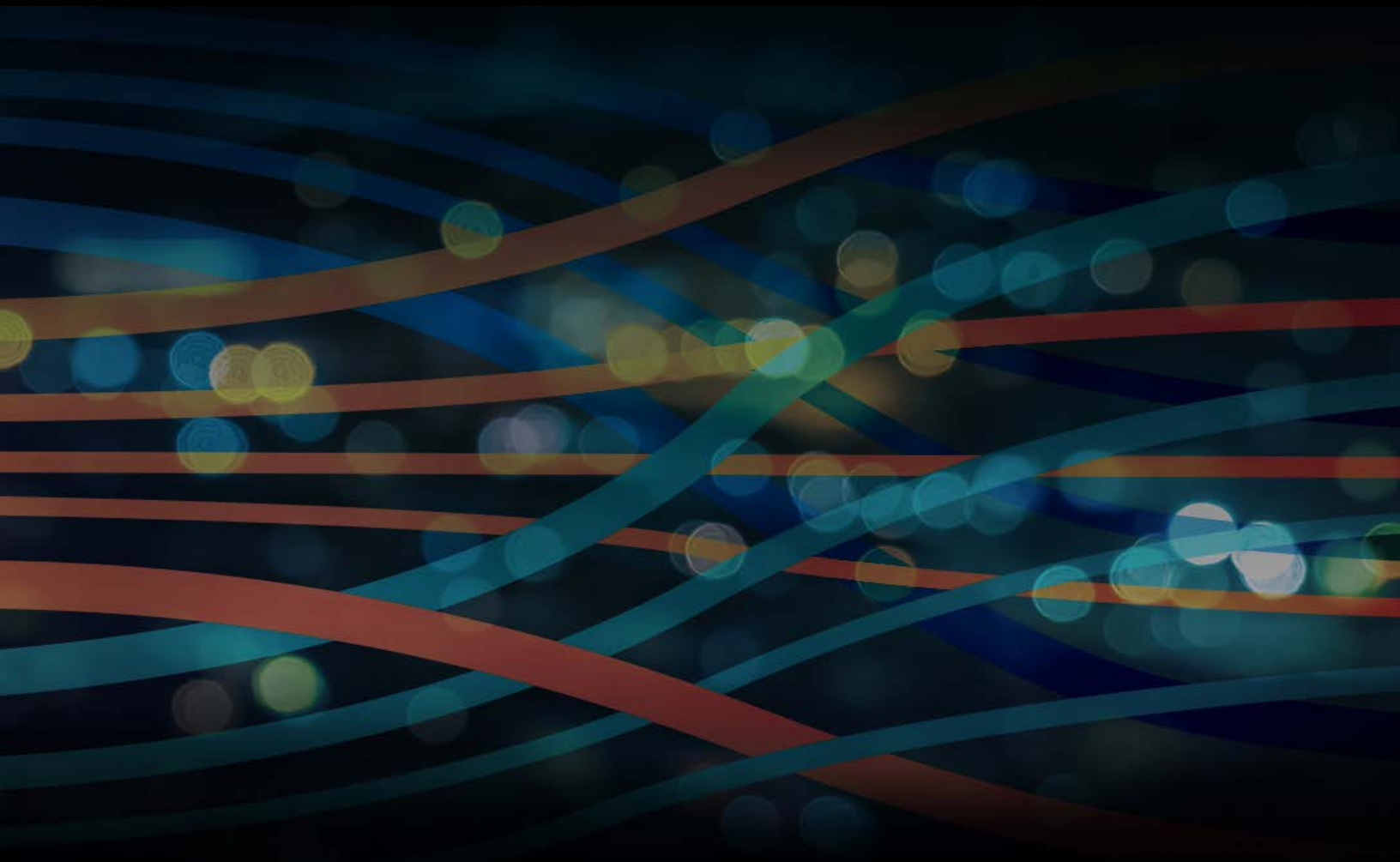
netskope

LIVRE BLANC

Comment aborder la gestion des risques de sécurité dans le cloud



Avec l'arrivée de la COVID-19, le télétravail est devenu la nouvelle norme, accélérant une tendance qui était déjà bien engagée. Aujourd'hui, 64 % des employés effectuent leur travail en dehors des bureaux de l'entreprise[1]. Peu d'analystes s'attendent à ce que cette tendance s'inverse complètement une fois que la pandémie ne sera plus une menace.

Mais des problèmes de sécurité liés à l'accès au cloud et aux applications se posaient déjà bien avant 2020. La pandémie a accentué ces défis, et il existe désormais un risque partout où les utilisateurs accèdent aux données via le cloud.

Le Secure Access Service Edge (SASE) est un cadre permettant aux entreprises et aux gouvernements de faire face aux facteurs de risque liés aux applications dans le cloud, aux données sensibles se déplaçant vers et entre ces applications, et aux utilisateurs effectuant des actions à risque. L'évolution constante de ces facteurs de risque, notamment l'apparition de nouvelles applications, l'augmentation du volume et du type de données transférées vers le cloud, ainsi qu'un plus grand nombre d'utilisateurs individuels avec des caractéristiques différentes, rendent nécessaire une gestion continue des risques. La gestion de la sécurité n'est pas quelque chose que les équipes peuvent « définir puis oublier » : les facteurs de risque changent, seconde après seconde, et les équipes doivent être en mesure d'ajuster en permanence les politiques en conséquence.

Les équipes de sécurité ne peuvent pas appréhender le paysage du cloud de la même manière qu'elles protègent les systèmes sur site. Et elles ne peuvent pas obliger des produits qui n'ont pas été conçus pour la sécurité et la connectivité du cloud à supporter cette charge. L'utilisation d'outils inefficaces et d'analyses incomplètes empêche les équipes d'évaluer avec précision le niveau de risque du cloud.

Examinons comment nous en sommes arrivés à ce défi actuel et comment le résoudre dès aujourd'hui.

Sortir des sentiers battus

Janvier 2020 (avant la COVID-19) :

89 % des utilisateurs d'entreprise étaient utilisaient des services et applications cloud managés et non managés.[2]

Projection de mars 2020 :

55 % des charges de travail des entreprises auront migré vers le cloud d'ici 2022.[3]

Août 2021 :

83 % des utilisateurs utilisent des instances d'applications personnelles sur des appareils managés et téléchargent en moyenne 20 fichiers par mois.[4]

[1]« Remote Work @ Risk: Cloud and Threat Report, » Netskope Threat Labs, août 2020.
[2]« The Dark Side of the Cloud: Cloud and Threat Report, » Netskope Threat Labs, févr. 2020.
[3]Tim Maurer et Garrett Hinck, « Cloud Security: A Primer for Policymakers, » Carnegie Endowment for International Peace, » 31 août 2020.
[4]"Cloudy with a Chance of Malice: Cloud and Threat Report, » Netskope Threat Labs, févr. 2021.

Après une recherche rapide, un responsable de marché tombe sur l'un des nombreux outils de transfert de fichiers freemium ou à bas prix disponibles. Il s'agit d'un outil facile à utiliser et accessible indépendamment du lieu de travail de l'employé. Le responsable utilise sa carte d'entreprise et offre à ses employés la solution de productivité dont ils ont besoin. Ce qu'il ignore, c'est que le passage à cette application dans le cloud ouvre une brèche de sécurité qui met les données de l'entreprise en danger.

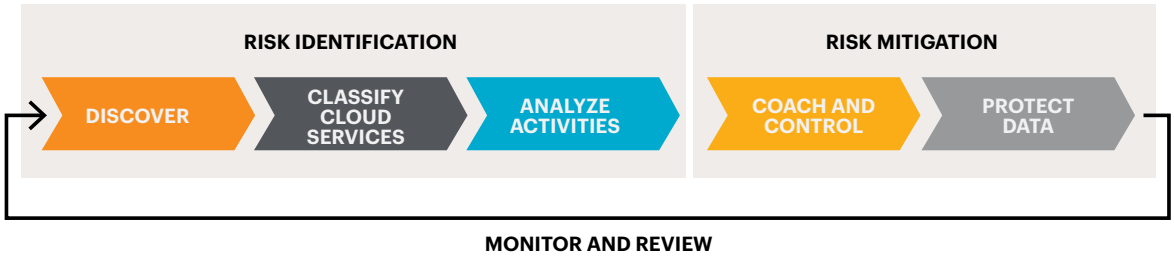
Quelques mois plus tard. L'équipe de sécurité apprend par inadvertance que 50 000 dossiers de clients se trouvent dans cet outil de partage de fichiers. Elle n'a pas la possibilité de contrôler la façon dont ces données sont protégées et n'a aucune visibilité sur les événements de sécurité qui pourraient affecter ces données. Le risque que cela représente pour l'entreprise est énorme.

La protection des données doit évoluer avec son temps

Comment pouvez-vous verrouiller les données et les applications de l'entreprise si vous ne déployez et ne configurez pas les serveurs, ne gérez pas les bases de données et ne définissez pas la politique de sécurité ? Vous pouvez adopter une approche de sécurité dans le cloud qui 1) déplace la sécurité entre les utilisateurs et les applications, quel que soit l'endroit où ils se trouvent, et 2) assure une gestion continue des risques.

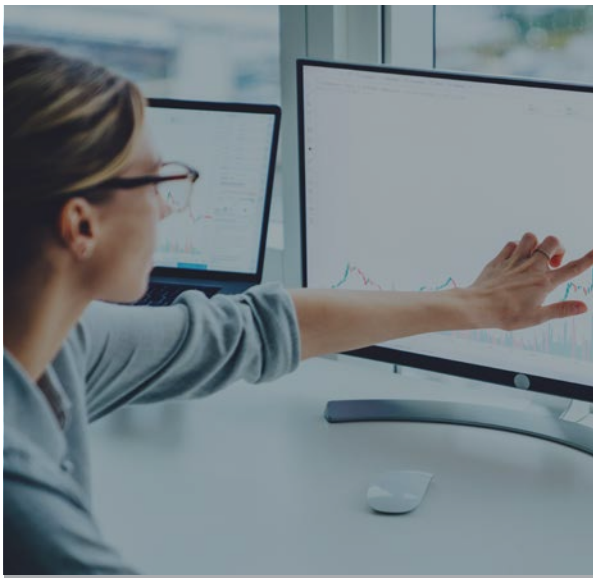
DÉVELOPPER UNE STRATÉGIE DE GESTION DES RISQUES

Plusieurs étapes sont nécessaires, elles sont représentées dans le diagramme ci-dessous.



Identification des risques

- Découvrez les applications cloud utilisées dans votre organisation.
- Classifiez le niveau de risque associé à chaque application ou lieu de stockage de données, ainsi que le risque organisationnel associé.
- Identifiez les utilisateurs qui accèdent à chacune de ces applications, ainsi que leurs activités et les activités associées qu'ils effectuent.



Réduction des risques

- Permettez aux utilisateurs d'utiliser les applications en atténuant les risques pour les données. Orientez les utilisateurs vers de meilleures alternatives lorsque le risque est faible, et établissez des contrôles pour gérer les facteurs de risque lorsque le risque est élevé.
- Protégez les données particulièrement sensibles en affinant les politiques de protection des données qui supervisent le stockage et contrôlent les mouvements.

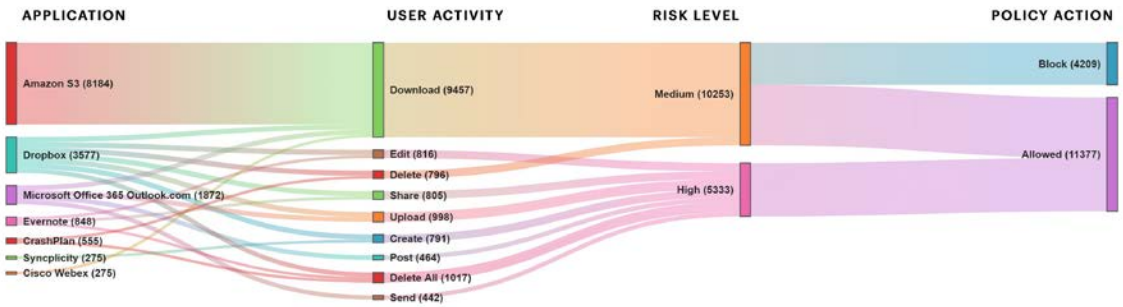
Suivi et révision

- Mettez en place une boucle de rétroaction pour surveiller les risques liés au cloud de manière continue, en fournissant les rapports appropriés à tout le monde, des professionnels de la sécurité de première ligne à la direction et au conseil d'administration.

Certaines de ces étapes peuvent sembler évidentes, mais le point essentiel réside dans le fait qu'il s'agit d'un processus qui doit être évalué en permanence dans une boucle de rétroaction, ce qui n'est pas simple. Si vous demandez aujourd'hui à votre équipe de sécurité de dresser la liste de toutes les applications cloud qui stockent certaines des données de votre entreprise, il est peu probable qu'elle ait une réponse toute prête. Cela peut être aussi difficile que d'identifier les applications utilisées par l'organisation, et cela se complique de plus en plus. Si vous leur demandez les risques associés aux applications, c'est encore plus difficile, car comment peut-on identifier et noter les facteurs de risque sur des applications que vous pouvez (ou non) connaître ?

Visibilité et contrôle des données et de l'accès au cloud

Pour mettre en place un programme de sécurité efficace, les entreprises doivent avoir une visibilité sur les applications qu'elles utilisent, savoir où se trouvent les données et où elles vont. Les solutions Netskope sont conçues pour suivre les données tout au long de leur cycle de vie, où qu'elles aillent. Cette approche est conçue pour créer une visibilité sur le stockage et le mouvement des données dans le cloud et permet aux équipes d'agir immédiatement si l'accès ou le mouvement présente un risque.



Le Netskope Security Cloud allie une passerelle Web sécurisée (SWG) de nouvelle génération, un Cloud Access Security Broker (CASB) et un système reconnu de prévention des pertes de données (DLP) avec des microservices de sécurité tels que la protection des données et le contrôle d'accès évolutif. La plateforme découvre l'utilisation par une entreprise de logiciels mode que service (SaaS), d'infrastructures en tant mode service (IaaS) et d'applications Web. Elle peut également identifier les utilisateurs et les appareils qui y accèdent, et fournir des détails granulaires sur leurs activités.

Advanced Analytics : une clé pour la gestion des risques

Une fois que le Netskope Security Cloud est en place, Netskope Advanced Analytics ferme la boucle de la gestion continue des risques.

En effet, le plus dur est de veiller à ce que votre organisation tienne compte des nouveaux vecteurs de risque et de supprimer les accès excessifs là où ils ne sont pas nécessaires. En d'autres termes, la gestion des risques exige une adaptation constante pour s'assurer que vous restez dans une fourchette acceptable de risques tolérables, même si les applications, les utilisateurs et les données utilisés sont en pleine évolution.

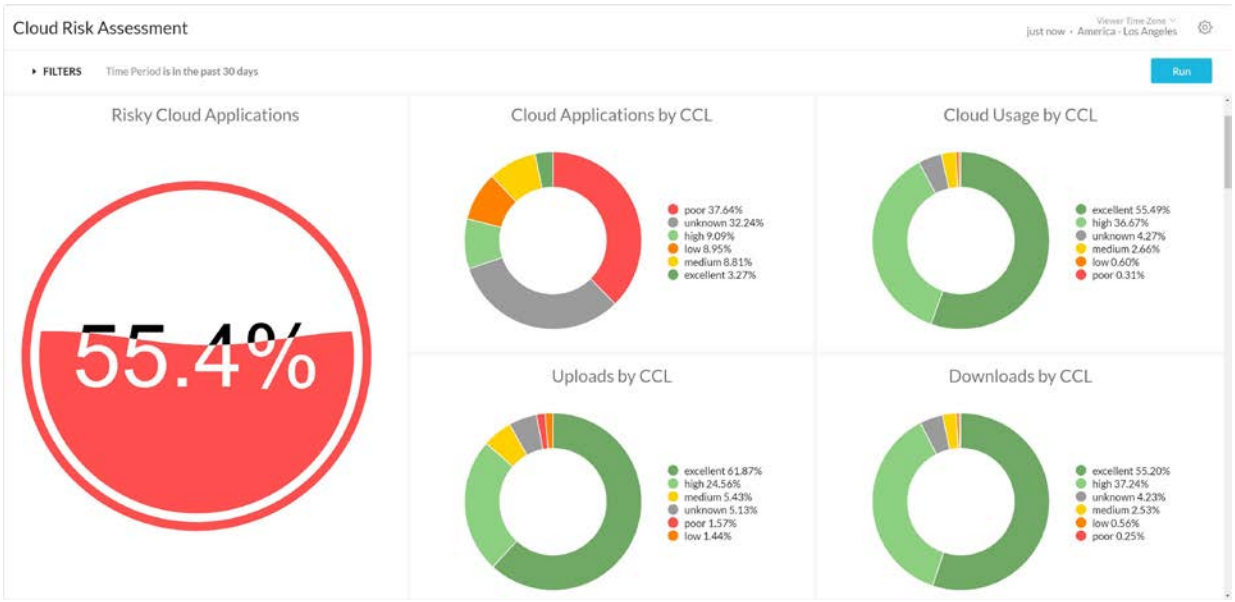
Si vous avez 10 000 dossiers clients répartis sur dix applications cloud, est-ce acceptable ou trop risqué ? Et s'il s'agit de 10 millions de dossiers ? Comment les RSSI peuvent-ils déterminer la tolérance au risque de l'entreprise et créer une politique de sécurité qui répond aux besoins de la direction et du conseil d'administration ?

Netskope Advanced Analytics aide les DSI, les RSSI et les équipes informatiques à répondre à ce type de questions. Vous devez définir des indicateurs clés de performance (KPI) qui décrivent l'état actuel et les tendances du risque de sécurité dans l'ensemble de l'entreprise.

Vous pouvez utiliser Advanced Analytics pour établir une base de référence pour chaque indicateur. Ensuite, au fil du temps, vous pouvez surveiller l'évolution de votre exposition au risque et adapter les politiques de sécurité en conséquence.

En fin de compte, Netskope Advanced Analytics aide les RSSI dans trois cas de figure spécifiques :

- Prioriser les efforts d'optimisation de la sécurité
- Améliorer l'efficacité
- Surveiller l'efficacité du programme de sécurité et le niveau de sécurité global du cloud



L'évaluation des risques liés au cloud de Netskope vous permet de surveiller le niveau de confiance du Cloud (CCL) dans l'ensemble de votre organisation afin que vous puissiez identifier le potentiel de risque et mettre en œuvre des politiques de sécurité appropriées pour une adoption sûre et conforme aux besoins de votre entreprise.

1. PRIORISER LES EFFORTS D'OPTIMISATION DE LA SÉCURITÉ

Du point de vue des menaces, votre objectif est d'empêcher un pirate de réussir à compromettre votre utilisateur ou vos données. Mais le paysage des menaces est vaste et se développe rapidement. Comme dans tous les autres domaines de l'informatique, la gestion des risques exige de hiérarchiser les ressources en fonction de l'exposition de l'entreprise au cloud.

Netskope Advanced Analytics soutient les décisions de priorisation en facilitant la compréhension des évaluations du paysage de la sécurité. Les tableaux de bord, les rapports et les alertes fournissent des informations adaptées à des groupes spécifiques de parties prenantes, dans un format conçu pour ces publics. Ainsi, le personnel d'exploitation, la direction et tous les autres intervenants peuvent accéder rapidement aux informations les plus pertinentes pour leur rôle. Grâce à un large éventail d'options de visualisation des données, Advanced Analytics permet de comprendre instantanément les tendances des données.

AVANTAGES DE NETSKOPE

- Les rapports préétablis comprennent des tableaux de bord adaptés au personnel d'exploitation, aux cadres supérieurs et autres.
- Possibilité d'importer et d'exporter des tableaux de bord pour collaborer avec d'autres équipes de sécurité.
- Les tableaux de bord personnalisés peuvent s'appuyer sur plus de 500 champs de données.
- Les alertes complètent les rapports à la demande, en signalant les indicateurs qui se situent en dehors d'une plage spécifiée.
- Les options de visualisation comprennent des graphiques à barres, des graphiques circulaires, des lignes de tendance, des tableaux, des diagrammes de dispersion, etc.
- Les données disponibles comprennent des détails sur le site, l'application, l'instance, l'utilisateur, l'activité, le fichier, la source/destination, etc.

2. AMÉLIORER L'EFFICACITÉ DU PERSONNEL DE SÉCURITÉ

Le personnel de sécurité qualifié est l'une des ressources les plus précieuses d'une organisation. Alors qu'ils s'efforcent de protéger les utilisateurs et les données de l'organisation, leur temps doit être consacré à l'analyse et à la stratégie, et non à la recherche de données pertinentes et appropriées, et au filtrage de la charge de travail des alertes pour découvrir les causes profondes. Les rapports personnalisés de Netskope Advanced Analytics donnent aux équipes de sécurité une visibilité instantanée de toutes les informations dont elles ont besoin, afin d'identifier le signal dans tout le bruit.

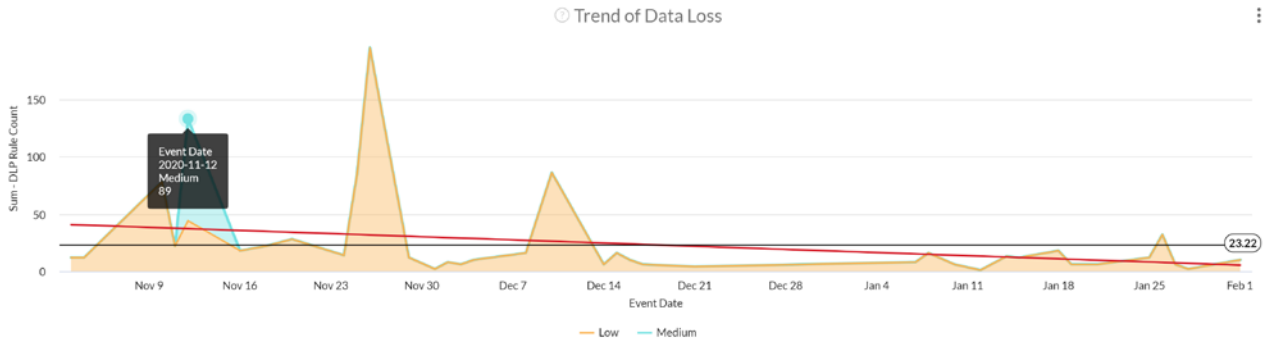
En même temps, la recherche des sources de risque est une étape essentielle pour gérer et contrôler le risque. Netskope Advanced Analytics rationalise également l'exploration des tendances en matière de sécurité. Des widgets interactifs rendent le processus d'exploration intuitif, réduisant ainsi l'effort nécessaire aux équipes de sécurité pour explorer en profondeur les informations granulaires du Netskope Security Cloud.

AVANTAGES DE NETSKOPE

- Une vaste bibliothèque de rapports prédéfinis pour des cas d'usage spécifiques comprend des tableaux de bord orientés RSSI, un rapport d'évaluation des risques du cloud, un tableau de bord pour la protection des données, un rapport de conformité au RGPD, etc.
- La personnalisation permet aux rapports de cibler étroitement une préoccupation de sécurité spécifique, pour un titre de poste spécifique, ce qui réduit le temps nécessaire pour accéder aux informations pertinentes.
- Le générateur de rapports simple à utiliser améliore l'efficacité de la création de rapports personnalisés.
- Effet global : les informations sont plus facilement accessibles, avec moins d'efforts, à tous les niveaux de l'organisation.

3. SURVEILLER L'EFFICACITÉ DU PROGRAMME DE SÉCURITÉ ET LE RISQUE GLOBAL

La capacité d'appréciation des politiques et programmes de sécurité et de la manière dont ils peuvent être améliorés est nécessaire pour la protection continue des activités cloud de l'entreprise.



Les rapports de synthèse de Netskope Advanced Analytics fournissent des données de tendances qui renseignent sur l'efficacité du programme de sécurité. Une politique donnée est-elle trop permissive ? Un utilisateur particulier prend-il de plus en plus de risques dans le cloud ? Restez à l'affût des changements de politique et expliquez à la direction que le nombre d'événements de sécurité augmentera à court terme en raison du renforcement des politiques, mais que les mesures prises réduiront le niveau de risque global au fil du temps. Des rapports complets avec une visualisation optimisée des données permettent de répondre facilement à ces questions.

Le personnel de sécurité peut surveiller l'efficacité de la sécurité du cloud de l'entreprise sur ses tableaux de bord, puis explorer les détails pour découvrir les causes sous-jacentes dans les domaines préoccupants. En utilisant cette approche, ils apprendront où réaliser des ajustements. Ils peuvent ensuite ajuster les politiques et les pratiques de sécurité pour toute l'entreprise, créant ainsi une boucle de rétroaction pour mettre à jour en permanence la gestion et l'atténuation des risques liés au cloud.

AVANTAGES DE NETSKOPE

- La vue à 360 degrés offre une visibilité complète de l'état des risques liés au cloud de l'entreprise pour l'ensemble des applications, des utilisateurs et des données.
- Des analyses sur les données sommaires et détaillées pour mettre en évidence les tendances de sécurité en temps réel.

« Malgré des années d'investissement et de concentration sur les cyber-risques, les coûts des cyber-incidents sont en hausse. Les organisations augmentent leurs dépenses en matière de cybersécurité mais ces investissements sont souvent insuffisants. »

— Tim Maurer et Garrett Hinck, Carnegie Endowment for International Peace[1]

[1]Tim Maurer et Garrett Hinck, « Cloud Security: A Primer for Policymakers, » Carnegie Endowment for International Peace, » 31 août 2020.

BOUCLER LA BOUCLE DE LA GESTION DES RISQUES

Le télétravail est de plus en plus répandu. Les technologies du cloud évoluent encore plus rapidement. Et les menaces qui pèsent sur les applications et les données du cloud se multiplient. La protection des utilisateurs, des données et des applications de votre entreprise nécessite une gestion des risques et un processus d'amélioration continue.

Heureusement, Netskope peut vous aider. Le Netskope Security Cloud, centré sur les données et adapté au cloud, fournit les informations nécessaires pour empêcher les menaces d'atteindre les données que vous êtes chargées de sécuriser. Netskope Advanced Analytics rend ces informations facilement accessibles à tous les niveaux de l'organisation.

Grâce à Advanced Analytics, votre équipe de sécurité peut obtenir les informations dont elle a besoin, repérer les tendances, se concentrer sur les domaines critiques et s'attaquer aux détails importants. Une meilleure analyse vous permet d'élaborer un programme de sécurité capable de vous protéger contre les menaces en constante évolution et de sécuriser efficacement les données dans le cloud.

netskope

Netskope Security Cloud offre une visibilité, une détection des menaces et une protection des données en temps réel et de manière inégalée, où que vous soyez et depuis n'importe quel périphérique. Seul Netskope comprend le cloud et adopte une approche centrée sur les données qui fournit aux équipes de sécurité le parfait équilibre entre protection et rapidité dont elles ont besoin pour sécuriser leur transformation numérique.

Pour en savoir plus, consultez, https://www.netskope.com.