ISG | kaspersky

Réduction des difficultés liées à la migration vers le cloud, grâce à une forte sécurité du cloud hybride et des conteneurs

DOCUMENT D'ANALYSE PAR ISG | MAI 2024

Table des matières

Introduction

Aperçu de l'étude

La demande d'environnements cloud hybrides a connu une croissance exponentielle ces dernières années. Dans le cadre des initiatives de transformation numérique, l'intégration de l'infrastructure sur site avec l'évolutivité et la flexibilité offertes par les environnements cloud est devenue impérative pour permettre aux organisations de mener leurs opérations sans interruption, en favorisant l'efficacité et l'agilité pour répondre aux attentes des clients. Si réunir le meilleur des deux mondes peut paraître fascinant, l'intégration fluide de deux environnements distincts nécessite une planification méticuleuse afin d'atténuer les problèmes de sécurité des données, d'interopérabilité des solutions, de frais généraux, etc.

Si les solutions sur site ont leurs avantages en matière de sécurité des données, l'adoption rapide de plateformes hybrides/multicloud peut être attribuée à leur capacité inégalée à simplifier les opérations, favoriser l'innovation, réguler l'infrastructure, réduire les frais généraux et améliorer l'efficacité opérationnelle. Dans un monde post-pandémique, les organisations se tournent rapidement vers les plateformes cloud pour renforcer leurs mécanismes de continuité des activités et de reprise après sinistre. L'intérêt accru pour les environnements cloud peut être attribué à la fourniture d'une solution de stockage géographiquement dispersée, garantissant que les applications et les données sensibles restent accessibles en cas de perturbations imprévues.

Les technologies cloud natives, comme Kubernetes et Docker, deviennent aujourd'hui des catalyseurs de premier plan pour la transformation numérique. À toutes les échelles, les organisations réorientent activement leurs efforts de développement technologique en adoptant une architecture de microservices conteneurisée. Cependant, notre étude indique que si les organisations sont plutôt pour l'adoption des technologies cloud, elles continuent à rencontrer des problèmes de sécurité liés au cloud. Ce combat permanent aboutit à des pannes récurrentes du système, à des pertes de revenus et à diverses perturbations opérationnelles.

Les constatations suivantes étayent cette affirmation :

- 96 % des organisations déclarent utiliser actuellement ou prévoir d'utiliser des technologies cloud natives, comme K8s, Dockers et service mesh, au cours des deux prochaines années.
- 41 % des entreprises n'ont pas encore mis en œuvre les principes DevSecOps, l'une de leurs cinq principales stratégies pour renforcer leur environnement cloud natif.
- Pour 48 % des entreprises, la sécurité et la conformité des données restent l'un des trois principaux enjeux des environnements cloud hybrides.
- Près de 60 % des organisations déclarent que leur incapacité à identifier les vulnérabilités et les risques grâce à une analyse continue est l'un des cinq principaux défis de leur solution de sécurité existante.
- Environ 54 % des organisations déclarent qu'investir dans des outils CWS qui hiérarchisent et classent les vulnérabilités selon leur comportement est l'une de leurs cinq priorités pour renforcer leur posture de sécurité dans le cloud hybride.

Ce document de réflexion commun à Kaspersky et l'ISG s'efforce d'identifier et d'analyser les facteurs les plus critiques qui continuent d'influencer les organisations à adopter des technologies cloud hybrides et natives au sein d'organisations de toutes tailles dans 12 pays et divers secteurs d'activités. Il vise à dévoiler des perspectives critiques sur l'adoption rapide par les organisations de solutions cloud afin d'assurer des opérations quotidiennes fluides. En plongeant dans les subtilités de l'environnement cloud, le document aborde les problèmes de sécurité les plus courants, décrit les stratégies d'investissement futures pour surmonter ces obstacles inhérents et envisage l'évolution prévue de l'infrastructure cloud telle qu'elle est perçue par ces organisations.

Méthodologie de recherche

Ce document de réflexion utilise une stratégie de recherche mixte et une analyse approfondie de la dynamique du marché et des sentiments englobant l'adoption de plateformes et de technologies hybrides et multicloud. Il explore en détail les défis de sécurité des organisations au cours de leur parcours de migration vers le cloud et souligne les points clés pour les fournisseurs de sécurité tiers afin d'améliorer l'assistance aux clients dans leurs efforts de transformation numérique. Nous avons mené une enquête exhaustive auprès de 310 entreprises de grande et moyenne taille dans 12 pays pour étayer notre hypothèse sur les étapes actuelles et futures de la posture de sécurité hybride, multi et native du cloud.

Profil des sondés

Les répondants au sondage sont des organisations de minimum 500 employés. Nous nous sommes adressés à des décideurs portant des titres comme RSSI, DPT et responsable de la transformation. Cette sélection stratégique a permis de s'assurer que le sondage englobe les perspectives informées et les opinions d'experts des responsables des prises de décisions stratégiques critiques sur les investissements dans l'infrastructure technologique au sein de ces organisations. Nous avons cherché à développer un aperçu global des aspects subjectifs et objectifs de la dynamique et des enjeux de la technologie cloud.

Résumé analytique et principaux résultats

L'adoption massive d'environnements cloud hybrides continue d'émerger comme une priorité pour les organisations désireuses de trouver un juste équilibre entre leurs efforts incessants d'innovation et le maintien de protocoles de sécurité. Les entreprises vont au-delà des environnements cloud hybrides et souhaitent explorer des stratégies multicloud. Selon l'étude Multi Public Cloud Solutions 2023, les organisations s'efforcent de plus en plus de concevoir une stratégie solide pour adopter plusieurs plateformes de cloud public. Cette tendance fait écho à notre sondage, selon lequel 71 % des organisations interrogées utilisent déjà des plateformes de cloud public pour leurs opérations quotidiennes. En outre, une analyse plus approfondie de notre sondage révèle que si 34 % intègrent harmonieusement l'infrastructure sur site avec le cloud public, 22 % naviguent dans le paysage hybride des environnements cloud publics et privés.

Cependant, l'intégration de technologies avancées dans les environnements hybrides et multicloud, comme les technologies de calcul informatisé pour un traitement plus rapide des données, l'intelligence artificielle (IA) et le machine learning (ML), pour extraire des informations riches à partir de données étendues situées dans des environnements sur site et cloud et l'informatique sans serveur, rendent l'infrastructure opérationnelle plus complexe. Les organisations ont donc largement investi dans le renforcement de leur posture de sécurité.

Notre analyse révèle des informations clés sur l'état actuel de l'adoption de la technologie cloud, y compris les principaux moteurs qui continuent à propulser cette tendance, les pièges potentiels à éviter et les priorités d'investissement et stratégies futures des organisations.

Infrastructure sur site coûteuse

- Pour 56 % des entreprises, l'infrastructure sur site offre une meilleure sécurité.
- 81 % des organisations estiment que les coûts élevés associés à la maintenance et à la gestion de l'infrastructure sur site posent encore problème.

Tendance croissante à la migration à grande échelle vers le cloud

- Près de 36 % des entreprises prévoient de transférer leurs applications dans le cloud au cours des trois prochaines années.

Importance de l'agilité et l'évolutivité pour l'adoption du cloud

- Pour 53 % des entreprises, l'agilité et la flexibilité accrues offertes par le cloud ont été l'un des cinq principaux facteurs dans leur décision d'adopter le cloud.

Menace des problèmes de sécurité pour l'infrastructure cloud des entreprises

- 60 % des entreprises déclarent que la surveillance et la prévention proactive des erreurs de configuration des ressources dans le cloud constituent l'un des cinq principaux défis liés à leur solution actuelle de sécurité dans le cloud.

Popularité croissante de la conteneurisation

- Pour 73 % des entreprises, la flexibilité offerte par les conteneurs pour s'adapter à l'évolution dynamique des charges de travail est l'un des cinq principaux facteurs d'adoption du modèle conteneurisé.
- 69 % des entreprises affirment que la mise en œuvre de mesures de sécurité d'exécution sur les conteneurs est plus facile que sur l'infrastructure traditionnelle, propulsant cet attribut parmi les cinq principaux facteurs d'adoption d'un modèle dedéveloppement d'applications conteneurisées.

Continuité probable de la priorité donnée par les entreprises à la sécurité du cloud

- Pour 54 % des entreprises, investir dans des outils CWS offrant une sécurité robuste pour les clouds hybrides et multiples est l'une des cinq principales priorités pour renforcer leur mécanisme de défense sur le cloud.
- 49 % des entreprises déclarent que l'une des cinq principales attentes à l'égard de leur partenaire de sécurité en cloud est de recevoir un rapport sur les profils de menaces fondé sur un persona.
- Pour 51 % des entreprises, investir dans des solutions en temps réel qui suivent les violations de la conformité et partagent les alertes avec les équipes de sécurité est l'une des cinq priorités pour renforcer leurs environnements cloud natifs.

Migrer vers le cloud ou rester sur site : analyse des sentiments du marché et des choix opérationnels

Comprendre les choix : facteurs influençant le choix de l'infrastructure d'exploitation

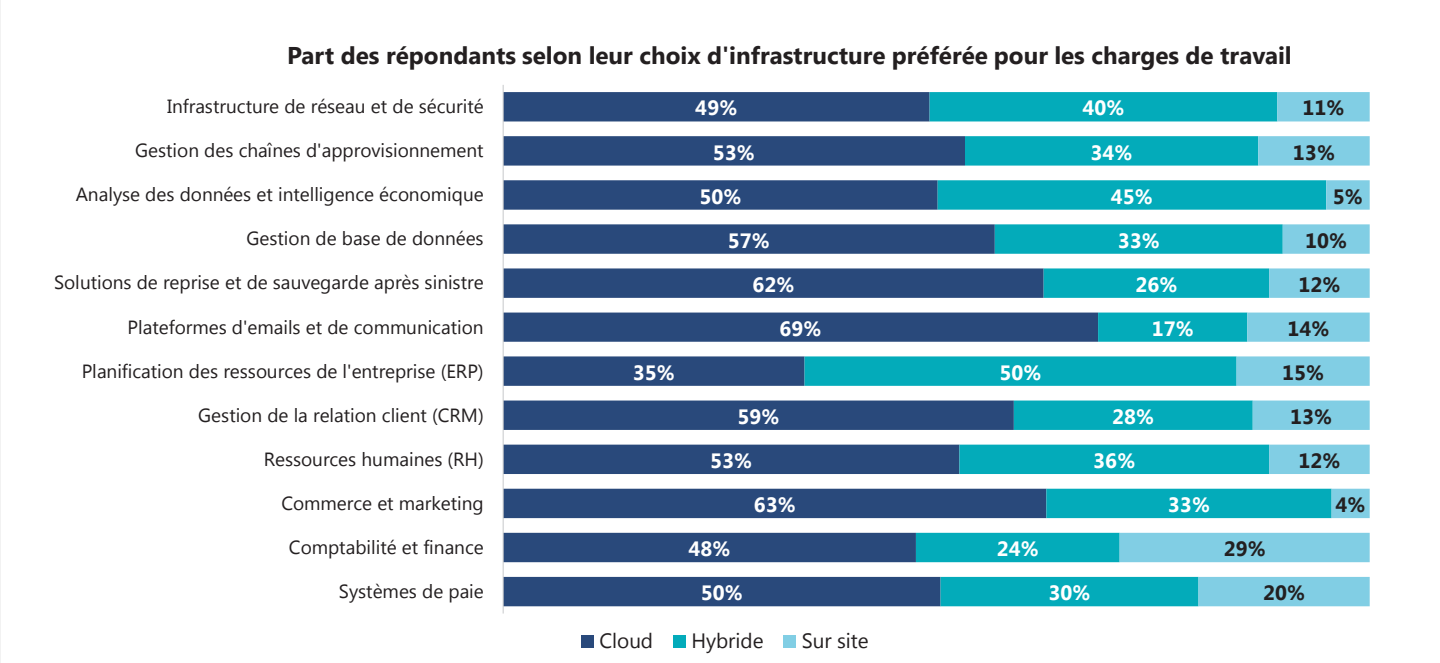
Historiquement, les organisations de grande envergure ont largement privilégié l'infrastructure sur site pour sauvegarder, surveiller et superviser efficacement leurs charges de travail vitales. Si l'on analyse ce choix d'un point de vue stratégique, la volonté d'investir ou de perpétuer leur infrastructure physique sur site peut être attribuée aux protocoles de contrôle et de sécurité des centres de données physiques qui autonomisent les utilisateurs finaux. Il convient de mentionner que, d'un point de vue réglementaire, les organisations qui utilisent une infrastructure sur site estiment disposer d'un cadre de conformité solide qui leur permet d'adhérer aux directives régionales et sectorielles, et donc d'adapter les configurations pour répondre à des exigences uniques en matière de flux de travail et d'opérations.

Relevons également que si la tendance à la modernisation de l'infrastructure est indéniable, les bénéfices ne sont pas immédiats et peuvent comprendre des risques, comme des perturbations dans les activités de l'entreprise pendant le processus de migration. La modernisation de l'infrastructure est désormais essentielle pour de nombreuses entreprises afin de rester compétitives et de répondre aux exigences changeantes de l'ère numérique.

Toutefois, ces dernières années, surtout après la pandémie, l'adoption des plateformes et technologies cloud est montée en flèche. En effet, la technologie cloud fait désormais partie intégrante des plans de continuité des activités des organisations, qui leur permettent de mettre en place des mécanismes solides de reprise après sinistre, afin d'éviter les perturbations opérationnelles et de poursuivre leurs activités même en cas d'imprévus. Les entreprises adoptent de plus en plus une approche d'externalisation en l'état, en se concentrant sur la répartition de leurs diverses charges de travail dans un environnement multicloud.

Les entreprises utilisent leur infrastructure informatique depuis des années, voire des décennies. Ces infrastructures ont atteint la fin de leur durée de vie, ne peuvent plus répondre aux exigences des applications modernes et des processus d'entreprise et sont plus vulnérables aux menaces de sécurité et à d'autres risques. Cette décision est stratégiquement alignée sur leurs choix opérationnels, où l'infrastructure sur site continue de jouer un rôle central en aidant les organisations à atteindre leurs objectifs critiques et à fournir des résultats supérieurs.

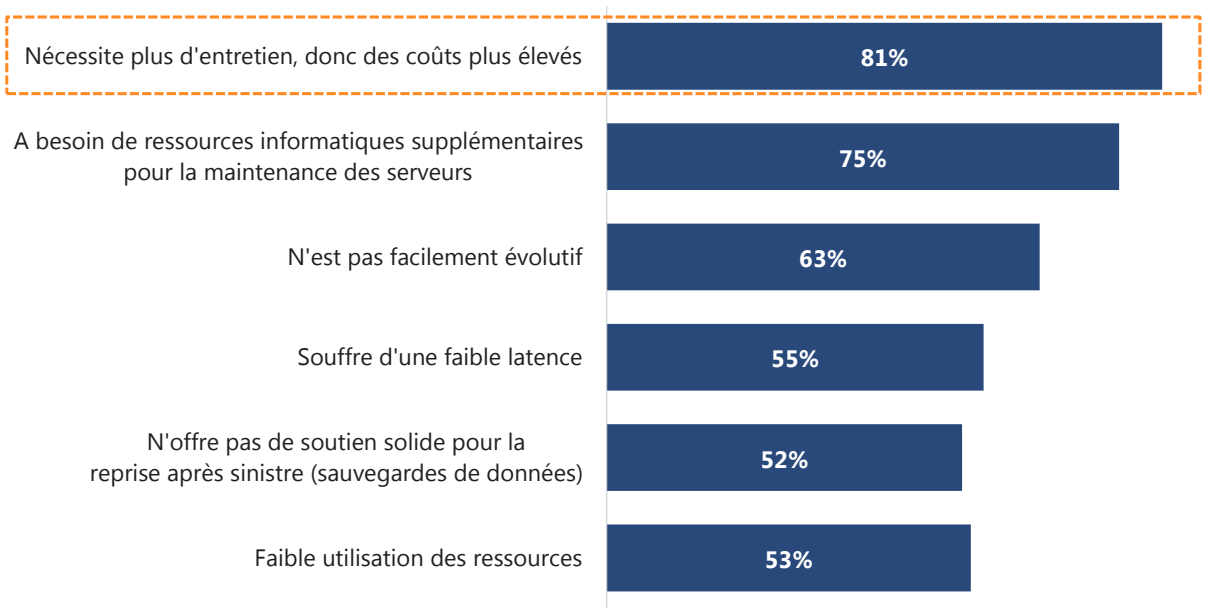
Tableau 1 : Influence des charges de travail sur les préférences en matière d'infrastructure



Source : Enquête de l'ISG, nombre de répondants = 310

D'après notre étude, les entreprises ont pris conscience de la flexibilité offerte par le cloud, qui leur permet d'adapter dynamiquement leurs charges de travail en fonction de leurs besoins dans l'environnement cloud, chose difficile avec une infrastructure sur site. Les coûts de maintenance plus élevés et les problèmes de latence associés à l'infrastructure sur site restent une source d'inquiétude majeure pour les entreprises clientes. La représentation visuelle ci-dessous aide à décrypter certains des défis importants auxquels les entreprises sont confrontées à l'échelle mondiale avec leur infrastructure traditionnelle sur site. Ces défis ont notamment joué un rôle essentiel dans l'adoption des technologies cloud par les entreprises.

Tableau 2 : Problèmes rencontrés par les organisations avec leur infrastructure sur site



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi les 5 principaux défis liés à leur infrastructure sur site.

Adoption du cloud : décryptage du paysage de la migration vers le cloud hybride

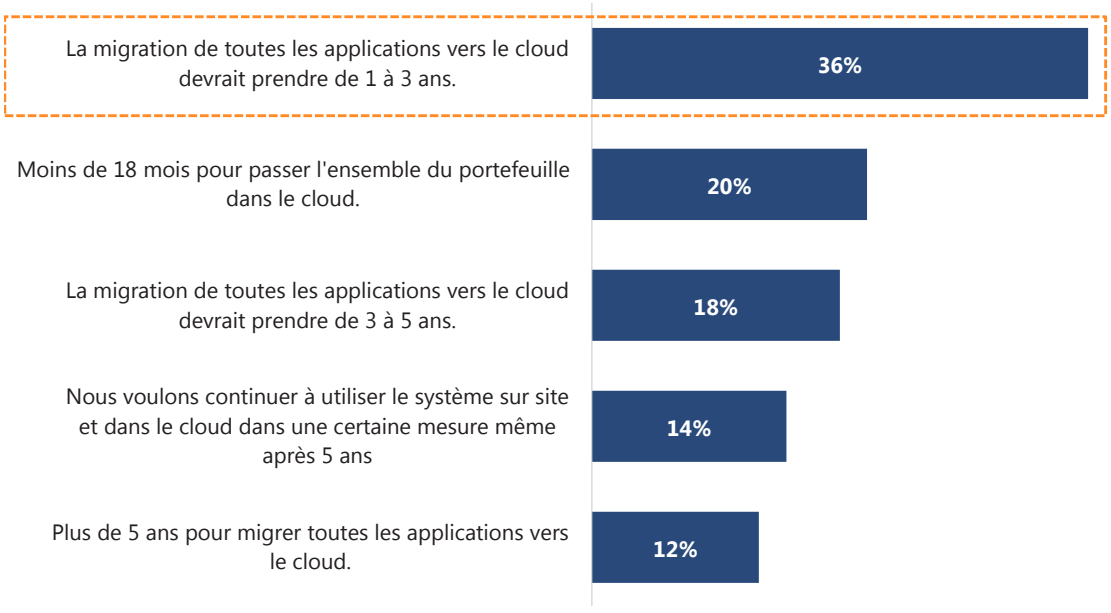
Ces dernières années, la demande croissante de solutions cloud hybrides a entraîné une complexité accrue et des défis de gestion au sein des environnements d'infrastructure informatique. Dans leur quête de croissance durable, les entreprises s'orientent de plus en plus vers l'adoption de multiples environnements cloud, ce qui nécessite la formulation d'une stratégie solide pour opérer dans un environnement multicloud.

Les stratégies de migration comme le transfert d'hébergement et de plateforme ont été largement adoptées par les entreprises pour migrer leurs solutions hébergées sur une infrastructure physique vers des environnements cloud. Par ailleurs, notre étude révèle que les entreprises s'orientent de plus en plus vers l'hébergement de leurs données critiques sur leur infrastructure physique, et vers l'exécution de leurs opérations d'analyse de données et de tableaux de bord sur des plateformes cloud essentiellement publiques. Les résultats de notre sondage nous ont permis de mieux comprendre les préférences des utilisateurs finaux.

Après examen des résultats, nous avons constaté que, bien que seulement 10 % des organisations interrogées utilisent actuellement des environnements cloud privés parallèlement à leur infrastructure sur site, une part non négligeable de 71 % des sondés a déclaré que leurs opérations étaient menées sur plusieurs environnements cloud publics. Notons que parmi les 71 % d'organisations qui utilisent des environnements cloud publics, environ 34 % ont également recours à des solutions sur site. La tendance à maintenir une dynamique de croissance dans un paysage concurrentiel en constante évolution continue de pousser les entreprises à diversifier leurs stratégies cloud. L'adoption de multiples plateformes cloud pour travailler en parallèle de leur infrastructure physique permet aux organisations de disposer d'une base opérationnelle plus résiliente et plus polyvalente.

Cela les aide à atténuer les risques liés à la rigidité opérationnelle et aux dépassements de coûts dus aux blocages des fournisseurs et à l'utilisation inefficace ou non optimisée des ressources en utilisant les atouts uniques des différents fournisseurs de services cloud. Cette observation est confirmée par notre étude, selon laquelle près de 32 % des organisations interrogées dépendent de plateformes cloud pour exploiter **plus de 60 % de leurs charges de travail existantes.** Nos recherches révèlent que près de 36 % des entreprises envisagent de transférer toutes leurs applications dans le cloud au cours des trois prochaines années. Environ 85 % des organisations interrogées prévoient d'utiliser le cloud à grande échelle au cours des cinq prochaines années, ce qui témoigne de la propension croissante des organisations à adopter des plateformes cloud.

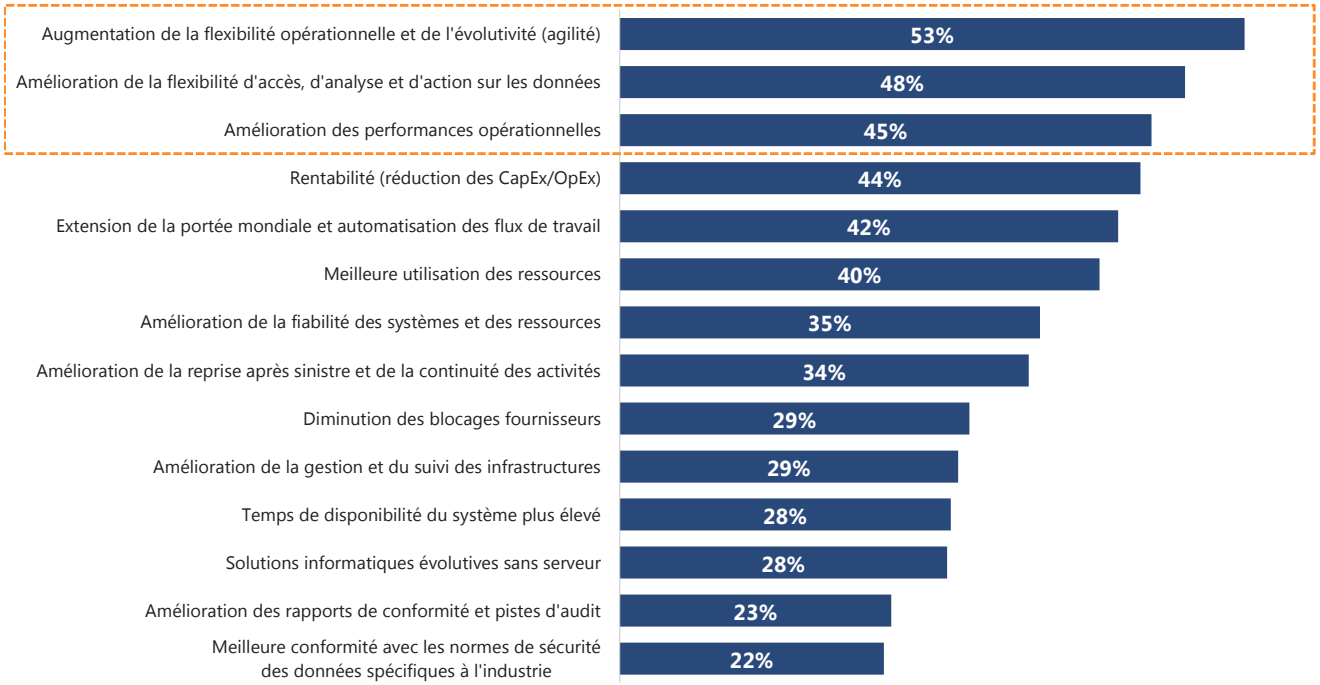
Tableau 3 : Stratégies d'entreprise pour exploiter le cloud dans les initiatives de transformation à court et à moyen terme



Source : Enquête de l'ISG, nombre de répondants = 310

Les entreprises tentent stratégiquement d'amalgamer leur infrastructure sur site et les capacités étendues du cloud afin d'optimiser les performances, d'amplifier l'évolutivité et d'induire une agilité opérationnelle. L'approche hybride garantit l'adaptabilité et permet aux entreprises de naviguer dans des paysages de données complexes, en s'adaptant sans effort à l'évolution des besoins. Tant que les entreprises continueront d'investir dans des environnements cloud hybrides pour atteindre une agilité et une innovation inégalées, les technologies et les solutions fonctionnant dans ces environnements continueront d'augmenter fortement dans les années à venir. Par exemple, près de 45 % des organisations interrogées estiment que l'adoption de plateformes cloud a amélioré leurs performances opérationnelles, qu'elles placent parmi les cinq principaux avantages obtenus. La représentation ci-dessous permet de mieux comprendre les facteurs qui favorisent l'adoption des plateformes cloud hybrides et comment elles se placent systématiquement parmi les cinq principaux avantages concrets.

Tableau 4 : Analyse des avantages concrets de l'adoption du cloud

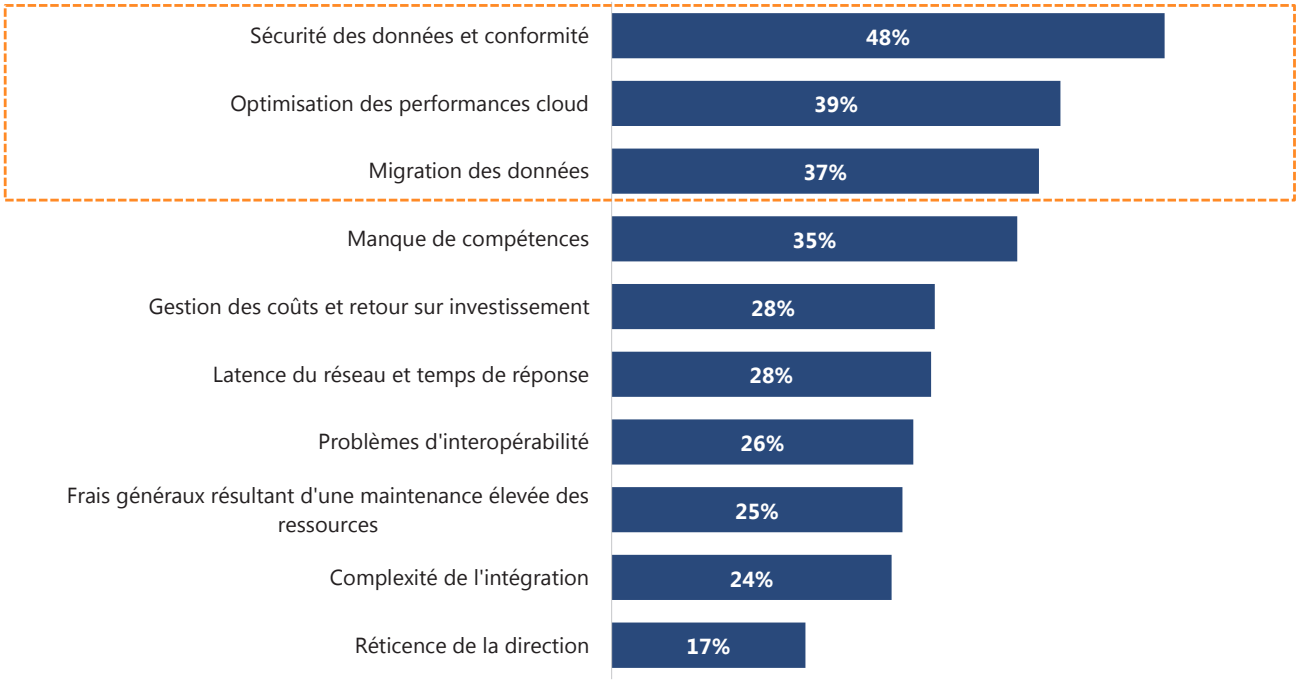


Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi les 5 principaux avantages concrets de l'adoption du cloud.

Notre étude indique que si l'adoption des technologies cloud pour des initiatives de transformation numérique expansives peut sembler théoriquement convaincante, il est crucial de comprendre les défis redoutables qui accompagnent une telle stratégie. Les complexités opérationnelles, les problèmes de sécurité et l'absence d'interopérabilité fluide, susceptibles de perturber la communication entre les ressources numériques dans les environnements sur site et cloud, représentent des défis considérables pour les entreprises. Il est donc nécessaire de formuler une stratégie solide d'adoption du cloud. Par exemple, notre analyse révèle que pour 48 % des organisations interrogées, le respect des normes de sécurité et de conformité des données a été l'un des trois principaux défis à relever lors de la migration vers les plateformes cloud. D'autre part, pour **39 %** des organisations, l'incapacité à optimiser les performances cloud reste l'un des trois principaux défis. Le manque de disponibilité d'un vivier de talents qualifiés et techniquement compétents reste la bête noire des entreprises.

Bien que conceptuellement séduisante, la transition vers le cloud pose un défi de taille aux organisations qui s'efforcent de trouver un équilibre entre leurs aspirations et les complexités pratiques. L'illustration ci-dessous aide à comprendre les problèmes fondamentaux qui continuent de faire surface parmi les trois principaux défis rencontrés par les organisations lors de l'adoption ou de la migration de leurs charges de travail des solutions sur site vers des environnements cloud.

Tableau 5 : Défis liés à l'adoption des technologies cloud



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi leurs 5 principaux défis lors de l'adoption du cloud.

Sécuriser les environnements cloud hybrides et natifs

Analyse des défis posés par la sécurité du cloud

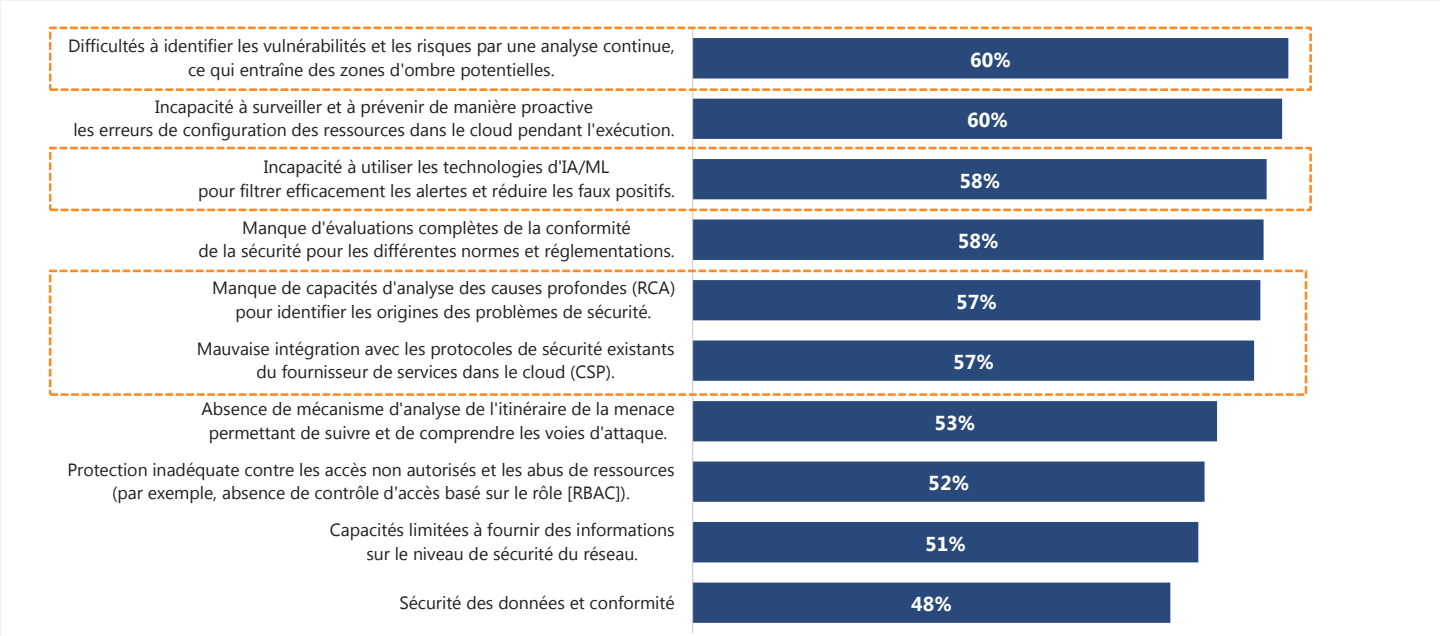
Dans le paysage évolutif de la transformation numérique, l'impératif d'une sécurité robuste du cloud est le pivot de la continuité et de la résilience des organisations. Les entreprises exploitant la puissance des architectures distribuées et des diverses plateformes cloud, il est essentiel de mettre en place un dispositif de sécurité complet. Alors que les organisations à toutes échelles continuent d'adopter rapidement des environnements hybrides et multicloud pour améliorer leur agilité et leur efficacité opérationnelle, elles sont confrontées à la menace croissante sur leur infrastructure opérationnelle des cyberattaques sophistiquées.

La surface d'attaque étendue des architectures hybrides et multicloud expose souvent les organisations à des cybermenaces sophistiquées en raison de l'indisponibilité de stratégies de défense robustes et adaptatives. Alors que l'environnement opérationnel des entreprises continue de se complexifier, l'absence de solutions utilisant les technologies d'IA et de ML pour filtrer efficacement les alertes et effectuer une analyse des causes profondes (RCA) pour identifier les origines des menaces rendra probablement les organisations vulnérables aux cyberattaques modernes et sophistiquées.

Les complexités inhérentes à la sécurisation des données décentralisées, à la gestion des contrôles d'accès et à la garantie de la conformité réglementaire rendent la sécurité complexe. Trouver un juste équilibre entre l'innovation et la sécurité reste un défi perpétuel, car les organisations continuent d'identifier des moyens de naviguer dans les relations dynamiques et les dépendances entre l'agilité, la connectivité et la nécessité de protéger les ressources numériques. Notre étude a montré que les organisations sont exposées aux nouvelles menaces en raison de l'absence de solutions pour protéger leurs ressources des accès non autorisés. Il convient de mentionner que l'incapacité des solutions de sécurité à s'intégrer à leur plateforme cloud a été une cause majeure d'inquiétude pour les organisations. Pour environ 57 % d'entre elles, il s'agit de l'une des cinq principales limites de leur fournisseur actuel de solutions de sécurité.

L'illustration ci-dessous nous aide à approfondir les points essentiels qui constituent les cinq principaux défis auxquels les organisations sont confrontées avec leur partenaire de sécurité existant. Ces éléments rendent leur posture de sécurité dans le cloud vulnérable aux menaces internes et externes.

Tableau 6 : Difficultés rencontrées par les entreprises avec leur fournisseur actuel de solutions de sécurité pour le cloud



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi leurs 5 principaux défis dans le cadre de la collaboration avec leur fournisseur de solutions de sécurité existant.

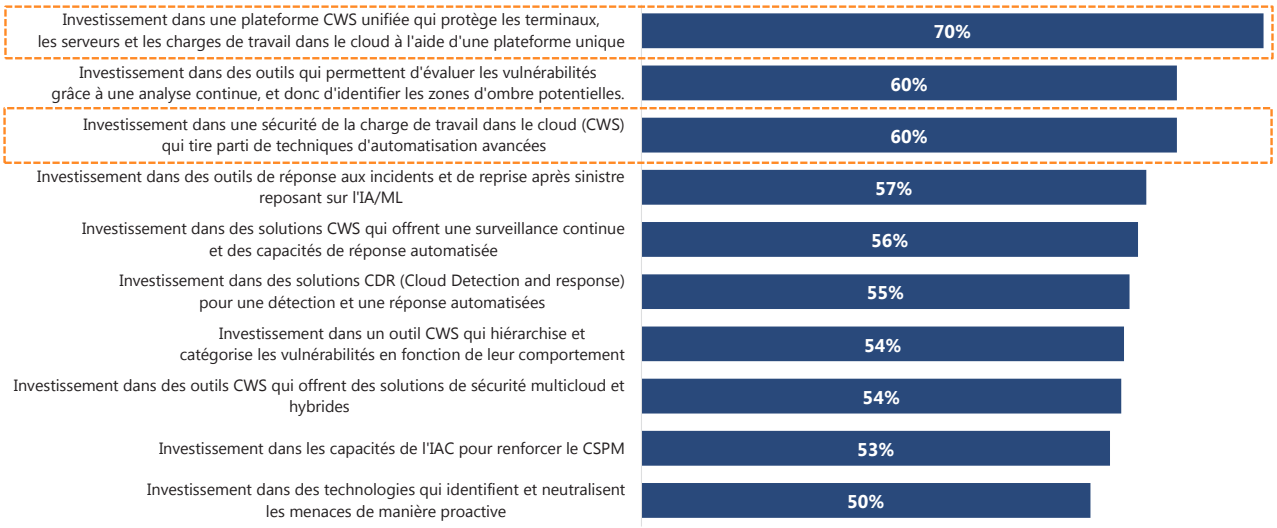
Décoder l'avenir des initiatives de sécurité dans le cloud

Les entreprises reconnaissent de plus en plus les avantages des technologies cloud, comme une plus grande évolutivité pour répondre à des demandes fluctuantes et des développements d'applications plus rapides grâce à l'approche de sécurité dite du décalage à gauche. En outre, l'intégration solide avec DevOps et les pipelines CI/CD, facilitée par les microservices et les architectures de conteneurs, est pour beaucoup dans l'adoption du cloud par les organisations de toutes tailles. Nous avons observé que les entreprises se concentrent également de plus en plus sur l'augmentation de leurs capacités cloud natives en incorporant des méthodes de développement d'applications disruptives, comme l'informatique sans serveur, l'architecture composable, les services d'infrastructure en tant que code (IaC) et l'intégration transparente avec DevSecOps dans un environnement multicloud. Les entreprises continueront probablement à exploiter tout le potentiel des environnements sur site et cloud, ce qui les obligera à adopter des solutions de sécurité pouvant communiquer avec ces deux environnements et fournir une vue d'ensemble de leur niveau de sécurité.

Notre étude indique que le paysage futur devrait mettre l'accent sur le développement de stratégies de migration des conteneurs, obligeant les organisations à investir massivement dans le renforcement de leur posture de sécurité hybride et multicloud. Les plateformes de sécurité qui fournissent à leurs clients des plateformes de sécurité des charges de travail dans le cloud (CWS) infusées par l'automatisation et qui leur permettent de protéger leurs terminaux, leurs serveurs et leurs charges de travail dans le cloud à l'aide d'une plateforme unifiée pourraient remporter un franc succès dans les années à venir.

Comme les organisations continuent à s'orienter vers une stratégie de développement conteneurisé, les fournisseurs de solutions de sécurité tierces affinent activement leurs portefeuilles de sécurité cloud native existants afin d'équiper les entreprises pour faire face aux menaces modernes introduites par les modèles de développement d'applications hautement distribuées et conteneurisées. Environ 56 % des organisations interrogées qui investissent dans des solutions CWS estiment qu'offrir des capacités de surveillance continue et de réponse automatisée est l'une de leurs cinq priorités pour les trois prochaines années. Les entreprises ont pris conscience de la nécessité d'adopter une approche proactive et multicouche de la sécurité qui prenne en compte toutes les facettes de l'infrastructure cloud, ce qui ouvre des horizons commerciaux aux fournisseurs de services de sécurité dans le cloud. L'illustration ci-dessous nous aide à approfondir les points essentiels qui constituent les cinq principaux défis auxquels les organisations sont confrontées avec leur partenaire de sécurité existant, ce qui rend leur posture de sécurité dans le cloud vulnérable aux menaces internes et externes.

Tableau 7 : Comprendre les priorités d'investissement des entreprises pour renforcer leur posture de sécurité dans le cloud



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi leurs 5 priorités d'investissement pour renforcer la posture de sécurité du cloud hybride.

Il est intéressant de noter que les priorités critiques sur lesquelles se concentrent les organisations interrogées soulignent une préférence croissante pour les environnements hybrides et multicloud. Toutefois, ce changement de mentalité opérationnelle rend plus complexes la gestion et le contrôle dynamiques de la sécurité des divers environnements opérationnels. Le défi s'étend également à l'incapacité des organisations à identifier et à résoudre de manière préventive les menaces potentielles avant qu'elles ne se transforment en menaces concrètes et ne causent des dommages importants.

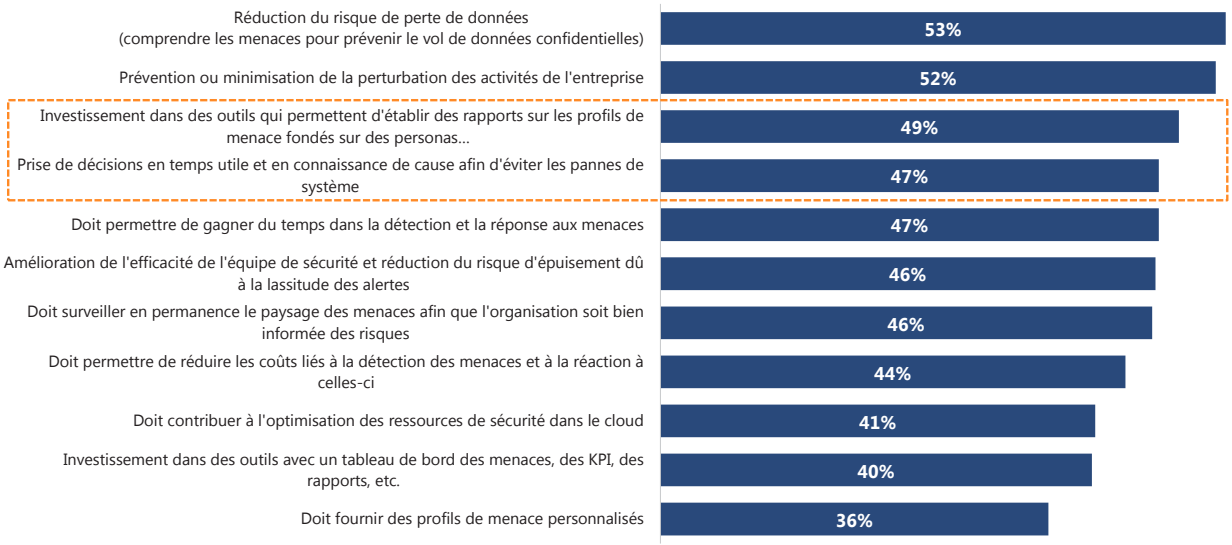
Bien que l'idée de fonctionner dans deux environnements distincts puisse présenter plusieurs avantages, les entreprises sont de plus en plus confrontées à des problèmes comme le risque élevé de vol de données, la réactivité limitée aux informations de sécurité en raison de la complexité des infrastructures et l'absence d'une plateforme qui établit un tableau de bord complet des risques capable de prévenir les perturbations opérationnelles à grande échelle. Pour faire face à cette volatilité opérationnelle, les entreprises attendent davantage de leurs partenaires en matière de solutions de sécurité.

Les entreprises sont de plus en plus enclines à collaborer avec des fournisseurs de solutions tiers disposant d'une grande expertise pour superviser et aider les clients à naviguer dans les complexités de l'infrastructure cloud hybride pour divers secteurs d'activité.

Du point de vue de la stratégie d'entreprise, les critères qui influencent le choix d'un fournisseur de solutions tiers pour gérer un environnement cloud hybride comprennent sa capacité à communiquer de façon fluide entre les deux environnements, son expertise en matière de conteneurisation, son adhésion aux normes de gouvernance et de conformité ainsi que sa capacité à éviter les temps d'arrêt et les pertes de données potentielles. Notre étude suggère que pour 49 % des organisations, les rapports sur les profils de menaces fondés sur des personas sont l'une des cinq principales attentes vis-à-vis de leur partenaire de sécurité au cours des deux prochaines années. Les entreprises sont susceptibles de s'orienter vers des fournisseurs de solutions qui leur permettent de prendre des décisions opportunes et éclairées afin d'éviter les temps d'arrêt du système. Nous avons pu le constater, car 47 % des organisations attendent cette approche de la part de leurs fournisseurs de services de sécurité à l'avenir.

La représentation ci-dessous donne un aperçu de la manière dont les entreprises attendent de leurs fournisseurs qu'ils dépassent leur rôle opérationnel conventionnel et deviennent des alliés stratégiques capables de fournir de meilleurs résultats et de contribuer à une gestion efficace du paysage de la sécurité en constante évolution. Notre étude révèle les facteurs clés qui figurent toujours parmi les cinq principales attentes des entreprises à l'égard de leur fournisseur de services de sécurité.

Tableau 8 : Décoder les attentes des entreprises vis-à-vis de leurs partenaires en solutions de sécurité



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi leurs 5 principales attentes à l'égard de leur partenaire en matière de solutions de sécurité dans le cloud.

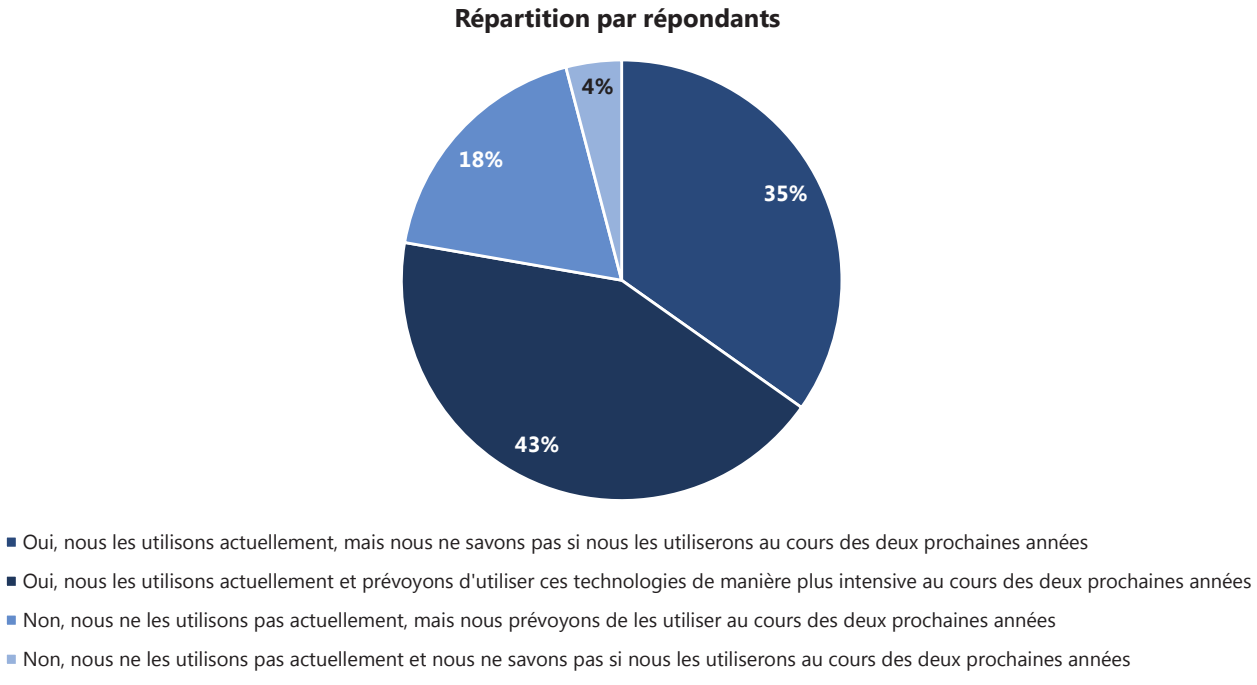
DevOps et conteneurs : comment surmonter les défis de sécurité

Dans le paysage technologique actuel en évolution rapide, DevOps est devenu une force centrale qui stimule l'innovation et aide les organisations à renforcer leur efficacité. La fusion fluide du développement et des opérations instaure un principe de travail collaboratif et permet aux entreprises de créer et de fournir plus rapidement des applications de haute qualité. En outre, étant donné que l'automatisation est au cœur des pratiques DevOps, les principes CI/CD sont devenus la pierre angulaire du développement d'applications.

Cependant, la complexité résultant du mélange d'infrastructures physiques et cloud a limité la visibilité des organisations sur le niveau de sécurité de leur environnement de développement, entraînant à terme des problèmes graves, comme la compromission de modèles de développement d'applications. Les principes traditionnels de DevOps sont rendus obsolètes pour faire face aux nouvelles menaces de cybersécurité dans les environnements cloud, laissant la place à un état d'esprit opérationnel DevSecOps.

Les organisations sont de plus en plus soucieuses de maintenir la crédibilité et la sécurité du code afin de répondre à la demande croissante de développement et de livraison rapides et efficaces de logiciels. Nous avons observé une croissance de l'affinité manifestée par les organisations pour l'adoption de technologies cloud natives, comme Kubernetes, service mesh et Docker, pour construire, déployer et maintenir des applications dans le cloud en exploitant le dynamisme et la flexibilité associés aux modèles de développement d'applications conteneurisées. Ce constat confirme à nouveau la nécessité d'intégrer les aspects de sécurité dans les principes DevOps. Cette conclusion est confirmée par notre étude, selon laquelle près de 96 % des organisations interrogées utilisent des technologies cloud natives ou prévoient de les utiliser dans un avenir proche, ce qui nécessite l'intégration de fonctions de sécurité essentielles, comme l'authentification centralisée, l'automatisation et la surveillance du réseau.

Tableau 9 : Le point de vue des utilisateurs finaux sur l'adoption des technologies cloud natives

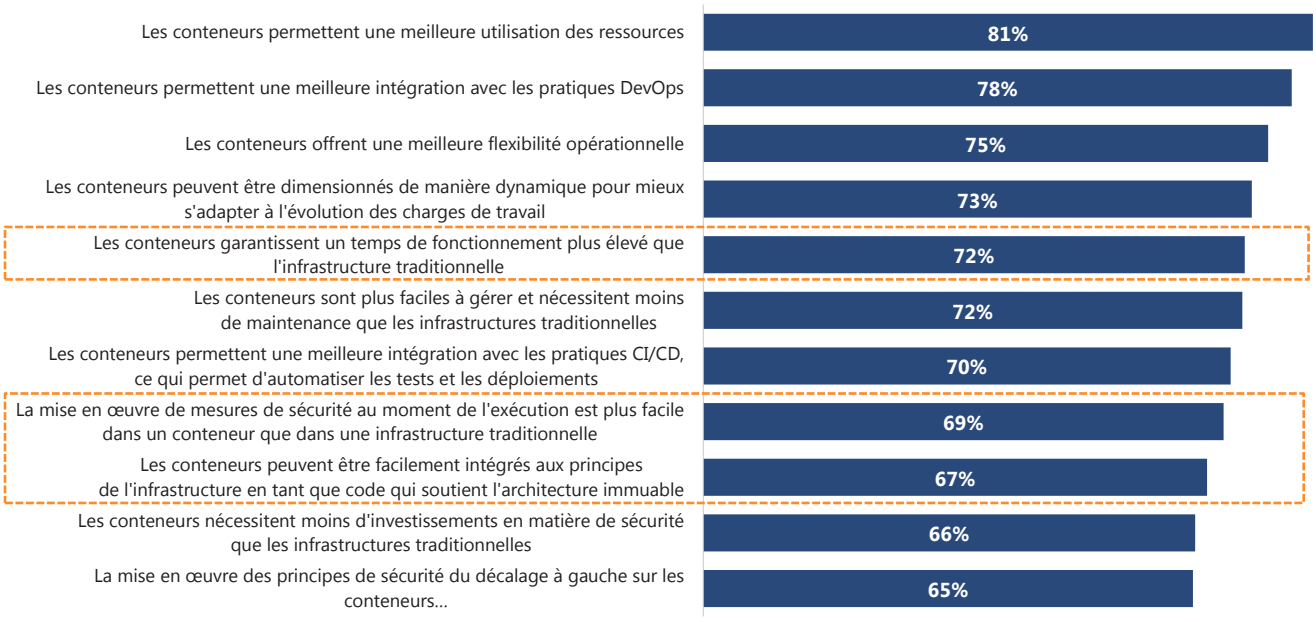


Source : Enquête de l'ISG, nombre de répondants = 310

Il convient de noter que, bien que 35 % des organisations utilisent actuellement, dans une certaine mesure, des technologies cloud natives, comme les K8, service mesh, etc., il existe une incertitude claire concernant leur adoption dans les années à venir. Celle-ci peut être attribuée non seulement à la complexité inhérente au déploiement et à la gestion des technologies susmentionnées, mais aussi aux problèmes de conformité découlant des nouvelles menaces de sécurité sophistiquées et des configurations opérationnelles décentralisées dans un environnement cloud. En outre, la volatilité associée à cet espace pose souvent des problèmes aux organisations qui peinent à suivre le rythme rapide de l'innovation, ce qui les rend finalement réticentes à réaliser des investissements importants dans ces technologies.

Cependant, la tendance à l'utilisation de technologies cloud natives démontrée par les organisations entraînera une forte demande pour plusieurs fonctionnalités de sécurité clés, comme la gestion centralisée des identités et les agents de sécurité des accès au cloud (CASB), pour améliorer la visibilité de la sécurité, la sécurité confiance zéro, les mécanismes prédictifs alimentés par l'IA et le ML permettant d'analyser synthétiquement le comportement de l'utilisateur afin de détecter et d'atténuer les attaques, les stratégies de protection des données robustes ainsi que l'intégration de plusieurs API de sécurité. En analysant plus en détail les réponses par le prisme des impératifs commerciaux, nous comprenons que plusieurs facteurs critiques, comme l'efficacité opérationnelle élevée, l'évolutivité robuste des processus et des systèmes, ainsi que la résilience accrue du réseau conduisant à une plus grande disponibilité du système et une forte intégration avec les pratiques CI/CD pour les tests et les déploiements automatisés, ont énormément contribué à l'adoption accrue des modèles de développement conteneurisés. Cette constatation est confirmée par notre étude, qui révèle que près de 81 % des entreprises estiment qu'adopter un principe opérationnel de conteneurisation leur a permis d'améliorer l'efficacité de leurs ressources. Environ 70 % des organisations estiment que les conteneurs permettent une meilleure intégration avec les pratiques CI/CD, en permettant l'automatisation des tests et du déploiement. La représentation ci-dessous permet de décoder les raisons pour lesquelles les organisations s'orientent progressivement vers des modèles de développement conteneurisés.

Tableau 10 : Facteurs d'adoption des conteneurs parmi les répondants

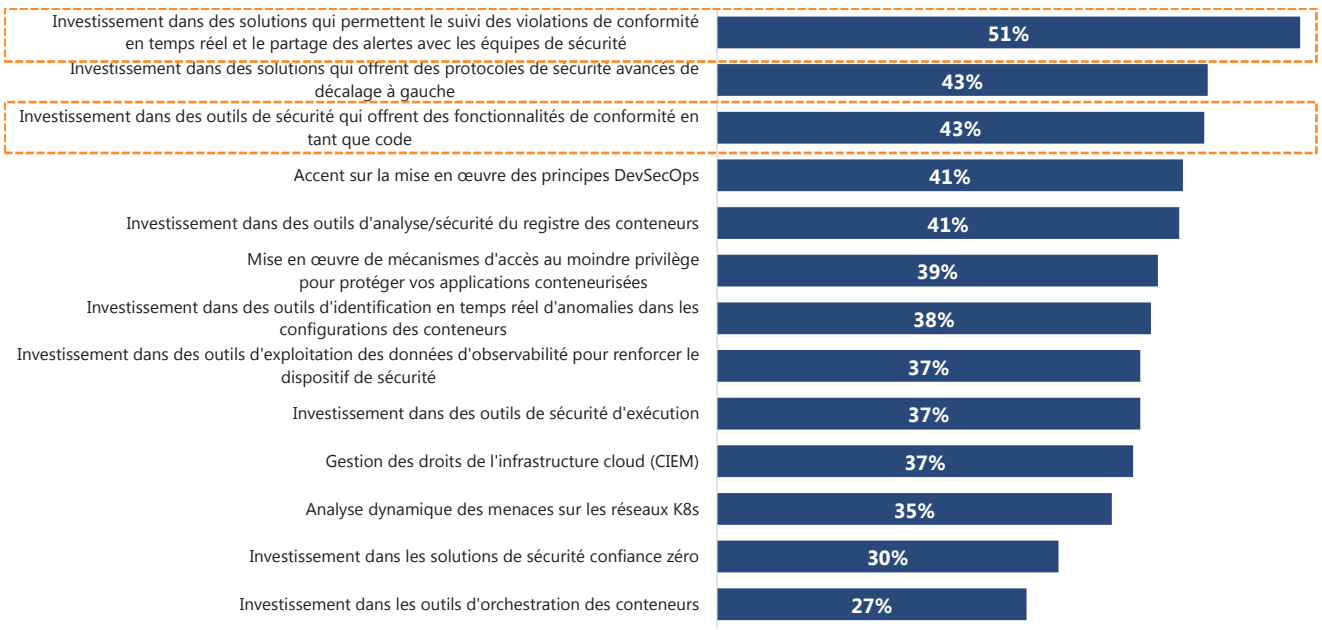


Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre spécifique parmi leurs 5 principales raisons d'adopter les conteneurs.

Cette croissance de l'adoption des technologies de conteneur oblige progressivement les organisations à adopter des plateformes de sécurité qui permettent d'analyser les vulnérabilités au niveau du code, de sécuriser les applications dans l'environnement d'exécution en utilisant les principes de sécurité du décalage à gauche, d'établir des systèmes de protection des clusters K8 et de mettre en œuvre l'accès au moindre privilège (mécanismes IAM et RBAC) pour empêcher l'abus de ressources.

Ces étapes leur permettront d'obtenir une microvisibilité de l'environnement opérationnel et de l'ensemble de la chaîne de valeur du développement. Par exemple, 51 % des sondés se disent prêts à investir dans des solutions qui dépistent les violations de conformité en temps réel et à partager les alertes avec les équipes de sécurité au cours des deux prochaines années. Pour 43 % des organisations, l'investissement dans des protocoles de sécurité shift-left est l'une des cinq priorités.

Tableau 11 : Décodage des intentions des organisations pour sécuriser leurs environnements cloud natifs



Remarque : Ce graphique montre le pourcentage d'organisations qui ont désigné un paramètre en particulier parmi leurs 5 priorités pour sécuriser leur environnement cloud natif.

Alors que les entreprises migrent de plus en plus vers le cloud et adoptent des technologies en constante évolution, la nécessité de mettre en place des mesures de sécurité complètes devient primordiale. Il est important d'avoir une stratégie de sécurité holistique pour garantir la confidentialité, l'intégrité et la disponibilité des données confidentielles grâce à l'intégration stratégique des contrôles de sécurité pour mettre en œuvre des contrôles d'accès rigoureux, des mesures de chiffrement, une surveillance continue des risques ainsi qu'une atténuation automatisée des menaces.

Principales recommandations et conclusion

Kaspersky – Un partenaire stratégique qui aide les entreprises à relever des défis complexes en matière de sécurité

L'adoption à grande échelle d'un environnement opérationnel hautement distribué dans le cloud expose les organisations à de nouveaux vecteurs de menace, ce qui appelle à investir dans des solutions permettant de protéger efficacement leur infrastructure. Notamment, parallèlement à l'adoption d'environnements cloud hybrides, les entreprises intègrent rapidement les principes de développement d'applications basées sur des conteneurs dans leurs opérations. Cette tendance a contraint les fournisseurs de solutions à affiner leurs offres de sécurité existantes, en mettant l'accent sur les points suivants :

- Identification précoce des problèmes de sécurité dans le processus de développement grâce à des approches de type décalage à gauche (shift-left).
- Analyse de la vulnérabilité au niveau du code.
- Analyse continue des conteneurs et des clusters K8.
- Analyse synthétique des menaces et identification des anomalies grâce aux comportements.
- Capacités IAC pour éviter les erreurs de configuration.
- Surveillance continue du niveau de sécurité du réseau.

Compte tenu de l'adoption rapide des environnements cloud hybrides et des technologies de conteneurisation, ainsi que des défis de sécurité auxquels les entreprises sont confrontées, Kaspersky a développé l'écosystème Kaspersky Cloud Workload Security (Kaspersky CWS). Ce système de défense complet vise à protéger de manière proactive l'infrastructure numérique des entreprises contre les différentes cybermenaces. En fusionnant Kaspersky Hybrid Cloud Security (KHCS) et Kaspersky Container Security, Kaspersky CWS va au-delà des normes de sécurité traditionnelles pour fortifier les organisations contre les cybermenaces modernes dans les environnements cloud hybrides et natifs.

Grâce à la puissance des données de Threat Intelligence en temps réel et des algorithmes ML enrichis d'une expertise humaine et d'audits des normes CIS pour l'environnement des conteneurs, la plateforme Kaspersky CWS fournit aux entreprises des mécanismes de défense robustes. Ces mesures protègent leurs charges de travail sur des hôtes, des machines virtuelles ou des conteneurs, quel que soit le déploiement dans des clouds privés, publics ou hybrides, le tout au sein d'un écosystème unifié. L'une des fonctionnalités les plus intéressantes de la plateforme Kaspersky CWS est l'intégration de la technologie Kaspersky Security for Virtualization (KSV) pour sécuriser les machines virtuelles contre les attaques de programmes malveillants.

Kaspersky CWS propose des options de déploiement flexibles dans les environnements hybrides, y compris des agents de sécurité traditionnels et KSV Light Agent, une technologie brevetée optimisée pour les clouds privés. KSV Light Agent réduit la consommation de ressources jusqu'à 30 %, en particulier pendant les mises à jour ou les « tempêtes » d'analyse, ce qui s'avère plus efficace à mesure que l'infrastructure se développe. Compatible avec les plateformes de virtualisation les plus courantes, Light Agent prend en charge Citrix, Microsoft Hyper-V, VMware, Nutanix et bien d'autres solutions.

Comme nous l'avons mentionné dans le chapitre précédent, la sécurité des environnements DevOps et des conteneurs est un défi majeur. Kaspersky CWS fournit un conteneur complet de protection de l'exécution et des images pour les installations sur site et dans le cloud (privé, public ou multicloud), quelle que soit leur taille. Son analyse comportementale des conteneurs basée sur des modèles et sa visibilité de l'environnement renforcent la sécurité et dépassent les limites des outils de visualisation intégrés.

Kaspersky CWS se distingue par l'accent mis sur l'efficacité, ainsi que l'optimisation du budget, des ressources informatiques, des délais de mise sur le marché et des heures de travail grâce à l'automatisation, à une console cloud unifiée et au Light Agent.

Pour continuer à suivre les tendances du marché, Kaspersky prévoit d'améliorer Kaspersky CWS avec des outils complets de gestion de la sécurité du cloud et des applications (CSPM et ASPM) dans les années à venir, car la société considère ces capacités comme essentielles pour les entreprises qui cherchent à sécuriser leur environnement de travail dans le cloud.

Dans le portefeuille de Kaspersky, Kaspersky CWS fait partie intégrante de la stratégie plus large de Kaspersky XDR, où toutes les données de l'écosystème remontent jusqu'à Kaspersky XDR pour permettre une détection et une réponse globales aux menaces.

Principaux avantages offerts par Kaspersky CWS

- Une protection performante conçue pour répondre aux risques de sécurité du cloud.
- Transformation numérique et migration vers le cloud plus aisées avec une sécurité prête à l'emploi et rentable.
- Protection supérieure basée sur le cloud conçue pour offrir des performances optimales dans des infrastructures complexes.
- Solution aux défis posés par les solutions traditionnelles et open source d'analyse de code et de protection des terminaux dans le domaine de la sécurité du cloud.
- Amélioration de la gestion de la sécurité dans le cloud et accélération de l'analyse des incidents, quel que soit l'environnement.

Sécuriser Kubernetes grâce à des principes de sécurité de décalage à gauche (shift-left)

Kaspersky sait que si les organisations de toutes tailles manifestent de plus en plus d'affinité pour les modèles de développement d'applications conteneurisées, elles continuent de s'inquiéter des problèmes de sécurité qui compromettent leur capacité à développer et à déployer des applications de manière sûre et harmonieuse. C'est dans cette optique que Kaspersky a développé le produit Kaspersky Container Security, qui offre des capacités de protection étendues lors de l'exécution grâce à l'utilisation de principes de sécurité de décalage à gauche. Les entreprises peuvent ainsi détecter les problèmes de sécurité à chaque étape de la chaîne de valeur, du développement à l'exploitation, ce qui réduit les retards opérationnels inutiles et leur permet d'accélérer leur processus de développement. En analysant les modèles comportementaux des vulnérabilités, Kaspersky Container Security aide les clients à obtenir des informations approfondies sur la posture de sécurité de leurs clusters de conteneurs, leur fournissant à terme un mécanisme proactif de défense contre les menaces pour leurs environnements Kubernetes. Cette microvision de l'architecture de sécurité aide les organisations à optimiser leur analyse des incidents de sécurité de manière plus automatisée, réduisant ainsi la nécessité d'une intervention manuelle importante et permettant aux utilisateurs finaux de consacrer leur capital humain à d'autres tâches essentielles.

Sécuriser les environnements hybrides grâce à la détection avancée des menaces

Dans le paysage actuel des environnements cloud hybrides, les organisations continuent à faire face à des défis qui les obligent à utiliser des plateformes de sécurité robustes pour les aider à gérer et à sécuriser efficacement leur infrastructure opérationnelle. Kaspersky Hybrid Cloud Security répond à ces problèmes en fournissant un mécanisme de défense complet. Voici les fonctionnalités offertes par le module Kaspersky Hybrid Cloud Security :

- **Stratégies robustes d'atténuation des risques :** Kaspersky Hybrid Cloud Security (KHCS) offre une protection complète contre un large éventail de cyberattaques, quelle que soit l'infrastructure de déploiement, à savoir cloud privé ou public.
- **Détection efficace des menaces :** Kaspersky Hybrid Cloud Security (KHCS) ne se contente pas d'atténuer les risques, mais donne également aux entreprises les moyens d'agir en leur offrant une visibilité granulaire sur l'ensemble de leur infrastructure. Cette visibilité accrue aide les entreprises à identifier les menaces et à y répondre de manière plus proactive et plus fluide. En outre, l'intégration de la Security Information and Event Management (SIEM) et du mécanisme Endpoint Detection and Response (EDR) renforce encore les capacités de détection des menaces.
- **Alignement avec la conformité réglementaire :** Kaspersky Hybrid Cloud Security (KHCS) aide non seulement les organisations à surmonter les complexités associées aux opérations de sécurité, mais leur permet également de se conformer aux directives réglementaires. Cette solution aide les organisations à s'y retrouver dans les complexités de la mise en conformité.
- **Amélioration des économies de coûts :** Kaspersky Hybrid Cloud Security (KHCS) ne se contente pas de renforcer la posture de sécurité, mais s'appuie également sur l'automatisation pour aider les entreprises à réduire de manière tangible les coûts opérationnels ainsi que le nombre d'heures et de personnes nécessaires aux opérations de sécurité.

Point de vue de l'ISG et perspectives

Formation des moteurs d'automatisation à la protection des ressources

Les entreprises cherchent de plus en plus à s'associer à des fournisseurs de solutions de sécurité qui utilisent des techniques d'automatisation avancées. Les technologies comme l'IA et le ML (Machine Learning) sont susceptibles de jouer un rôle central pour aider les utilisateurs finaux à détecter les vulnérabilités potentielles de leur infrastructure opérationnelle, à réglementer l'accès aux ressources critiques, à reconnaître les vulnérabilités aux premiers stades du développement des applications et à traiter les risques avant qu'ils ne se transforment en menaces véritables. Cependant, nous observons qu'en raison de l'introduction de suites d'hyperautomatisation, les entreprises sont souvent confrontées à un grand nombre de faux négatifs ou de faux positifs. Les entreprises font souvent face à des problèmes d'interopérabilité lors de l'intégration d'une solution de sécurité à forte composante d'automatisation dans leur infrastructure opérationnelle. Cette ambiguïté des informations limite la visibilité des organisations sur leur situation en matière de sécurité et les empêche de prendre les mesures correctives nécessaires pour renforcer leur architecture de sécurité. Les fournisseurs de solutions doivent impérativement mettre constamment à jour leurs bibliothèques de menaces et former leurs moteurs d'IA à minimiser l'ambiguïté de leurs opérations.

Augmentation potentielle de l'intégration de plateformes de Threat Intelligence indépendantes à l'infrastructure cloud

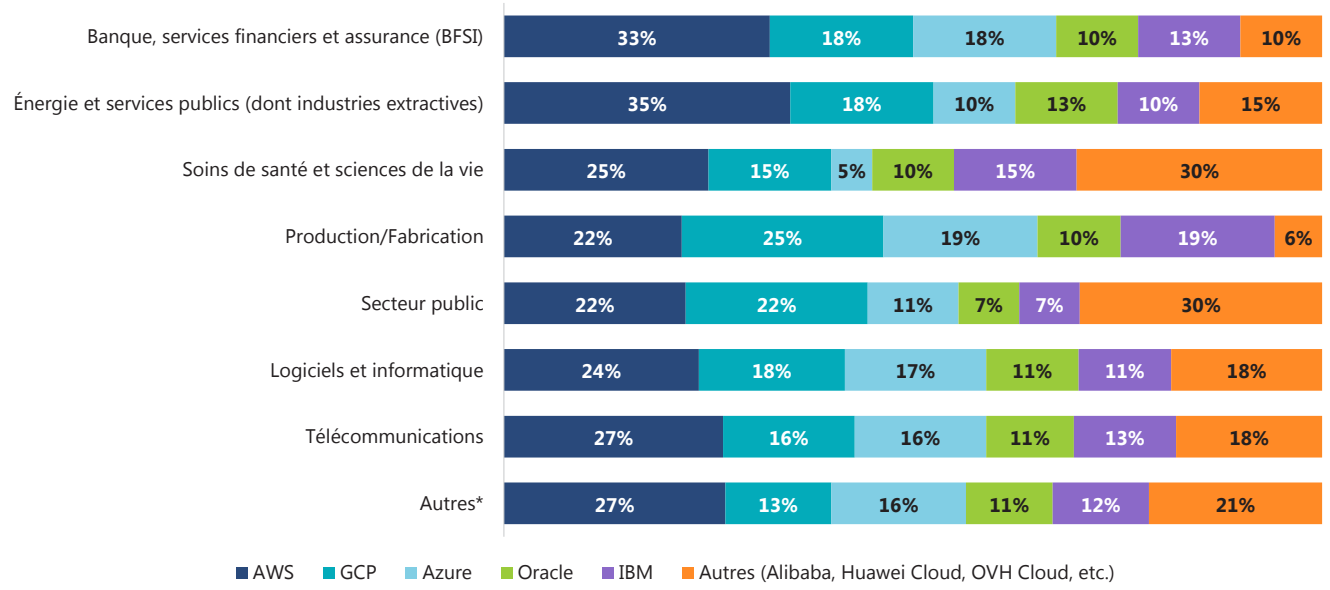
Si la technologie cloud offre une évolutivité, une souplesse et une accessibilité inégalées, elle introduit également un large éventail de risques qui nécessitent une évaluation critique. À mesure que les entreprises adoptent des environnements cloud hybrides, la gestion des aspects de la sécurité sous leur contrôle, comme l'accès aux données et la configuration, deviendra essentielle. Nous prévoyons un scénario dans lequel l'intégration de flux de Threat Intelligence personnalisés pour les services cloud hybrides sera déterminante pour faire progresser la sophistication de l'analyse des itinéraires des menaces dans les environnements cloud. L'indisponibilité d'outils de sécurité indépendants de l'infrastructure oblige les entreprises à s'associer à différents fournisseurs de solutions de sécurité pour sécuriser leurs environnements physiques et cloud de manière isolée, ce qui réduit leur capacité à appréhender leur infrastructure de sécurité dans l'environnement cloud hybride par le biais d'une plateforme unique. Les organisations peuvent obtenir une vision nuancée du paysage dynamique des menaces spécifiques aux plateformes cloud hybrides en utilisant des flux de Threat Intelligence personnalisés, ce qui réduit la nécessité d'investir dans de multiples plateformes de sécurité. Il s'agit d'accéder en temps réel à des informations riches en contexte sur les menaces, y compris des détails sur leurs origines, leurs tactiques, leurs techniques et leurs procédures.

Demande croissante de solutions de sécurité dans le cloud propres à l'industrie

L'adoption de services et de plateformes cloud pour l'industrie devrait connaître une croissance régulière dans les années à venir. Les industries affichent généralement des comportements distincts en matière d'opérations, de confidentialité des données et d'exigences réglementaires. Cette tendance souligne le besoin pressant pour les fournisseurs de solutions de sécurité tierces d'évoluer et de concevoir des solutions personnalisées pour répondre aux exigences uniques d'industries particulières. Cette approche les aidera à proposer des offres qui complètent diverses normes réglementaires particulières à l'industrie, comme HIPPA, FedRAMP et PCI DSS. Alors que les entreprises continuent à faire face aux complexités de la conformité, les solutions de sécurité dans le cloud propres à l'industrie pourraient jouer un rôle essentiel pour assurer une meilleure adhésion aux cadres réglementaires et positionner les entreprises pour un succès durable dans le paysage dynamique de l'informatique dans le cloud.

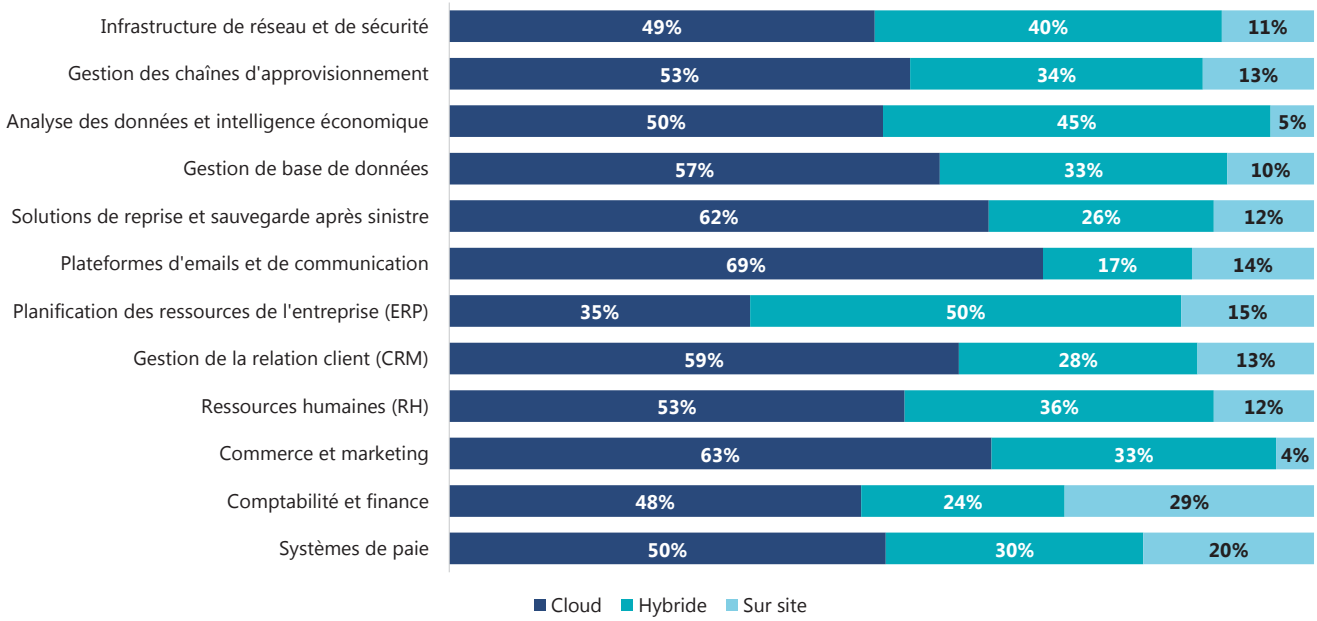
Annexe – Impératifs de l'industrie

Analyse des partenariats avec les fournisseurs de clouds publics par industrie



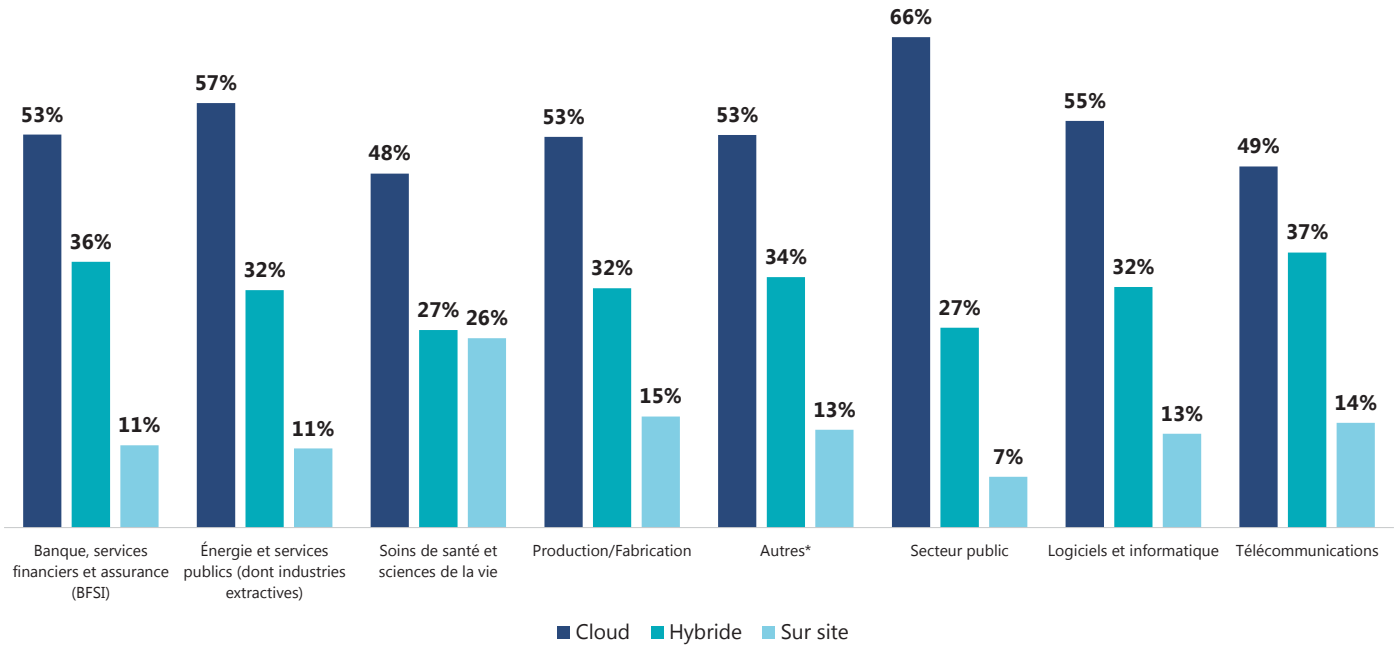
Remarque : Les autres* comprennent les médias et les divertissements, la vente au détail et les biens de consommation courante, les voyages, les transports et la logistique.

Part des répondants selon leur choix d'infrastructure préférée pour les charges de travail



Source : Enquête de l'ISG, nombre de répondants = 310

Décodage du choix de l'environnement opérationnel par industrie



Source : Enquête de l'ISG, nombre de répondants = 310

Banque, services financiers et assurance (BFSI)

3 enjeux principaux liés à la solution de sécurité actuelle	3 principales priorités pour renforcer la sécurité du cloud	3 meilleures façons de renforcer l'environnement cloud natif
❑ Incapacité à utiliser les technologies d'IA/ML pour filtrer efficacement les alertes et réduire les faux positifs.	❑ Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.	❑ Investissement dans une solution qui suit les violations de conformité en temps réel et partage les alertes avec les équipes de sécurité.
❑ Manque de capacités d'analyse des causes profondes (RCA) pour identifier les origines des problèmes de sécurité.	❑ Investissement dans des outils de sécurité de la charge de travail dans le cloud (CWS) qui tirent parti de techniques d'automatisation avancées.	❑ Accent sur la mise en œuvre des principes DevSecOps.
	❑ Investissement dans des outils de réponse aux incidents et de reprise après sinistre reposant sur l'IA/ML.	❑ Analyse dynamique des menaces sur les réseaux K8s.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Énergie et services publics (dont industries extractives)

3 enjeux principaux liés à la solution de sécurité actuelle

- Difficultés à identifier les vulnérabilités et les risques par une analyse continue, ce qui entraîne des zones d'ombre potentielles.
- Manque d'évaluations complètes de la conformité de la sécurité pour les différentes normes et réglementations.
- Absence de mécanisme d'analyse de l'itinéraire de la menace permettant de suivre et de comprendre les voies d'attaque.

3 principales priorités pour renforcer la sécurité du cloud

- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans les capacités de l'IAC pour renforcer le CSPM.
- Utilisation des technologies trompeuses pour identifier et neutraliser de manière proactive les menaces.

3 meilleures façons de renforcer l'environnement cloud natif

- Investissement dans une solution qui suit les violations de conformité en temps réel et partage les alertes avec les équipes de sécurité.
- Investissement dans des outils de sécurité qui offrent des fonctionnalités de conformité en tant que code.
- Accent sur la mise en œuvre des principes DevSecOps.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Soins de santé et sciences de la vie

3 enjeux principaux liés à la solution de sécurité actuelle

- Difficultés à identifier les vulnérabilités et les risques par une analyse continue, ce qui entraîne des zones d'ombre potentielles.
- Absence de mécanisme d'analyse de l'itinéraire de la menace permettant de suivre et de comprendre les voies d'attaque.
- Incapacité à surveiller et à prévenir de manière proactive les erreurs de configuration des ressources au moment de l'exécution

3 principales priorités pour renforcer la sécurité du cloud

- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans des outils de réponse aux incidents et de reprise après sinistre reposant sur l'IA/ML.
- Investissement dans des solutions CWS qui offrent une surveillance continue et des capacités de réponse automatisée.

3 meilleures façons de renforcer l'environnement cloud natif

- Investissement dans des outils d'analyse/sécurité du registre des conteneurs.
- Investissement dans des outils d'exploitation des données d'observabilité pour renforcer le dispositif de sécurité.
- Investissement dans des outils d'identification en temps réel d'anomalies dans les configurations des conteneurs.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Production/Fabrication

3 enjeux principaux liés à la solution de sécurité actuelle

- Protection inadéquate contre les accès non autorisés et les abus de ressources (par exemple, absence de contrôle d'accès basé sur le rôle [RBAC]).
- Manque d'évaluations complètes de la conformité de la sécurité pour les différentes normes et réglementations.
- Manque de capacités d'analyse des causes profondes (RCA) pour identifier les origines des problèmes de sécurité.

3 principales priorités pour renforcer la sécurité du cloud

- Exploitation des solutions CDR (Cloud Detection and Response) pour une détection et une réponse automatisées.
- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans une solution CWS qui exploite des techniques d'automatisation avancées.

3 meilleures façons de renforcer l'environnement cloud natif

- Investissement dans une solution qui suit les violations de conformité en temps réel et partage les alertes avec les équipes de sécurité.
- Accent sur la mise en œuvre des principes DevSecOps.
- Gestion des droits de l'infrastructure cloud (CIEM).

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Secteur public

3 enjeux principaux liés à la solution de sécurité actuelle

- Mauvaise intégration avec les protocoles de sécurité existants du fournisseur de services dans le cloud (CSP).
- Protection inadéquate contre les accès non autorisés et les abus de ressources (par exemple, absence de contrôle d'accès basé sur le rôle [RBAC]).
- Manque d'évaluations complètes de la conformité de la sécurité pour les différentes normes et réglementations.

3 principales priorités pour renforcer la sécurité du cloud

- Investissement dans des solutions CWS qui offrent une surveillance continue et des capacités de réponse automatisée.
- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans les capacités de l'IAC pour renforcer le CSPM.

3 meilleures façons de renforcer l'environnement cloud natif

- Mise en œuvre de mécanismes d'accès au moindre privilège pour protéger vos applications conteneurisées.
- Investissement dans des outils d'identification en temps réel d'anomalies dans les configurations des conteneurs.
- Investissement dans des solutions qui offrent des protocoles de sécurité avancés de décalage à gauche.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Télécommunications

3 enjeux principaux liés à la solution de sécurité actuelle

- Manque d'évaluations complètes de la conformité de la sécurité pour les différentes normes et réglementations.
- Incapacité à utiliser les technologies d'IA/ML pour filtrer efficacement les alertes et réduire les faux positifs.
- Mauvaise intégration avec les protocoles de sécurité existants du fournisseur de services dans le cloud (CSP).

3 principales priorités pour renforcer la sécurité du cloud

- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans des outils CWS qui offrent des solutions de sécurité multicloud et hybrides.

3 meilleures façons de renforcer l'environnement cloud natif

- Gestion des droits de l'infrastructure cloud (CIEM).
- Investissement dans des outils de sécurité qui offrent des fonctionnalités de conformité en tant que code.
- Investissement dans une solution qui suit les violations de conformité en temps réel et partage les alertes avec les équipes de sécurité.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Logiciels et informatique

3 enjeux principaux liés à la solution de sécurité actuelle

- Incapacité à utiliser les technologies d'IA/ML pour filtrer efficacement les alertes et réduire les faux positifs.
- Difficultés à identifier les vulnérabilités et les risques par une analyse continue, ce qui entraîne des zones d'ombre potentielles.
- Absence de mécanisme d'analyse de l'itinéraire de la menace permettant de suivre et de comprendre les voies d'attaque.

3 principales priorités pour renforcer la sécurité du cloud

- Investissement dans des outils de sécurité de la charge de travail dans le cloud (CWS) qui tirent parti de techniques d'automatisation avancées.
- Investissement dans une plateforme CWS unifiée qui protège les terminaux, les serveurs et les charges de travail dans le cloud à l'aide d'une plateforme unique.
- Investissement dans des outils de réponse aux incidents et de reprise après sinistre reposant sur l'IA/ML.

3 meilleures façons de renforcer l'environnement cloud natif

- Investissement dans une solution qui suit les violations de conformité en temps réel et partage les alertes avec les équipes de sécurité.
- Investissement dans des solutions qui offrent des protocoles de sécurité avancés de décalage à gauche.
- Investissement dans des outils d'exploitation des données d'observabilité pour renforcer le dispositif de sécurité.

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

Analyse des 3 principaux avantages des solutions de conteneurs pour chaque industrie

Banque, services financiers et assurance (BFSI)	Énergie et services publics (dont industries extractives)	Soins de santé et sciences de la vie	Production/ Fabrication	Secteur public	Logiciel et informatique	Télécommunications
Les conteneurs permettent une meilleure intégration avec les pratiques DevOps	Les conteneurs permettent une meilleure intégration avec les pratiques DevOps	Les conteneurs offrent une meilleure flexibilité opérationnelle	Les conteneurs permettent une meilleure utilisation des ressources	Les conteneurs permettent une meilleure intégration avec les pratiques DevOps	Les conteneurs permettent une meilleure utilisation des ressources	Les conteneurs permettent une meilleure utilisation des ressources
Les conteneurs peuvent être dimensionnés de manière dynamique pour mieux s'adapter à l'évolution des charges de travail	Les conteneurs permettent une meilleure utilisation des ressources	Les conteneurs sont plus faciles à gérer et nécessitent moins de maintenance que les infrastructures traditionnelles	Les conteneurs permettent une meilleure intégration avec les pratiques DevOps	Les conteneurs permettent une meilleure utilisation des ressources	Les conteneurs garantissent un temps de fonctionnement plus élevé que l'infrastructure traditionnelle	Les conteneurs permettent une meilleure intégration avec les pratiques DevOps
Les conteneurs offrent une meilleure flexibilité opérationnelle	Les conteneurs peuvent être dimensionnés de manière dynamique pour mieux s'adapter à l'évolution des charges de travail	Les conteneurs permettent une meilleure utilisation des ressources	Les conteneurs peuvent être dimensionnés de manière dynamique pour mieux s'adapter à l'évolution des charges de travail	Les conteneurs peuvent être facilement intégrés aux principes de l'infrastructure en tant que code (IAC) qui soutient l'architecture immuable	Les conteneurs offrent une meilleure flexibilité opérationnelle	Les conteneurs offrent une meilleure flexibilité opérationnelle

Remarque : Les modules ont été classés par ordre de priorité. L'élément le plus haut a la priorité la plus élevée.

À propos des auteurs

Shashank Rajmane

Directeur et analyste principal
à l'ISG

Shashank Rajmane a plus de dix ans d'expérience dans le domaine de la recherche et travaille comme analyste principal à l'ISG. Il dirige les efforts des études ISG Provider Lens™ – Public Cloud Services & Solutions and Private/Hybrid Cloud & Data Center Outsourcing Services. Il est également l'auteur des rapports américain et mondial. En outre, Shashank a participé à de nombreuses missions de conseil et aidé les entreprises clientes de l'ISG à élaborer leur stratégie cloud et à sélectionner les bons prestataires de services/fournisseurs en fonction de leurs besoins d'achat en informatique. Il est l'auteur de plusieurs livres blancs, articles de leadership éclairé, notes d'information, blogs et rapports d'information sur les prestataires de services, en particulier dans le domaine des services d'infrastructure et de cloud hybride de nouvelle génération. Shashank a également animé plusieurs ateliers, webinars et podcasts et a été cité dans des revues informatiques.

Partha Chakraborty

Analyste principal
à l'ISG

Partha est analyste principal à l'ISG et dirige l'étude ISG Provider Lens Multi-Public Cloud Solutions Study. Il dispose d'une solide expérience en matière de recherche commerciale et technologique, de positionnement des fournisseurs, etc. Partha gère également les opérations de la division Custom Research de l'ISG. Il présente des récits d'entreprises autour de divers impératifs stratégiques, comme la préparation technologique des PME, les principes de fabrication numérisée, la mobilité intelligente, les écosystèmes sans numéraire et la gouvernance numérique, et commente souvent des sujets comme le cloud, les jumeaux numériques, la blockchain et les mesures disruptives en matière de cybersécurité.

Tanya Varshney

Analyste de recherche
à l'ISG

Tanya est une analyste de recherche spécialisée dans la recherche transversale, avec un accent particulier sur les innovations disruptives et les technologies de convergence dans les secteurs de la vente au détail, de la banque et des soins de santé. Tanya a plus de 4 ans d'expérience dans l'industrie de la recherche technologique et à son poste précédent, elle a effectué des recherches primaires et secondaires dédiées à l'IA et à l'analytique. À l'ISG, Tanya est membre de l'équipe de recherche personnalisée, où elle contribue activement à un portefeuille diversifié d'engagements et de projets personnalisés. Elle est responsable de la série Digital Innovator, consacrée à l'analyse et à l'évaluation d'innovateurs numériques moins connus dans diverses industries.

Résumé

kaspersky

Siège social

Moscou

Chiffre d'affaires

752 M $

Nombre d'employés

Plus de 5 000

Portefeuille de services

Sécurité du cloud hybride, services de cybersécurité, gestion et défense des menaces, sécurité des terminaux

À propos de Kaspersky

Kaspersky est une entreprise mondiale de cybersécurité et de protection de la vie privée numérique fondée en 1997. Kaspersky s'appuie sur sa Threat Intelligence et son expertise en matière de sécurité informatique pour développer des solutions destinées aux entreprises, aux infrastructures critiques, aux gouvernements et aux utilisateurs du monde entier. Le portefeuille de solutions de cybersécurité complet de l'entreprise comprend une protection des terminaux de haut niveau, des produits et services de sécurité spécialisés, ainsi que des solutions de cyberimmunité pour lutter contre les menaces numériques sophistiquées et en constante évolution. Plus de 400 millions d'utilisateurs sont protégés par les technologies de Kaspersky et nous aidons plus de 220 000 clients professionnels à protéger ce qui compte le plus à leurs yeux.

Plus d'informations sur : **www.kaspersky.fr**

À propos de l'ISG

L'ISG (Information Services Group) (Nasdaq : III) est une société de recherche et de conseil technologiques de premier plan à l'international. Partenaire de confiance de plus de 900 clients, dont plus de 75 des 100 premières entreprises mondiales, l'ISG s'engage à aider les entreprises, les organisations du secteur public ainsi que les fournisseurs de services et de technologies à atteindre l'excellence opérationnelle et à accélérer leur croissance. L'entreprise est spécialisée dans les services de transformation numérique, y compris l'IA et l'automatisation, le cloud et l'analyse de données, le conseil en sourcing, les services de gouvernance et de risque gérés, les services d'opérateurs de réseau, la conception de stratégies et d'opérations, la gestion du changement, l'intelligence de marché, et la recherche et l'analyse technologiques. Fondé en 2006 et basé à Stamford, Connecticut, l'ISG emploie 1 600 professionnels prêts pour le numérique, opérant dans plus de 20 pays. Il s'agit d'une équipe mondiale, connue pour sa pensée innovante, son influence sur le marché, son expertise approfondie de l'industrie et de la technologie, et ses capacités de recherche et d'analyse de classe mondiale fondées sur les données de marché les plus complètes de l'industrie.

Pour en savoir plus, consultez le site **www.isg-one.com.**