netskope

5 cas d’usage critiques du SASE pour les environnements de travail hybrides

5 cas d'usage critiques du SASE pour les environnements de travail hybrides

La pandémie a accéléré l'adoption de modèles de travail hybrides s'appuyant sur des réseaux, des datacenters et des applications cloud. Bien que 63 % des entreprises à forte croissance soient déjà passées au travail hybride, cette approche peut constituer un véritable défi pour les équipes de réseau et de sécurité mal préparées. Un réseau domestique peu fiable et à forte latence diminuer la productivité des utilisateurs, et le manque de connaissances en matière de cloud peut aboutir à des failles de sécurité. Les systèmes de réseau et de sécurité existants, complexes et coûteux freinent le passage au cloud. Voilà notamment pourquoi les entreprises ont aujourd'hui tout intérêt à se doter des fonctionnalités du Security Service Edge (SSE) dans le cadre d'une architecture Secure Access Service Edge (SASE) pour réussir leur déploiement hybride.

netskope

[1] Source: Accenture https://www.accenture.com/us-en/blogs/business-functions-blog/hybrid-workforce

5 cas d'usage critiques du SASE pour les environnements de travail hybrides

Cas d'usage n° 1 | Garantir les bonnes performances du réseau, l'expérience utilisateur et la sécurité

Cas d'usage n° 2 | Voir et contrôler ce qui se passe dans le cloud

Cas d'usage n° 3 | Réaliser des économies et améliorer l'efficacité opérationnelle

Cas d'usage n° 4 | Se protéger contre les menaces émanant des SaaS et du web basées sur le cloud

Cas d'usage n° 5 | Prévenir le risque de fuite et de vol de données ainsi que les risques internes

netskope

Garantir les bonnes performances du réseau, l'expérience utilisateur et la sécurité

Avec le travail hybride, les équipes de sécurité doivent trouver le juste milieu entre la sécurité d'une part, et les performances du réseau et l'expérience utilisateur d'autre part. La raison en est que tout impact sur les utilisateurs fait naître le risque que ceux-ci cherchent un moyen de contourner les contrôles de sécurité. Les solutions de sécurité existantes nuisent à l'expérience utilisateur, soit car elles sont compartimentées, d'où une latence accrue du réseau, soit car elles sont centralisées, auquel cas le trafic doit être acheminé à travers la pile de sécurité périphérique et repose sur des technologies lentes et dépassées, comme le MPLS et le VPN.

Pour répondre à ce cas d'usage, tournez-vous vers les capacités SASE suivantes :

Grâce à une **architecture cloud-native** avec des datacenters partout, plus besoin faire passer le trafic à distance par le biais du réseau central pour l'inspection de la sécurité. À la place, une architecture cloud-native permettra d'intégrer l'inspection de la sécurité dans des flux de trafic simplifiés « direct-to-Internet », diminuant ainsi la latence. De plus, une plateforme SSE convergée, qui joue le rôle de la pile de sécurité dont le SASE a besoin, permet d'adopter une approche « en un seul passage » : toutes les vérifications de sécurité se font au même endroit, et la sécurité est transparente pour l'utilisateur, sous forme de solution de type « bump-in-the-wire » performante et à faible latence.

L'**accès réseau zero-trust (ZTNA)** permet lui aussi de ne pas avoir à réacheminer le trafic par le réseau d'entreprise. L'utilisation d'un ZTNA permet aux équipes de sécurité et de réseau de garantir un accès performant et sécurisé aux applications privées, qu'elles soient basées dans le réseau d'entreprise ou sur le cloud.

Les **fonctionnalités de sécurité en périphérie** contribuent elles aussi à diminuer la latence du réseau, tout en dopant sa fiabilité globale. Privilégiez les plateformes cloud-native qui permettent un calcul complet à chaque point de service pour bénéficier d'un traitement inline en temps réel à l'échelle, et qui ont forgé des partenariats de peering direct avec des prestataires cloud, des réseaux de diffusion de contenu et SaaS pour gagner encore plus en performances.

Une intégration solide avec des solutions de SD-WAN permet de supprimer les connexions MPLS coûteuses et lentes, qui réacheminent de force tout le trafic des filiales vers le réseau d'entreprise. En lieu et place, vos utilisateurs bénéficient d'une connectivité à haut débit « direct-to-Internet » rapide et abordable aux applications web et cloud, ce qui dynamise leur productivité.

Les outils de **monitoring de l'expérience digitale (DEM)** donnent aux organisations une visibilité de bout en bout sur l'activité des utilisateurs, avec à la clé des insights exploitables sur les performances du réseau et des applications, facilitant ainsi la résolution des problèmes et l'optimisation de l'expérience utilisateur. En vous dotant de fonctionnalités de DEM, vous bénéficierez d'une vraie protection sur le cloud sans faire de concessions sur les performances.

02

Voir et contrôler ce qui se passe dans le cloud

Lorsque l'on migre des applications et des données vers le cloud, les architectures de sécurité existantes peinent à garantir la visibilité et le contrôle de la sécurité. Avec le travail hybride, les organisations doivent composer avec un nouveau risque, puisqu'elles autorisent des appareils non managés et des réseaux domestiques/publics à accéder aux ressources de l'entreprise. Les équipes réseau doivent veiller à ce que les contrôles de sécurité ne nuisent pas aux performances du réseau. Par conséquent, certaines choisissent de contourner les contrôles de sécurité, exposant ainsi l'entreprise aux risques.

Pour répondre à ce cas d'usage dans une architecture SASE, tournez-vous vers les fonctionnalités suivantes du SSE :

Embedded Les **technologies intégrées de protection des données** dont la couverture s'étend partout où se trouvent des données, et qui surveillent les données sensibles et empêchent l'accès ou le téléchargement sur des sites web ou des applications cloud non managées par des employés.

Les **technologies de protection contre les menaces**, dont le sandboxing et l'isolation de navigateur à distance, qui détectent et préviennent jusqu'aux attaques les plus sophistiquées. Privilégiez des outils capables de détecter et d'arrêter les logiciels malveillants provenant de menaces liées au cloud en temps réel et dans l'ensemble de l'environnement de travail hybride. En adoptant la bonne approche, vous serez plus à même de lutter contre l'exfiltration de données et les menaces internes, de donner l'alerte en cas de compromission de compte, et de signaler les comportements d'utilisateurs anormaux.

Les **technologies de gestion des risques** qui évaluent et améliorent automatiquement la sécurité cloud des entreprises. Ces outils doivent être capables d'analyser l'ensemble des applis et des services cloud de l'entreprise pour en comprendre le contenu et le contexte (ce qui relève de l'entreprise ou du personnel, les risques des applis, la sensibilité des données, etc.), et permettre ainsi l'instauration de contrôles adaptatifs satisfaisant les besoins précis de l'organisation.

L'**analyse comportementale** associée à l'IA et à l'apprentissage automatique permet de détecter des menaces inconnues et des traits de comportement anormaux cachés dans les données du réseau, ce qui en fait un élément indispensable de toute solution de cybersécurité complète adaptée au travail hybride. La clé de la réussite est de trouver une solution à même d'appréhender le spectre complet des activités des utilisateurs à travers les applications SaaS, les infrastructures cloud et les sites web qu'ils consultent.

Les capacités de **proxy inverse** qui permettent aux appareils non managés d'accéder aux ressources de l'entreprise sans compromettre la sécurité de l'entreprise. Ces fonctionnalités font office de zone tampon entre les appareils externes et les systèmes internes, de sorte que les utilisateurs à distance ne peuvent accéder directement au réseau sans être au préalable vérifiés par le proxy inverse.

L'**accès réseau zero-trust (ZTNA)** garantit un accès hautement granulaire aux applications et aux ressources, ce qui diminue le risque de mouvement latéral lié à l'octroi aux utilisateurs de VPN d'un accès à tout le réseau. Contrairement aux VPN, le ZTNA fournit un accès aux applications à la fois contextuel et optimisé en fonction des risques, au lieu d'un accès inconditionnel au réseau. Associé à une architecture de connectivité « à l'envers », le ZTNA limite la surface d'attaque globale en supprimant l'exposition des protocoles et des services à l'Internet public.

Se protéger contre les menaces émanant des SaaS et du web basées sur le cloud

Étant donné que le travail hybride englobe de plus en plus d'applications, de données et d'utilisateurs hors du périmètre du réseau, le cloud est désormais la nouvelle surface d'attaque pour les entreprises. Les hackers ont eux aussi adopté le cloud, et l'utilisent pour propager leurs menaces avec succès. Ces menaces peuvent aisément passer inaperçues, car les hackers exploitent des domaines fiables, des certificats valides et les instances des mêmes applis managées que celles utilisées par les entreprises. Dorénavant, toutes les étapes du processus de la cybercriminalité sont propulsées par le cloud, de la reconnaissance à l'exfiltration et à la persistance des données.

Pour répondre à ce cas d'usage, tournez-vous vers les capacités SSE suivantes :

La **protection avancée contre les menaces** est un système de défense pour la détection une fois que tous les contrôles de prévention possibles ont été effectués : désobfuscation et décompressage de fichiers récurrents, analyse de pré-exécution et heuristique, bare-metal et sandboxing, et analyse avec apprentissage automatique, auxquels se rajoutent des analyses comportementales pour détecter les menaces internes, les compromissions de compte et l'exfiltration de données.

Les **identifiants d'accès sous forme de formulaire** : étant donné que l'identité, les applis et les données sont les nouveaux axes de contrôle de la sécurité, il n'est guère étonnant que les cyberattaques se concentrent sur le vol d'identifiants et sur le recours à des attaques brutales pour forcer l'accès. Utilisez des outils de DLP cloud pour déterminer si des identifiants de connexion sont publiés sous forme de formulaires web indésirables créés par des cybercriminels et se font passer pour des applis et instances managées de confiance. Ce type de phishing cloud échappe aisément aux anciennes défenses web, email et d'endpoint.

Le **partage de renseignements sur les menaces** est un autre atout de la convergence des technologies dans le cloud (voir plus haut) : les divers éléments d'une solution SSE peuvent partager des renseignements, ce qui accroît la probabilité de découvrir des menaces basées sur le cloud. De plus, les investissements dans les flux de renseignement sur les menaces peuvent être automatisés pour permettre le partage avec des outils tels que Cloud Threat Exchange (CTE), évitant par ailleurs aux entreprises de surcharger leur configuration de filtrage web.

La **recherche des menaces cloud** met l'accent sur les menaces basées sur le cloud, et nécessite une visibilité des données et du contexte au sein des applis et des services cloud pour le trafic des utilisateurs. Si votre solution de sécurité existante ne peut voir les données dans l'appli cloud, il y a peu de chances que vous puissiez identifier la menace.

Prévenir le risque de fuite et de vol de données ainsi que les risques internes

Étant donné que les environnements de travail hybrides nécessitent la migration de données dans le cloud, le contexte des données est un principe cardinal du SSE au sein d'une architecture SASE. Les défenses existantes ne peuvent pas voir les flux de données transitant par les applis managées ou non managées, et les services cloud ne sont pas à la hauteur pour ce cas d'usage. En outre, si l'on ne comprend pas les risques associés aux applications cloud, il est impossible de limiter l'accès ou les activités des utilisateurs pour les applis cloud lorsque des données risquent d'être compromises.

04

Prévenir le risque de fuite et de vol de données ainsi que les risques internes

Pour répondre à ce cas d'usage, tournez-vous vers les capacités SASE suivantes :

Une **architecture à passage unique** permet d'appliquer la protection des données, en un même point et avec un passage unique, au web, aux applis managées et non managées, au trafic des utilisateurs sur un cloud public IaaS et aux applis personnalisées. Ceci vaut pour les politiques contextuelles, les modèles de conformité, la correspondance exacte de données (EDM), l'empreinte avec un certain degré de similarité et plus de 3 000 identifiants de données pour plus de 1 400 types de fichier.

Les **contrôles de protection des données** réduisent la surface avant d'appliquer la DLP en bloquant les sites web malveillants et risqués, en bloquant les applis à risque élevé, en bloquant les chargements vers des applis et instances non managées et en restreignant les activités de partage avec des domaines approuvés.

La **DLP cloud avancée** permet d'appliquer une DLP cloud à des données en mouvement pour les appareils managés via un forward proxy, les données en mouvement pour les appareils non managés via un proxy inverse, et les données au repos dans les applis managées via une API. Optez pour un outil de DLP qui vous permette de bien comprendre le contenu, le contexte, l'instance, la catégorie et le niveau de risque des applications cloud utilisées. Ces variables (inexistantes dans les anciennes défenses web) pourront vous aider à élaborer directement dans le cloud des politiques de protection des données efficaces.

Réaliser des économies et améliorer l'efficacité opérationnelle

Le travail hybride devenant peu à peu la norme, le coût et la complexité de la sécurité risquent d'échapper à tout contrôle. En moyenne, une organisation gère 76 outils de sécurité différents, et doit réfléchir à en ajouter un nouveau chaque fois qu'une nouvelle menace ou une évolution informatique survient. Il lui faut ainsi plus de temps et de personnel pour gérer tous ces outils, politiques et rapports de sécurité, sans compter le coût grandissant des solutions. En même temps, les entreprises cherchent à s'éloigner des technologies de MPLS et de VPN coûteuses pour passer au SD-WAN, mais peinent à le faire en raison de leur manque d'outils de sécurité intégrés.

[2] Source: https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

Pour répondre à ce cas d'usage, tournez-vous vers les capacités SASE suivantes :

La **convergence des technologies dans le cloud** (notamment la convergence des passerelles web sécurisées (SWG), des agents de sécurité des accès au cloud (CASB), des outils de prévention de la perte de données (DLP), des ZTNA et des systèmes de pare-feu en mode service (FWaaS) simplifie énormément le processus d'achat et d'installation pour les entreprises, tout en optimisant la gestion continue des solutions par le biais d'un agent et d'une console de gestion communs. En parallèle, la gestion de politique unifiée que permet cette convergence simplifie grandement le processus administratif.

L'**intégration SD-WAN** permet aux organisations de réaliser des économies importantes en supprimant la nécessité d'avoir des connexions MPLS coûteuses, lentes et peu performantes pour les filiales, et en les remplaçant par du haut débit rapide et abordable tout en baissant le coût de la connectivité WAN au siège. En intégrant les technologies de SWG à un SD-WAN, vous pourrez sécuriser et protéger votre trafic web, cloud et SaaS lorsque vous migrerez vers ce modèle de réseau plus rentable.

L'**accès réseau zero-trust (ZTNA)** rend caducs les clients VPN lourds pour les utilisateurs passés au travail hybride, et réduit les coûts du réseau du siège liés à la bande passante et à l'infrastructure VPN. De plus, avec la découverte d'applications et l'utilisation d'une API pour l'automatisation, un ZTNA simplifie encore plus les opérations liées à la gestion des applications privées, à la mise à disposition des accès utilisateurs et à la maintenance continue.

En résumé

En misant sur le SASE, les entreprises en travail hybride ayant adopté une stratégie cloud-first peuvent concilier la sécurité, les performances et la productivité.

Dorénavant, la majorité des employés ne travailleront plus dans les bureaux de l'entreprise. Ils s'attendent à pouvoir travailler et accéder aux informations depuis tout appareil et en tout lieu. De plus en plus d'employeurs adoptent le travail hybride pour sa flexibilité, et on estime d'ailleurs qu'à long terme, la moitié des travailleurs sera en télétravail. Au fur et à mesure de cette évolution, les entreprises devront poser les bonnes bases technologiques. En misant sur des capacités de SSE dans le cadre d'une stratégie SASE, elles vont pouvoir transformer leurs filiales à l'aide d'une architecture cloud intégrant sans difficulté la sécurité à un SD-WAN performant et offrant un bon rapport qualité-prix, pour s'aligner parfaitement sur les architectures cloud-first qui caractérisent l'entreprise moderne.

Outre les filiales, le SASE peut contribuer à sécuriser et autonomiser les utilisateurs à distance en créant une trame cloud qui permettra un accès rapide, simple et sécurisé au web, au cloud et aux applis privées, et ce depuis n'importe où et depuis n'importe quel appareil. Les entreprises vont ainsi pouvoir gagner en agilité, mieux atténuer les risques pour la sécurité, et simplifier leurs opérations pour bénéficier d'un meilleur TCO (coût total de possession).

[3] Source: https://www.inc.com/bill-murphy-jr/a-stanford-economist-who-studiesremote-work-says-half-of-allworkers-will-make-thisbig-change-in2022.html

Pour en savoir plus

Netskope est un leader mondial de la cybersécurité qui révolutionne la sécurité du cloud, des données et des réseaux pour aider les organisations qui appliquent les principes du Zero Trust à protéger leurs données. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et sécurise vos collaborateurs, vos appareils et vos données, où qu'ils se trouvent.

Pour découvrir comment Netskope aide ses clients à se préparer à tout contexte dans leur transition vers le SASE, rendez-vous sur netskope.com.