netskope

eBook

6 cas d'utilisation de Zero Trust pour Netskope One, une plateforme SASE unifiée

6 cas d'utilisation de Zero Trust pour Netskope One, une plateforme SASE unifiée

Introduction

De nombreuses équipes chargées des réseaux et de la sécurité ont aujourd'hui pour tâche de prendre en charge un environnement de travail hybride en utilisant des mécanismes de défense pour la plupart anciens. Elles se trouvent dans une position difficile, car lorsque les ressources migrent vers le cloud et les employés vers des environnements de télétravail (comme cela s'est produit à grande échelle depuis 2020 et le début de la pandémie de COVID-19), la sécurité du périmètre sur site et la segmentation du réseau centrée sur le matériel ne sont plus efficaces.

Reposant sur trois principes, le Zero Trust est une meilleure approche pour sécuriser les ressources d'une organisation moderne. Dans le modèle de sécurité Zero Trust, les utilisateurs et les appareils doivent être authentifiés pour chaque nouvelle session, et ils n'ont accès qu'aux ressources dont ils ont besoin. Cette approche du moindre privilège est soutenue par une surveillance complète de la sécurité, grâce à laquelle les activités, les comportements et les tendances des utilisateurs et des ressources sont *continuellement* observés et analysés.

Éléments essentiels d'une stratégie Zero Trust

La sécurité Zero Trust n'est pas un produit que les entreprises peuvent acheter. Il s'agit d'une stratégie d'entreprise essentielle alignée sur des contrôles adaptés au lieu de travail d'aujourd'hui. Un modèle de sécurité Zero Trust repose sur plusieurs technologies fonctionnant de manière interopérable, notamment :

- ***La gestion des utilisateurs et des identités :*** gestion des identités et des accès (IAM) ou gestion des accès à privilèges, contrôles d'accès basés sur les rôles et analyse du comportement des utilisateurs et des entités (UEBA).
- ***La gestion des appareils :*** contrôles de santé des appareils et indices de confiance
- ***La gestion des applications et des charges de travail :*** passerelles web sécurisées (SWG) et solutions SSE (Security Service Edge) avec fonctionnalité de courtier en sécurité d'accès au cloud (CASB)
- ***Les dispositifs de sécurité réseau :*** pare-feu de nouvelle génération (NGFW), passerelles de messagerie sécurisées et solutions SSE avec fonctionnalités SWG, CASB et accès au réseau Zero Trust (ZTNA).

Figure 1 : Modèle de sécurité Zero Trust

Par où commencer et que faire ensuite ensuite avec le Zero Trust ?

Un modèle de sécurité Zero Trust efficace offre une excellente expérience utilisateur, en rendant la sécurité transparente et en imposant peu de contraintes voire aucune sur les charges de travail de l'entreprise. Cela signifie que les entreprises doivent d'abord prendre en compte les personnes et les processus. Une organisation qui passe au Zero Trust doit commencer par définir ses cas d'utilisation et ses processus.

Quand elles commencent à se soucier de la technologie, de nombreuses entreprises se concentrent sur la sécurisation de l'accès des collaborateurs à distance aux ressources, dans le cloud et dans le datacenter. L'approche traditionnelle consistant à placer des dispositifs de sécurité matériels au domicile des employés est coûteuse et difficile à adapter, tandis que le backhauling du trafic des employés distants vers les pare-feux de l'entreprise crée des goulets d'étranglement. La solution la plus simple consiste à installer sur les appareils des employés un client logiciel qui se connecte aux services de sécurité de la périphérie du cloud. En d'autres termes, une plateforme de sécurité cloud SSE qui intègre CASB, SWG et ZTNA.

Une autre approche courante du parcours technologique vers le Zero Trust est de prioriser et de sécuriser le trafic des applications d'entreprise. Les applications basées sur le Software-as-a-Service (SaaS), telles que Microsoft 365 et Salesforce, ont besoin de connexions directes à Internet pour les collaborateurs distants et tous les bureaux. L'introduction d'une solution SSE permet d'inspecter le trafic web, SaaS et Infrastructure-as-a-Service (IaaS) de chaque utilisateur, appareil et emplacement, offrant ainsi une visibilité et un contrôle sur l'ensemble de l'écosystème numérique de l'entreprise.

Un modèle de sécurité Zero Trust efficace offre une excellente expérience utilisateur. Cela signifie qu'une organisation qui passe au Zero Trust doit commencer par cartographier ses cas d'utilisation et ses processus métier.

Comment Netskope SSE soutient le parcours Zero Trust

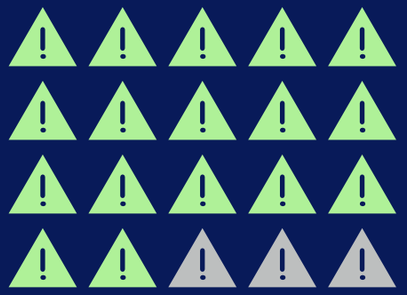
Plutôt que les contrôles binaires basés sur des règles d'autorisation ou de blocage des ports, des protocoles, des domaines, des URL et des applications de la sécurité périmétrique traditionnelle, Netskope Intelligent SSE évalue les risques transactionnels de chaque session. Aucun réseau, appareil ou utilisateur ne se voit accorder une confiance implicite.

Le cœur de la plateforme Netskope One et du composant Intelligent SSE est le moteur Zero Trust Engine (ZTE). Technologie sous-jacente de Netskope Intelligent SSE, ce moteur prend en charge les profils de risque des applications, les profils de risque des utilisateurs et les contrôles de la posture de sécurité des appareils et peut échanger ces profils de risque avec des solutions de sécurité tierces. Il s'intègre aux principales solutions IAM de gestion des identités et à l'authentification multifactorielle (MFA) et peut demander une authentification progressive en fonction du risque transactionnel de la session.

Enfin, la surveillance complète de la sécurité au sein de Netskope Intelligent SSE recourt à des analyses d'informatique décisionnelle et des visualisations de données pour parfaire l'affinement des politiques de moindre privilège Zero Trust d'une organisation. Les tableaux de bord et les graphiques identifient tous les risques utilisateur à signaler, les mouvements de données entre les instances d'application, les profils et les tendances en matière de risques liés à des applications, ainsi que les comportements d'utilisateurs préoccupants. Un même contexte enrichi donnant lieu aux contrôles d'accès adaptatifs à moindre privilège est disponible sur un horizon de 3, 6 ou 13 mois.

Netskope Intelligent SSE et le moteur Zero Trust Engine offrent des avantages importants à toute entreprise ayant des charges de travail dans le cloud. Voici six cas d'utilisation clés qui mettent en évidence leur valeur.

Netskope Intelligent SSE prend des décisions d'accès à l'aide de contrôles évolutifs basés sur un contexte et des données utilisateur riches, renforcés par une gamme exclusive de plus de 100 activités détaillées concernant des milliers d'applications. Par exemple, si Netskope Intelligent SSE exécute une douzaine de contrôles d'activité pour une application donnée et détecte les risques en fonction du contexte de l'utilisateur et de la session, il peut limiter à bon escient les comportements de l'utilisateur au sein de l'application plutôt que de simplement bloquer l'accès au logiciel.



Source : Enterprise Strategy Group

85 %

de réduction des risques liés à l'utilisation des services de sécurité en périphérie, tout en augmentant l'agilité de l'entreprise.

Cas d'utilisation 1 de Zero Trust :

Accroître la visibilité du SaaS

Les recherches menées par Netskope ont révélé que les employés d'une entreprise moyenne utilisent plus de 800 applications, tandis que les employés des grandes entreprises peuvent en utiliser 2 400 ou plus. Nombre d'entre elles sont des applications SaaS basées sur le cloud, et 97 % sont adoptées par des unités opérationnelles ou des utilisateurs individuels sans la supervision de l'équipe informatique.

Il est déconcertant de penser que des employés déplacent des données d'entreprise dans des applications SaaS non gérées. C'est pourquoi Netskope Intelligent SSE s'accompagne d'une option de CASB pour l'inspection en ligne de milliers d'applications. Tout comme les pare-feux inspectent les paquets à travers les ports et les protocoles, les solutions SSE dotées de capacités CASB décodent les applications en ligne pour comprendre le contexte et le contenu de chaque transaction. Cela permet aux stratégies de contrôle d'accès de pouvoir s'adapter et de suivre les principes du Zero Trust.

Netskope Intelligent SSE référence également les profils de risque de plus de 75 000 applications via le Cloud Confidence Index afin d'établir un classement des risques pour toutes les applications utilisées au sein de l'organisation.

Ces fonctionnalités améliorent considérablement la capacité d'une équipe de sécurité à comprendre l'utilisation que font les employés des applications cloud, qu'elles soient autorisées par l'entreprise ou personnelles, et qu'elles soient gérées ou non. L'équipe de sécurité peut mieux comprendre les comportements à risque des employés dans le cloud et limiter l'exposition des ressources de l'entreprise aux solutions SaaS à haut risque.

97 % des applications utilisées dans les entreprises ne sont pas gérées par les services informatiques, mais sont adoptées de manière indépendante par les unités opérationnelles ou les utilisateurs finaux.

800 applications utilisées par les entreprises de taille moyenne

à plus de 2 400 applications utilisées par les grandes entreprises

Cas d'utilisation 2 de Zero Trust :

Protéger la collaboration dans le cloud

Dans les entreprises qui dépendent fortement du télétravail, les plateformes de collaboration cloud sont essentielles. Les employés les utilisent pour partager des informations, rencontrer des clients et des fournisseurs, et accomplir tout ce qui se faisait auparavant dans des salles de conférence ou autour de la machine à café.

Les solutions de collaboration dans le cloud présentent un niveau de risque de sécurité sans précédent car elles sont utilisées très souvent, pour un large éventail d'activités professionnelles, mais ne sont généralement pas gérées par le service informatique de l'entreprise. Le personnel chargé de la sécurité doit pouvoir contrôler la manière dont les employés utilisent ces solutions et les informations qui y sont partagées.

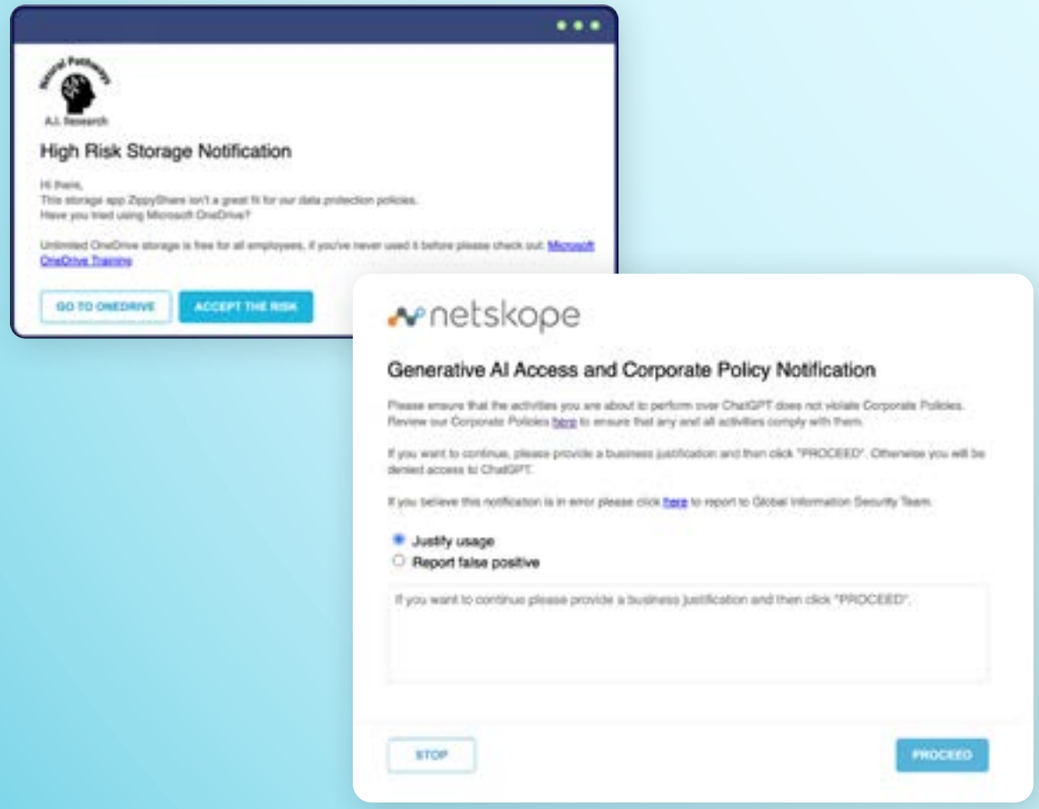
Les contrôles d'accès adaptatifs de Netskope Intelligent SSE constituent une excellente solution pour pallier ces lacunes. La plateforme Netskope comprend des contrôles d'activité pour les solutions de collaboration cloud les plus courantes. Ainsi, Netskope Intelligent SSE décrit 15 contrôles d'activité pour Slack et 10 pour Zoom. Cela signifie que les équipes de sécurité peuvent utiliser Netskope Intelligent SSE pour restreindre les comportements des utilisateurs autour de l'une de ces activités sans interrompre l'accès des utilisateurs à Slack ou Zoom. Ainsi, les utilisateurs peuvent être autorisés à créer des réunions Zoom et à y participer aussi souvent qu'ils le souhaitent, mais le partage d'images et de données est limité, restreint ou contrôlé d'une autre manière.

Historiquement, les équipes de sécurité ont la réputation de dire toujours « non » à tout. Cependant, la capacité à contrôler les actions des individus au sein d'une application non gérée, que Netskope Intelligent SSE rend possible, aide ces équipes à changer son fusil d'épaule pour dire « Comment pouvons-nous rendre ces capacités disponibles, en toute sécurité ? ».

Cas d'utilisation 3 de Zero Trust :

Encadrement actif des utilisateurs

Lorsque les utilisateurs tentent d'entreprendre une action risquée, Netskope Intelligent SSE peut soit bloquer purement et simplement cette activité, soit fournir des conseils. Par exemple, si un utilisateur tente d'ouvrir une application à risque ou de transférer des données sensibles vers l'instance personnelle d'une application approuvée par l'entreprise, Netskope Intelligent SSE peut l'aider en temps réel à choisir une option plus sûre. Par exemple :



Netskope Intelligent SSE peut également demander à l'utilisateur de justifier le choix le plus risqué. Il peut également être paramétré pour alerter simplement les utilisateurs de toute transaction risquée qu'ils tentent d'effectuer et leur donner la possibilité d'annuler la décision. Lorsqu'ils sont informés que l'utilisation des données qu'ils envisagent est risquée, plus de 95 % des utilisateurs annulent la transaction. Pour les 5 % restants, l'équipe de sécurité peut recueillir leurs justifications et les utiliser afin d'affiner les règles de sécurité pour les cas d'utilisation correspondants, le cas échéant.

En s'appuyant sur un contexte et un contenu riches ainsi que sur une évaluation des risques transactionnels, Netskope Intelligent SSE aide les utilisateurs à prendre les bonnes décisions. La solution les guide au lieu de les empêcher d'accéder aux applications dont ils ont besoin. Cette approche plus douce contribue à créer de bons citoyens numériques qui s'efforcent de respecter les règles de sécurité de l'entreprise.

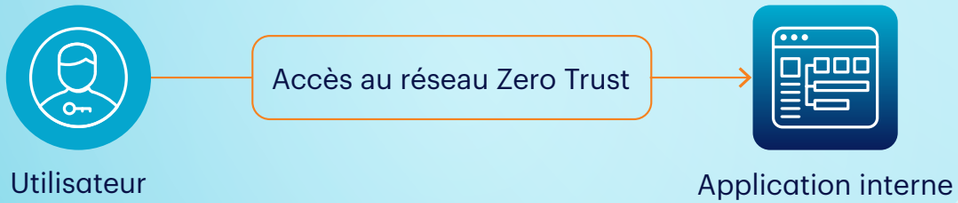
« Les humains ne sont pas le maillon faible de notre dispositif de sécurité, ils sont notre dernière ligne de défense. Il est donc important que nous le reconnaissions et que nous les formions. »

— Dane Blackmore, Netskope

Cas d'utilisation 4 de Zero Trust :

Accès sécurisé aux applications internes

Bien que les données des entreprises soient de plus en plus transférées vers des applications SaaS, de nombreuses organisations continuent à utiliser des applications développées en interne. Il est également préférable de verrouiller ces applications avec la sécurité Zero Trust, de sorte que les utilisateurs accèdent à l'application interne par l'intermédiaire du logiciel ZTNA de l'entreprise. Cette approche garantit que les utilisateurs n'accèdent qu'à ce dont ils ont besoin et ne se déplacent pas inutilement sur le réseau de l'entreprise.



Un autre avantage de l'approche ZTNA dans le développement d'applications est qu'elle permet d'intégrer les équipes de sécurité dans les processus de développement et d'exploitation (DevOps). Trop souvent, les équipes de développement de logiciels ignorent la sécurité jusqu'à ce qu'il soit bien trop tard, puis attendent de leurs collègues de la sécurité qu'ils ajoutent des contrôles après la conception d'une solution. Au contraire, les équipes de sécurité devraient être impliquées dans le DevOps du début à la fin.

Le modèle de sécurité Zero Trust permet d'y parvenir. En faisant de la sécurité un catalyseur, l'approche Zero Trust encourage les équipes de développement à impliquer le personnel de sécurité plus tôt dans le processus, en déployant des contrôles de sécurité au cours du développement. Dans certains cas, cette coopération plus étroite entre les équipes aboutit à un groupe DevSecOps intégré.

Un tel partenariat entre les fonctions de l'entreprise favorise la réussite de l'ensemble de l'organisation. Cela peut réduire les failles de sécurité des logiciels développés en interne, éliminer les problèmes liés à la chaîne d'approvisionnement en logiciels et minimiser les faiblesses en matière de sécurité des applications web.

Cas d'utilisation 5 de Zero Trust :

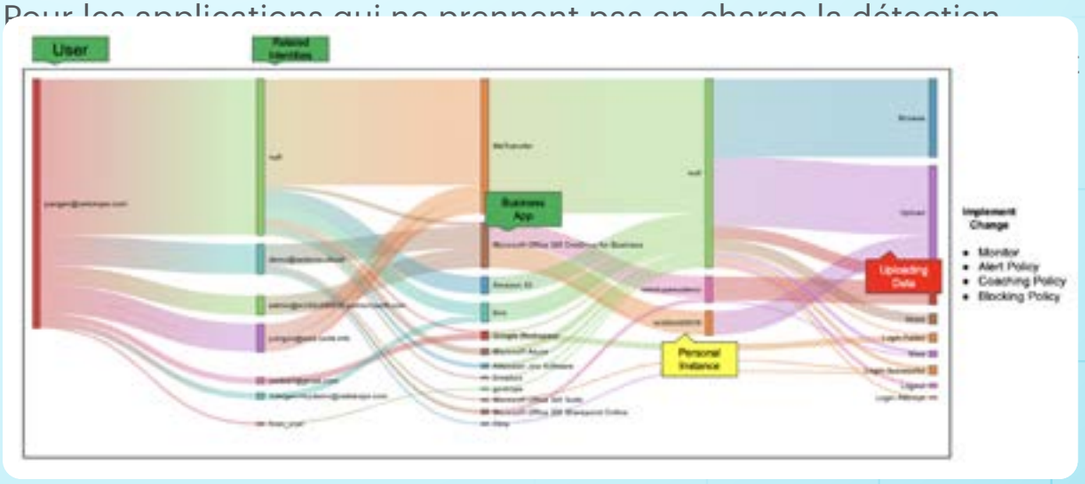
Mouvements de données non approuvés

La sécurité des données a toujours été un élément essentiel de gestion des risques de l'entreprise. Aujourd'hui, cependant, le périmètre du réseau de l'entreprise ne peut empêcher le transfert des données hors site, de sorte que les approches traditionnelles de la sécurité des données ne sont pas adaptées.

En revanche, Netskope Intelligent SSE aide les professionnels de la sécurité à comprendre comment leur organisation collecte, transmet, stocke et partage des données sur l'ensemble des applications SaaS, IaaS et développées en interne. Ils peuvent répondre à des questions telles que : où circulent nos données et dans quelles applications ? Quels sont les profils de risque des utilisateurs qui tentent de déplacer des données ? Quels appareils utilisent-ils et sur quels réseaux ? Lorsqu'un employé quitte l'entreprise, l'équipe de sécurité peut évaluer les mouvements de données et l'utilisation des applications de cette personne au cours des derniers mois. Et lorsque les applications SaaS sont mises à jour, le personnel de sécurité peut vérifier si ces changements ont entraîné de nouveaux chemins de données ou de nouvelles transactions.

Netskope Intelligent SSE permet de connaître les instances de plus de 450 applications, ce qui permet à l'équipe de sécurité de savoir si les données résident dans une instance d'entreprise d'une application ou dans une instance personnelle de la même application. Cela permet à Netskope Intelligent SSE de savoir si les utilisateurs ont tenté d'exfiltrer des données. Par exemple, alors que les contrôles traditionnels peuvent permettre aux utilisateurs de déplacer des données sensibles de la suite Google Workspace de l'entreprise vers leur environnement de travail personnel, Netskope Intelligent SSE comprend la différence et peut fournir un encadrement en temps réel ou simplement empêcher l'exfiltration.

Pour les applications qui ne prennent pas en charge la détection



Netskope Advanced Analytics offre une visibilité sur les exfiltrations de données inconnues vers le stockage personnel.

Cas d'utilisation 6 de Zero Trust :

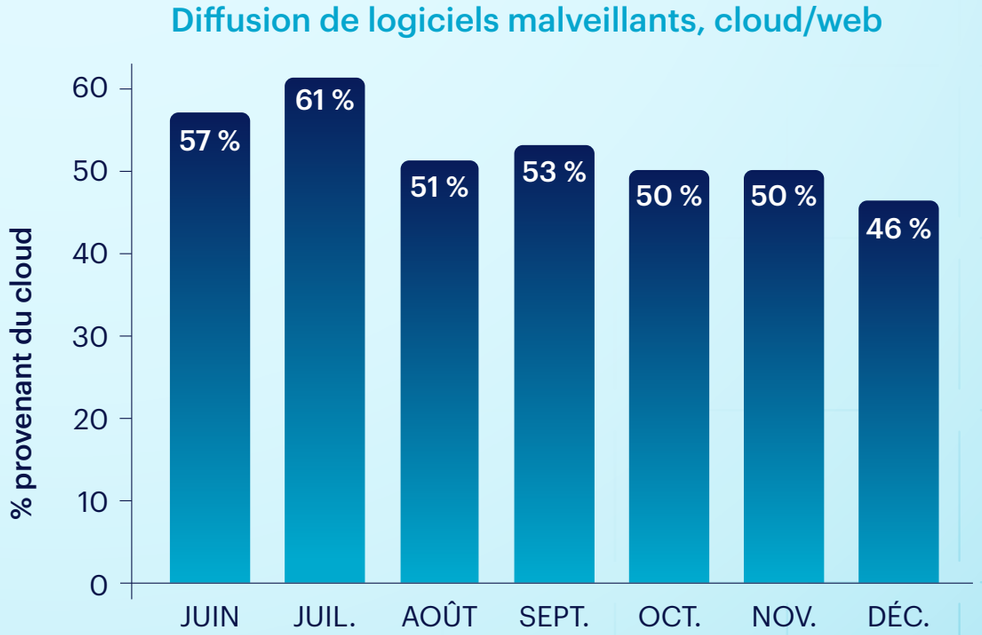
Mauvaises configurations du cloud

La grande majorité des défaillances en matière de sécurité du cloud sont dues à des erreurs de configuration. L'implémentation adéquate des solutions de gestion du niveau de sécurité dans le cloud (CSPM) et de gestion du niveau de sécurité SaaS (SSPM) est le meilleur moyen pour une organisation de s'assurer que les employés utilisent le cloud de manière sûre et sécurisée.

Ces systèmes aident les organisations à comprendre le niveau de sécurité des charges de travail qu'elles ont déployées dans un cloud public IaaS ou dans des applications SaaS, respectivement. Ils évaluent les configurations, la conformité et le niveau global des plateformes ou des applications cloud d'une entreprise, puis comparent ces résultats aux recommandations en matière de contrôle de sécurité formulées par des experts tiers tels que le National Institute of Standards and Technology (NIST) et la Cloud Security Alliance (CSA). Et comme les systèmes CSPM et SSPM utilisent des API pour étudier les configurations du cloud, ils ne nécessitent pas d'arrêt de la production ni de longue période d'intégration.

Netskope Intelligent SSE comprend des centaines de règles prêtes à l'emploi pour les applications SaaS les plus courantes, notamment Salesforce, Microsoft Exchange et SharePoint, et pour les plateformes IaaS, notamment Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform. Dans toutes ces solutions, Netskope Intelligent SSE peut auditer en continu les configurations de sécurité et, lorsqu'il détecte un problème, il peut indiquer les étapes à suivre pour le résoudre, réduisant ainsi le risque qu'une mauvaise configuration dans un système cloud entraîne une crise cyber pour l'organisation.

46 % **des téléchargements de logiciels malveillants proviennent d'applications cloud populaires.***



Source : Rapport Netskope Cloud and Threat 2024.

Les coulisses de Netskope Zero Trust Engine

Comme nous l'avons indiqué dans notre introduction, toutes ces fonctionnalités sont rendues possibles par Netskope Zero Trust Engine au cœur de Netskope Intelligent SSE. Zero Trust Engine est la technologie qui évalue la myriade de variables au moment d'une transaction commerciale, fournit un encadrement en temps réel aux utilisateurs, recueille leurs justifications et enregistre les événements avec de nombreux détails pour une surveillance continue. La figure 2 décrit comment le moteur Zero Trust prend en charge les six cas d'utilisation clés que nous avons décrits.

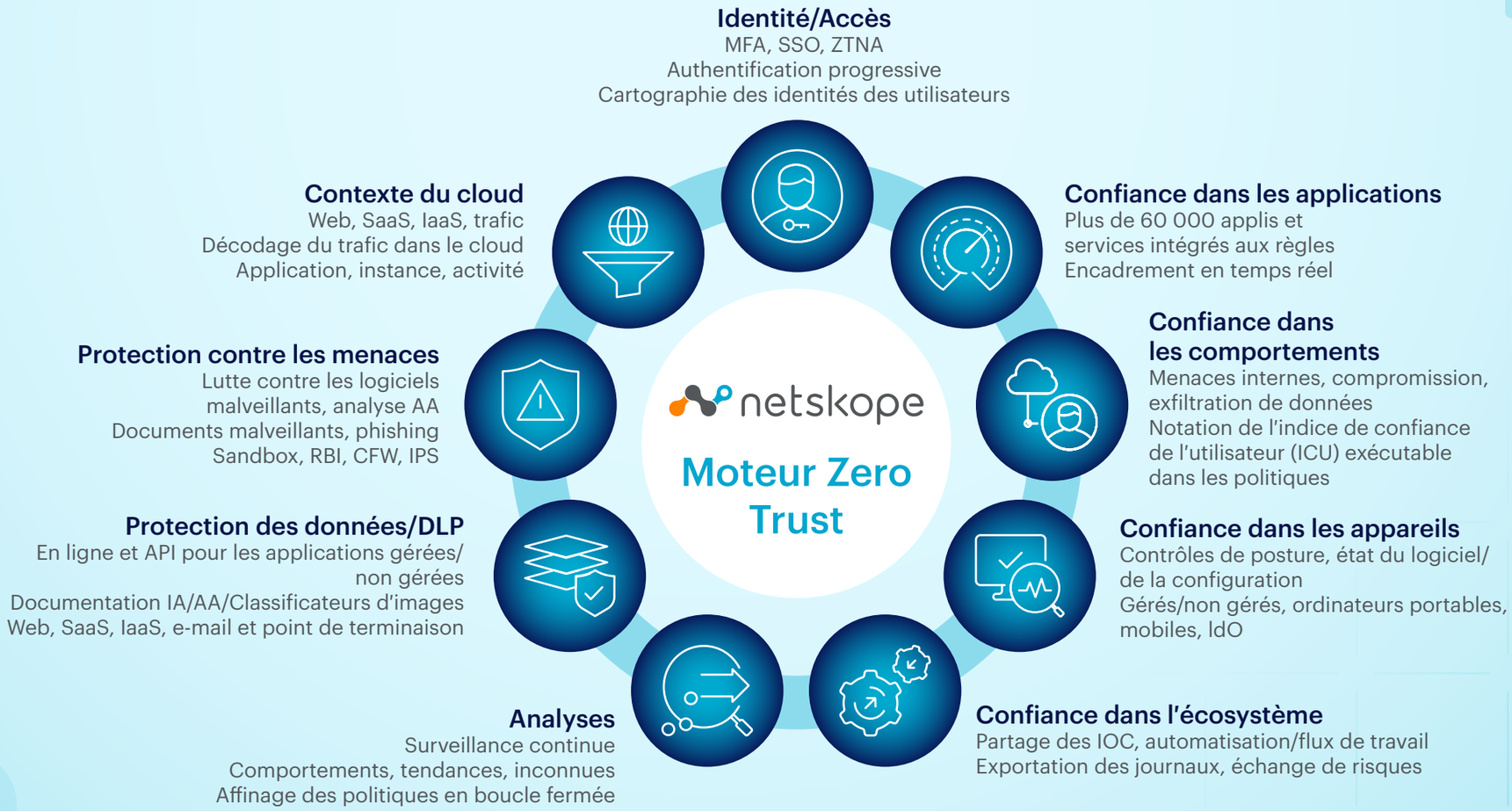


Figure 2 : Netskope Zero Trust Engine fournit le paysage des risques sur lequel repose une stratégie Zero Trust.

L'intégration étroite de toutes les technologies critiques de Zero Trust dans Netskope Zero Trust Engine en fait un puissant allié dans le déploiement d'un modèle de sécurité Zero Trust à tous les niveaux de l'entreprise. Des enquêtes menées auprès de centaines de clients de Netskope ont montré que l'adoption d'une solution de SSE avait trois principaux résultats :

85 % de réduction du risque de sécurité grâce à la protection des ressources critiques, à la stabilité, à la résilience et au fait que les utilisateurs deviennent de meilleurs citoyens numériques

51 % de réduction du coût total des opérations grâce à la mise hors service d'appareils, au gain de temps pour le personnel, à la réduction des liaisons réseau dédiées et à l'optimisation des dépenses liées au cloud

19 % d'amélioration de l'agilité de l'entreprise car l'adoption des principes du Zero Trust rapproche les mécanismes de défense des utilisateurs, accélérant la vitesse de commercialisation et les décisions basées sur les données

Pour en savoir plus, rendez-vous sur https://www.netskope.com/resources/analyst-reports/2023-gartner-magic-quadrant-for-security-service-edge.

À propos de Netskope

Netskope est un leader dans le domaine du Secure Access Service Edge, redéfinissant la sécurité du cloud, des données et des réseaux et aidant les organisations à appliquer les principes du Zero Trust. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et protège les personnes, les appareils et les données où qu'ils se trouvent. Netskope aide les entreprises à réduire les risques, à accroître l'efficacité et à obtenir une visibilité inégalée sur l'ensemble des activités des applications cloud, web et personnelles.

Des milliers de clients, dont plus de 25 entreprises figurant au classement Fortune 100, font confiance à Netskope et à son puissant réseau NewEdge pour atténuer les menaces et faire face aux changements technologiques, organisationnels, en matière de réseau et réglementaires.

netskope