Enterprise Strategy Group™ by TechTarget

DOCUMENT TECHNIQUE

Alimenter la croissance des entreprises grâce à la sécurité dans les environnements hybrides et multinuages

Gérer efficacement la sécurité pour soutenir la transformation numérique

Par Melinda Marks, directrice des pratiques, cybersécurité
Enterprise Strategy Group

Octobre 2023

Ce document technique du Enterprise Strategy Group a été commandé par Cisco et est distribué avec l'autorisation de TechTarget, Inc.

Table des matières

Introduction

À l'heure actuelle, les entreprises sont contraintes d'effectuer une transformation numérique pour pouvoir optimiser leur productivité et acquérir un avantage concurrentiel. Elles migrent donc de plus en plus d'applications vers des services en nuage pour pouvoir accélérer le développement de logiciels sans avoir à se préoccuper du provisionnement des serveurs ou du matériel. Elles doivent également pouvoir prendre en charge le travail à distance pour pouvoir offrir une certaine flexibilité aux employés et aux équipes en pleine croissance. Dans leurs parcours de transformation numérique, les entreprises sont cependant confrontées à une complexité informatique accrue avec des applications distribuées dans des environnements hybrides et multinuages, ainsi qu'à la nécessité de devoir prendre en charge une main-d'œuvre décentralisée.

Ces éléments créent de nouvelles exigences pour la sécurité qui doit désormais s'assurer de pouvoir évoluer pour prendre en charge les applications dans tous les environnements, ainsi que permettre la croissance de l'entreprise. La sécurité doit également prendre en charge les applications et les utilisateurs dans divers environnements ayant chacun leurs propres plateformes d'architecture, leurs propres fonctionnalités et leurs propres capacités. Quant aux équipes de sécurité, elles doivent avoir la souplesse nécessaire pour s'adapter à l'évolution des besoins de l'entreprise, ce qui inclut la croissance organique et les acquisitions.

Elles sont toutefois confrontées à de nombreux défis lorsqu'il s'agit d'adapter les stratégies de sécurité à l'utilisation croissante des services en nuage et au développement infonuagique natif. Les problèmes de visibilité liés à la nature éphémère des ressources et des infrastructures en nuage, dont la taille et le nombre peuvent rapidement changer, sont à l'origine de cette situation. Le rythme de productivité accru des développeurs et la capacité de prévenir l'exposition aux menaces en raison de la multiplication des accès et des autorisations sont d'autres éléments qui augmentent encore plus la complexité.

Même si de nombreuses organisations tentent de relever ces défis en utilisant plusieurs solutions ou plateformes de sécurité, elles sont souvent confrontées à des incidents de sécurité liés à des problèmes communs comme des configurations erronées ou un accès surprovisionné. Les angles morts et les lacunes entre les différents outils créent également des problèmes de visibilité. En outre, bien que leurs outils puissent les alerter à propos des vulnérabilités de sécurité, les équipes de sécurité ne parviennent que rarement à hiérarchiser les problèmes critiques et à les résoudre à temps pour protéger leurs applications contre les attaques. Avec la multiplication des ressources et des applications dans les environnements infonuagiques, ces défis ne peuvent que se décupler.

Les équipes de sécurité ont donc besoin d'une stratégie efficace pour sécuriser les applications dans tous les environnements, assurer une visibilité omniprésente et fournir une protection d'accès capable de prendre en charge la mobilité des charges de travail. Ce document explore les éléments clés d'une approche efficace en matière de sécurité des applications qui offre la flexibilité nécessaire pour soutenir la croissance rapide de l'entreprise et ses exigences en ce qui concerne les environnements hybrides et multinuages.

Les entreprises doivent donc chercher une approche flexible qui permet à toutes les équipes de sécurité, quelles que soient leurs compétences, d'avoir une visibilité totale sur les ressources pour corriger efficacement les vulnérabilités, ainsi que de pouvoir utiliser une approche de vérification systématique pour protéger les applications contre les attaques dans l'ensemble des environnements. Cette approche doit notamment inclure la détection rapide des problèmes de sécurité, ainsi que l'accès à des renseignements contextuels et à des informations sur les menaces qui permettront de hiérarchiser les actions qui auront le plus de répercussions sur l'atténuation des risques. Elle doit également fournir des moyens simplifiés et centralisés pour établir des politiques de protection des ressources.

Grâce à une approche qui tient compte des applications et des accès dans les environnements interconnectés, dynamiques, multinuages et hybrides, les équipes de sécurité peuvent optimiser les ressources et les opérations pour ainsi gérer efficacement les risques et intervenir rapidement en cas de menaces. Cela leur permettra notamment d'évoluer efficacement et de pouvoir soutenir le développement rapide et la croissance de l'entreprise.

Défis de sécurité associés à la transformation numérique

Une étude menée par le Enterprise Strategy Group de TechTarget a révélé qu'une tempête parfaite créée par les très nombreux développements récents pose de nombreux défis aux équipes de sécurité. Ces développements récents incluent notamment la complexité accrue des environnements informatiques, la prolifération des applications infonuagiques natives en raison de l'augmentation de la productivité des développeurs et le manque de visibilité entre plusieurs nuages publics qui cause un large éventail d'incidents. Les équipes de sécurité ont donc besoin d'une stratégie efficace pour relever ces défis et permettre à l'entreprise de grandir, tout en assurant la sécurité et la protection de leurs applications dans différents environnements sans cependant exiger de compétences spécialisées.

Complexité accrue des TI

À mesure que les entreprises tirent parti de la transformation numérique pour augmenter leur productivité et acquérir un avantage concurrentiel, cela crée de la complexité et de nouvelles exigences pour les TI et la sécurité. Une étude du Enterprise Strategy Group montre que plus de la moitié (53 %) des entreprises déclarent que leur environnement informatique est plus complexe ou nettement plus complexe qu'il y a deux ans.[1] La principale raison invoquée par ces entreprises pour expliquer cette complexité accrue est l'augmentation du travail à distance et du travail hybride (40 %). Parmi les autres raisons principales, notons le cadre de la cybersécurité qui évolue constamment (35 %), l'augmentation du nombre et des types de terminaux (35 %), les nouvelles réglementations sur la sécurité des données et la protection de la vie privée (34 %) et l'augmentation des volumes de données (34 %). Plus loin dans la liste, la nécessité d'utiliser à la fois des centres de données sur site et des fournisseurs de nuages publics a été citée par 29 % des personnes interrogées (voir la figure 1).

[1] Rapport de recherche du Enterprise Strategy Group, *2023 Technology Spending Intentions Survey* (enquête sur les intentions de dépenses technologiques 2023), novembre 2022

Figure 1. Raisons qui expliquent la complexité des TI

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

Les entreprises peuvent trouver des moyens efficaces de soutenir la croissance et l'évolution, même si elles sont confrontées à ces multiples sphères de plus en plus complexes.

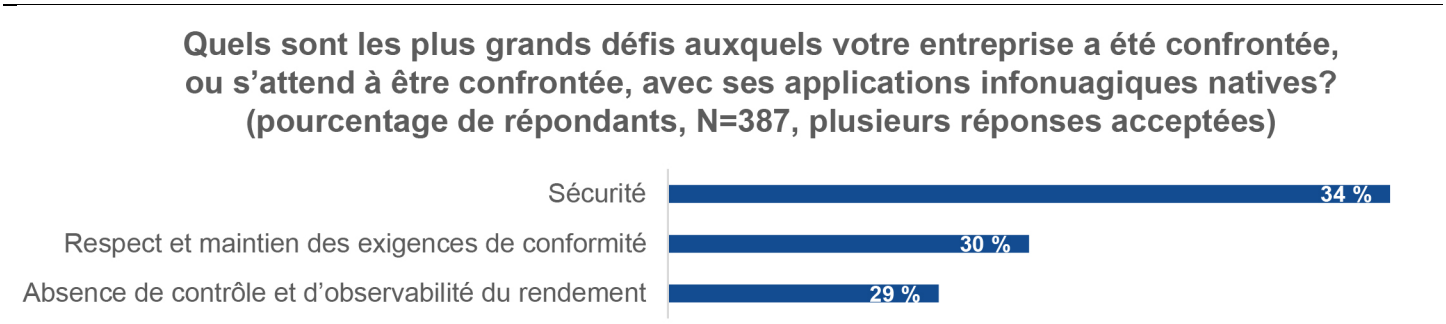
Migration croissante des applications vers les environnements en nuage

Les entreprises s'appuient également de plus en plus sur l'infrastructure du nuage public pour accroître la productivité et l'innovation grâce au développement infonuagique natif. Elles n'ont pas à se soucier de l'infrastructure sous-jacente ou de la maintenance, et peuvent profiter d'économies d'échelle grâce aux modèles de paiement à l'usage proposés par les fournisseurs de services infonuagiques (CSP).

Une étude menée par le Enterprise Strategy Group sur les tendances en matière de modernisation de l'infrastructure des applications montre que 88 % des entreprises interrogées exécutent des charges de travail de production sur des infrastructures ou des plateformes en nuage public, et que les entreprises transfèrent de plus en plus leurs charges de travail de production vers le nuage.[2] Elle montre également que les entreprises qui ont transféré leurs applications dans le nuage en ont tiré de nombreux avantages, notamment une plus grande souplesse, des coûts d'infrastructure moins élevés et un déploiement plus rapide.

L'adoption du nuage permet également le développement et l'exploitation, ce qui permet de déplacer les opérations vers la gauche pour permettre aux développeurs de provisionner leur propre infrastructure plutôt que d'attendre que les équipes informatiques ou d'exploitation provisionnent les serveurs. Les développeurs peuvent donc travailler plus efficacement, ce qui permet d'obtenir un délai de rentabilisation plus court qu'avec les méthodes traditionnelles de développement d'applications. Ajouter cette façon plus efficace de travailler à l'augmentation de la productivité du développement de logiciels crée cependant des défis en matière de sécurité et de conformité pour les applications infonuagiques natives.

Figure 2. Trois principaux défis auxquels les entreprises sont confrontées avec les applications infonuagiques natives



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

Les entreprises ont besoin d'un moyen efficace pour gérer les risques de sécurité et offrir un volume élevé de versions à un rythme plus rapide pour ainsi répondre aux demandes des organisations qui souhaitent migrer vers le développement infonuagique natif. Les équipes de sécurité capables d'optimiser l'efficacité pour soutenir cette évolution et cette croissance peuvent jouer un rôle important en permettant à l'entreprise d'obtenir de meilleurs résultats, au lieu de faire obstacle à l'adoption de nouvelles technologies susceptibles d'accroître la productivité et l'innovation des développeurs.

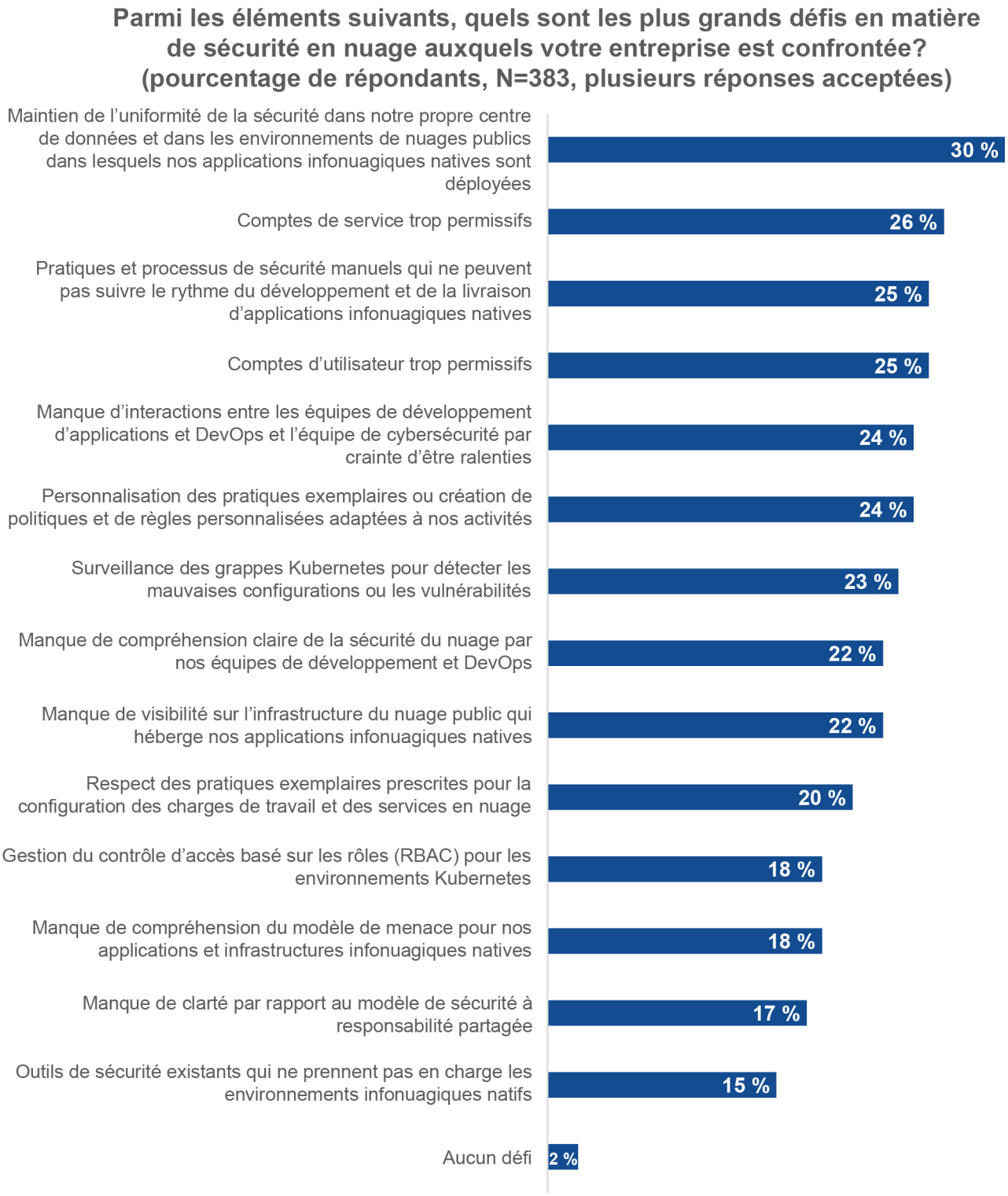
[2] Source : Rapport de recherche du Enterprise Strategy Group, *Cloud-native Applications* (applications infonuagiques natives), mai 2022.

Gestion de la posture de sécurité dans les environnements multinuages

La croissance des environnements en nuage exige également des équipes de sécurité qu'elles prennent en charge les environnements multinuages. Une étude du Enterprise Strategy Group sur la gestion de la posture de sécurité en nuage montre que la plupart des entreprises (94 %) ont recours à plusieurs fournisseurs de services d'infrastructure en nuage et que la majorité d'entre elles (69 %) en utilisent au moins trois.[3] Bien qu'une majorité des entreprises (68 %) aient déclaré avoir mis en place des solutions robustes de gestion de la posture de sécurité en nuage, elles ont cependant mentionné un certain nombre de défis, principalement en ce qui concerne l'obtention de la visibilité et du contrôle dont elles ont besoin pour gérer efficacement les risques dans les environnements et les équipes, ce qui inclut l'uniformisation de la sécurité dans leur centre de données et dans leurs environnements infonuagiques (mentionné par 30 % d'entre elles). Parmi les autres défis, citons les comptes de services et d'utilisateur trop permissifs (mentionnés par 25 % et 26 % des entreprises, respectivement), les pratiques et processus de sécurité manuels qui ne peuvent pas suivre la vitesse de livraison des applications infonuagiques natives (25 %), le manque de participation dans les processus de développement et le manque de contrôle sur ces processus (24 %), le manque de visibilité sur l'infrastructure du nuage public (22 %) et une compréhension insuffisante en ce qui concerne les menaces infonuagiques natives (18 %, voir la figure 3).[4]

[3]Source : Rapport *de recherche du Enterprise Strategy Group, Cloud-native Applications (applications infonuagiques natives),* mai 2022.
[4] Idem.

Figure 3. Plus grands défis de la sécurité en nuage pour les entreprises



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

Les entreprises ont donc besoin d'une approche efficace pour relever ces défis et protéger leurs applications dans tous les environnements. Il leur faut trouver une façon d'obtenir visibilité et contrôle sur les applications, peu importe où elles se trouvent, et de les visualiser comme si elles se trouvaient dans un environnement interconnecté et dynamique plutôt que dans des environnements distincts. Rassembler les informations provenant d'environnements multinuages et hybrides permet d'accroître l'efficacité des opérations de sécurité pour atténuer les risques et intervenir rapidement en cas de menaces. C'est, en fait, le seul moyen de faire évoluer la sécurité pour soutenir une croissance de l'entreprise dont l'empreinte infonuagique est de plus en plus importante.

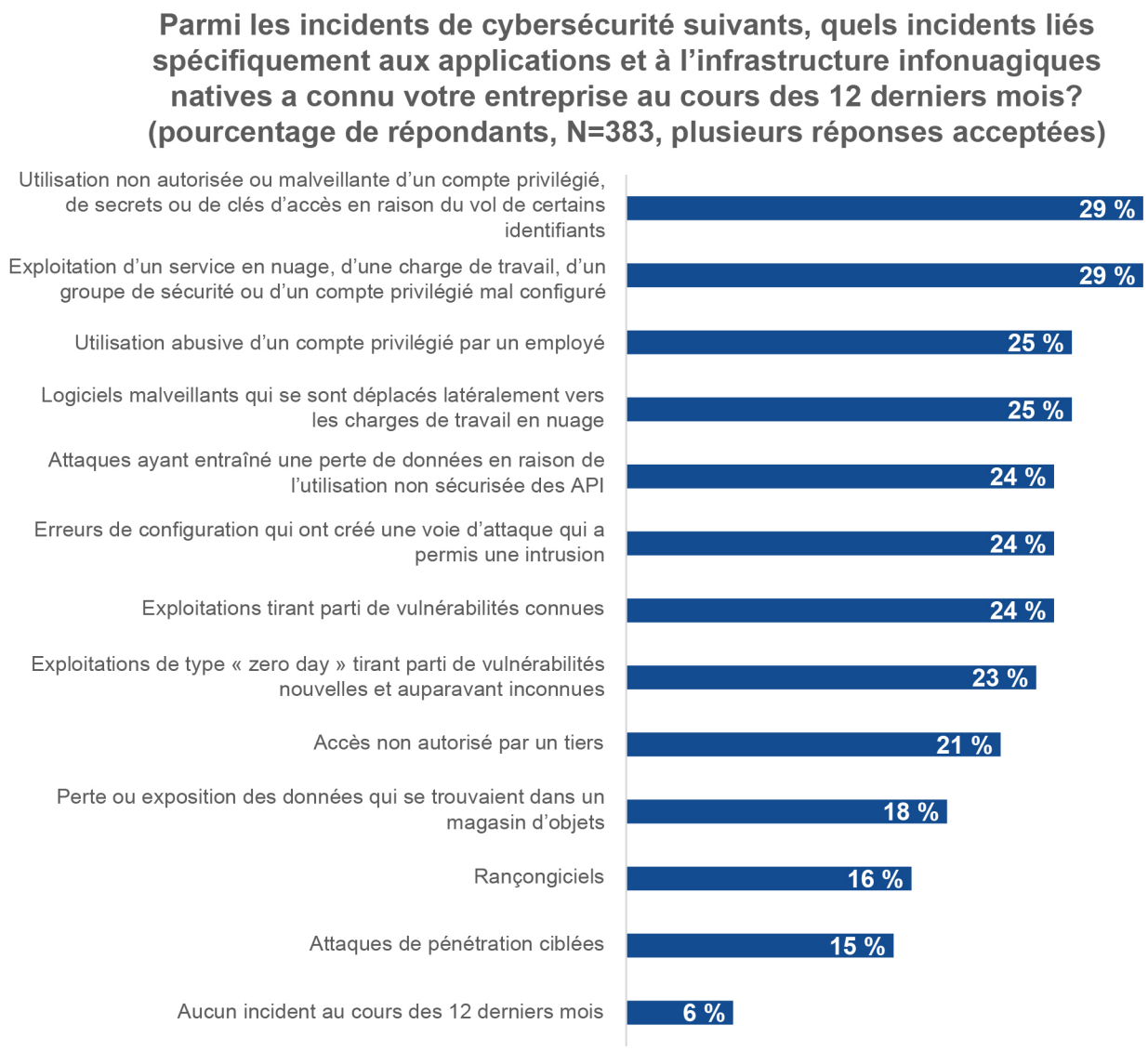
Large éventail d'incidents

Bien que les entreprises aient généralement mis en place plusieurs solutions de sécurité, la plupart d'entre elles ont été confrontées à des incidents touchant leurs applications infonuagiques natives ou leur infrastructure. Plus précisément, l'étude montre que 94 % des entreprises ont déclaré avoir été confrontées à des incidents comprenant des attaques ou des mouvements latéraux au cours des 12 derniers mois, allant du vol d'identifiants (29 %) à l'exploitation d'une mauvaise configuration (29 %), en passant par la perte de données en raison d'une utilisation non sécurisée des API (24 %) et des rançongiciels (16 %, voir la figure 4).[5]

Ces incidents se sont produits soit parce que les organisations n'étaient pas conscientes de leur exposition au risque, soit parce qu'elles n'ont pas été en mesure de remédier aux problèmes de sécurité à temps pour prévenir ou contenir les incidents. La nécessité d'avoir une visibilité sur l'ensemble des environnements est mise en évidence, tout comme celle d'avoir une approche par plateforme pour effectuer des opérations de sécurité efficaces, en accordant la priorité aux actions qui auront le plus d'impact sur la réduction des risques.

[5] Idem.

Figure 4. Types d'incidents liés à des applications et à des infrastructures infonuagiques natives pendant l'année qui s'est écoulée



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

Trop grand nombre d'outils et de données cloisonnés

En plus de ralentir les opérations de sécurité, l'utilisation fréquente, par les équipes des TI, du réseau et de la sécurité d'outils multiples et cloisonnés représente un autre défi pour les organisations. Bien que la sécurité traditionnelle des applications utilise plusieurs produits de sécurité pour assurer la couverture, grâce à des tests et à une surveillance qui permet de détecter les problèmes de sécurité, elle ne peut pas évoluer au même rythme que les applications infonuagiques natives. Elle ne peut pas non plus suivre la vitesse croissante des cycles de développement ni continuer à ajouter des outils distincts qui généreront des alertes sans avoir le contexte qui lui permettra de déterminer comment prioriser les différentes actions à effectuer.

33 % ont déclaré que le fait de devoir combiner les résultats de plusieurs produits de sécurité représentait un défi majeur.

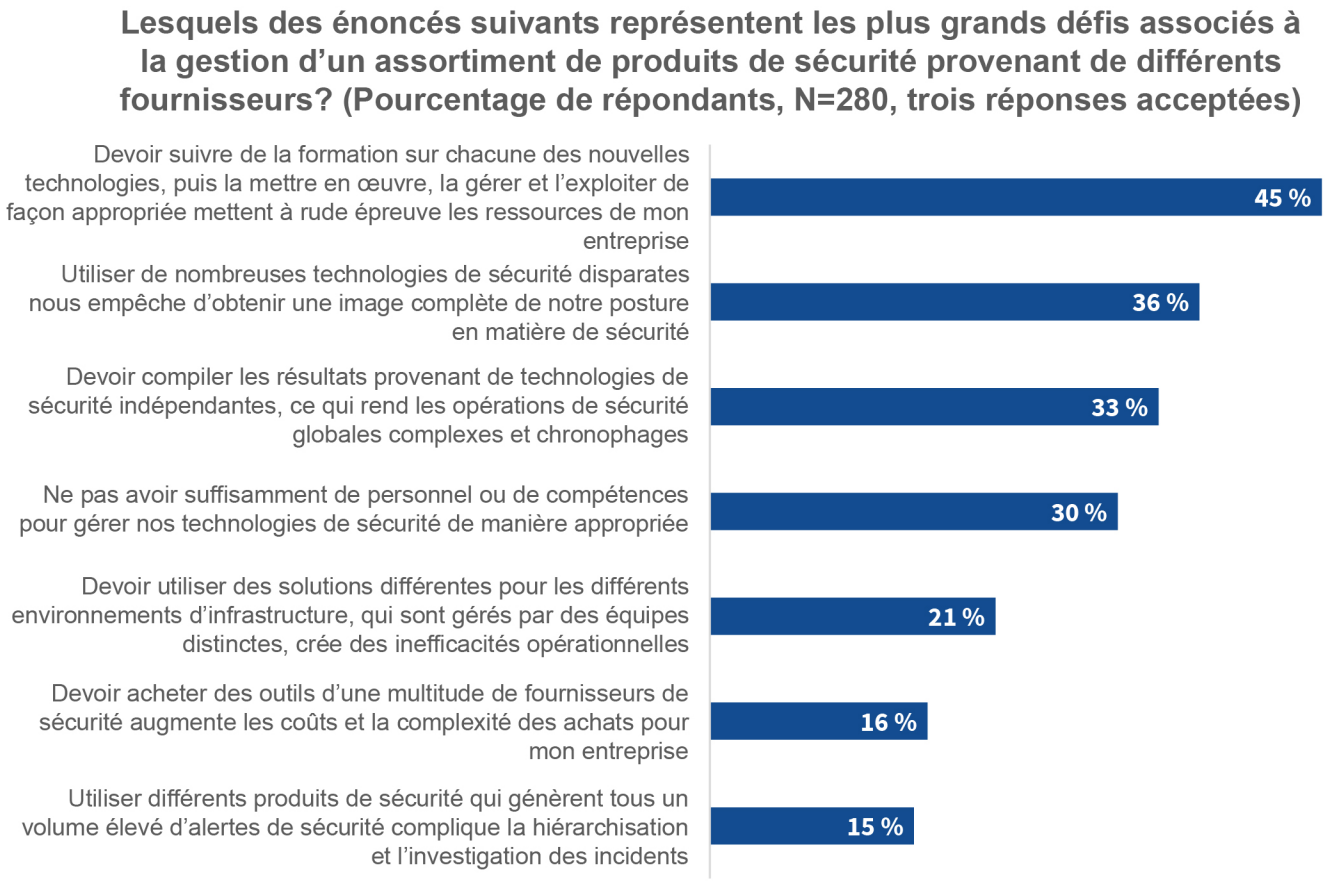
Lorsque le personnel de sécurité doit rassembler des données provenant de plusieurs technologies de sécurité indépendantes, les opérations de sécurité globales deviennent alors trop complexes et chronophages.

Les développeurs et les équipes de sécurité ne parviennent alors plus à suivre le nombre élevé d'alertes envoyées par les nombreux produits. Puisque ces différents outils sont souvent conçus dans des langages différents, cela complique encore plus l'analyse des résultats qui pourrait permettre d'en tirer le contexte nécessaire pour établir les priorités. Il ne faut pas non plus oublier que chacun des outils peut générer des alertes ou des faux positifs qui feront aussi perdre du temps aux différentes équipes.

Dans une étude du Enterprise Strategy Group, 45 % des personnes interrogées ont indiqué que la gestion d'outils multiples pose problèmes pour le personnel responsable de la cybersécurité, notamment parce que les employés doivent suivre de la formation pour pouvoir utiliser chacun des outils de sécurité et qu'il faut aussi tenir compte du temps pour déployer et gérer ces outils. Les entreprises ont également indiqué qu'il était difficile d'obtenir une image complète de l'état de la sécurité à partir d'outils distincts (36 %) et que le regroupement des résultats des différents outils alourdissait la tâche du personnel responsable de la sécurité (33 %, voir la figure 5).[6]

[6] Source : Résultats complets du sondage du Enterprise Strategy Group, *ESG/ISSA Cybersecurity Process and Technology Survey (sondage ESG/ISSA sur les processus et les technologies de cybersécurité),* juin 2022.

Figure 5. Défis que pose la gestion de plusieurs produits de sécurité



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

C'est pourquoi les entreprises s'orientent désormais vers des produits et des services qui peuvent être utilisés avec toutes les plateformes de services en nuage (CSP). Elles pourront ainsi obtenir toutes les données dont elles ont besoin et les examiner de manière globale. Cela permettra également aux équipes de sécurité de gérer plus efficacement les risques de sécurité, ce qui inclut la gestion efficace des vulnérabilités et de la surface d'attaque, et analyser les chemins d'attaque pour mieux comprendre l'exposition de l'entreprise aux menaces à la sécurité.

Une plateforme unifiée pour les environnements hybrides et multinuages peut fournir :

- L'accès de moindre privilège, avec des contrôles centralisés pour arrêter les mouvements latéraux.
- Une visibilité étendue sur la découverte des ressources et la gestion des voies d'attaque pour toutes les applications, charges de travail et ressources.
- Des renseignements, des actions et des priorités fiables destinés aux équipes des opérations de sécurité, ce qui permet d'adopter une posture de sécurité fondée sur une seule source de données fiables.

Accès au réseau surprovisionné

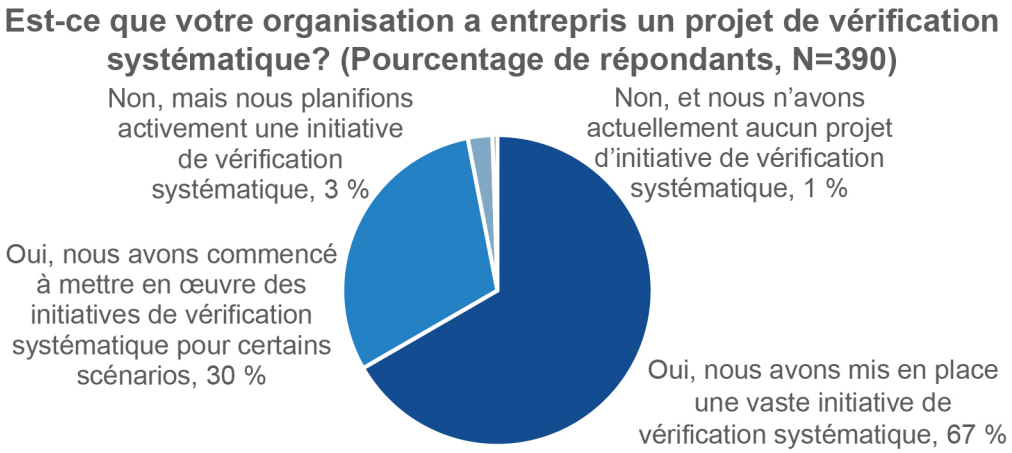
La gestion des identités et de l'accès sécurisé joue également un rôle clé dans l'efficacité du programme de sécurité. En effet, le développement infonuagique natif permet aux entreprises et à leurs développeurs de déployer facilement leurs applications infonuagiques et de les rendre accessibles aux clients, aux employés et aux partenaires. Une fois déployées dans le nuage, les utilisateurs prévus peuvent alors accéder aux applications, mais il faut s'assurer de gérer correctement l'accès pour limiter les risques et l'exposition qui pourraient mettre en péril les données de l'entreprise et des clients. En d'autres termes, le nuage n'offre aucun périmètre de protection aux charges de travail, puisque l'identité et l'accès déterminent le périmètre.

Si l'on examine les problèmes de sécurité et les incidents dans les environnements infonuagiques natifs mentionnés plus haut, on constate qu'un grand nombre d'entre eux sont liés à des questions d'identité et d'accès. En effet, il est facile de surprovisionner l'accès pour faciliter un développement rapide, mais si cet accès n'est pas géré de façon appropriée, l'accès accru élargit la surface d'attaque et expose l'organisation aux risques en laissant les applications ouvertes aux attaques ou en facilitant le déplacement latéral d'un agresseur après qu'il ait réussi à pénétrer dans un système.

La mise en œuvre d'une approche de vérification systématique des accès réseau (ZTNA) contribue à protéger les applications en s'assurant que chaque demande d'accès est vérifiée avant que la connexion ne soit établie, ce qui permet aux équipes de sécurité de réduire au minimum la probabilité et les répercussions d'un incident. Ainsi, si une charge de travail ou une application est compromise, un environnement de vérification systématique empêchera l'accès aux données ou la sortie des données. Une étude du Enterprise Strategy Group montre qu'une grande majorité d'entreprises (97 %) ont mis en place ou sont en train de mettre en place des initiatives de vérification systématique afin de mieux protéger leurs charges de travail dans les différents environnements.[7]

[7] Source : Résultats complets du sondage du Enterprise Strategy Group, *2023 SASE Series : SSE Leads the Way Toward SASE* (séries SASE 2023 : Le SSE ouvre la voie au SASE), août 2023.

Figure 6. Pourcentage d'entreprises qui adoptent des initiatives de vérification systématique



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

Les entreprises sont cependant confrontées à des défis lorsqu'elles veulent implémenter l'accès de moindre privilège pour leurs applications dans des environnements multinuages et hybrides. Elles doivent notamment s'assurer de faciliter la collaboration entre les équipes des TI, des opérations et de la sécurité, fournir un accès sécurisé à partir d'un éventail d'appareils, gérer les coûts, assurer la sécurité des données, maintenir les performances et fournir une visibilité et des rapports complets.

C'est pourquoi elles devraient chercher une solution qui convienne à la fois aux environnements hybrides et multinuages, et intègre une approche de vérification systématique. Une telle solution aiderait les entreprises à réduire les risques tout en optimisant l'efficacité opérationnelle, en plus d'aider les équipes des TI, des réseaux et de la sécurité à protéger leurs applications dans les différents environnements.

Présentation de la suite Cisco Cloud Protection

La suite Cisco Cloud Protection offre une approche moderne de la sécurité des applications avec une sécurité de bout en bout pour les environnements d'applications hybrides et multinuages. De l'absence de système d'exploitation à la solution infonuagique native, la suite Cisco Cloud Protection offre aux clients une sécurité globale pour les applications qui protège les charges de travail dans tous les environnements, qu'elles soient sur site ou en nuage.

Cisco Cloud Protection offre ce qui suit :

- **Sécurité hybride et multinuage complète.** Grâce à la suite Cisco Cloud Protection, les utilisateurs peuvent gérer efficacement les risques de sécurité dans tous les environnements.
- **Visibilité omniprésente sur toutes les ressources.** Grâce à une vision claire de chacun des réseaux, applications et ressources en nuage, les entreprises peuvent valider la posture de sécurité et hiérarchiser les risques pour l'entreprise.
- **Cohérence entre les environnements.** La suite logicielle de Cisco simplifie la mise en place de cadres de sécurité, de contrôles et de politiques de conformité, ce qui permet de réduire les risques et de respecter les pratiques exemplaires du secteur.

- **Efficacité optimisée des mesures correctives.** La suite logicielle de Cisco utilise un système d'évaluation des risques optimisé par la science des données pour hiérarchiser les vulnérabilités qui posent un véritable risque dans l'environnement hybride.
- **Protection des applications.** Puisqu'elle protège le trafic dans le réseau, les nuages et le nuage privé virtuel (VPC), la suite logicielle permet une macro et une microsegmentation cohérente et précise dans tous les environnements.
- **Accès de moindre privilège et approche à vérification systématique.** Cisco Cloud Protection utilise la vérification systématique des accès réseau (ZTNA) pour protéger les charges de travail sur site et en nuage, ce qui réduit la surface d'attaque et empêche les mouvements latéraux.

Utiliser Cisco Cloud Protection pour gérer la sécurité des applications dans les environnements en nuage permettra aux clients :

- De réduire leurs frais généraux d'exploitation et d'optimiser les ressources.
- D'atténuer les risques de sécurité en hiérarchisant les vulnérabilités en fonction des risques.
- De faciliter le respect de la réglementation en matière de conformité.
- D'intervenir plus rapidement face aux menaces grâce à une visibilité complète.
- De favoriser la transformation numérique pour ainsi soutenir la croissance de l'entreprise.

Conclusion

Alors que les entreprises déplacent de plus en plus leurs charges de travail vers le nuage pour optimiser la productivité, les équipes responsables de la sécurité sont confrontées à de nombreux défis lorsque vient le temps de protéger leurs applications dans les différents environnements et de suivre la croissance de l'entreprise. La complexité qui se révèle au moment de prendre en charge des applications dans des environnements hybrides et multinuages et de permettre la migration vers le nuage, ou le rapatriement du nuage, exige une approche unifiée et flexible.

La suite Cisco Cloud Protection offre aux équipes de sécurité un moyen efficace pour gérer la sécurité des applications dans plusieurs nuages et centres de données. En fournissant une visibilité complète et un contrôle d'accès de moindre privilège, elle fournit une méthode globale et efficace pour sécuriser les ressources et les applications dans tout l'environnement. Le fait d'offrir un moyen uniforme pour gérer les risques, en utilisant pour ce faire l'automatisation, la cohérence entre les environnements et des outils de sécurité consolidés réduit également le nombre de tâches qui doivent être effectuées manuellement et permet d'optimiser l'efficacité des équipes des TI, du réseau et de la sécurité.

Grâce à la suite Cisco Cloud Protection, les équipes de sécurité sont mieux outillées pour soutenir la croissance de l'entreprise et la transformation numérique, ce qui inclut l'évolution dans les équipes de développement, l'adoption de nouvelles technologies et les fusions et acquisitions qui permettent aux entreprises de rester concurrentielles.

À propos du Enterprise Strategy Group
Ce groupe de TechTarget fournit des renseignements sur le marché ciblés et exploitables, des études liées à la demande, des services consultatifs d'analystes, des conseils stratégiques pour la mise en marché, des validations de solutions et du contenu personnalisé au soutien de l'achat et de la vente de technologies d'entreprise.

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