
Cybersecurity
INSIDERS

Méthodes de déploiement cloud

Les entreprises ont intérêt à bien choisir leur stratégie de déploiement cloud pour maximiser les avantages du cloud computing tout en minimisant les risques associés.

Dans notre étude, la majorité d'entre elles (78 %) privilégient une stratégie hybride ou multicloud consistant à intégrer de multiples déploiements au sein d'un environnement opérationnel unique, avec une grande partie (43 %) recourant à une infrastructure hybride conjuguant cloud et on-prem. Elles sont 35 % à avoir opté pour le multicloud, préférant ainsi exploiter les atouts de différents fournisseurs de services cloud (CSP) en fonction des cas d'usage. Notons que seulement 22 % d'entreprises font appel à un CSP unique, dénotant une volonté manifeste de simplicité qui peut néanmoins accroître la dépendance envers le fournisseur.

► Quelle stratégie de déploiement cloud votre entreprise privilégie-t-elle ?



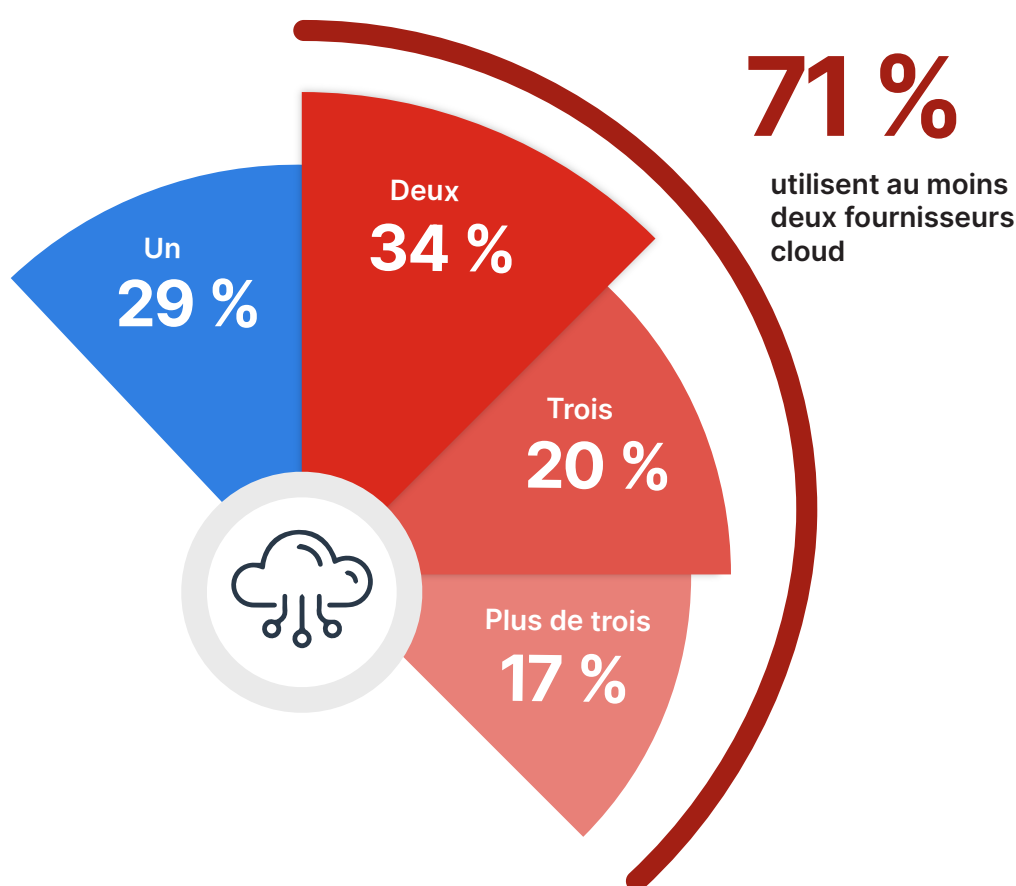
Face aux complexités des déploiements hybrides et multicloud, les organisations devraient prioriser un cadre de sécurité intégré, garant d'une protection fluide et transparente de tout leur écosystème digital. Seule cette intégration leur apportera l'agilité, l'évolutivité et la sécurité indispensables à une défense solide face aux menaces en perpétuelle évolution.

Adoption multicloud

Le nombre de fournisseurs cloud utilisés par une entreprise influe directement sur sa flexibilité opérationnelle, sa gestion des risques et la complexité de sa sécurité. Parmi les structures sondées, une très grande majorité (71 %) fait appel à au moins deux CSP, indiquant vouloir conjuguer flexibilité, contrôle et avantages propres à chaque fournisseur. Cette augmentation de deux points de pourcentage par rapport à l'étude 2023 révèle une tendance de fond vers des stratégies multicloud, elles-mêmes impulsées par un besoin de redondance, de disponibilité régionale et de services cloud spécialisés.

Fait notable, seulement 29 % des organisations dépendent d'un fournisseur cloud unique, soulignant une réelle volonté de simplicité s'inscrivant potentiellement dans le cadre d'un accord stratégique avec un CSP partenaire.

► Combien de fournisseurs cloud utilisez-vous actuellement ?



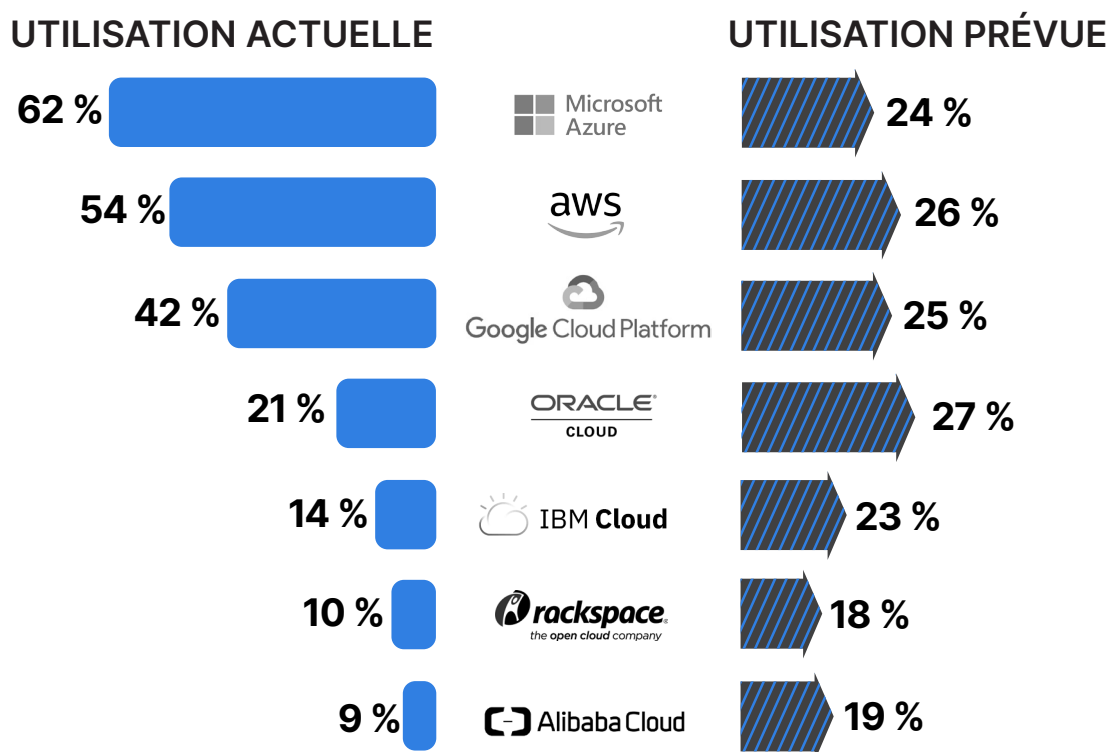
Pour sécuriser de multiples environnements cloud, nous recommandons aux entreprises une approche transparente et agnostique, garante de l'homogénéité des politiques de sécurité et d'une visibilité sur l'ensemble de leur écosystème digital. Elles parviendront ainsi à réduire la complexité tout en renforçant leurs mécanismes de défense face à des menaces toujours plus sophistiquées.

Classement des fournisseurs cloud

Pour mieux cerner l'évolution du marché du cloud, nous avons interrogé notre échantillon de professionnels de la cybersécurité sur leurs choix actuels et futurs de fournisseurs cloud. Microsoft Azure, dont 62 % de nos répondants utilisent les services, continue de dominer le marché, suivi par Amazon Web Services (AWS) avec 54 % de clients parmi nos sondés. Les entreprises tendent donc à privilégier les géants du secteur.

Toutefois, elles montrent aussi un intérêt notable pour d'autres acteurs de marché, en particulier Oracle Cloud et Google Cloud Platform qui recueillent respectivement 27 % et 25 % d'intentions de déploiement à terme. Autant dire que l'adoption du cloud tend à se diversifier de plus en plus.

► À quels fournisseurs IaaS faites-vous appel actuellement et lesquels pensez-vous utiliser à l'avenir ? (plusieurs choix possibles)



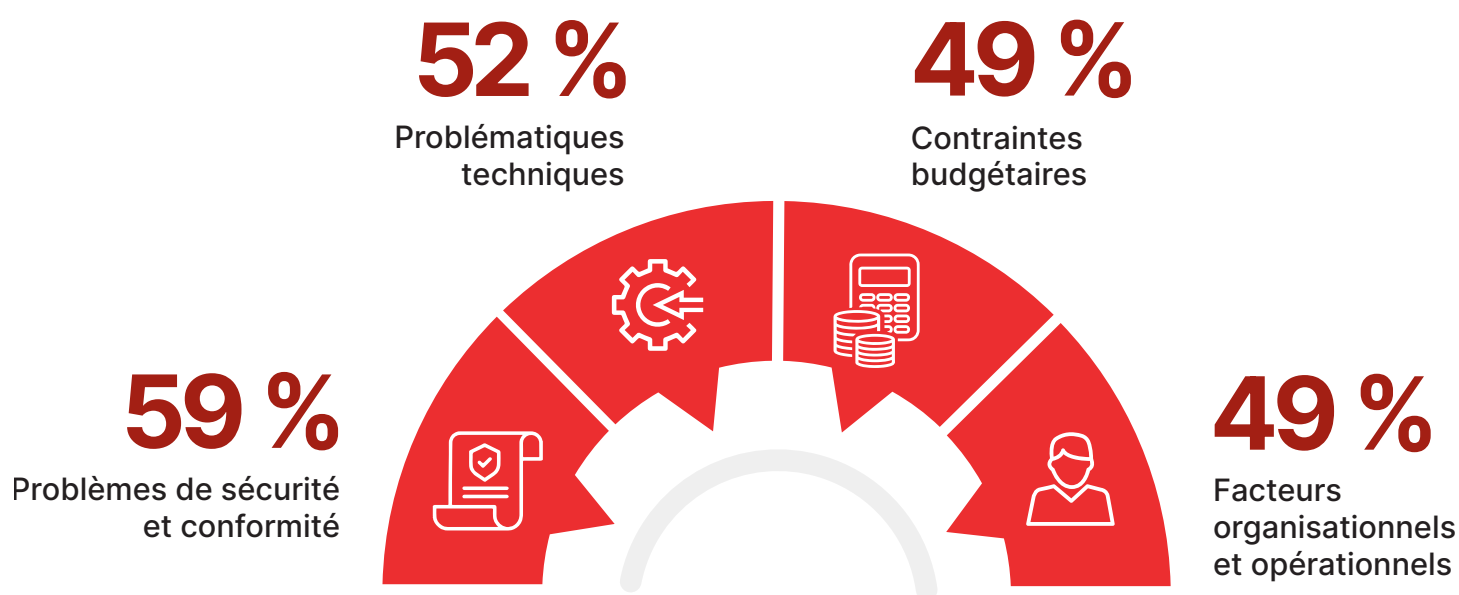
Surmonter les obstacles à l'adoption du cloud

Pour mieux appréhender les difficultés d'une migration vers des solutions cloud, les entreprises doivent d'abord comprendre les principaux freins à une adoption plus rapide et plus entière.

Parmi eux, les problèmes de sécurité et de conformité arrivent en tête selon 59 % des sondés. D'où la nécessité pour les entreprises d'intégrer cet enjeu au cœur même de leur stratégie d'adoption du cloud. Suivent les problématiques techniques (52 %) qui rappellent que la migration vers le cloud est loin d'être une formalité.

Le manque de ressources, notamment le déficit de compétences et les contraintes budgétaires, est cité par 49 % des répondants. Ce chiffre souligne à quel point les initiatives cloud demandent un investissement financier et humain conséquent. Au même niveau (49 %), les obstacles organisationnels et opérationnels montrent que le cloud computing ne se réduit pas à une simple technologie. C'est aussi un nouveau modèle opérationnel qui ouvre la voie à des méthodes de travail innovantes, et à ce titre requiert l'adhésion de la direction pour surmonter les potentielles résistances au changement.

► Quels sont les principaux obstacles à l'adoption du cloud au sein de votre entreprise ? (plusieurs choix possibles)



Autres réponses :

Inquiétudes à l'égard des services cloud 28 % | Problèmes juridiques liés au fournisseur 27 %

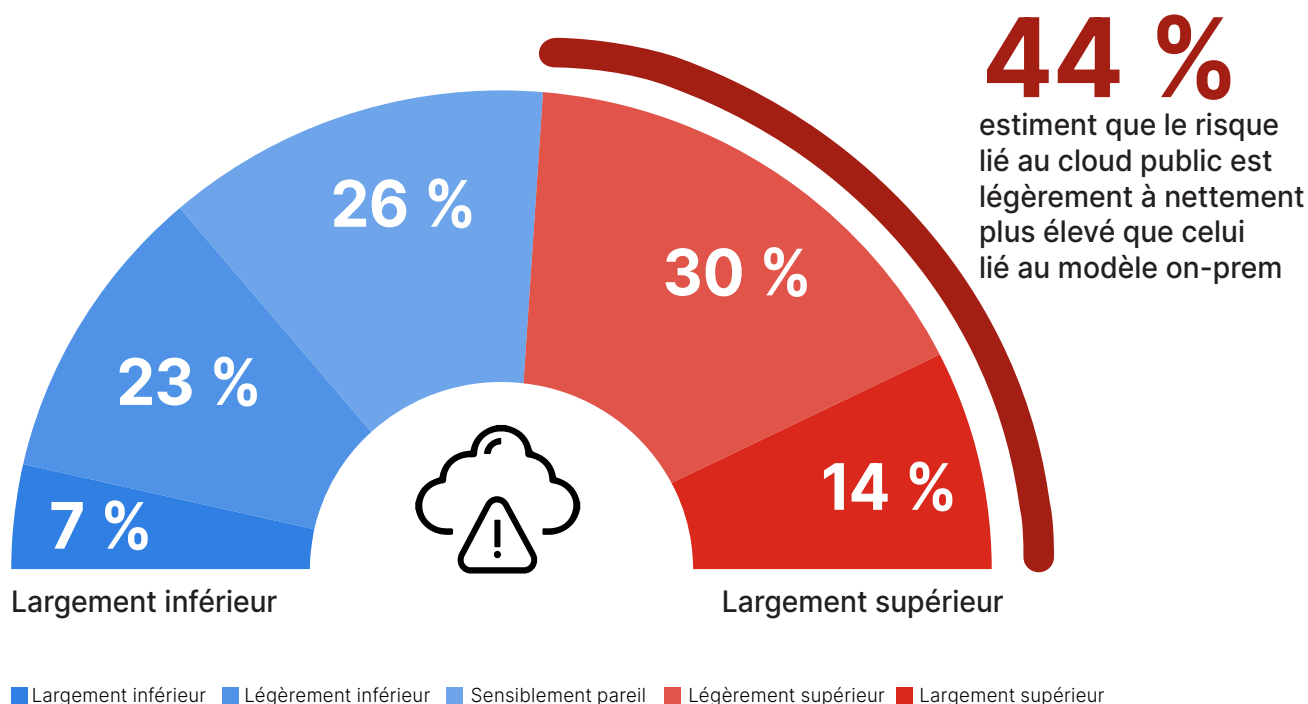
Perception des risques de sécurité du cloud

L'évaluation des risques de compromission de sécurité dans le cloud public a mis au jour une inquiétude palpable face aux dangers et aux défis de sécurité inhérents à ces environnements.

Ainsi, ils sont en tout 44 % de sondés à considérer que dans le cloud public, le risque d'incident est supérieur à celui des environnements on-prem traditionnels. Parmi eux, 30 % l'estiment légèrement supérieur et 14 % nettement supérieur.

À l'inverse, 30 % des personnes interrogées jugent le risque de compromission inférieur dans le cloud public, marquant ainsi leur confiance dans les mesures de sécurité et les progrès réalisés par les fournisseurs cloud dans ce domaine. Une proportion non négligeable de répondants pensent que les risques sont identiques, sous-entendant que malgré les nouvelles dynamiques engendrées par le cloud, les grands défis de sécurité demeurent les mêmes indépendamment du type d'environnement.

► Selon vous, le risque de compromission de sécurité est-il plus élevé ou plus faible dans le cloud public que dans les environnements on-prem traditionnels ?



Le cloud public offre aux entreprises la possibilité d'adopter une approche plus proactive et automatisée de la sécurité. En s'inscrivant dans cette démarche de « security-by-design », elles réduisent les risques tout en capitalisant sur les trois grands atouts du cloud : l'évolutivité, la flexibilité et l'innovation.


Problématiques de sécurité du cloud

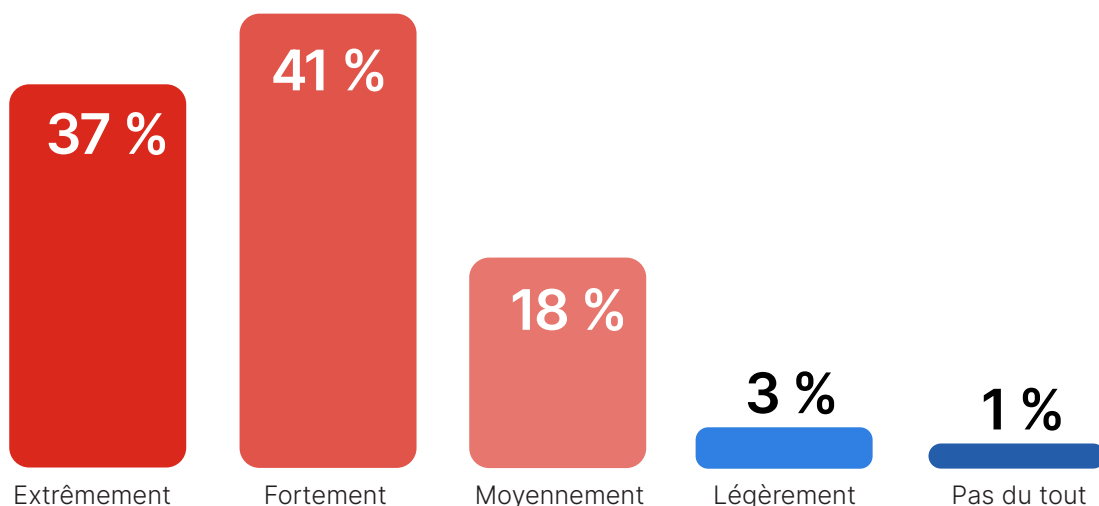
Le degré d'inquiétude que suscite la sécurité du cloud public est emblématique d'un sentiment répandu chez les professionnels de la cybersécurité, mais aussi d'une volonté affirmée de se confronter aux risques et aux dangers potentiels.

Malgré une adoption croissante du cloud, les craintes quant à sa sécurité restent très prégnantes dans les entreprises. La quasi-totalité des sondés se disent ainsi moyennement à extrêmement préoccupés par leur posture de sécurité dans le cloud public (96 %). Parmi eux, ils sont 37 % à être extrêmement préoccupés, et 41 % fortement préoccupés. Ce degré élevé d'inquiétude, qui reste peu ou prou le même au fil des ans, soulève des réticences face aux risques perçus et à la difficulté à sécuriser les environnements cloud, freinant de fait son adoption. Seule une petite proportion (22 %) d'entreprises se disent moyennement à pas du tout préoccupées, signe révélateur d'un large consensus autour de l'importance de mesures de sécurité robustes dans le cloud public.

Ces chiffres corroborent la statistique évoquée plus haut, indiquant que 44 % des répondants considèrent le risque d'incident plus élevé dans le cloud public que dans les environnements on-prem. En dépit des nombreux atouts du cloud, la sécurité reste donc au centre des préoccupations.

► À quel point la sécurité du cloud public vous préoccupe-t-elle ?

 **96 %**
des entreprises se disent modérément à
extrêmement préoccupées par la sécurité du cloud



Pour apaiser les inquiétudes, les entreprises doivent certes poursuivre leur approche de « security-by-design », mais également investir dans une surveillance continue, une Threat Intelligence et des capacités de réponse à incident spécifiques aux environnements dématérialisés. Par ailleurs, la sécurité et la résilience des infrastructures cloud passent par des solutions de pointe et une collaboration étroite avec les CSP.

Problématiques SecOps du cloud

Pour les entreprises, la gestion courante des opérations de sécurité du cloud constitue un défi complexe où s'entremêle une variété de facteurs technologiques, réglementaires et humains. La question de la confidentialité et de la sécurité des données arrive en tête. Ils sont en effet 58 % de répondants à souligner la nécessité de protéger les informations sensibles et de prévenir les fuites de données dans le cloud. D'où l'importance d'une solide gouvernance des données et de pratiques de chiffrement robustes. La gestion des configurations suit de près, avec 55 % des réponses. Cette deuxième place souligne la complexité et les risques associés aux configurations. Une seule erreur suffit pour exposer les entreprises à de graves dangers.

Autre défi de taille pour 54 % des sondés, la gestion des identités et des accès (IAM), qui met en avant le besoin de contrôler rigoureusement les utilisateurs et leurs privilèges pour empêcher tout accès non autorisé. Les problématiques de détection et réponse aux menaces (50 %) et de sécurité des terminaux (45 %) illustrent bien la double difficulté actuelle des professionnels à identifier et neutraliser les menaces en temps réel d'une part, et à sécuriser la myriade d'appareils accédant aux services cloud, d'autre part. Également citées, la gestion des politiques et de la conformité (45 %) et la gestion de la sécurité du cloud révèlent à quel point les entreprises peinent à mettre en place des politiques de sécurité homogènes dans tous les environnements et à aligner les fonctions de sécurité cloud sur les solutions de sécurité on-prem.

► Quelles sont les principales problématiques auxquelles vous vous heurtez dans la gestion courante des opérations de sécurité du cloud ? (plusieurs choix possibles)



Face à ce casse-tête SecOps, une stratégie de sécurité unifiée reposant sur l'automatisation, des analyses avancées et des plateformes intégrées s'impose comme une priorité. Objectif : simplifier la sécurité des données, l'application des politiques, la gestion des accès, la détection des menaces et la réponse. En parallèle, le développement des compétences de sécurité cloud-native des équipes et l'instauration d'une culture de sensibilisation à la sécurité ne peuvent que renforcer l'efficacité de la gestion des opérations de sécurité du cloud.

Autres réponses :

Shadow IT et utilisation d'applications non autorisées 36 % | Intégration cloud et automatisation 35 % | Agilité opérationnelle et complexité 32 % | Allocation des ressources 30 % | Pratiques DevSecOps 28 %

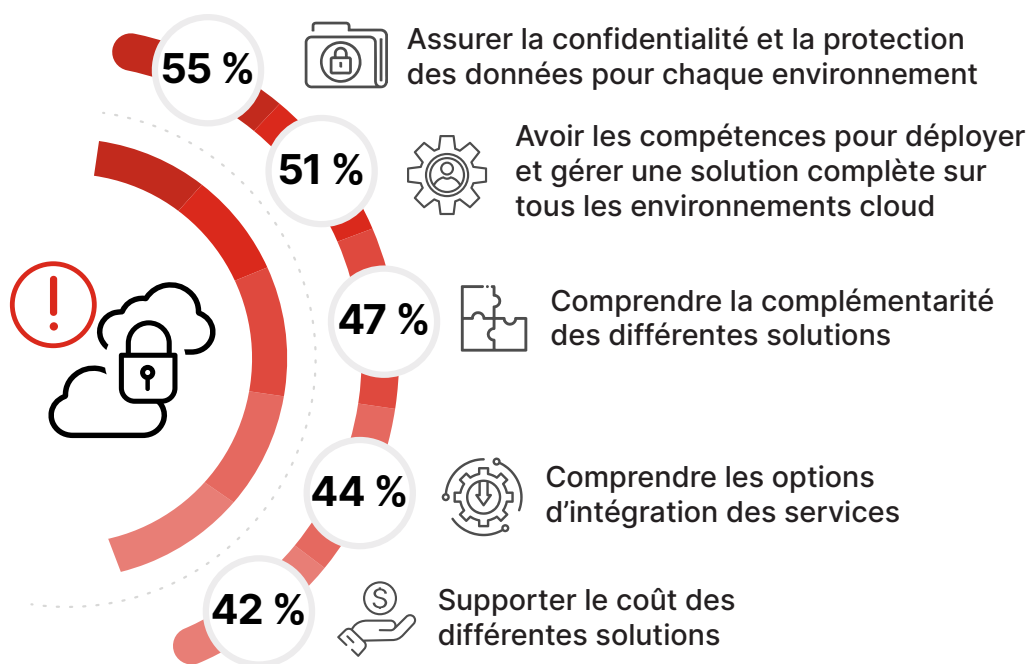
Défis de sécurité multicloud

Les environnements multicloud augmentent fortement la complexité et la difficulté à sécuriser les workloads cloud. Pour 55 % des professionnels interrogés, garantir la protection et la confidentialité des données dans chaque environnement constitue le challenge n° 1 de la sécurité multicloud. Cette préoccupation fait écho à la question précédente concernant les problèmes opérationnels associés à la sécurité et à la confidentialité des données. Une équation d'autant plus difficile à résoudre que les données sont éparpillées sur une multitude d'environnements cloud.

Deuxième défi aux yeux de 51 % des répondants, la pénurie de compétences pour déployer et gérer des solutions de sécurité transverses à l'ensemble des environnements cloud. Cette inquiétude rejoint un besoin que nous évoquions précédemment, à savoir celui d'une expertise en sécurité cloud-native pour faire face aux diverses facettes de la sécurité du cloud. Comprendre la complémentarité des différentes solutions, d'une part, et les options d'intégration des services, d'autre part, pose problème à respectivement 47 % et 44 % des sondés.

Dans les deux cas, ces réponses mettent en avant le parcours du combattant pour parvenir à une intégration fluide et à une interopérabilité entre des environnements cloud très variés. Or ces deux ressorts sont essentiels à une sécurité et une efficacité opérationnelle robustes. Enfin, le coût des différentes solutions préoccupe 42 % des personnes interrogées et souligne une fois de plus le difficile équilibre financier et opérationnel qu'exige une stratégie multicloud.

► Quels sont les plus grands problèmes que vous rencontrez pour sécuriser vos environnements multicloud ? (plusieurs choix possibles)



Face à ces enjeux, les entreprises devraient miser sur des solutions de sécurité intégrées. En offrant visibilité et contrôle sur tous les environnements multicloud, celles-ci favorisent l'uniformité de la protection des données et du respect des standards de confidentialité. Parmi les autres pistes à explorer pour surmonter la complexité des architectures multicloud, on citera également une collaboration étroite avec des fournisseurs proposant un éventail complet de capacités de sécurité multicloud et le développement de compétences internes. En plus de lever les problématiques révélées par les répondants, une telle approche libère tout le potentiel d'agilité, d'évolutivité et d'innovation de ces environnements multicloud.

Autres réponses :

Fluidité des accès utilisateurs par saisie des identifiants 38 % | Perte de visibilité et de contrôle 37 % | Sélection de services adaptés 36 %
| Difficulté à suivre le rythme du changement 33 %

Pénurie de talents en cybersécurité

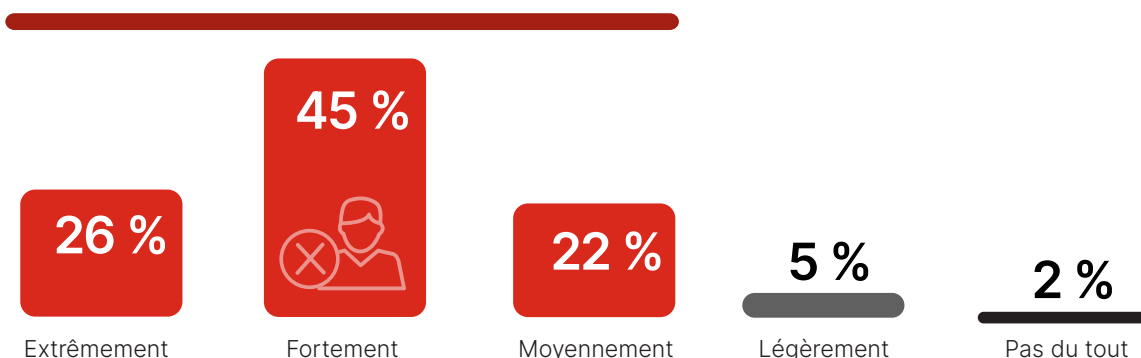
Le déficit chronique de professionnels qualifiés, capables de protéger des environnements multicloud complexes, constitue un problème majeur et persistant pour les entreprises.

Pour preuve, une très grande majorité des sondés (93 %) se disent préoccupés par le manque de compétences en cybersécurité qui sévit dans tout le secteur. Cette profonde inquiétude montre qu'ils sont parfaitement conscients du fossé qui ne cesse de se creuser entre le besoin croissant en compétences et le vivier actuel de talents disponibles. Or cette pénurie ne fait qu'aggraver les vulnérabilités et les difficultés opérationnelles dans un paysage cyber de plus en plus complexe.

► Dans quelle mesure le déficit actuel de compétences en cybersécurité vous préoccupe-t-il ?

93 %

des entreprises se disent modérément à extrêmement préoccupées par le déficit actuel de compétences en cybersécurité



Parmi les personnes interrogées, près des trois quarts (74 %) confirment être concernées par cette pénurie de talents en cybersécurité. Un chiffre qui illustre à quel point ce déficit de compétences impacte les opérations courantes de sécurité et les initiatives stratégiques des entreprises.

► Votre entreprise fait-elle face à une pénurie de talents en cybersécurité ?



Pour en réduire l'impact, les entreprises devraient actionner différents leviers. Parmi eux : la création de partenariats avec des établissements d'enseignement supérieur pour attirer de nouveaux talents, et l'investissement dans la formation continue pour favoriser l'éclosion de potentiels en interne et ainsi s'adapter à l'évolution constante des besoins en matière de sécurité du cloud. En parallèle, le remplacement des produits spécialisés par des solutions de sécurité unifiées et pilotées par l'IA permettrait de réduire la complexité opérationnelle et de pallier le déficit de compétences. Avec en prime, un net renforcement de la détection des menaces, des capacités de réponse et de la posture de sécurité générale.

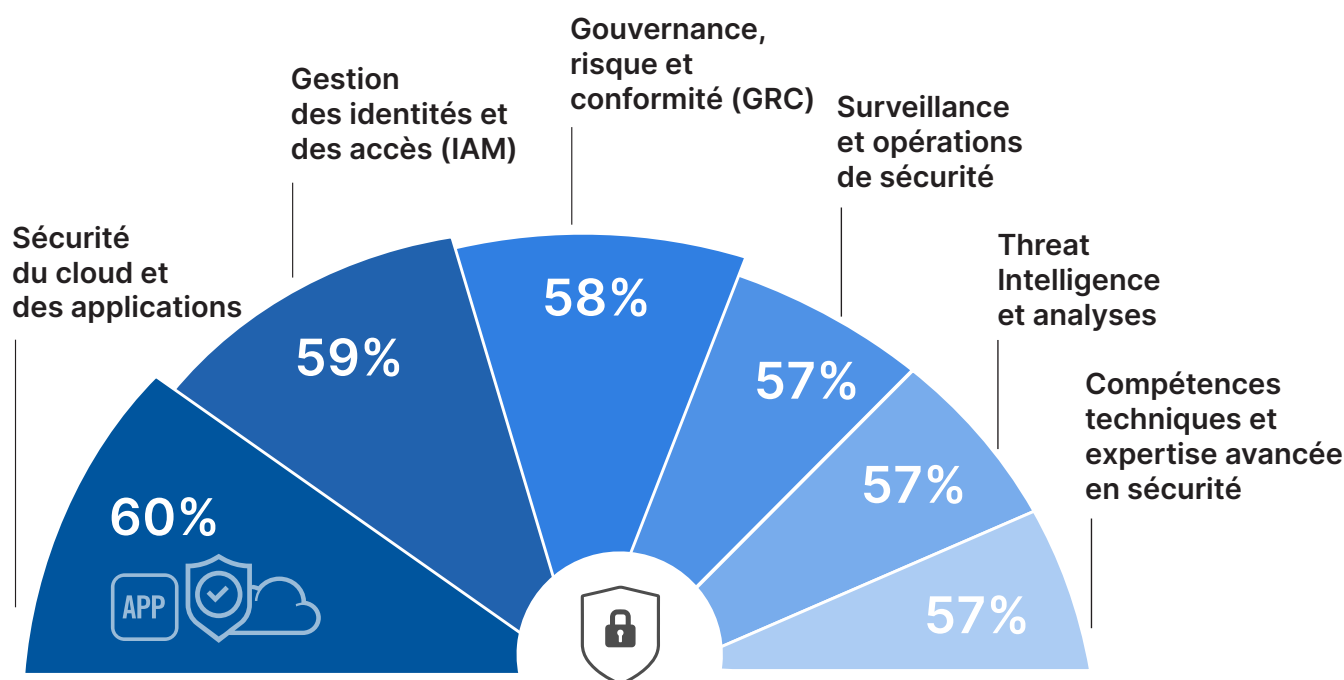
Compétences critiques en cybersécurité

Dans un contexte où les talents en cybersécurité se font rares, nous avons demandé aux répondants d'énumérer les domaines de compétence qu'ils estiment indispensables pour surmonter leurs défis actuels de sécurité.

En ordre d'importance, 60 % des répondants citent la sécurité du cloud et des applications. Ce large consensus met en relief la prépondérance croissante des services cloud et souligne la nécessité de pratiques de sécurité robustes dans les pipelines DevOps. La gestion des identités et des accès (IAM) arrive juste derrière à 59 %, à l'heure où les accès utilisateurs deviennent toujours plus difficiles à sécuriser dans des environnements IT de plus en plus distribués.

Les sondés sont 58 % à juger importantes les compétences en matière de gouvernance, risque et conformité (GRC), soulignant par là même le rôle incontournable de la conformité réglementaire et des cadres de gouvernance des risques dans le champ actuel des menaces. Arrivent ensuite à égalité, avec 57 % des réponses, la surveillance et les opérations de sécurité, la Threat Intelligence, et les compétences techniques avancées en sécurité. Par ces réponses, les professionnels démontrent un même intérêt pour une détection proactive des menaces, une connaissance pointue des cyberattaquants et le recours à des technologies de pointe pour renforcer leur posture de sécurité.

- Quelles compétences en sécurité comptent le plus dans votre entreprise ? (plusieurs choix possibles)



Autres réponses :

Réponse à incident et analyses forensiques 55 % | Communication et stratégie 39 % | Formation et sensibilisation 38 %

Budget de sécurité cloud : les tendances

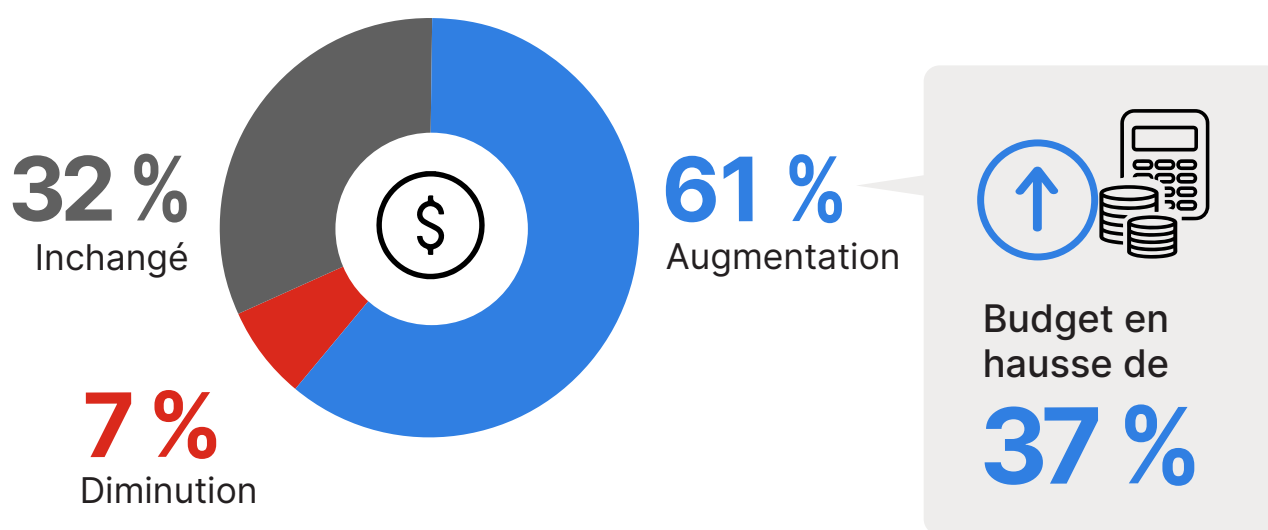
Les ressources allouées à la sécurité du cloud constituent un indicateur clé des priorités de l'entreprise, mais aussi de l'importance perçue de la protection de l'infrastructure cloud dans un contexte d'évolution des cybermenaces et d'innovation technologique.

Sur ce point, 61 % des professionnels interrogés anticipent une augmentation de leur budget dédié à la sécurité du cloud dans les douze prochains mois. Cette forte majorité indique une réelle prise de conscience de l'accentuation des problématiques de cybersécurité, en même temps qu'un besoin de renforcement des mesures de sécurisation des environnements cloud. Les sondés tablent ainsi sur un bond de 37 % en moyenne de leurs budgets de sécurité.

En consentant une telle augmentation des investissements, les entreprises indiquent qu'elles ont compris que, dans le nouveau monde du cloud, la protection des données sensibles et le respect des réglementations passent désormais par des mécanismes de défense renforcés.

Notons que dans un tiers des organisations sondées (32 %), les fonds alloués à la sécurité du cloud devraient rester inchangés. Seule une petite fraction (7 %) prévoit de revoir son budget à la baisse.

► Comment va évoluer votre budget de sécurité cloud au cours des 12 prochains mois ?

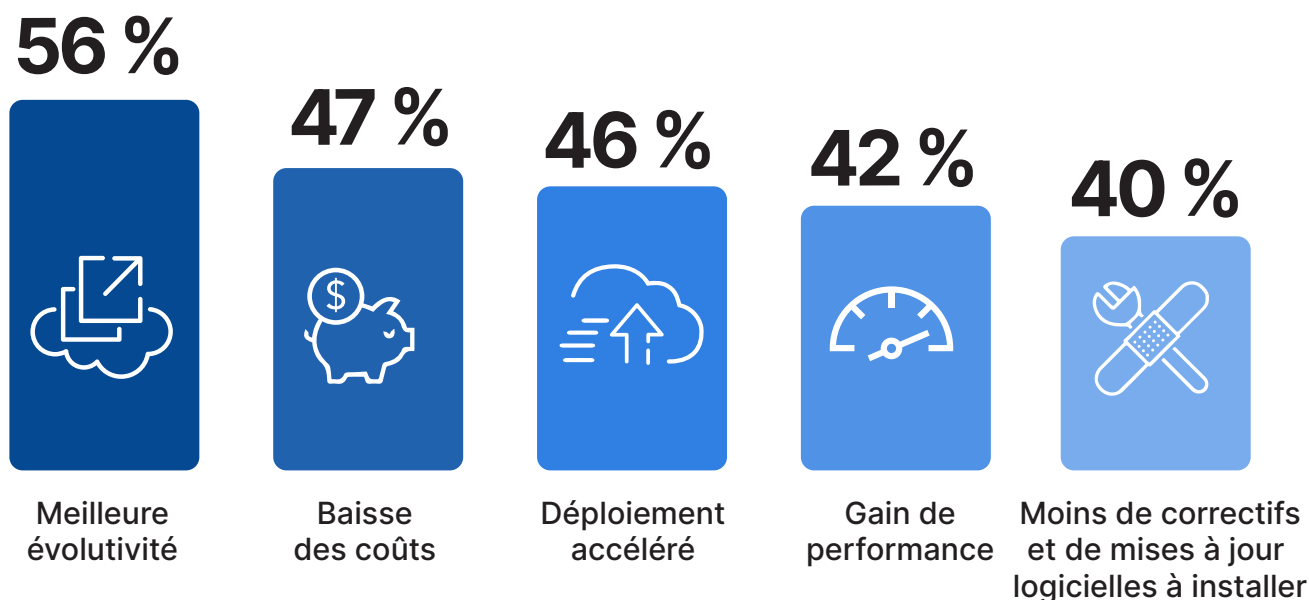


Au vu de la tendance haussière des investissements dans la sécurité du cloud, les entreprises devraient allouer ces nouvelles lignes budgétaires aux domaines les plus exposés et à l'impact le plus fort (détection des menaces, gestion des identités et des accès et automatisation de la sécurité). En plus de mieux armer les entreprises contre des menaces sophistiquées, cette approche renforce leur posture de sécurité globale car elle s'appuie sur les toutes dernières innovations de sécurité du cloud.

Adoption d'une sécurité basée dans le cloud

La décision d'opter pour des solutions de sécurité en mode cloud s'inscrit dans la même logique organisationnelle d'agilité, d'efficacité et de protection renforcée. Parmi les facteurs invoqués, 56 % des sondés citent une meilleure évolutivité, démontrant ainsi la capacité du cloud à s'ajuster aux fluctuations de la demande. Puis vient la baisse des coûts pour 47 % d'entre eux, talonnée par le déploiement accéléré (46 %). Ces deux raisons mettent en évidence les avantages économiques et opérationnels qui motivent les entreprises à prendre le virage du cloud. L'amélioration des performances (42 %) et la réduction des efforts manuels pour implémenter les correctifs et mises à niveau logicielles (40 %) continuent de stimuler cette adoption, en particulier dans un contexte marqué par une pénurie chronique des compétences en cybersécurité.

► Quels sont les principaux arguments en faveur des solutions de sécurité basées dans le cloud ? (plusieurs choix possibles)



Les entreprises qui envisagent de migrer leur sécurité dans le cloud devraient prioriser l'évolutivité, la rentabilité et le déploiement accéléré pour capitaliser sur les bénéfices opérationnels et économiques du cloud. Autre axe prioritaire : opter pour des solutions garantissant une gestion simplifiée des politiques et d'une conformité continue pour améliorer leur posture de sécurité, et in fine, leur résilience face à l'évolution constante des menaces et des réglementations.

Autres réponses :

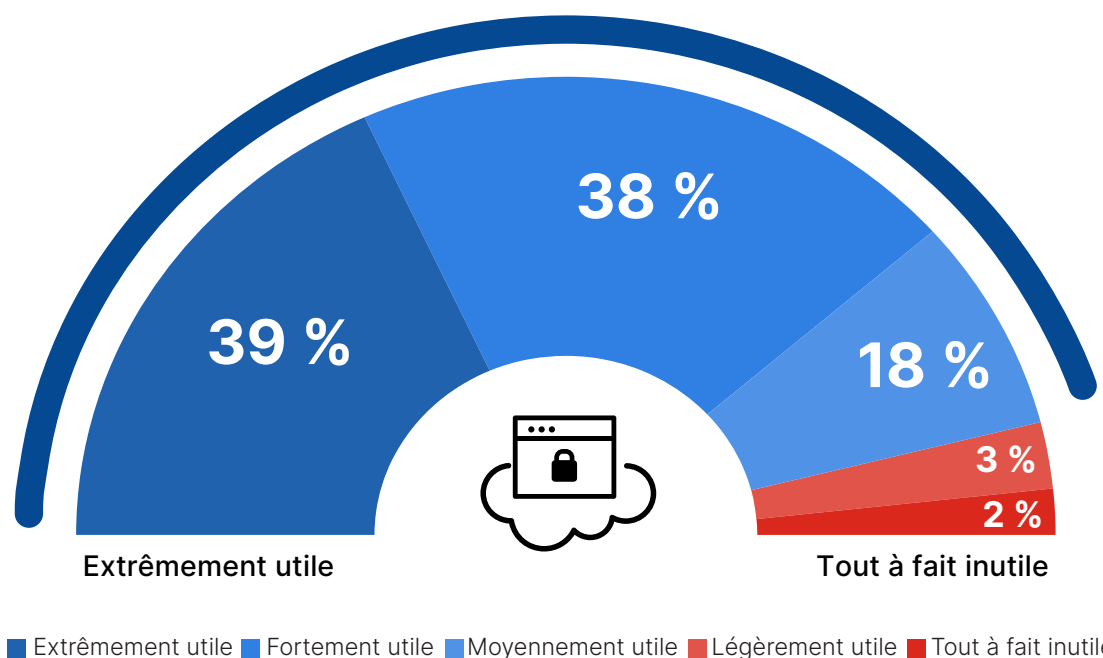
Gestion simplifiée des politiques 39 % | Disponibilité accrue 38 % | Respect des exigences de conformité du cloud 34 % | Meilleure visibilité sur l'activité des utilisateurs et le comportement des systèmes 33 % | Capacité à sécuriser l'accès aux applications de n'importe où 32 % | Nos données ou nos workloads sont hébergés dans le cloud (ou vont y être transférés) 28 % | Empreinte matérielle réduite sur les sites distants 27 %

Plateforme de sécurité cloud unifiée

Face à la complexité, au casse-tête opérationnel et au déficit de compétences déjà mentionnés, les entreprises souhaitent sans surprise se tourner vers une plateforme de sécurité unifiée pour simplifier et consolider la gestion de la sécurité sur leurs divers environnements cloud. L'écrasante majorité des sondés (95 %) confirme les avantages d'une telle plateforme pour assurer une protection complète et homogène des données dans le cloud.

- Quelle serait l'utilité d'une plateforme de sécurité cloud centralisée, avec un tableau de bord unique rassemblant toutes les politiques nécessaires afin de protéger les données de façon homogène et complète sur toute l'infrastructure cloud ?

95 % considèrent que le choix d'une plateforme cloud centralisée, avec un tableau de bord unique, s'avère de moyennement à extrêmement utile



Ce véritable plébiscite en faveur d'une solution de sécurité du cloud unique et intégrée fait écho à la tendance du secteur à consolider les plateformes dans une démarche de sécurité plus efficace, d'intégrations simplifiées et de coûts de gestion réduits. Seule cette approche est en mesure de pallier la pénurie de compétences en cybersécurité et de juguler des attaques de plus en plus sophistiquées et automatisées. Une plateforme unifiée, c'est aussi une visibilité complète et des politiques de sécurité homogènes. Les entreprises peuvent ainsi tirer un trait sur la multiplicité des interfaces qui alourdissent la charge opérationnelle et renforcer la posture de sécurité globale sur tous leurs environnements cloud.

Conjuguer cloud et sécurité : les stratégies qui ont fait leurs preuves

Dans un univers cloud en perpétuelle mutation, le renforcement de la posture de sécurité cloud s'impose comme un impératif absolu pour les entreprises de toutes tailles. Ce guide recense les bonnes pratiques indispensables à la sécurisation de vos environnements dématérialisés, de la consolidation des plateformes de sécurité à l'investissement dans des compétences spécialisées. Le but : renforcer vos défenses contre les attaques sophistiquées actuelles et futures.



ADOPTER UNE PLATEFORME DE SÉCURITÉ UNIFIÉE

Comme 95 % des entreprises interrogées, optez pour une stratégie de centralisation pour renforcer votre contrôle de la sécurité, simplifier vos opérations et améliorer la visibilité sur l'ensemble de vos environnements cloud.



OPTER POUR UNE SÉCURITÉ COUVRANT TOUS LES CLOUDS

Avec 78 % des entreprises optant pour une approche hybride ou multicloud, il est plus que jamais indispensable d'élaborer des stratégies en phase avec les spécificités de ces environnements et de garantir une application homogène des politiques de sécurité.



AUTOMATISER LA GESTION DES POLITIQUES ET DE LA CONFORMITÉ

Implémentez des systèmes d'automatisation et de rationalisation des politiques de sécurité sur tous vos environnements cloud pour satisfaire systématiquement aux exigences de sécurité.



PRIORISER LA PROTECTION DES DONNÉES

Considérée comme primordiale pour 58 % des entreprises, la protection des informations sensibles sur l'ensemble des services cloud requiert une stratégie solide de gouvernance et de chiffrement des données.



AMÉLIORER LA GESTION DES CONFIGURATIONS

Pour empêcher les erreurs et réduire le risque de vulnérabilités, optez pour une gestion active de vos configurations cloud.



RENFORCER LE CONTRÔLE DES ACCÈS

L'implémentation des principes Zero Trust passe par une gestion rigoureuse des identités et des accès. Vous diminuerez ainsi le risque d'accès non autorisés.



BOOSTER LA DÉTECTION DES MENACES ET LA RÉPONSE

Les analyses avancées et la réponse automatisée permettent d'identifier et de neutraliser les menaces en temps réel.



INVESTIR DANS LES COMPÉTENCES DE SÉCURITÉ CLOUD-NATIVE

Face à l'inquiétude généralisée (93 %) que suscite la pénurie de talents en cybersécurité, il est essentiel de favoriser le développement de spécialistes de la sécurité du cloud en interne. Fortes de ces compétences, vos équipes pourront naviguer plus efficacement dans les méandres de la sécurité du cloud.

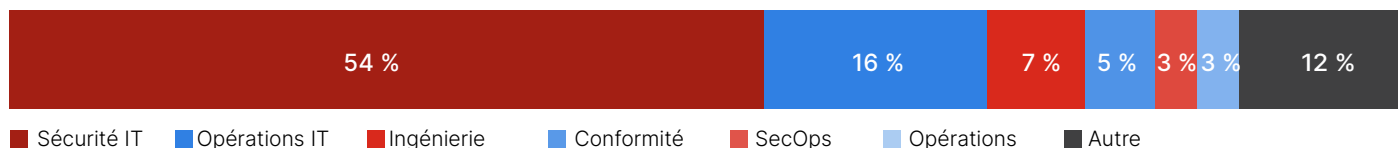
Méthodologie et données démographiques

Ce rapport 2024 sur la sécurité du cloud s'appuie sur une étude menée en février 2024 auprès de 927 professionnels de la cybersécurité. Son objectif : dresser un état des lieux de l'adoption du cloud, évaluer l'évolution des enjeux de sécurité prioritaires, et mettre en lumière les bonnes pratiques de sécurité adoptées dans la transition vers le cloud. Cet échantillon rassemble une grande diversité de profils allant des responsables techniques aux professionnels de la sécurité IT, dans des entreprises de tailles variées évoluant dans différents secteurs d'activité.

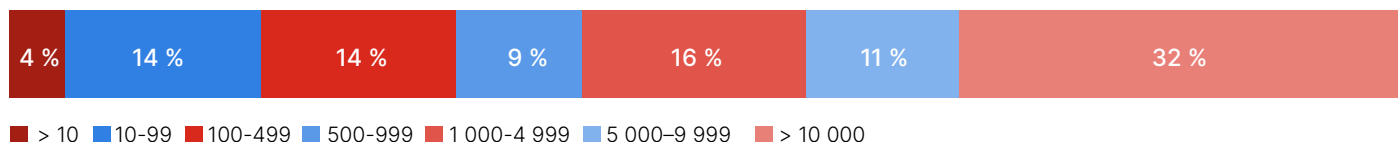
POSTE/NIVEAU HIÉRARCHIQUE



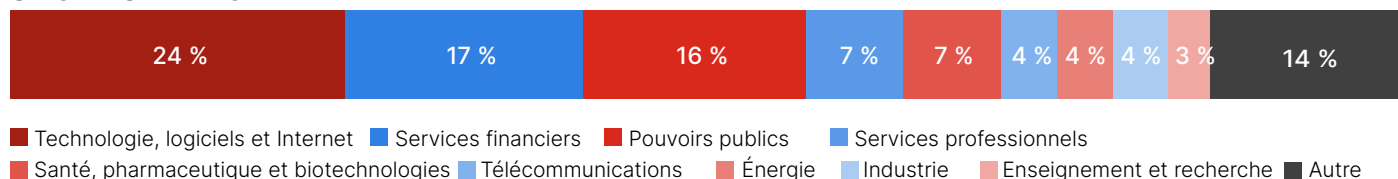
DÉPARTEMENT



TAILLE DE L'ENTREPRISE



SECTEUR D'ACTIVITÉ



Réutilisation du contenu

Nous encourageons nos lecteurs à réutiliser les données, graphiques et textes publiés dans ce rapport conformément à la [Licence publique de Creative Commons Attribution 4.0 International](#). Libre à vous de partager et d'utiliser cette étude à des fins commerciales, dans la mesure où vous en citez la source, comme le stipulent les conditions générales de la licence. Exemple : « Rapport Fortinet et Cybersecurity Insiders 2024 sur la sécurité du cloud ».



Fortinet (NASDAQ : FTNT) sécurise les plus grandes entreprises, prestataires de services et administrations aux quatre coins du globe.

Nous offrons à nos clients une visibilité et un contrôle complets sur une surface d'attaque en pleine expansion, tout en leur apportant la puissance indispensable pour répondre durablement à des impératifs de performance de plus en plus élevés. La plateforme Security Fabric de Fortinet permet aux entreprises de résoudre les défis de sécurité les plus critiques afin de protéger leurs données sur l'ensemble de l'infrastructure digitale (réseaux, applications, environnements edge ou multicloud). Fortinet est le n° 1 des ventes d'équipements de sécurité dans le monde. Plus de 730 000 clients nous font confiance pour protéger leur entreprise.

www.fortinet.com/fr

Cybersecurity

I N S I D E R S

Cybersécurité Insiders réunit une communauté de plus de 600 000 professionnels de la sécurité IT et de fournisseurs de technologies de pointe. Sa mission : favoriser la collaboration et la résolution des problèmes face aux principaux enjeux de cybersécurité du moment.

Notre approche privilégie la création et la sélection de contenus uniques visant à former et informer les professionnels de la cybersécurité sur les dernières tendances, solutions et bonnes pratiques de cybersécurité. Études exhaustives, évaluations objectives de produits, guides pratiques, webinars captivants, articles foisonnants... nous mettons à votre disposition une mine de contenus pour vous apporter des réponses objectives et factuelles aux enjeux complexes de la cybersécurité d'aujourd'hui.

Envie de vous démarquer sur un marché de la cybersécurité saturé ? Cybersecurity Insiders vous aide à impulser la demande pour vos produits, la visibilité de votre marque et votre thought leadership. Contactez-nous pour en savoir plus.

Écrivez-nous à info@cybersecurity-insiders.com ou rendez-vous sur cybersecurity-insiders.com