Enterprise Strategy Group™ by TechTarget

LIVRE BLANC

Stimuler la croissance de l'entreprise en sécurisant les environnements hybrides et multicloud

Gérer efficacement la sécurité pour soutenir la transformation numérique

Par Melinda Marks, Directrice,
Cybersecurity Enterprise Strategy Group

Octobre 2023

Ce livre blanc d'Enterprise Strategy Group a été réalisé à la demande de Cisco.
Il est distribué sous licence de TechTarget Inc.

Sommaire

Introduction

Aujourd'hui, les entreprises sont sommées de passer au numérique pour optimiser leur productivité et gagner un avantage concurrentiel. C'est pourquoi elles font migrer de plus en plus d'applications vers le cloud afin d'accélérer les capacités de développement logiciel sans avoir à se soucier du provisionnement des serveurs ni du matériel. Elles doivent également prendre en charge le télétravail pour offrir plus de flexibilité et de capacités d'évolution à leurs équipes. Au cours de leur transformation numérique, les entreprises font face à une complexité IT croissante. En effet, les applications sont désormais distribuées dans des environnements hybrides et multicloud, et la plupart des équipes sont décentralisées.

Cette tendance crée de nouvelles exigences en matière de sécurité, car celle-ci doit s'adapter à tous les environnements applicatifs et favoriser la croissance de l'entreprise. Le système de sécurité doit être en mesure de prendre en charge les applications et les utilisateurs dans divers environnements, avec leurs propres architectures, fonctionnalités et capacités. Les équipes de sécurité ont également besoin de flexibilité pour s'adapter à l'évolution des besoins de l'entreprise, notamment la croissance organique de l'activité et les acquisitions.

Malheureusement, elles font face à de nombreux défis pour adapter leurs stratégies à l'utilisation croissante des services cloud et au développement cloud natif. Elles manquent de visibilité notamment à cause de la nature éphémère des ressources cloud et des changements d'échelle rapides de l'infrastructure. Il est également difficile pour les équipes de sécurité de suivre l'accélération de la productivité des développeurs et de bloquer les menaces liées à la prolifération des accès et des autorisations.

De nombreuses entreprises tentent de relever ces défis en utilisant plusieurs solutions ou plateformes de sécurité, mais elles sont fréquemment confrontées à des incidents liés à des problèmes courants, notamment une mauvaise configuration ou un surprovisionnement des accès. Les angles morts et les écarts entre les outils créent également des problèmes de visibilité. En outre, même si leurs outils les alertent sur les vulnérabilités, les équipes de sécurité ne parviennent souvent pas à hiérarchiser et à résoudre les problèmes critiques à temps pour protéger les applications contre les attaques. Plus les ressources et les applications prolifèrent dans les environnements cloud, plus les défis se multiplient.

Les équipes de sécurité ont besoin d'une stratégie efficace pour sécuriser les applications dans tous les environnements, en offrant une visibilité totale et une protection des accès capable de prendre en charge la mobilité des workloads. Ce livre blanc examine les éléments clés d'une approche efficace de la sécurité des applications, suffisamment flexible pour à la fois prendre en charge la croissance rapide de l'entreprise et répondre aux exigences des environnements hybrides et multicloud.

Les entreprises doivent opter pour une approche flexible qui aide les équipes de sécurité, quelles que soient leurs compétences, à fournir une visibilité complète sur les ressources afin d'assurer une remédiation efficace des vulnérabilités et une approche Zero Trust pour protéger les applications contre les attaques dans tous les environnements. Cette approche doit inclure la détection rapide des problèmes de sécurité, ainsi que des informations contextualisées et une Threat Intelligence pour classer les mesures en fonction de leur impact sur la réduction des risques. Elle doit également fournir des moyens simplifiés et centralisés de définir des politiques pour protéger les ressources.

Avec une approche qui prend en charge les applications et l'accès dans leurs environnements multicloud et hybrides interconnectés et dynamiques, les équipes de sécurité peuvent optimiser les ressources et l'exploitation afin de gérer efficacement les risques et de répondre rapidement aux menaces. Une telle approche leur permet également d'évoluer efficacement pour accélérer les capacités de développement et la croissance de l'entreprise.

Les défis de la transformation numérique pour la sécurité

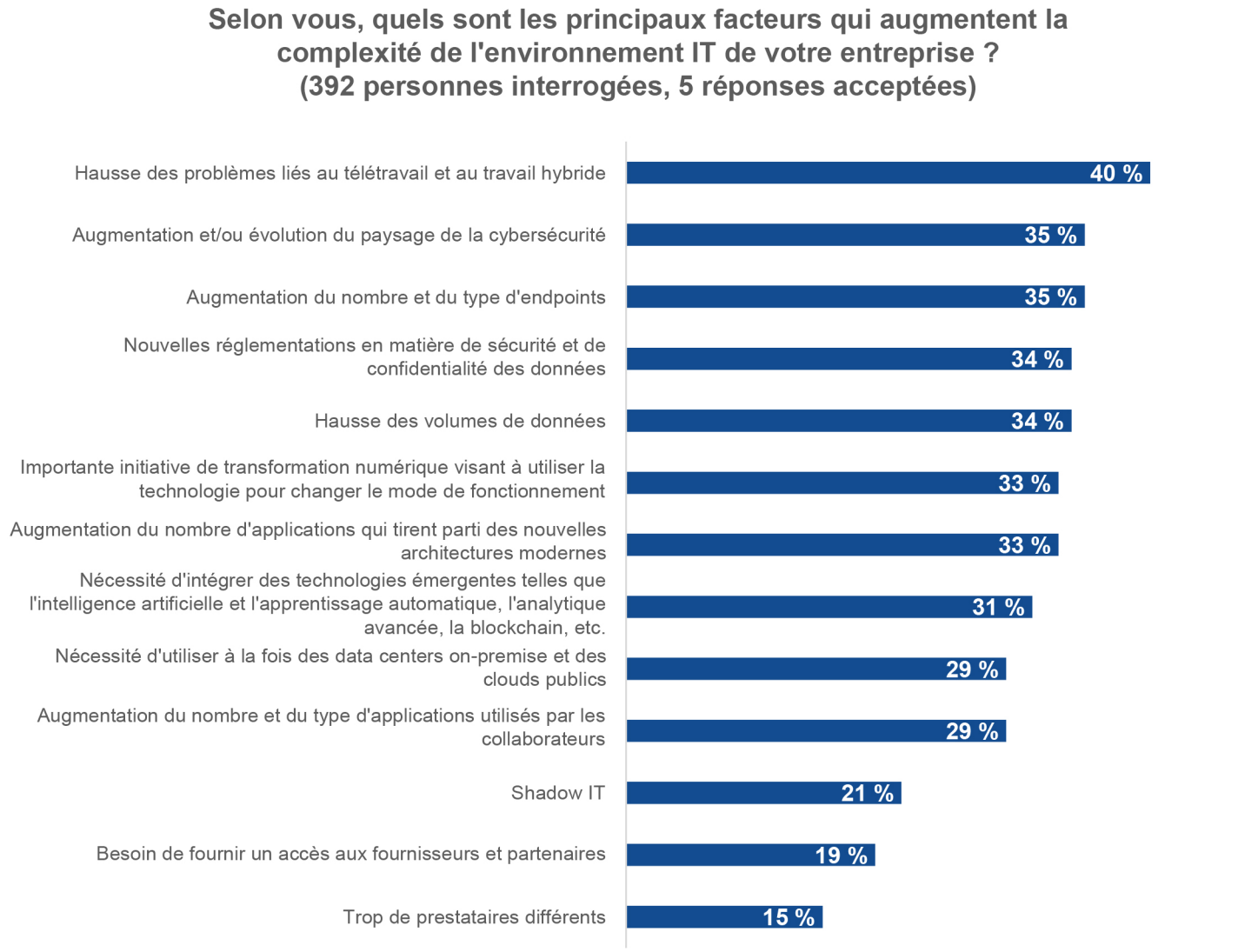
Les études de la division Enterprise Strategy Group de TechTarget illustrent de nouveaux défis pour les équipes de sécurité. Elles citent notamment l'accroissement de la complexité dans les environnements IT, la multiplication du nombre d'applications cloud natives résultant de la productivité accrue des développeurs et le manque de visibilité sur les divers clouds publics. Tous ces facteurs entraînent un large éventail d'incidents liés à la sécurité. Les équipes de sécurité ont besoin d'une stratégie efficace pour relever ces défis et permettre à l'entreprise de se développer tout en assurant la sécurité des applications dans les différents environnements, le tout, sans compétences spécialisées.

La complexification de l'IT

À mesure que les entreprises tirent parti de la transformation numérique pour augmenter leur productivité et acquérir un avantage concurrentiel, elles créent de la complexité et de nouveaux besoins en matière d'IT et de sécurité. Selon une étude d'Enterprise Strategy Group, plus de la moitié (53 %) des entreprises déclarent que leur environnement IT est plus, voire beaucoup plus, complexe qu'il y a deux ans[1]. Parmi elles, 40 % citent l'augmentation du travail à distance et hybride comme premier facteur de complexification. Les autres raisons les plus mentionnées incluent notamment l'évolution de la cybersécurité (35 %), l'augmentation du nombre et des types d'endpoints (35 %), les nouvelles réglementations en matière de sécurité et de confidentialité des données (34 %) et l'augmentation des volumes de données (34 %). Plus bas dans la liste, 29 % des entreprises interrogées mentionnent la nécessité d'utiliser à la fois des data centers on-premise et des fournisseurs de cloud public (voir la Figure 1).

[1] Rapport d'étude Enterprise Strategy Group, *Enquêtes sur les dépenses IT prévues en 2023*, novembre 2022

Figure 1. Facteurs à l'origine de la complexité IT



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Il existe des moyens efficaces de soutenir la croissance et l'évolutivité de l'entreprise, même si la complexité augmente dans plusieurs domaines.

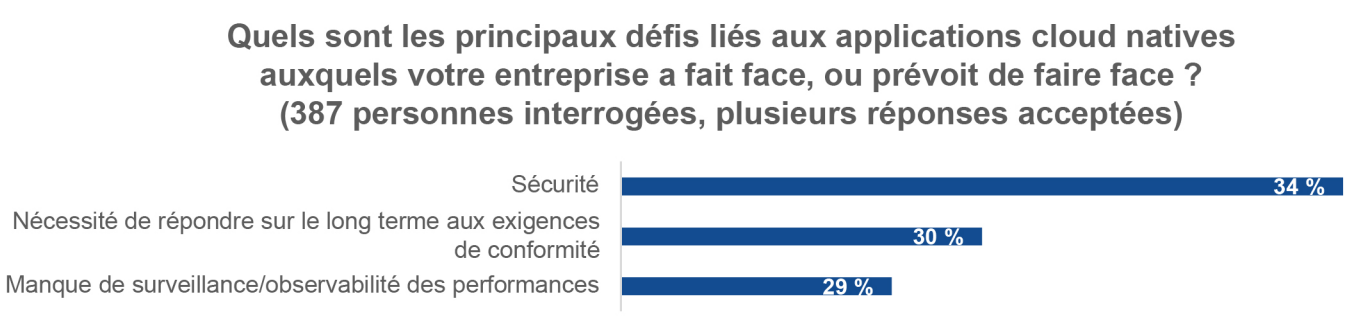
La migration des applications vers les environnements cloud

Les entreprises s'appuient également de plus en plus sur l'infrastructure de cloud public pour gagner en productivité et innover grâce au développement cloud natif. Elles n'ont pas à se soucier de l'infrastructure sous-jacente ni de la maintenance, et profitent d'économies d'échelle grâce aux modèles « pay-as-you go » proposés par les fournisseurs de services cloud (CSP).

Selon une étude sur les tendances en matière de modernisation de l'infrastructure applicative menée par Enterprise Strategy Group, 88 % des entreprises interrogées exécutent des workloads de production sur des plateformes/infrastructures de cloud public. Elles sont aussi de plus en plus nombreuses à faire migrer leurs workloads de production vers le cloud[2]. L'étude montre aussi que les entreprises qui font migrer leurs applications dans le cloud obtiennent de nombreux avantages, notamment une plus grande agilité, des coûts d'infrastructure réduits et un déploiement plus rapide.

Le cloud permet par ailleurs l'adoption de pratiques DevOps. Les équipes de développement peuvent ainsi provisionner leur propre infrastructure au lieu d'attendre que les équipes IT ou d'exploitation provisionnent les serveurs. Les développeurs travaillent plus efficacement et produisent plus vite de la valeur qu'avec les méthodes de développement d'applications classiques. Cependant, l'augmentation de la productivité du développement logiciel crée des problèmes de sécurité et de conformité au niveau des applications cloud natives.

Figure 2. Les trois principaux défis auxquels les entreprises sont confrontées avec les applications cloud natives



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Les entreprises ont besoin d'une solution efficace pour gérer les risques liés à la sécurité afin de favoriser le passage au développement cloud natif, d'augmenter le nombre de versions des applications et d'accélérer leur lancement. Les équipes de sécurité capables d'optimiser l'efficacité pour prendre en charge ce niveau d'évolutivité et de croissance, sans bloquer l'adoption des nouvelles technologies susceptibles d'augmenter la productivité et l'innovation des développeurs, peuvent jouer un rôle important dans l'amélioration des résultats de l'entreprise.

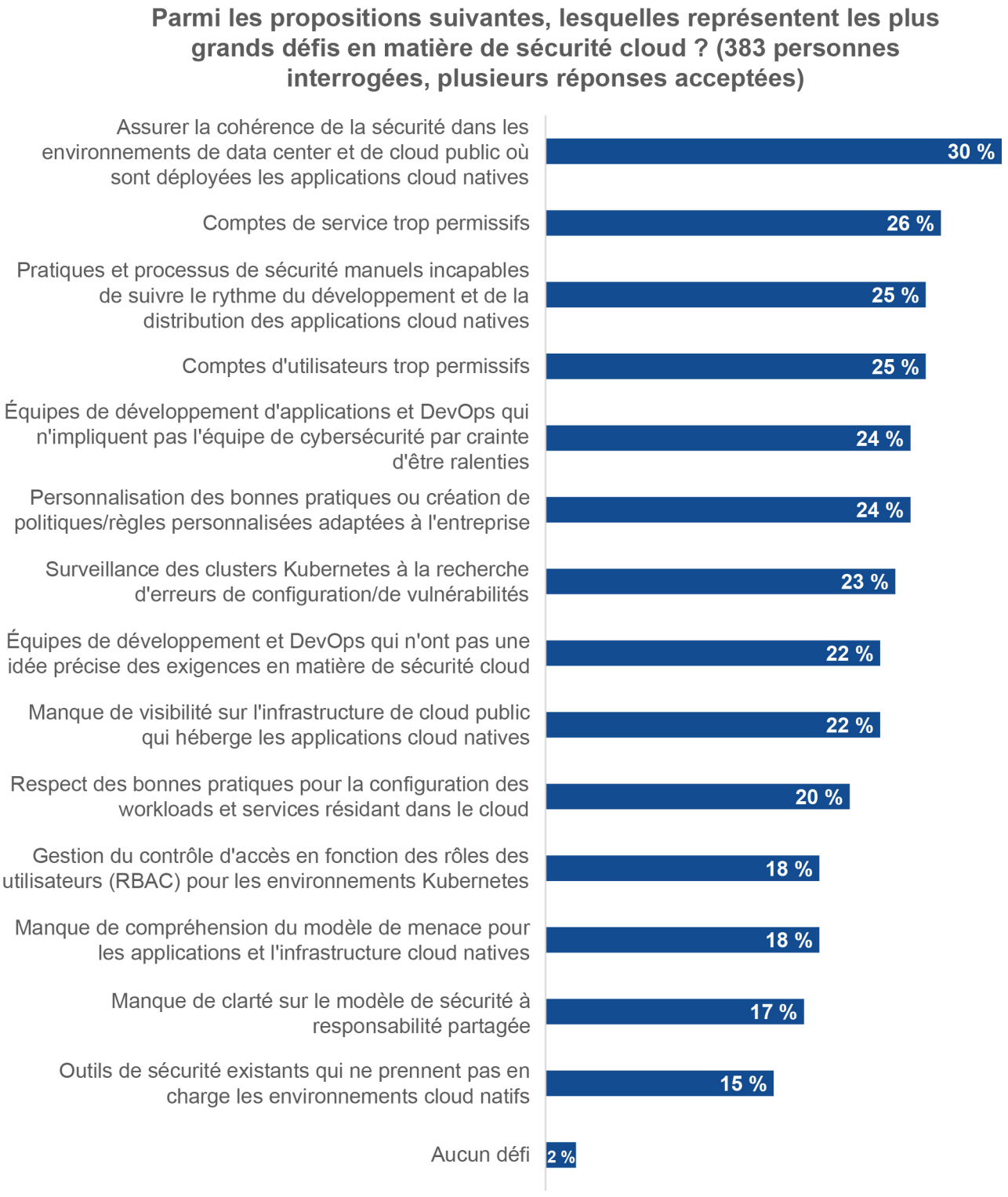
[2] Source : rapport d'étude Enterprise Strategy Group, *Applications cloud natives*, mai 2022

La sécurité des environnements multicloud

Pour favoriser la croissance dans les environnements cloud, les équipes de sécurité doivent également prendre en charge les environnements multicloud. Une étude menée par Enterprise Strategy Group sur la gestion de la sécurité dans le cloud montre que la plupart des entreprises (94 %) font appel à plusieurs fournisseurs de services d'infrastructure cloud, et que parmi elles, la majorité (69 %) en utilise au moins trois[3]. Bien que 68 % des entreprises déclarent disposer de solutions robustes de gestion de la sécurité dans le cloud, elles font état de diverses difficultés. Elles peinent principalement à obtenir la visibilité et le contrôle nécessaires pour gérer efficacement les risques pour l'ensemble de leurs environnements et de leurs équipes, notamment pour assurer la cohérence de la sécurité dans le data center et les environnements cloud (30 %). Parmi les autres défis figurent les comptes de service et d'utilisateurs trop permissifs (cités par 25 % et 26 %, respectivement), les pratiques et les processus de sécurité manuels qui ne suivent pas le rythme de la distribution d'applications cloud natives (25 %), le manque d'implication et de contrôle sur les processus de développement (24 %), le manque de visibilité sur l'infrastructure de cloud public (22 %) et une compréhension insuffisante des menaces cloud natives (18 %) (Figure 3)[4].

[3] Source : rapport d'étude Enterprise Strategy Group, *Cloud Entitlements and Posture Management Trends*, avril 2023.
[4] Ibid.

Figure 3. Les plus grands défis en matière de sécurité cloud pour les entreprises



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Les entreprises ont besoin d'une approche efficace pour relever ces défis, afin de protéger leurs applications dans tous les environnements. Pour cela, elles nécessitent plus de visibilité et de contrôle sur les applications, où qu'elles se trouvent. Elles ont besoin de les visualiser comme si elles résidaient dans un même environnement interconnecté et dynamique plutôt que dans des environnements distincts. Le regroupement des informations provenant d'environnements multicloud et hybrides augmente l'efficacité des opérations de sécurité, ce qui limite les risques et accélère la réponse aux menaces. Il s'agit de la seule façon de faire évoluer la sécurité pour soutenir la croissance de l'entreprise dans un environnement cloud de plus en plus important.

Des incidents liés à la sécurité aussi nombreux que variés

Bien que les entreprises aient généralement mis en place plusieurs solutions de sécurité, la plupart d'entre elles ont fait face à des incidents impliquant leur infrastructure ou leurs applications cloud natives. Plus précisément, l'étude montre que 94 % des entreprises ont déclaré avoir été victimes d'attaques et/ou de déplacements latéraux au cours des 12 derniers mois : vol d'identifiants (29 %), exploitation d'une mauvaise configuration (29 %), perte de données suite à une utilisation non sécurisée des API (24 %), ransomwares (16 %) (Figure 4)[5].

Ces incidents se sont produits soit parce que les entreprises n'étaient pas au courant de leur niveau d'exposition au risque, soit parce qu'elles n'ont pas été en mesure de résoudre les problèmes de sécurité à temps pour déjouer ou limiter les attaques. Ce phénomène souligne la nécessité d'une visibilité sur tous les environnements, ainsi que d'une approche globale pour favoriser l'efficacité des opérations de sécurité par la hiérarchisation des mesures selon leur impact sur la réduction des risques.

[5] Ibid.

Figure 4. Types d'incidents liés à la sécurité impliquant des applications et une infrastructure cloud natives au cours de l'année écoulée

Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Des outils et des données trop cloisonnés

Autre défi pour les entreprises : l'utilisation fréquente de plusieurs outils en silos par les équipes responsables de l'IT, du réseau et de la sécurité ralentit les opérations de sécurité. Si les approches classiques exploitent plusieurs produits pour assurer une couverture maximale, avec des tests et des fonctions de surveillance pour détecter les problèmes de sécurité, elles ne s'adaptent pas aux applications cloud natives. De plus, la vitesse croissante des cycles de développement requiert constamment l'ajout de nouveaux outils distincts qui génèrent des alertes sans contexte, ce qui complique la hiérarchisation des mesures à prendre.

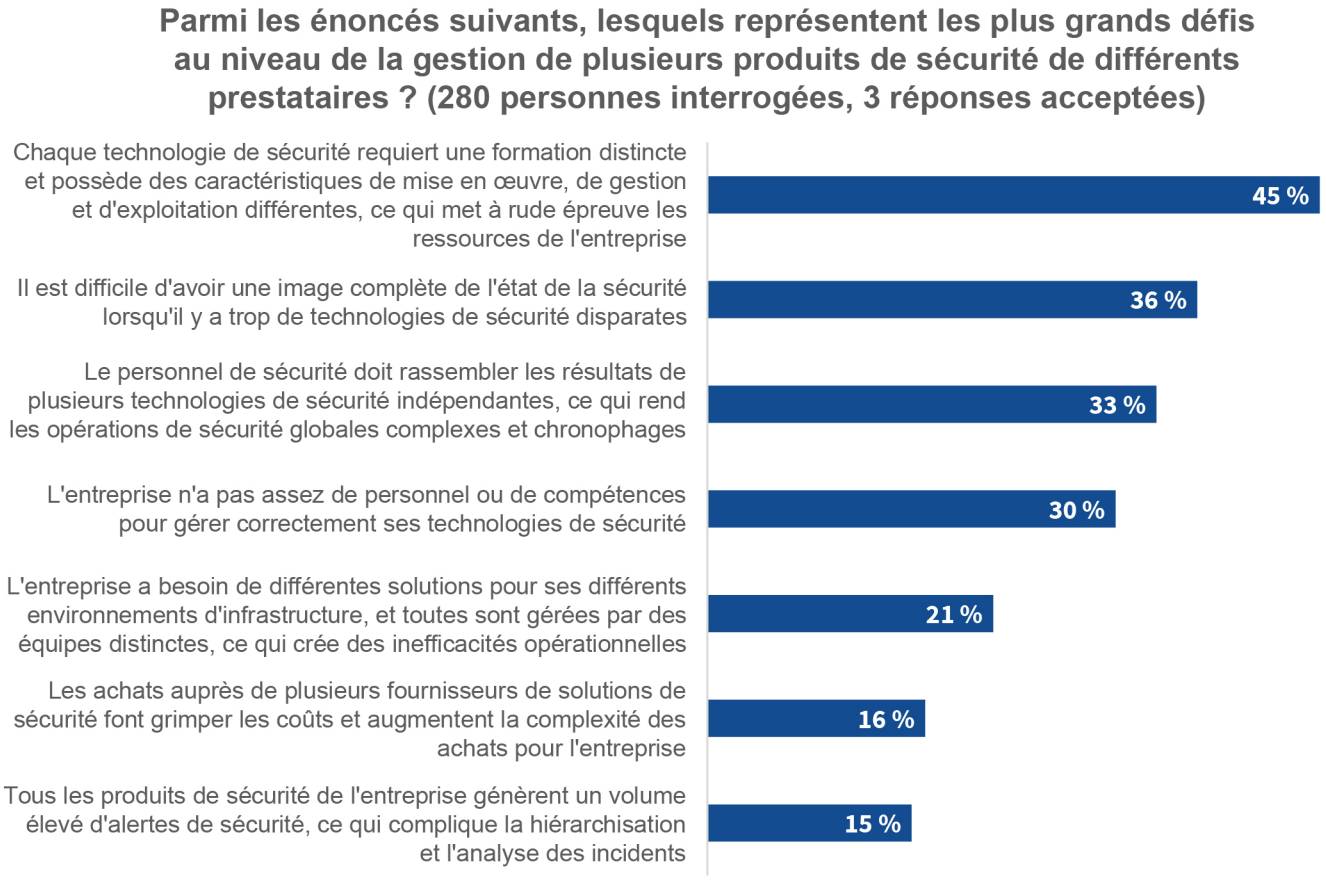
33 % indiquent que le regroupement des résultats de plusieurs produits de sécurité constitue un défi majeur

Lorsqu'il faut rassembler les données provenant de plusieurs outils de sécurité indépendants pour opérer, tout devient complexe et chronophage.

Les équipes de développement et de sécurité ne peuvent pas gérer le nombre élevé d'alertes provenant de plusieurs produits. En outre, ces outils distincts sont souvent conçus dans des langages différents, ce qui complique l'analyse des résultats et l'extraction du contexte nécessaire pour dégager des priorités. Enfin, chaque outil peut générer des alertes ou des faux positifs qui font perdre du temps.

Une étude ESG montre que pour 45 % des personnes interrogées, gérer plusieurs outils est difficile pour les équipes responsables de la cybersécurité, notamment à cause des formations requises et du temps passé au déploiement et à la gestion de chaque outil. Les entreprises rapportent également qu'il est difficile d'obtenir une vision complète de l'état de la sécurité à partir d'outils distincts (36 %) et que le regroupement des résultats de chaque outil créait plus de travail pour les équipes de sécurité (33 %) (Figure 5)[6].

Figure 5. Les défis liés à la gestion de plusieurs produits de sécurité



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

[6] Source : résultats de l'enquête menée par Enterprise Strategy Group, *ESG/ISSA Cybersecurity Process and Technology*, juin 2022

Par conséquent, les entreprises se tournent vers des produits et services qui fonctionnent avec l'ensemble des opérateurs télécoms afin de collecter les données nécessaires et les présenter de manière globale. Cette approche permet aux équipes de sécurité de gérer plus efficacement les risques, notamment les vulnérabilités, la surface d'exposition aux attaques et l'analyse des chemins d'attaque pour une meilleure compréhension de l'exposition de l'entreprise.

Bénéfices d'une plateforme unifiée dans les environnements hybrides et multicloud :

- Principe d'accès de moindre privilège avec des contrôles centralisés qui bloquent les déplacements latéraux
- Visibilité totale sur la détection des ressources et la gestion des chemins d'attaque pour toutes les applications, tous les workloads et toutes les ressources
- Informations, mesures et priorités haute fidélité pour les équipes SecOps, avec état de sécurité établi à partir d'une source unique d'informations fiables

Le surprovisionnement de l'accès réseau

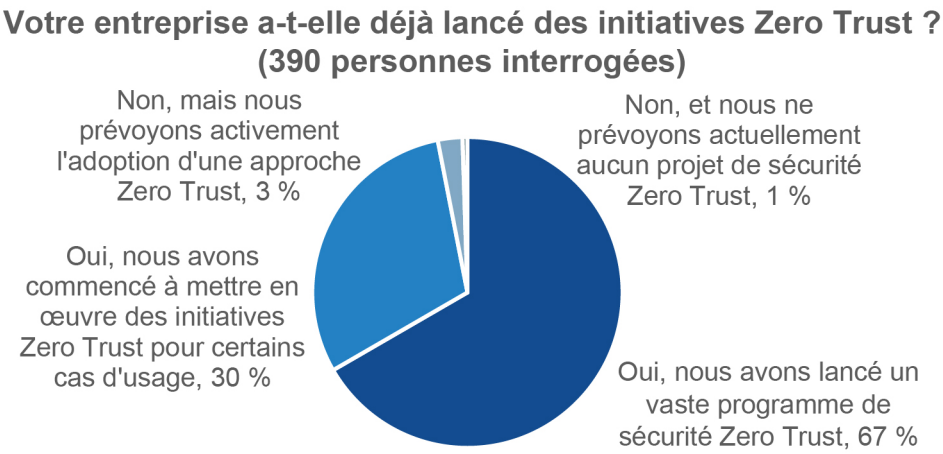
La gestion des identités et la sécurisation des accès jouent également un rôle clé dans l'efficacité des programmes de sécurité. En effet, le développement cloud permet aux entreprises et à leurs développeurs de déployer facilement des applications dans le cloud et de les mettre à disposition des clients, collaborateurs et partenaires. Une fois dans le cloud, ces applications sont disponibles pour les utilisateurs qui en ont besoin. Toutefois, il est crucial d'en gérer l'accès correctement pour limiter les risques et les expositions susceptibles de mettre en danger les données de l'entreprise et des clients. En d'autres termes, dans le cloud, il n'y a pas de périmètre pour protéger les workloads ; c'est l'identité et l'accès qui forment le périmètre.

Si l'on examine les problèmes et les incidents liés à la sécurité cloud native mentionnés précédemment, beaucoup concernent l'identité et les accès. En effet, les entreprises sont tentées de surprovisionner les accès pour accélérer le développement, mais s'ils ne sont pas gérés correctement ces nombreux accès étendent la surface d'exposition aux attaques et aux risques. Les applications se retrouvent ainsi vulnérables et les hackers peuvent se déplacer latéralement sans obstacle après avoir infiltré le système.

La mise en œuvre d'une approche d'accès réseau Zero Trust (ZTNA) protège les applications, car chaque demande d'accès est vérifiée avant l'établissement des connexions. Cette méthode permet aux équipes de sécurité de minimiser la probabilité et l'impact d'un incident. Ainsi, en cas de compromission d'un workload ou d'une application, l'environnement Zero Trust empêche l'accès aux données ou leur sortie. Selon une étude ESG, la grande majorité des entreprises (97 %) a mis en œuvre, ou est en train de mettre en œuvre, des initiatives de sécurité Zero Trust pour mieux protéger les workloads dans tous les environnements[7].

[7] Source : résultats complets de l'enquête menée par Enterprise Strategy Group, *2023 SASE Series: SSE Leads the Way Toward SASE*, août 2023

Figure 6. Pourcentage d'entreprises ayant adopté des initiatives Zero Trust



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Cependant, les entreprises rencontrent des difficultés pour appliquer le principe d'accès de moindre privilège à leurs applications dans des environnements multicloud et hybrides. Elles peinent notamment à faciliter la collaboration entre les équipes IT, d'exploitation et de sécurité, à protéger les accès à partir de divers endpoints, à gérer les coûts, à garantir la sécurité des données, à préserver les performances, à offrir une visibilité totale et à proposer des rapports complets.

C'est pourquoi les entreprises doivent opter pour une solution capable de répondre aux exigences des environnements hybrides et multicloud, tout en intégrant une approche Zero Trust. Une telle solution contribuerait à réduire les risques tout en optimisant l'efficacité opérationnelle, en aidant les équipes responsables de l'IT, du réseau et de la sécurité à protéger leurs applications dans tous les environnements.

Présentation de la suite Cisco Cloud Protection

La suite Cisco Cloud Protection Suite propose une approche moderne de la sécurité des applications, ainsi qu'une protection de bout en bout pour les environnements applicatifs hybrides et multicloud. Que ce soit pour des serveurs dédiés ou des applications cloud natives, la suite Cisco Cloud Protection assure la sécurité globale des applications et protège les workloads dans tous les environnements, on-premise et dans le cloud.

Les avantages de la solution :

- **Sécurité hybride et multicloud complète.** Avec la suite Cisco Cloud Protection, les utilisateurs peuvent gérer efficacement les risques dans tous les environnements.
- **Visibilité totale sur toutes les ressources.** Avec une vue claire de chaque réseau, application et ressource cloud, les entreprises peuvent vérifier leur niveau de sécurité et hiérarchiser les risques plus facilement.
- **Meilleure cohérence entre les environnements.** La suite facilite l'application des cadres de sécurité, des contrôles et des politiques de conformité pour limiter les risques et respecter les bonnes pratiques du secteur.
- **Remédiation optimisée.** La suite utilise un système d'évaluation des risques basé sur la science des données pour hiérarchiser les vulnérabilités qui présentent un risque réel dans l'environnement hybride.

- **Protection des applications.** En protégeant le trafic sur le réseau, les clouds et les VPC, la suite assure une macro et une microsegmentation précises et cohérentes dans tous les environnements.
- **Accès de moindre privilège avec une approche Zero Trust.** Cisco Cloud Protection tire parti de l'accès réseau zero trust (ZTNA) pour protéger les workloads on-premise et dans le cloud, réduisant ainsi la surface d'exposition aux attaques et empêchant les déplacements latéraux.

En utilisant Cisco Cloud Protection pour gérer la sécurité des applications dans les environnements cloud, les clients peuvent :

- Réduire les efforts opérationnels et optimiser les ressources
- Réduire les risques pour la sécurité en hiérarchisant les vulnérabilités
- Faciliter le respect des réglementations en matière de conformité
- Réagir plus rapidement aux menaces grâce à une visibilité complète
- Favoriser la transformation numérique pour soutenir la croissance de l'entreprise

Conclusion

Plus les workloads de l'entreprise migrent vers le cloud pour optimiser la productivité, plus l'équipe de sécurité peine à protéger les applications dans tous les environnements et à s'adapter à la croissance de l'activité. Pour gérer la complexité engendrée par les applications hébergées dans des environnements hybrides et multicloud, tout en assurant la migration vers le cloud, voire le rapatriement de certains workloads, il devient essentiel d'adopter une approche flexible et unifiée.

La suite Cisco Cloud Protection permet aux équipes responsables de la sécurité de protéger les applications sur plusieurs clouds et data centers. En offrant une visibilité complète et un contrôle d'accès basé sur le principe du moindre privilège, cette suite permet de sécuriser les ressources et les applications dans l'ensemble de l'environnement de manière complète et efficace. L'automatisation, la cohérence entre les environnements et la consolidation des outils de sécurité permettent également de réduire le nombre de tâches manuelles et d'optimiser ainsi l'efficacité des équipes responsables de l'IT, du réseau et de la sécurité.

Grâce à la suite Cisco Cloud Protection, les équipes de sécurité sont mieux équipées pour soutenir la croissance et la transformation numérique de l'entreprise, notamment l'évolution des équipes de développement, l'adoption de nouvelles technologies et autres fusions et acquisitions.

À propos d'Enterprise Strategy Group
L'équipe Enterprise Strategy Group de TechTarget fournit des informations ciblées et exploitables sur le marché, des études de la demande, des services de conseil aux analystes, des conseils de commercialisation stratégiques, des validations de solutions et du contenu personnalisé pour l'achat et la vente de technologies d'entreprise.

contact@esg-global.com
www.esg-global.com