Nouvelles perspectives pour la protection des données et contre les menaces

+ eBook

Ce que les fournisseurs traditionnels veulent cacher

netskope

Table des matières

Introduction

Les pratiques traditionnelles en matière de protection des données et contre les menaces peuvent faire plus de mal que de bien. Ces pratiques archaïques permettent également aux fournisseurs de sécurité de dissimuler des problèmes qu'ils ne souhaitent pas voir exposés.
La pandémie a accéléré l'adoption du SaaS et du cloud, plaçant davantage d'utilisateurs et de données au-delà de périmètres de plus en plus restreints et hors de portée des solutions de sécurité traditionnelles. En travaillant avec des entreprises et des multinationales sur des déploiements de SSE (Security Service Edge), nous avons compilé dix perspectives en matière de contrôles basés sur les règles, de bonnes pratiques et de détection des angles morts. Nous vous recommandons de mettre à jour vos critères dans le cadre de votre demande d'informations (RFI) à l'aide de ces perspectives obtenues sur le terrain lorsque vous envisagez une solution SSE ou SASE (Secure Access Service Edge).

À qui s'adressent ces informations ?

Architectes, directeurs et gestionnaires de la sécurité et des réseaux.

À quel moment lire ces informations ?

Avant de lancer un projet SSE/SASE et d'émettre une RFI.

Pourquoi lire ces informations ?

Pour comprendre les changements significatifs dans le paysage de la protection.

Perspective 1

Contourner l'inspection du trafic de Microsoft 365 engendre un angle mort

Les meilleures solutions SSE de leur catégorie suppriment désormais le compromis performance/sécurité pour contourner l'inspection du trafic de Microsoft 365 (M365). En outre, cet angle mort de la protection des données et contre les menaces est devenu trop important pour être ignoré. Interrogez-vous sur tout fournisseur de sécurité en ligne qui contourne le trafic M365 dans votre environnement.

Points clés

- **Plus d'un tiers des menaces diffusées dans le cloud proviennent de OneDrive et de SharePoint.** Cette tendance est constante depuis quelques années et se retrouve dans le rapport Netskope Threat Labs 2024 où ces applications occupent respectivement la première et la troisième place en termes de popularité.
- **Plus de la moitié du trafic web chiffré est lié au cloud, et M365 peut en représenter la plus grande partie.** Nous avons franchi un seuil critique puisque le trafic des services SaaS et cloud a dépassé celui du web classique. Les applications M365 peuvent représenter 35 à 40 % du trafic SaaS lié au cloud, car les utilisateurs informatiques passent leurs journées de travail dans ces applications à créer et à gérer du contenu.
- **L'inspection du trafic M365 à l'aide de solutions de sécurité traditionnelles a un impact sur l'expérience utilisateur.** Le backhauling du trafic des utilisateurs distants et hybrides vers les appliances de sécurité sur site du datacenter peut avoir un impact sur l'expérience utilisateur. En revanche, l'accès direct par les utilisateurs qui contournent ces passerelles de sécurité crée un angle mort pour la protection des données et contre les menaces. Les solutions SSE remplacent ces appliances de sécurité et les anciens VPN par une expérience utilisateur plus sûre, plus granulaire et plus rapide.
- **Les certificats des partenaires Microsoft exigent un contournement avec une absence d'inspection par défaut.** Rétrospectivement, cette certification avait sa raison d'être, compte tenu de l'impact des solutions de sécurité traditionnelles sur l'expérience utilisateur. Cependant, aujourd'hui, les solutions SSE fournissent un ensemble d'accès globaux avec une expérience utilisateur performante sans compromis entre la sécurité et la performance. Le choix par défaut doit se porter sur l'inspection du trafic M365, source principale de menaces véhiculées par le cloud et de vols de données potentiels.
- **Affichez le certificat de connexion sécurisée de votre navigateur web pour valider l'inspection.** Cliquez sur l'icône devant l'URL lorsque vous travaillez dans une application M365 pour afficher la connexion sécurisée du navigateur web et son certificat. Si vous constatez un certificat Microsoft pour le tunnel TLS, cela signifie que vous contournez l'inspection : il s'agit d'un angle mort. Une solution SSE assure le contrôle et utilise son certificat (ou un certificat signé par l'autorité de certification du client) pour le tunnel TLS sécurisé entre l'utilisateur et la plateforme cloud SSE. Vous devriez donc voir le certificat de la solution SSE pour la connexion sécurisée, et non le certificat Microsoft.

Perspective 2

La ligne de front est maintenant en temps réel à T+0 pour les menaces et non plus tard

La protection contre les menaces en temps réel à T+0 heure constitue la ligne de front ; évitez de vous laisser induire en erreur par des taux de détection plus élevés quelques heures ou quelques jours plus tard, provenant du partage de renseignements sur les menaces parmi la masse. C'est un domaine dans lequel vous devez insister auprès des fournisseurs de sécurité en ligne pour qu'ils fournissent des taux d'efficacité de détection des menaces à T+0 avec un faible pourcentage de faux positifs.

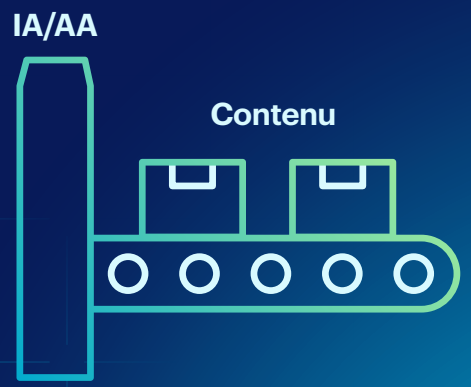
Points clés

- **Les attaques présentent des cycles de vie plus rapides, peuvent être ciblées et utilisent des applications/domaines de confiance.** Le patient zéro est la première personne infectée par une nouvelle menace et, dans le cas d'attaques ciblées, il peut être le seul. Étant donné que les attaques utilisent des applications et des services cloud de confiance pour l'hébergement et la diffusion, ces domaines sont souvent autorisés et, comme indiqué précédemment, souvent contournés.
- **Validez l'efficacité de la protection contre les menaces en temps réel à T+0 plutôt qu'à T+4 heures ou plus.** Lorsque vous consultez des rapports d'analyse sur l'efficacité de la protection contre les menaces en ligne, examinez les résultats en temps réel à T+0 et, s'ils ne sont pas fournis, demandez-les. De nombreux rapports font état des taux d'efficacité les plus élevés quelques heures ou quelques jours plus tard, lorsque les renseignements sur les menaces partagés parmi la masse permettent à tout le monde de faire bonne figure.
- **Prêtez attention au taux de faux positifs (FP) dans les rapports de test, un pourcentage plus faible étant préférable.** Une astuce connue lors des tests de protection contre les menaces consiste à augmenter les capacités de détection au détriment des détections de faux positifs. Alors qu'une solution peut obtenir 98 % et 99 % d'efficacité après plusieurs heures de tests, vérifiez si le taux de faux positifs est de 2 % ou plus. Il est peu probable que vous obteniez les mêmes résultats de détection élevés lorsque la protection contre les menaces est réduite pour abaisser le taux de faux positifs à un niveau acceptable inférieur à 1 % pour les clients.
- **Exigez un rapport de test récent sur l'efficacité des menaces pour les défenses en ligne.** Les attaques changent et toutes les menaces ne sont pas des fichiers exécutables. En effet, les attaques sans fichier augmentent, tandis que les faux formulaires et les attaques par phishing ciblent la compromission des identifiants d'accès. Les faux formulaires de connexion hébergés dans des services cloud de confiance pour des applications auxquelles les utilisateurs accèdent chaque jour de travail nécessitent une protection en temps réel pour protéger le patient zéro et les autres dès la première exposition. Les rapports de test devraient couvrir les fichiers PE (exécutables), les attaques non PE (sans fichier) et les attaques par phishing. La plupart des tests de points de terminaison ne couvrent pas ces trois types d'attaques en même temps, c'est pourquoi les solutions SSE sont là pour combler les lacunes. Si aucun rapport de test ne peut être fourni, il est possible d'envisager l'utilisation des meilleurs outils de test d'intrusion.
- **T+0 est la ligne de front ; tout le monde peut faire bonne figure quelques heures plus tard grâce aux renseignements partagés sur les menaces.** Évitez de jeter un coup d'œil rapide ou de parcourir les rapports d'analyse des tests de protection contre les menaces et comprenez les détails pour obtenir des résultats en temps réel à T+0 plutôt que des heures ou des jours plus tard. Assurez-vous également que le taux de FP est acceptable pour les tests et qu'il correspond à vos attentes. La protection contre les menaces en temps réel à T+0 et la vitesse à laquelle les solutions peuvent assimiler de nouvelles attaques en l'espace d'une heure sont essentielles.

Perspective 3

La visibilité du contenu rend possible des mécanismes de défense IA/AA pour une protection en temps réel

L'IA générative est désormais largement répandue et devrait transformer de nombreux aspects de notre vie quotidienne, y compris au travail et à la maison. Pour que l'IA et l'apprentissage automatique (AA) fonctionnent en temps réel, il faut du contenu. C'est là que réside la valeur ajoutée des solutions SSE en matière de protection des données et contre les menaces.



Points clés

- **Les défenses IA/AA en temps réel ne fonctionnent que si elles disposent du contenu suffisant.** Supposer que les attaques sont basées sur des fichiers, c'est ignorer les faux formulaires de connexion et autres tactiques hébergées dans des services cloud utilisés au sein des attaques. La détection du phishing en temps réel avec des défenses IA/AA est possible étant donné que le contenu peut être exposé en ligne pendant la transaction commerciale pour protéger l'utilisateur. Les défenses IA/AA utilisées uniquement en arrière-plan ne protègent pas en temps réel.
- **Les défenses en ligne doivent fournir une visibilité du contenu pour les applications SaaS.** Toutes les solutions de sécurité SSE en ligne ne peuvent pas exposer le contenu des applications SaaS et des services cloud gérés et non gérés : il faut donc faire l'inventaire du contenu qui peut être inspecté. Rappelez-vous également que la plupart des menaces proviennent de tenants extérieurs à votre entreprise et d'instances personnelles d'applications SaaS populaires où l'inspection en ligne est votre première ligne de défense. En effet, les points de terminaison et la sécurité des messageries n'ont pas la capacité de décoder le contenu des applications SaaS en temps réel pour l'analyse IA/AA.
- **La protection des données et contre les menaces utilise des défenses en ligne basées sur l'IA/AA.** Selon la recherche sur les menances de Netskope, les fichiers exécutables portables (PE) peuvent être détectés en ligne avec des classificateurs AA alors que 6 fichiers PE malveillants sur 10 n'ont pas de signature connue au moment de la détection. Les attaques par phishing peuvent également être détectées, lorsque l'IA/AA analyse les faux formulaires pour protéger en temps réel bien avant que les URL de phishing ne soient partagées dans les flux de renseignements sur les menaces. Voici quelques **exemples d'attaques par phishing** détectées à l'aide de défenses IA/AA en temps réel.
- **Le code source est le contenu le plus utilisé dans ChatGPT.** En tant qu'application d'IA générative la plus populaire à ce jour, ChatGPT est principalement utilisée pour optimiser le code source. Les classificateurs de données AI/AA de Netskope peuvent détecter plus de 20 types de code source en ligne sans la classification traditionnelle des données, l'enregistrement ou les identificateurs de données de la DLP. Cela permet aux solutions SSE dotées de connecteurs d'applications GenAI d'assurer immédiatement la protection des données du code source de l'entreprise et d'encadrer les utilisateurs en temps réel pour qu'ils utilisent des applications et des tenants GenAI approuvés par l'entreprise.
- **Les défenses IA/AA doivent être présentes en ligne, et pas seulement en arrière-plan.** Les fonctionnalités d'IA/AA sont utilisées depuis des années en arrière-plan pour la détection, l'optimisation, la classification et même les opérations. La focalisation explosive sur les applications GenAI a entraîné une surutilisation de l'IA dans les messages et le contenu marketing. Concentrez-vous sur ce que les solutions SSE fournissent en ligne avec les fonctionnalités d'IA/AA en temps réel plutôt qu'en arrière-plan.

Perspective 4

Le pishing dépasse le cadre des e-mails et s'étend à toutes les communications

Les canaux de communication largement répandus vers les utilisateurs permettent le pishing, la fraude et la compromission des entreprises au-delà des e-mails traditionnels. Tirant parti des services SaaS et d'hébergement dans le cloud, les attaques par pishing peuvent s'appuyer sur ces domaines populaires et échapper à la détection par les défenses de sécurité traditionnelles incapables de décoder et d'analyser le contenu SaaS avec des défenses en temps réel. À l'avenir, la visibilité du contenu est une exigence clé pour les solutions SSE afin de permettre des défenses en temps réel.

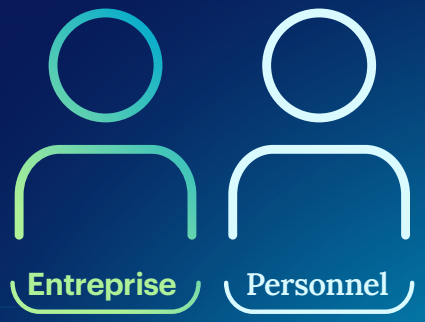
Points clés

- **Le pishing est un point d'entrée principal pour les ransomwares.** D'une semaine à l'autre, l'actualité ne cesse de rappeler l'impact des ransomwares et les rapports de recherche relèvent les points d'entrée clés du pishing, y compris les progiciels et correctifs logiciels, la compromission d'accès, les téléchargements ponctuels, la publicité malveillante et les attaques sans fichier. Tout au long de la chaîne d'exécution des attaques de ransomwares, la visibilité du contenu permet de protéger les données et de lutter contre les menaces, notamment par la détection des anomalies, les compromissions d'accès et l'exfiltration des données.
- **Les communications sur les réseaux sociaux, par messagerie instantanée, chat et personnelles font l'objet de pishing.** Les institutions financières sont la principale cible des attaques par pishing. Cependant, les réseaux sociaux se sont hissés quasiment à leur niveau en occupant la deuxième place à un point de pourcentage près, suivis par les solutions SaaS/webmail en troisième position sur la base des dernières tendances.
- **Les utilisateurs exigent un équilibre entre vie professionnelle et vie privée et un accès à leurs applications personnelles.** Le travail hybride et le télétravail ont imposé de nouvelles exigences aux appareils gérés pour que les utilisateurs accèdent à leurs communications personnelles. Même de retour au bureau, les utilisateurs exigent un équilibre entre vie professionnelle et vie privée en ce qui concerne l'accès. Efforcez-vous de limiter l'accès aux applications à haut risque, contrôlez les activités des applications pour protéger les données, et envisagez l'isolation du navigateur à distance (RBI) pour les solutions SaaS et webmail personnelles pour protéger les appareils gérés. Bloquer l'accès ne fait que frustrer les utilisateurs et conserver le personnel informatique à forte valeur ajoutée constitue un avantage concurrentiel.
- **Les applications SaaS hébergent de faux formulaires de connexion dans des domaines de confiance pour les utilisateurs.** L'adoption des solutions SaaS continue d'augmenter d'année en année à un taux de croissance de plus de 20 % dans un contexte où plus de 98 % des nouvelles applications SaaS sont adoptées par les unités opérationnelles et les utilisateurs, et non par l'administration informatique. Au-delà des applications SaaS gérées, les tenants et instances personnelles non gérés des applications constituent des angles morts pour les attaques par pishing hébergeant de faux formulaires de connexion.
- **L'accès des attaques ne se limite plus aux e-mails traditionnels, il convient donc d'inspecter la solution SaaS en ligne.** Ce qui fait souvent défaut entre les passerelles web sécurisées (SWG) traditionnelles et les solutions de courtier en sécurité d'accès au cloud (CASB) est l'inspection en ligne des applications SaaS et des services cloud, qui se comptent par milliers pour beaucoup d'entreprises et d'organisations. Évitez de tomber dans le piège du CASB en tant que DLP pour les solutions SaaS gérées et le SWG traditionnel pour tout ce qui concerne le web et le cloud.

Perspective 5

Attention aux menaces et à l'exfiltration de données dans les instances d'applications personnelles

La nouvelle zone à haut risque pour la diffusion de menaces et le vol de données réside dans l'angle mort des instances SaaS personnelles (par opposition à celles de l'entreprise). Bien que vous puissiez fournir des applications de productivité bureautique SaaS gérées à vos utilisateurs, ces derniers peuvent également disposer de leur propre version d'instance personnelle. Cela ne permet que trop facilement l'exfiltration de données de l'entreprise vers des instances personnelles dans des applications et ce, dans un domaine que vous autorisez et que vous n'inspectez peut être pas en ligne.



Points clés

- **Le vol de données augmente de 300 % au cours des 30 derniers jours de travail des utilisateurs qui quittent l'entreprise.** Au cours des deux années qui ont suivi le début de la pandémie, les recherches de Netskope sur le mouvement et l'étalement des données ont révélé un résultat intéressant. Pour les utilisateurs qui ont quitté leur emploi, les chercheurs ont examiné les 30 derniers jours d'activité des données et ont constaté une augmentation de plus de 300 % de l'exfiltration des données par rapport aux utilisateurs actifs. Travaillant à distance, les utilisateurs collectaient des données et des informations qu'ils considéraient comme utiles pour leur prochain emploi quelques semaines avant leur départ.
- **Pendant ces 30 jours, 74 % des vols de données ont lieu dans des applications personnelles de stockage dans le cloud.** Sans surprise, es utilisateurs ont collecté les données dans un stockage cloud personnel au cours des 30 derniers jours d'emploi, l'application la plus utilisée étant Google Drive. Les applications et les services cloud fournissant un stockage de fichiers gratuit sont les plus propices à l'exfiltration de données et à la diffusion de menaces, étant donné leur facilité d'utilisation et d'accès.
- **Surveillez et contrôlez les mouvements de données entre les instances de l'entreprise et les instances personnelles.** Plus de 480 applications disposent d'instances personnelles et d'instances d'entreprise dans lesquelles les mouvements et activités de données doivent être surveillés, contrôlés et évalués pour détecter les anomalies de comportement. Et pour les applications sans connaissance des instances, votre solution SSE devrait être en mesure de mapper les identités des utilisateurs pour les connexions afin de contrôler les politiques par tenant d'application.
- **L'écrasante majorité des menaces diffusées dans le cloud proviennent d'instances personnelles.** Le premier point clé de cet e-book indiquait que OneDrive et SharePoint sont à l'origine de plus d'un tiers des logiciels malveillants diffusés dans le cloud. La nuance à apporter à ce point clé est que les menaces proviennent principalement d'instances personnelles malveillantes, et non d'instances gérées par l'entreprise. Les pirates créent et utilisent facilement des applications publiques gratuites ou des comptes compromis pour diffuser des menaces et exfiltrer des données. Ainsi, l'inspection du trafic SaaS en ligne avec des défenses en temps réel est nécessaire.
- **Évitez le blocage et les restrictions de tenants et activez la connaissance des instances des applications SaaS**. Les solutions SSE sans connaissance des instances pour des centaines d'applications suggéreront de bloquer les tenants non gérés et donc d'autoriser uniquement l'accès SaaS géré en ligne. Cette situation est frustrante pour les unités opérationnelles et les utilisateurs, car plus de 98 % des applications utilisées ne sont pas gérées par le service informatique, et vous supprimez une option viable de résilience et de basculement si vos applications gérées sont mises hors ligne pour une raison quelconque.

Perspective 6

Les utilisateurs ont besoin d'un encadrement et d'une orientation en temps réel, et non de transparence

Les programmes de formation à la sécurité peuvent satisfaire aux règles de conformité une fois par an, mais les connaissances sont rapidement oubliées et les vieilles pratiques prévalent. Si la pratique traditionnelle de la transparence en matière de défense demeure, nous évoluons maintenant dans un environnement SaaS et de services cloud en pleine croissance où les utilisateurs ont besoin d'être guidés en temps réel pendant les transactions commerciales pour protéger les données. Imaginez un trajet en voiture dans la nuit noire vers une ville inconnue sans GPS pour vous repérer.

Points clés

- **L'encadrement et l'orientation en temps réel aident les utilisateurs pendant les transactions commerciales.** Assistez les utilisateurs au cours de leurs transactions en leur indiquant les applications à risque et en leur recommandant des alternatives plus sûres. Ou avertissez les utilisateurs des activités à risque au sein des applications lorsqu'ils partagent des données en dehors de l'entreprise. L'encadrement en temps réel, à l'instar de la navigation GPS pendant la conduite, est une option disponible qui devrait être exploitée rapidement dans les nouveaux déploiements de SSE pour guider les utilisateurs.
- **Dans plus de 95 % des cas, les utilisateurs font ce qu'il faut lorsqu'ils sont guidés et évitent les risques.** Lorsque les utilisateurs reçoivent une alerte en temps réel au cours d'une transaction commerciale concernant une application ou une activité risquée, nos résultats et les commentaires des clients montrent que, dans plus de 95 % des cas, ils annulent la transaction commerciale pour éviter l'activité risquée.
- **Pour les 5 % restants, recueillez des justifications pour en tirer les enseignements et affiner les contrôles de la politique d'accès**. Pour les utilisateurs avertis d'une activité risquée grâce à l'encadrement en temps réel, vous pouvez collecter un motif justifiant la poursuite de la transaction commerciale. Cela vous permet d'affiner davantage les contrôles granulaires de votre politique avec une meilleure compréhension de cas d'utilisation et de scénarios plus variés.
- **Le blocage de l'activité frustre les utilisateurs, augmente le nombre de tickets d'assistance et réduit l'agilité de l'entreprise**. Les contrôles grossiers dans le cadre de politiques qui bloquent les transactions commerciales devraient être remplacés par un encadrement en temps réel et par la collecte de justifications. Cela permet d'obtenir un scénario gagnant-gagnant-gagnant : la plupart des utilisateurs annulent la transaction risquée, les quelques utilisateurs qui ont besoin de finaliser la transaction vous en informent et vous augmentez l'agilité de votre entreprise.
- **Évitez le blocage lorsque l'encadrement en temps réel est possible et formez les utilisateurs aux activités à risque.** Les commentaires des DSI et RSSI clients montrent que l'encadrement en temps réel entraîne également une diminution des tickets d'assistance liés aux politiques de blocage. L'expérience utilisateur, la rapidité d'accès et la transparence restent importantes, mais comme pour la navigation GPS, les utilisateurs apprécient d'être guidés pour protéger les données et l'entreprise.

Perspective 7

Protection des données ou DLP classique, sachez faire la différence

Si vous travaillez dans le domaine des réseaux ou de la sécurité et que la protection contre la perte de données (DLP) est évoquée lors d'une réunion, vous vous dites probablement qu'il est temps de sortir ou de vérifier vos messages. La réduction de la surface d'attaque grâce à la protection des données avant la mise en œuvre d'une DLP classique est inestimable pour les équipes réseaux et sécurité. Les contrôles dans le cadre de politiques et les accès fonctionnent comme un entonnoir pour la protection des données, de sorte que lorsque la DLP est sollicitée, vous disposez de l'effort stratégique le plus efficace et le plus ciblé.

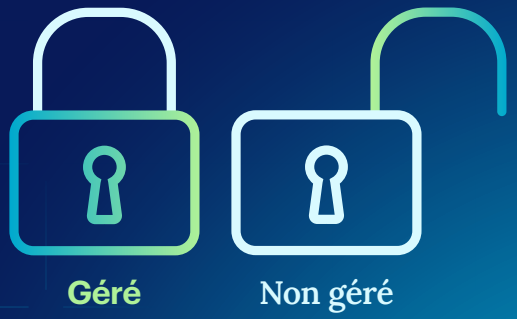
Points clés

- **La DLP classique nécessite souvent la classification et l'enregistrement des données, ce qui prend du temps**. Pour les données structurées, la DLP classique est la réponse appropriée ainsi que pour tous les canaux d'activité des données à travers le web, les solutions SaaS, le cloud, les e-mails et les points de terminaison. Oui, il faut du temps pour trouver les sources de données sensibles, classer les données et enregistrer les données pour une correspondance exacte des données ou une empreinte digitale, où la performance et l'échelle sont vitales pour des millions, voire des milliards, d'enregistrements.
- **La protection des données surveille et contrôle les mouvements de données par application et par instance.** Avant la DLP classique, vous deviez mettre en œuvre des contrôles dans le cadre de votre politique d'accès aux données, y compris l'accès aux applications à risque, les activités des applications et les mouvements des données par application et par instance. Mettez en place des garde-fous avec la sécurité du réseau SSE autour de la circulation des données pour les utilisateurs afin de réduire la surface des risques et de l'exposition des données.
- **Recommandez des alternatives plus sûres pour les applications et activités à risque, ainsi qu'un encadrement en temps réel**. La protection des données en amont de la DLP repose en partie sur l'utilisation de l'encadrement en temps réel pendant les transactions commerciales. À l'instar du guidage GPS et du signalement des accidents de la route, vous pouvez proposer des alternatives plus sûres pour protéger les utilisateurs, les données et votre entreprise.
- **Recueillez des justifications pour faire progresser et affiner les contrôles des mouvements de données dans le cadre de votre politique.** Découvrez les nouveaux cas et scénarios d'utilisation dans leurs justifications afin d'affiner les contrôles des politiques de protection des données qui peuvent ou non nécessiter des politiques et des règles DLP classiques. Une solution SSE fournit la visibilité et le contrôle du contenu au-delà des solutions de sécurité traditionnelles : réservez du temps pour apprendre ces nouvelles capacités.
- **Réduisez la surface d'attaque avec une approche en entonnoir pour les contrôles de protection des données.** Alors que vous travaillez sur les critères de votre RFI et sur une preuve de concept, vous devriez mettre en place une structure en entonnoir pour les contrôles dans le cadre de votre politique qui continue à réduire la surface d'attaque bien avant que les politiques et les règles DLP n'interviennent. Un ensemble complet de contrôles devrait se concentrer sur le mouvement et l'activité des données, l'encadrement, les justifications et les alternatives plus sûres.

Perspective 8

Les applications gérées et non gérées redéfinissent les défenses en ligne

Le cloisonnement du service en charge de la sécurité s'estompe, parallèlement à l'idée que les équipes informatiques ne doivent gérer que ce qu'ils adoptent et ce à quoi ils ont accès. La transformation numérique va de l'avant et pousse les unités opérationnelles et les utilisateurs à adopter des services SaaS et cloud sans l'intervention du service informatique. Alors que le service informatique peut gérer 40 à 60 applications SaaS et services cloud, il y a probablement des milliers d'applications en cours d'utilisation au sein d'une entreprise ou d'une organisation. Si elles ne sont pas connues, la première étape devrait être une appréciation du risque lié au cloud.



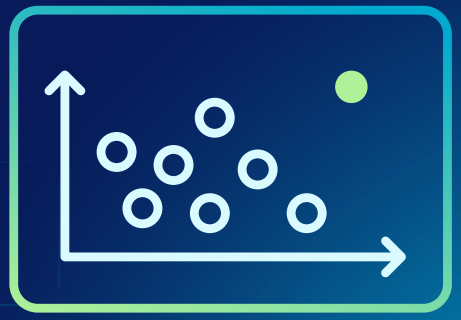
Points clés

- **Plus de 97 % des applications utilisées ne sont pas adoptées et gérées par les services informatiques.** C'est la vitesse d'adoption du SaaS, qui connaît une croissance de plus de 20 % d'une année sur l'autre. À mesure que les entreprises adoptent une stratégie « cloud first », elles recherchent des applications SaaS pour remplacer celles qu'elles utilisent dans leurs datacenters. Certains pays ont même adopté une stratégie « cloud first », comme c'est le cas de l'Australie.
- **Les unités opérationnelles et les utilisateurs sont les premiers à adopter les applications non gérées.** Ces publics ont des objectifs et des calendriers qui les poussent vers la transformation numérique, et c'est une question de survie pour certaines entreprises. Ils sont les premiers à adopter des applications SaaS non gérées et des services cloud en dehors de l'administration informatique. Une solution SSE peut activer en toute sécurité des tenants non gérés et des instances personnelles avec des contrôles en ligne dans le cadre de politiques et un encadrement.
- **L'inspection des API ne s'applique qu'aux applications et services cloud gérés.** Le principe du « mieux ensemble » s'impose étant donné que l'inspection des API est limitée aux applications applications et services cloud gérés et que le mastodonte évoqué précédemment de l'inspection en ligne couvre à la fois les instances d'applications gérées, non gérées et personnelles. Vous voulez contrôler le partage de fichiers, puis vous intéresser à l'inspection des API ? Vous voulez limiter les applications à risque et encadrer les utilisateurs ? Dans ce cas, optez pour l'inspection en ligne avec des contrôles en temps réel dans le cadre de votre politique.
- **Votre stockage dans le cloud est probablement propre, tandis que le reste héberge des menaces malveillantes.** Aucun problème ici, le stockage dans le cloud géré par votre entreprise est probablement propre et étroitement protégé. C'est pourquoi les pirates utilisent l'hébergement cloud gratuit avec des comptes frauduleux et des instances personnelles compromises pour diffuser des menaces et du pishing hébergés dans le cloud. C'est là que l'évidence passe inaperçue, au-delà de ce qui est visible pour les tenants et les instances gérés.
- **Inspectez les applications non gérées et les instances personnelles en ligne.** Votre RFI doit couvrir la capacité à fournir une inspection en ligne pour des milliers d'applications non gérées et des centaines d'applications pour la détection des instances. La capacité d'inspecter ce contenu en ligne est essentielle pour la protection contre les menaces et les données, la détection des anomalies de comportement et l'utilisation de l'analyse pour découvrir des risques inconnus et des mouvements de données.

Perspective 9

La détection des anomalies de comportement n'est plus facultative

Pendant des années, la détection des anomalies de comportement des utilisateurs et des entités (UEBA) s'est heurtée à la difficulté d'obtenir des événements et des journaux optimaux pour les cas d'utilisation souhaités, à savoir les initiés, la compromission d'accès et l'exfiltration de données. L'ajout de journaux et d'événements SSE fournissant des informations sur les utilisateurs, les applications et l'activité des données a ouvert les portes à la prise en charge de ces cas d'utilisation avec une grande efficacité.



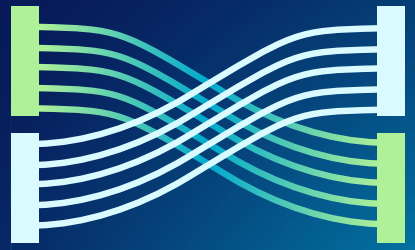
Points clés

- **Les utilisateurs sont plus confiants en ce qui concerne les données, qu'ils soient en télétravail ou en travail hybride.** Quelques mois après la pandémie, les tendances étaient très claires : les utilisateurs en télétravail prenaient plus de risques en accédant aux sites web, au contenu et en partageant les appareils gérés. Les utilisateurs ont également trouvé des alternatives aux solutions connues pour le partage des données et l'activité lorsqu'ils travaillent à distance avec plusieurs applications SaaS et services cloud, y compris leurs propres instances personnelles. Au fur et à mesure que la pandémie prenait de l'ampleur, les utilisateurs ont également augmenté leur productivité, peut-être en raison de l'absence de conversations autour de la machine à café et de distractions au bureau.
- **Les accès compromis forment une économie souterraine en soi.** L'adoption croissante du SaaS avec un accès direct depuis des postes en télétravail et hybrides a également ouvert la porte aux attaques par compromission d'accès et à une économie souterraine de vente de ces informations d'identification. Pour riposter, votre solution SSE doit fournir des adresses IP de sortie dédiées pour l'accès SaaS géré, uniques à votre entreprise ou organisation. Cela permet d'éviter l'utilisation d'informations d'identification compromises et les problèmes de réputation liés aux pools d'adresses IP partagées.
- **Utilisez l'inspection en ligne pour créer des références d'activité des utilisateurs et des groupes de pairs.** Les solutions SSE qui inspectent des milliers d'applications SaaS et pour des centaines d'instances fournissent d'excellentes données d'événements et de journaux. Cela permet de créer des références d'activité d'utilisateurs et de groupes de pairs UEBA très recherchées pour la détection d'anomalies allant au-delà de ce que les règles et les requêtes d'anomalies séquentielles peuvent détecter avec précision. De plus, les groupes de pairs éliminent tout comportement anormal préexistant au sein d'une référence d'utilisateur unique.
- **Tirez parti de l'UEBA basée sur l'apprentissage automatique (AA) pour détecter les anomalies.** Compte tenu des contrôles granulaires d'une solution SSE dans le cadre de politiques, les alertes, les journaux et les événements permettent de multiples modèles d'apprentissage automatique (AA) et des détecteurs uniques. Une solution SSE devrait disposer de plus de 50 modèles AA et de plus de 100 détecteurs pour la détection des anomalies pour un degré de maturité et d'expérience souhaité.
- **Évaluez et surveillez les utilisateurs pour détecter les comportements à risque et l'exfiltration de données.** Les solutions SSE ouvrent la porte à la notation de l'indice de confiance de l'utilisateur (UCI) pour une utilisation dans les contrôles de stratégie d'accès évolutifs et pour signaler les enquêtes dans les chronologies de corrélation d'événements pour les activités à risque et les mouvements de données. Consultez notre **article de blog sur la manière de rendre l'UEBA opérationnelle** pour en savoir plus.

Perspective 10

Surveiller pour découvrir les inconnues dans les analyses et les visualisations

L'utilisation d'analyses et de visualisations avancées pour comprendre les tendances et les comportements des applications, ainsi que les anomalies connues ou inconnues, est comparable à l'utilisation de l'IA/AA pour les défenses. Une évaluation des risques liés au cloud peut servir de base pour commencer à mettre en œuvre des mesures de contrôle et pour surveiller les changements de comportement et d'activités afin d'obtenir les résultats souhaités. L'encadrement en temps réel et la collecte de justifications peuvent être présentés dans des visualisations graphiques, ainsi que dans des nuages de mots. Dépassez les anciens rapports de filtrage SWG et Web avec la nouvelle visibilité apportée par le SSE sur l'activité des applications, des utilisateurs et des données.



Points clés

- **La visibilité est essentielle à l'activité des utilisateurs, des applications et des données afin de trouver des inconnues.** Combien d'applications de stockage dans le cloud sont utilisées dans votre entreprise et votre organisation ? Combien sont gérées ou non et y a-t-il un partage de données avec des tiers, des partenaires et des consultants ? Il en va de même pour les applications d'IA générative, auxquelles s'ajoute l'éventail plus large d'applications utilisées dans les services de marketing, de vente et de ressources humaines qui travaillent avec des données sensibles.
- **Supprimez les angles morts de M365, des instances et des applications non gérées.** Les solutions SSE suppriment l'angle mort de la non-inspection du trafic M365 et des instances personnelles cachées ou des tenants partenaires non gérés souvent liés à la diffusion de menaces et à l'exfiltration de données. L'époque du filtrage par domaine et catégorie web pour les applications primaires et les services cloud les plus fréquemment utilisés est révolue. Désormais, les détails se trouvent dans les instances, l'activité et le mouvement des données.
- **Exploitez les tableaux de bord et les visualisations graphiques (par exemple, les diagrammes de Sankey).** Grâce aux visualisations, l'être humain est très efficace dans la détection des anomalies et des zones d'intérêt afin de les détailler et de les explorer. Les solutions de SSE devraient offrir un large éventail de tableaux de bord et de visualisations allant au-delà des rapports traditionnels, ainsi que la possibilité de stocker les événements et les journaux pendant 3, 6 ou 13 mois, ce qui permet d'effectuer des analyses d'une année sur l'autre. La diffusion de journaux en temps quasi réel à partir de plateformes SSE est également préférable, mais la destination peut ne pas disposer de visuels analytiques avancés et de tableaux de bord prêts à l'emploi.
- **Surveillez les flux d'exfiltration de données pour les utilisateurs, les applications et les instances.** Les données sont le composant Zero Trust qui relie les utilisateurs, les appareils, les applications et les réseaux entre eux. Les données circulent entre ces composants et sont au cœur de ce qu'il faut protéger. Les solutions SSE dotées d'une visibilité et d'un contrôle granulaires permettent un accès au moindre privilège et une surveillance continue afin d'affiner et de faire mûrir les contrôles stratégiques pour soutenir les principes du Zero Trust. Fournir un accès Zero Trust avec un angle mort pour les utilisateurs, les applications et l'activité des données revient à passer à côté de la stratégie et des objectifs du Zero Trust.
- **Découvrez les inconnues grâce à l'analyse du contexte et aux visualisations.** Les utilisateurs adoptent et trouvent chaque jour de nouveaux résultats pour les mouvements de données inconnus et non approuvés. L'analyse peut révéler ces inconnues dans des visualisations graphiques de manière rapide et efficace. À moins que la nouvelle activité de données ne déclenche des alertes, elle pourrait rester cachée pour un initié, des utilisateurs à risque ou un employé sur le départ qui recueille des informations sensibles pour son prochain emploi.

Synthèse

Ces dix perspectives mettent en évidence de nouvelles fonctionnalités et exigences pour une RFI SSE ou SASE et pour des projets futurs. De par les observations issues de clients, il est recommandé d'effectuer une transformation SSE à partir des fonctionnalités existantes des solutions de sécurité traditionnelles en premier lieu. Ensuite, le parcours SSE commence par le développement de nouvelles compétences, l'ajout de nouvelles défenses comme des adresses IP de sortie dédiées, l'assistance par intelligence artificielle, la suppression des angles morts et des compromis, l'ajout de garde-fous et la protection des données avant la DLP, l'exploitation des défenses en temps réel (T+0), y compris la détection basée sur l'IA/AA et la surveillance des anomalies de comportement tout en recourant à l'analyse pour présenter les inconnues sous forme de graphiques.

- En savoir plus sur Netskope Security Service Edge
- **Études de cas clients**
- **Les fonctionnalités critiques pour le SSE selon Gartner**