ManageEngine

RAPPORT

PERSPECTIVES DE LA SÉCURITÉ DU CLOUD 2023

ManageEngine

INDEX

Table des matières

Introduction

Le paysage du cloud s'est considérablement développé au cours de la dernière décennie, ce qui a incité de nombreuses organisations à passer au cloud. L'adoption rapide du cloud s'explique en partie par son efficacité et en partie par le fait que le travail à distance et hybride est devenu la norme à la suite de la pandémie. Suite à l'augmentation de l'adoption du cloud, la surface d'attaque s'est accrue et les différentes manières d'exécuter les attaques se sont également développées, mais en raison de l'approche "lift and shift" que de nombreuses organisations ont suivie, une attention négligeable a été accordée à la sécurité du cloud. De ce fait, de nombreuses organisations sont devenues vulnérables aux menaces et aux violations de données, ce qui a eu des répercussions sur leurs finances et leur réputation.

Depuis, les organisations ont opté pour des outils de sécurité du cloud tels que les courtiers de sécurité d'accès au cloud (CASB) afin d'obtenir une visibilité sur leur réseau cloud et de prévenir d'autres attaques. Mais un outil CASB ne suffit pas à lui seul à protéger adéquatement une organisation contre toutes sortes de menaces ; l'intégration avec d'autres outils de sécurité est ce que le marché demande actuellement. La consolidation est-elle la voie à suivre ?

Pour comprendre le paysage du cloud et la demande du marché pour les outils de sécurité du cloud, nous avons mené une enquête avec Censuswide.

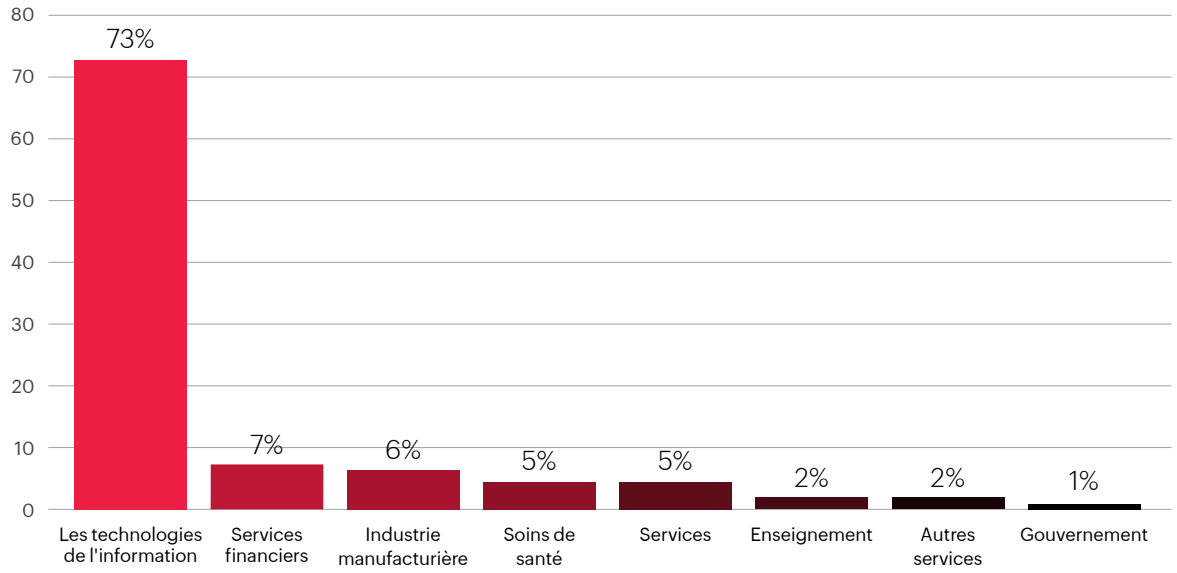
Nous avons enquêté auprès de

500+

professionnels de l'informatique aux États-Unis dans divers secteurs, notamment la santé, les services financiers, l'industrie et l'administration.

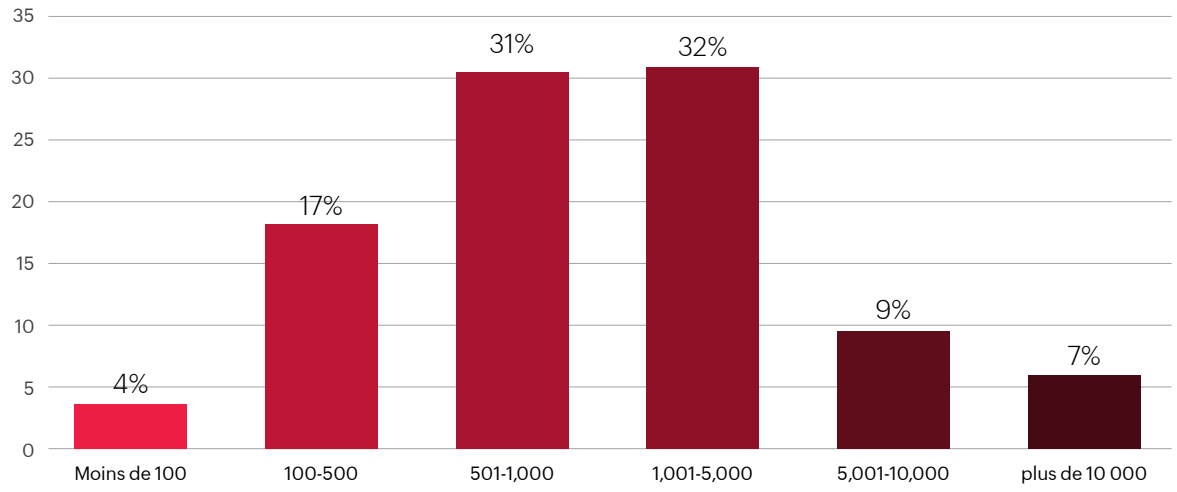
L'industrie

Q. Quel est le secteur d'activité de votre organisation ?



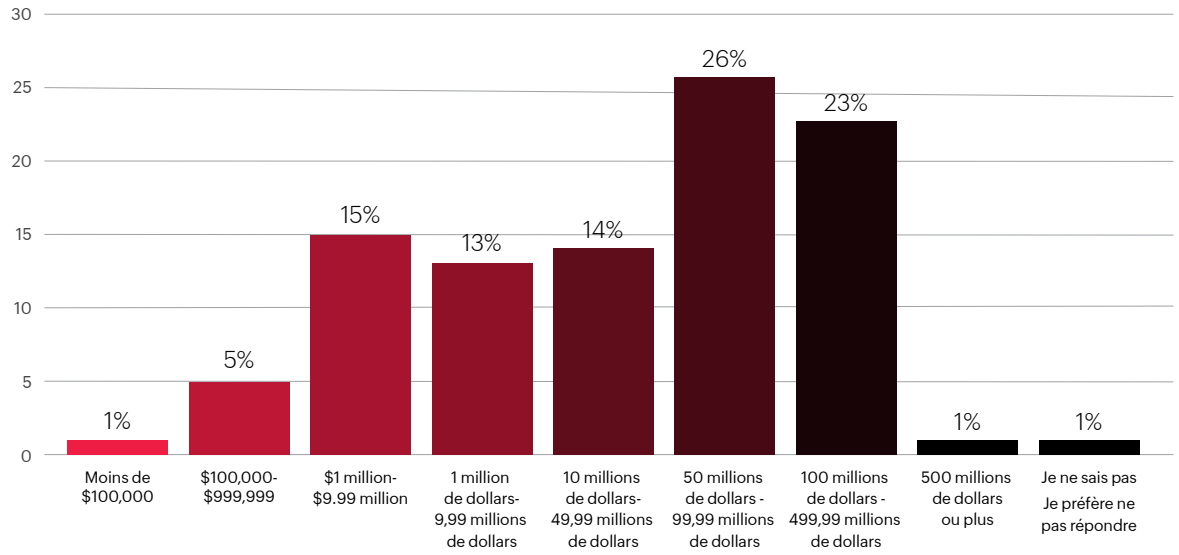
Taille de l'entreprise

Q. Quel est le chiffre d'affaires annuel moyen de votre entreprise ?



Chiffre d'affaires des entreprises

Q. Quel est le chiffre d'affaires annuel moyen de votre entreprise ?



L'enquête comprenait un total de 20 questions, qui portaient sur l'utilisation du cloud dans les organisations interrogées, le budget et les ressources consacrés à la sécurité du cloud, l'utilisation des outils de sécurité du cloud, les attentes et les priorités des organisations vis-à-vis des CASB, et les menaces de sécurité du cloud que les organisations considèrent comme les plus importantes. Le présent rapport contient nos conclusions.

Le développement du multi-cloud

Il faut une équipe pour détecter et sécuriser le réseau contre les menaces, non seulement en termes d'analystes de la sécurité et de ressources informatiques, mais aussi en termes de capacités d'outils.

72%

des organisations interrogées optent pour des applications multi-cloud.

5%

ont déployé un système de cloud hybride.

23%

prévoient d'adopter le cloud computing au cours des 24 prochains mois.

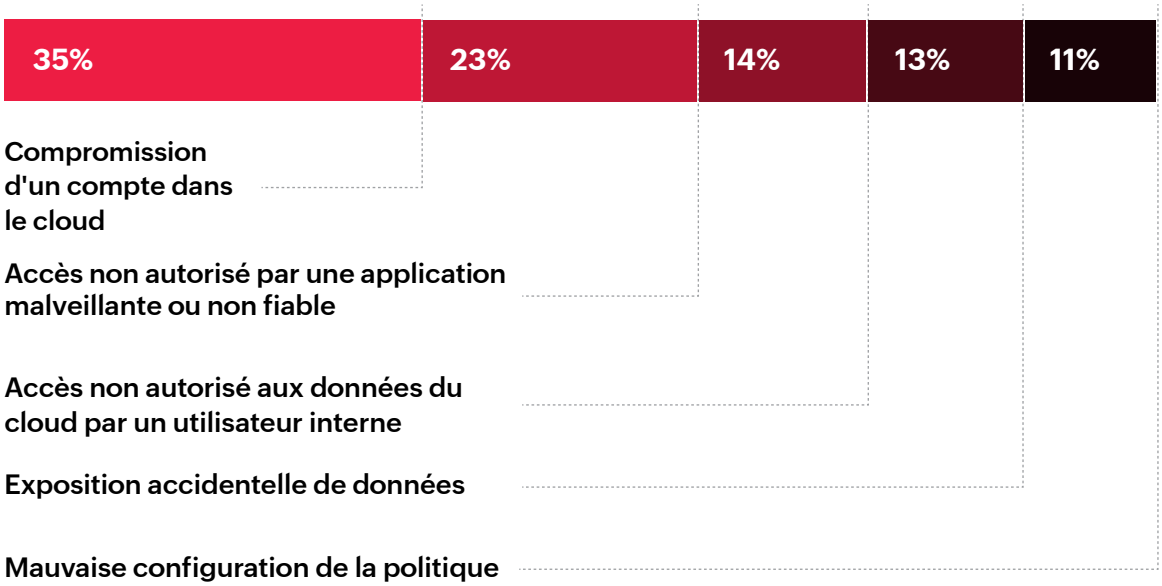
Les organisations optent pour des applications multi-cloud en raison des capacités spécifiques offertes par chaque fournisseur de services et pour éviter une concentration des données au sein d'une seule plateforme cloud. Mais cela peut rendre difficile l'élaboration d'une stratégie de sécurité cloud concise pour toutes les plateformes, car chaque fournisseur de services cloud (CSP) a son propre ensemble de politiques de sécurité qui doivent être respectées.

Le paysage des menaces pour la sécurité du cloud

Les organisations se sont tournées en masse vers le cloud en raison de son évolutivité. Cependant, cela a également augmenté la probabilité de cybermenaces, car l'urgence de passer au cloud a pris le pas sur la mise en œuvre de stratégies de sécurité du cloud. Les organisations sont ainsi devenues vulnérables aux cyberattaques qui ont eu un impact sur leur réputation et leurs finances.

La question suivante a été posée aux participants à l'enquête :

Quelle est, selon vous, la menace la plus courante et la plus importante en matière de sécurité du cloud ?



Trente-cinq pour cent des répondants à l'enquête estiment que la compromission d'un compte cloud est la menace la plus importante pour la sécurité du cloud. Viennent ensuite l'accès non autorisé par des applications externes malveillantes ou non fiables (23 %) et les utilisateurs internes (14 %). **Ensemble, les menaces de sécurité basées sur l'identité sont les préoccupations les plus importantes en matière de sécurité dans le cloud.**

Après le passage au cloud, les attaques basées sur l'identité ont augmenté, probablement en raison de l'augmentation du nombre d'utilisateurs et d'identités dans le cloud au sein des organisations pour s'adapter aux environnements de travail à distance et hybrides. En outre, les identités sont plus faciles à cibler que les systèmes de sécurité périmétrique, car ces systèmes ont plusieurs couches de protection qu'il est difficile pour l'attaquant de contourner. Les utilisateurs sont une cible facile, car un simple courriel d'hameçonnage suffit souvent à l'auteur de la menace pour accéder au réseau.

C'est pour cette raison que les organisations considèrent que la compromission des comptes cloud et l'accès non autorisé sont les menaces les plus importantes en matière de sécurité cloud.

> **L'entreprise américaine Civicom a été victime d'une violation de données après avoir laissé son compte Amazon S3 ouvert et accessible sans avoir mis en place de processus d'authentification des utilisateurs. Le bac S3 mal configuré a laissé plus de 100 000 fichiers vidéo et audio de clients exposés, ce qui équivaut à plus de 8 To de données. La violation a exposé des milliers d'heures de conversations privées entre les clients de Civicom, ainsi que des informations personnelles identifiables (PII) telles que les noms complets et les images des employés des clients.**

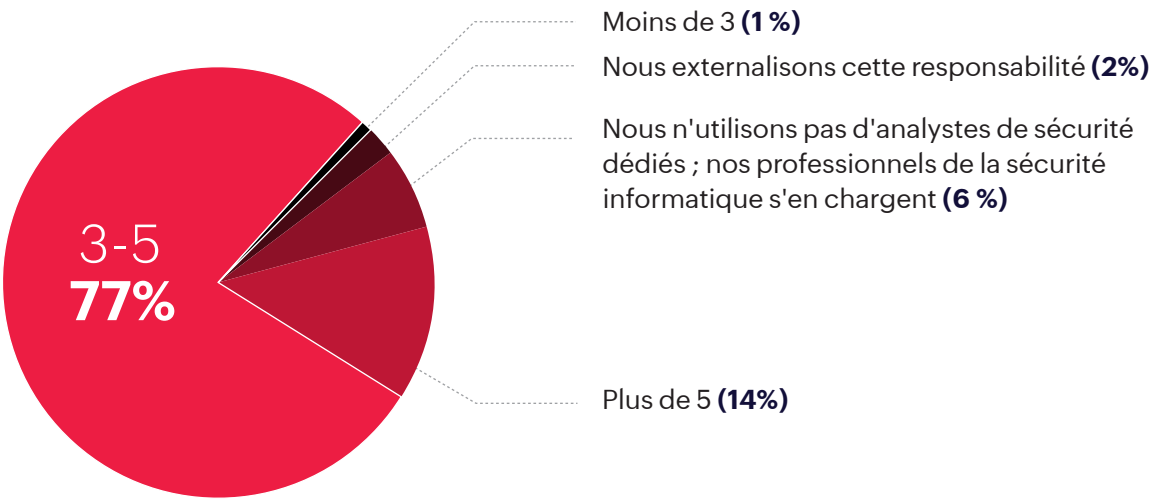
Cet incident met en évidence la manière dont des menaces telles qu'un accès non autorisé peuvent avoir un impact sur une organisation. L'attaque n'a pas seulement porté atteinte à la réputation de Civicom, mais aussi à la vie privée de ses clients. Cela montre à quel point il peut être facile pour des pirates d'accéder à un réseau et à quel point il est important de mettre en place une stratégie de sécurité dans le cloud pour détecter et prévenir les attaques.

Les petits SOC sont-ils suffisants ?

Il faut une équipe pour protéger efficacement un réseau contre les menaces. Cependant, seulement 14 % des organisations interrogées ont plus de cinq analystes de sécurité dans leur SOC. Six pour cent n'ont pas d'analystes de sécurité dédiés à l'élaboration de stratégies de sécurité et 2 % externalisent cette tâche.

La question suivante a été posée aux participants à l'enquête :

Combien d'analystes de sécurité y a-t-il dans votre centre d'opérations de sécurité ?



Un réseau comporte plusieurs terminaux qui doivent faire l'objet d'une surveillance continue - il faut surveiller en permanence les systèmes, les utilisateurs et l'accès aux ressources au sein du réseau. Les SOC doivent non seulement assurer la sécurité des données et du réseau, mais aussi répondre aux exigences de conformité, ce qui peut s'avérer difficile pour une petite équipe SOC.

En outre, la majorité des organisations ont adopté des applications multi-cloud, et chaque fournisseur de services cloud applique ses propres politiques de sécurité. Il est donc difficile d'élaborer une stratégie de sécurité concise, raison pour laquelle de nombreuses organisations ont recours à un outil CASB.

Le grand CASB

Selon Gartner, les CASB sont des "points d'application des politiques de sécurité sur site ou sur le cloud, placés entre les consommateurs de services cloud et les fournisseurs de services cloud pour combiner et interjeter les politiques de sécurité de l'entreprise lors de l'accès aux ressources basées sur le cloud". Les CASB consolident plusieurs types d'application des politiques de sécurité".

Les fonctionnalités d'un CASB peuvent être divisées en quatre piliers : visibilité, détection des menaces, sécurité des données et conformité. Ce sont ces fonctions qui font d'un CASB un élément crucial de la stratégie de sécurité dans le cloud d'une organisation.

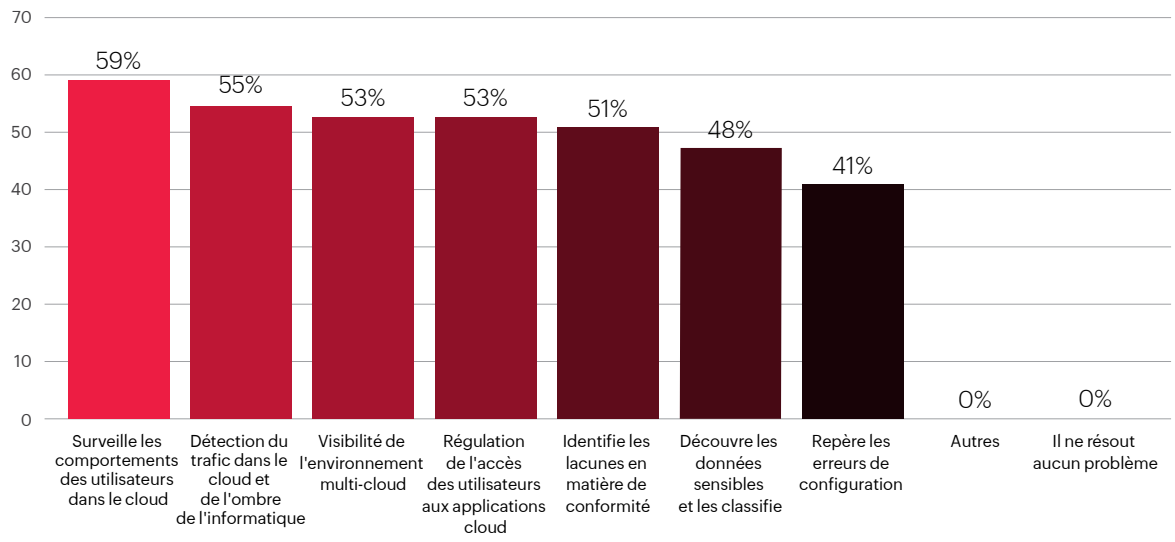
96%

des organisations interrogées utilisent une solution CASB pour sécuriser leur architecture de sécurité cloud.

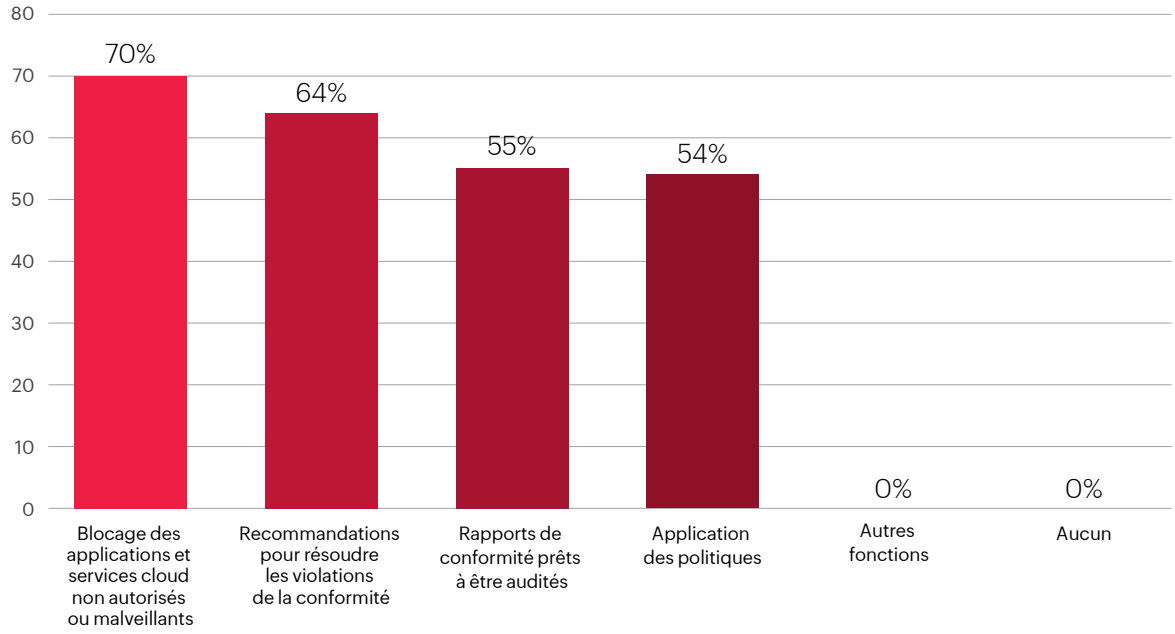
Sur ce pourcentage, 70 % utilisent un outil CASB hébergé dans le cloud et 30 % ont déployé la solution sur site.

Les questions suivantes ont été posées aux participants à l'enquête :

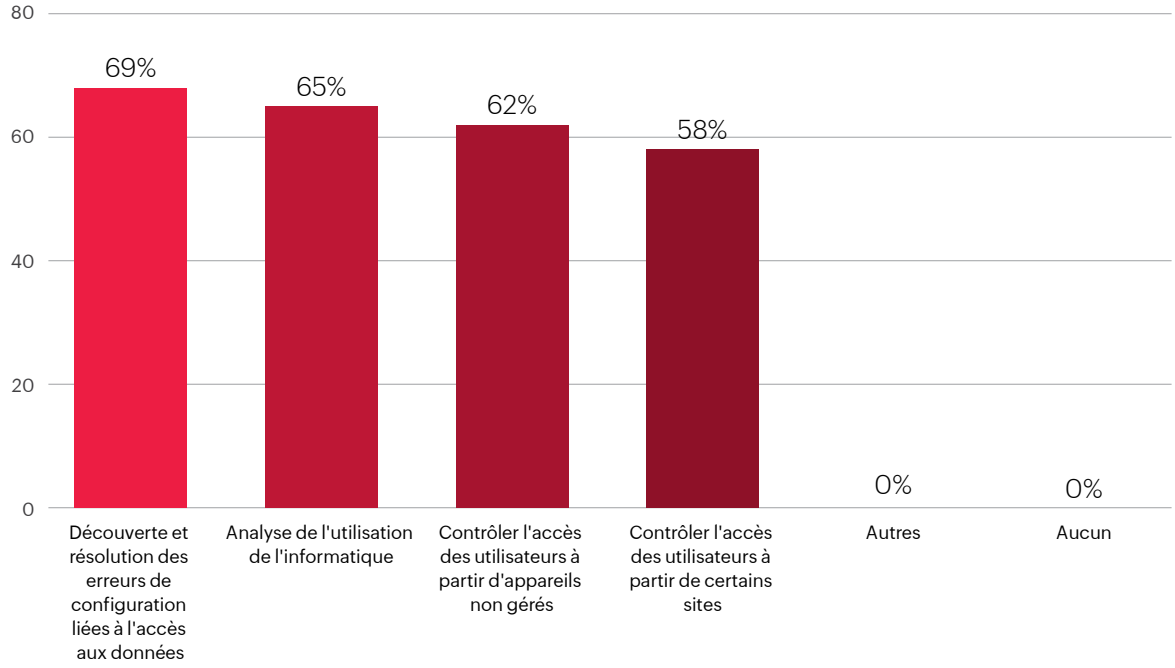
Quel est l'objectif de votre solution CASB ?



Quelles sont les fonctionnalités de conformité les plus importantes de votre solution CASB ?



Quelles sont les capacités de contrôle de sécurité les plus importantes de votre solution CASB ?



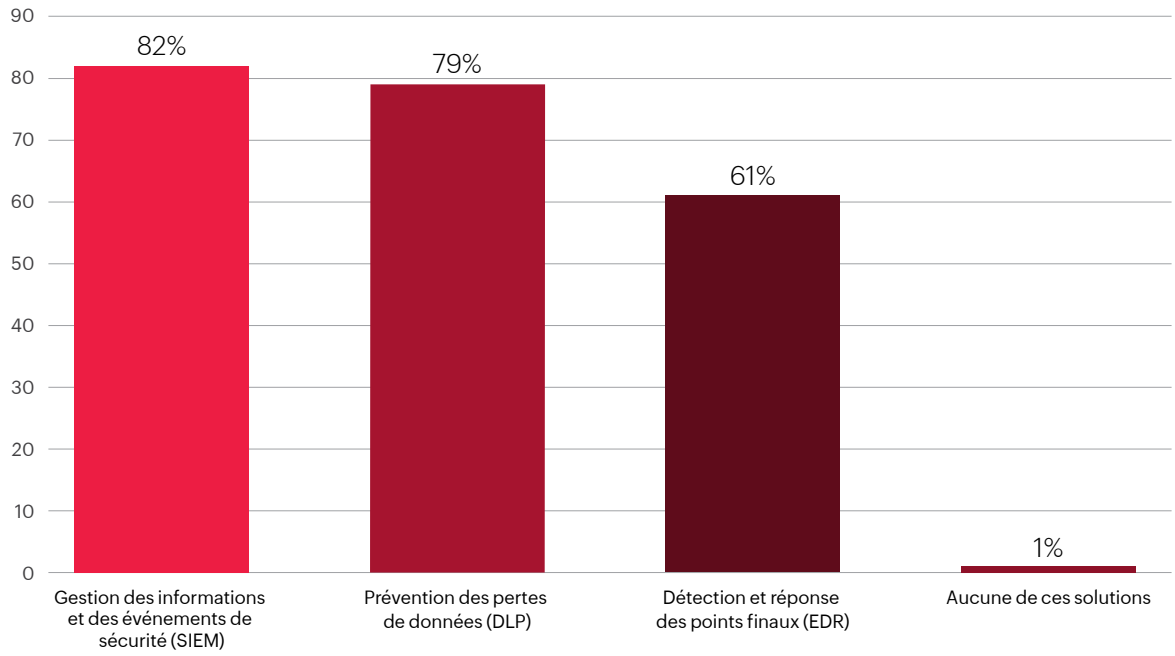
Stratégie et solutions de sécurité dans le cloud

Il est donc impératif de mettre en œuvre une stratégie de sécurité qui offre une visibilité sur les différentes plateformes cloud, surveille les mouvements de données sur toutes les plateformes, assure la défense contre les menaces internes et externes et respecte simultanément les règles de conformité.

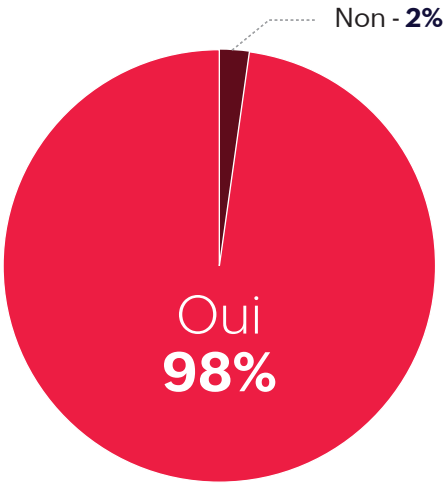
La plupart des organisations utilisent différents outils pour remplir ces diverses fonctions.

Les questions suivantes ont été posées aux participants à l'enquête :

Parmi les solutions de sécurité suivantes, lesquelles utilisez-vous dans votre organisation ?



Contrôlez-vous les accès de vos utilisateurs aux données stockées dans le cloud ?



Les CASB consolident ces différentes fonctions - ils offrent une visibilité sur les différents environnements cloud et aident à respecter les mandats de conformité, à sécuriser les données et à se protéger contre les menaces, devenant ainsi une partie intégrante de l'architecture de sécurité cloud. Mais un outil CASB ne suffit pas à lui seul à sécuriser un réseau, car il ne surveille que le cloud. Le marché exige donc l'intégration et l'orchestration des CASB avec d'autres outils pour créer une solide architecture de sécurité dans le cloud.

Perspectives 2023 en matière de sécurité du cloud : Tendances prédites sur la base des résultats de l'enquête

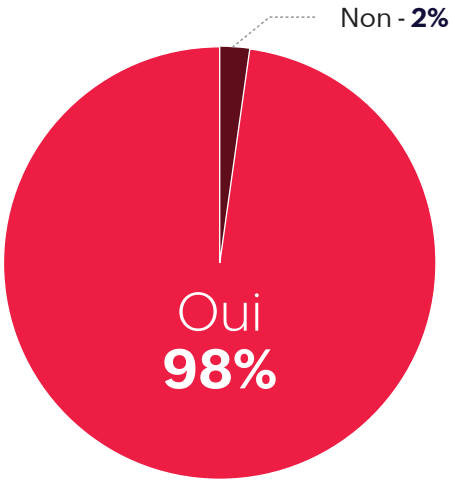
Intégration et consolidation

Il existe un décalage entre la demande et la main-d'œuvre disponible dans le domaine de la cybersécurité. L'étude (ISC)² Cybersecurity Workforce Study indique que bien que la main-d'œuvre augmente rapidement (la main-d'œuvre en cybersécurité s'élève à 4,7 millions en 2022, soit une augmentation de 11,1 % par rapport à l'année précédente et le nombre le plus élevé enregistré à ce jour), la demande croît beaucoup plus rapidement, alimentée par le passage rapide au cloud. Les organisations ont besoin d'une équipe tout aussi importante pour faire face aux différentes menaces qui se profilent à l'horizon.

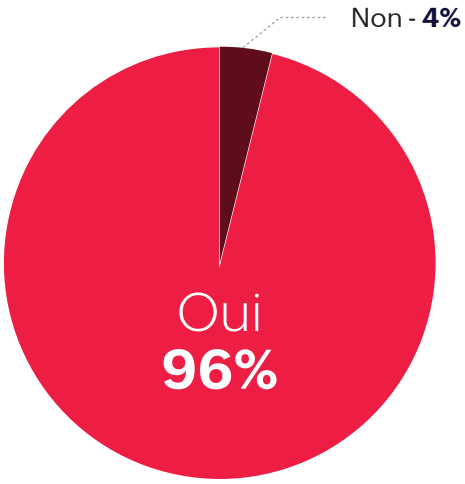
L'étude indique également que le déficit de main-d'œuvre dans le domaine de la cybersécurité a augmenté de 26,2 % en 2022. Ce déficit doit être comblé, et l'un des moyens d'y parvenir est la consolidation. Quatre-vingt-quatorze pour cent des personnes interrogées ont déclaré utiliser différents outils de sécurité pour couvrir les différents aspects de leur stratégie de sécurité informatique. Quatre-vingt-seize pour cent des organisations interrogées ont déclaré qu'elles évalueraient une solution qui exécute toutes les fonctions à partir d'une console unique.

Les questions suivantes ont été posées aux participants à l'enquête :

Utilisez-vous différents outils de sécurité pour protéger les données, contrôler l'accès des utilisateurs, respecter les obligations de conformité et obtenir une visibilité sur les activités dans les plates-formes cloud ?



Allez-vous évaluer une solution capable d'exécuter toutes ces fonctions à partir d'une seule console ?



La consolidation des infrastructures de sécurité et l'intégration du CASB avec d'autres solutions de sécurité telles que le SIEM est un moyen d'améliorer la résilience du cloud et de réduire la charge de travail.

Budgétiser avant la récession

Compte tenu de la récession mondiale probable en 2023, les organisations doivent se préparer à des coupes budgétaires et à des dépenses plus restreintes. Cependant, un budget réduit et moins de ressources dans le SOC d'une organisation laissent place à de nombreuses vulnérabilités.

La consolidation joue ici encore un rôle, car elle offre une meilleure visibilité, une plus grande efficacité opérationnelle et améliore la bande passante interne pour laisser moins de place aux erreurs et aux vulnérabilités.

Lois sur la protection des données

Des États américains comme la Californie, l'Utah, le Colorado, la Virginie et le Connecticut introduisent des lois sur la protection des données à caractère personnel qui doivent entrer en vigueur à partir de 2023, et de nombreux États cherchent à les suivre. Bien que des lois sur les données et la protection de la vie privée existent déjà aux États-Unis, elles concernent plus ou moins des secteurs spécifiques. Ce nouvel ensemble de lois projette une tendance à protéger le droit général des utilisateurs à la vie privée plutôt que de spécifier les types de données que des industries particulières peuvent traiter. Cette tendance à la conformité peut s'expliquer par les nombreuses violations de données constatées en 2022.

Quarante-huit pour cent de ceux qui surveillent leur accès au cloud ou qui ont déployé des systèmes de cloud hybride déclarent que le processus de mise en conformité est très difficile. Seules 16 % d'entre elles affirment qu'elles sont parfaitement au point. Un outil de sécurité consolidé qui assure la conformité tout en surveillant le cloud et en protégeant les données est la voie à suivre.

Conclusion

Avec plus de 77% des organisations utilisant des applications multi-cloud ou des déploiements hybrides et la récession annoncée pour 2023, il est devenu essentiel d'assurer la résilience de la sécurité du cloud.

Compte tenu du grand nombre de menaces et d'attaques qui peuvent se produire au sein d'un réseau, du grand nombre de ressources nécessaires pour se défendre contre ces attaques et du manque de personnel dans le domaine de la cybersécurité, les entreprises ont besoin d'un outil concis et consolidé capable de fournir une visibilité sur les différentes plateformes cloud, de se défendre contre les menaces, de protéger les données et d'aider à la conformité, tel qu'un CASB.

Si un CASB protège efficacement les données dans le cloud, il n'est pas aussi efficace en dehors du cloud. Une solution CASB seule n'est pas suffisante pour sécuriser un réseau de manière adéquate. Pour construire une architecture de sécurité solide, un CASB doit fonctionner en tandem avec d'autres outils de sécurité tels que EDR, SOAR, SIEM et UEBA afin de construire une architecture de sécurité cloud solide et d'atteindre la résilience de la sécurité cloud.

À propos de ManageEngine

Les entreprises établies et émergentes - y compris 9 des 10 organisations du Fortune 100 - s'appuient sur les outils de gestion informatique en temps réel de ManageEngine pour assurer la performance optimale de leur infrastructure informatique, y compris les réseaux, les serveurs, les applications, les postes de travail et bien plus encore. ManageEngine possède des bureaux dans le monde entier, notamment aux États-Unis, aux Pays-Bas, en Inde, aux Émirats arabes unis, au Mexique, à Singapour, au Japon, en Chine et en Australie, ainsi que plus de 200 partenaires mondiaux qui aident les entreprises à aligner étroitement leurs activités et leurs technologies de l'information.

Pour plus d'informations, veuillez consulter le site **manageengine.com/fr**

Blog | LinkedIn | Facebook | Twitter

ManageEngine

Solutions SIEM de ManageEngine

ManageEngine Log360

Log360 est une solution SIEM unifiée avec des capacités DLP et CASB intégrées qui fournit une visibilité holistique de la sécurité à travers les réseaux sur site, cloud et hybrides grâce à ses capacités d'analyse et de surveillance de la sécurité intuitives et avancées.

Log360 est également disponible en tant que déploiement dans le cloud (Log360 Cloud) qui fournit des fonctionnalités SIEM en tant que service. Il peut détecter, prioriser et résoudre les incidents de sécurité, et vous aider à vous conformer aux mandats réglementaires, le tout à partir du cloud.

ManageEngine EventLog Analyzer

EventLog Analyzer est le composant de gestion des journaux de Log360 qui peut collecter, analyser, corréler et stocker en toute sécurité les données des journaux, et effectuer des analyses des menaces pour repérer et atténuer les incidents de sécurité.

ManageEngine ADAudit Plus

ADAudit Plus est le composant d'audit de sécurité de Log360 qui surveille et audite l'environnement Active Directory afin de détecter, d'analyser et d'atténuer les menaces de sécurité internes, et de surveiller les changements de GPO. C'est un auditeur piloté par UBA qui aide à maintenir votre AD, Azure AD, les systèmes de fichiers (y compris Windows, NetApp, EMC, Synology, Hitachi, et Huawei), les serveurs Windows, et les stations de travail sécurisés et conformes. ADAudit Plus transforme les données brutes et bruyantes des journaux d'événements en rapports et alertes en temps réel, ce qui vous permet d'obtenir une visibilité complète des activités qui se déroulent dans votre écosystème Windows Server en quelques clics seulement.

Courriel d'assistance : **support@log360.com**

Numéro d'appel direct : **+1-408-352-9254**

Numéros gratuits

Canada: +86 400 660 8680

ROYAUME-UNI : 0800 028 6590

ÉTATS-UNIS: +1 844 649 7766

International: +1 925 924 9500

AUSTRALIE: 1800 631 268