Ecrit par :

netskope

Security Service Edge (SSE)

pour les nuls

Concevez votre infrastructure IT pour l'avenir de la sécurité dans le cloud

Utilisez CASB, SWG, ZTNA et pare-feu à partir d'une seule plateforme

Maîtrisez le SSE dans le cadre d'une architecture SASE et Zero Trust

Édition spéciale Netskope

Jason Clark

Steve Riley

À propos de Netskope

Netskope, le leader du SASE, connecte rapidement et en toute sécurité les utilisateurs directement à Internet, à n'importe quelle application et à leur infrastructure depuis n'importe quel appareil, sur le réseau ou en dehors. Grâce aux CASB, SWG, pare-feu en mode service et ZTNA intégrés nativement dans une seule plateforme, Netskope Security Cloud fournit le contexte le plus granulaire, via une technologie brevetée, pour permettre l'accès conditionnel et la sensibilisation des utilisateurs tout en appliquant systématiquement les principes Zero Trust à la protection des données et à la prévention des menaces. Contrairement à d'autres fournisseurs qui imposent des compromis entre la sécurité et la gestion réseau, le cloud privé de sécurité globale de Netskope offre des fonctionnalités de traitement complètes à la source des données.

Netskope fournit une solution omniprésente rapide, centrée sur les données et « cloud smart », tout en favorisant un Internet citoyen et en offrant un coût total de possession plus faible. Pour en savoir plus, consultez www.netskope.com.

Nous tenons à remercier un certain nombre de personnes qui ont rendu possible la publication de ce livre :

Chez Netskope : Amanda Anderson, Lauren Baker, Chad Berndtson, Jeff Brainard, Tim Chiu, Tom Clare, Catie Halliday, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Sasi Murthy, Shamla Naidoo, Lauren Polito, Zoe Revis,

James Robinson, James Yokota, Svetlana Rubin

Chez Evolved Media : David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Security Service Edge (SSE)

pour les nuls®

Security Service Edge (SSE)

Édition spéciale Netskope

par Jason Clark et Steve Riley

pour les nuls®

Security Service Edge (SSE) pour les Nuls®, une édition spéciale Netskope

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-89667-8 (pbk) ; ISBN 978-1-119-89668-5 (ebk)

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Rédacteur projet : Elizabeth Kuball

Rédacteur chargé des acquisitions : Ashley Coffey

Responsable éditorial : Rev Mengle

Représentant du développement commercial : Jeremith Coward

Éditeur de production : Tamilmani Varadharaj

Assistance spéciale : Nicole Sholly

Table des matières

Introduction

La transition globale des entreprises vers le cloud se fait beaucoup plus rapidement que ne le prévoyaient de nombreux experts. Cette rapidité a laissé la plupart des entreprises dépendantes de plateformes de sécurité conçues pour un monde révolu, dominé par les datacenters sur site. La pandémie de COVID-19 a encore accéléré et compliqué la situation, mettant à rude épreuve les RSSI chargés de protéger un personnel travaillant à domicile et qui ne retournera peut-être jamais complètement au bureau.

La bonne nouvelle est que le Secure Access Service Edge (SASE), un cadre d'architecture de sécurité, ouvre la voie à une solution basée sur le cloud qui offre la protection dont chaque entreprise a besoin, où que se trouve son personnel. Mieux encore, le Security Service Edge (SSE), qui est l'ensemble fondamental de services de sécurité du SASE, fournit les fonctionnalités nécessaires à la mise en œuvre de services de sécurité pour protéger les employés à distance, les technologies basées sur le cloud et les applications et infrastructures existantes sur site.

Le SASE est un cadre. Le SSE est un ensemble de services que vous pouvez acheter dès aujourd'hui. Ce livre explique le SSE et explore ses fondements, qui partent d'idées novatrices comme le Zero Trust, la sécurité adaptable basée sur le contexte et de nouvelles approches en matière de conception des réseaux. Cet ouvrage montre ensuite comment des services familiers s'imbriquent dans le SSE, aux côtés de technologies nouvelles et avancées qui peuvent renforcer considérablement la sécurité.

À propos de ce livre

Il est temps de remodeler le paysage de la sécurité moderne. La mise à disposition de plus amples informations sur le SSE permettra au personnel chargé de la sécurité et de la gestion de l'entreprise de se préparer aux étapes nécessaires pour refaire de la sécurité de l'entreprise, qui est actuellement un goulot, un amplificateur et un catalyseur de la transformation numérique. Ce livre pose les bases en expliquant les notions du SASE et du SSE, puis propose une feuille de route pour vous aider à mettre en œuvre cette nouvelle sécurité. L'utilisation du cloud exige que chaque entreprise transforme sa sécurité. Ce livre vous conseille sur la manière de vous préparer.

Quelques suppositions idiotes

Vous connaissez bien l'Internet et le domaine de la sécurité. Vous savez que le modèle de sécurité traditionnel que nous utilisons tous est poussé à sa limite. Vous savez également que le cloud est à la fois un catalyseur de productivité et un endroit dangereux où les informations d'identification et les données des individus et des entreprises sont attaquées. Enfin, vous souhaitez relever ce défi pour votre entreprise, vos employés, vos actionnaires, vos clients et vos partenaires commerciaux en utilisant la puissance des fonctionnalités du SASE et du SSE.

Pictos utilisés dans ce livre

Nous utilisons des pictogrammes tout au long du livre pour mettre en évidence les informations importantes.

CONSEIL

Le picto Conseil propose des raccourcis et d'autres informations qui peuvent vous faciliter la vie.

RAPPEL

Le picto Rappel signale les faits qu'il est particulièrement important de connaître.

ATTENTION

Les informations du picto Attention pourront vous épargner des soucis, essayez de les intégrer dans votre réflexion.

Au-delà de ce livre

Pour de plus amples informations sur les solutions Netskope, rendez-vous sur `www.netskope.com` Pour une analyse approfondie du SSE (Security Service Edge), rendez-vous sur le site `www.netskope.com/security-defined/security-service-edge-sse`.

DANS CE CHAPITRE

- Explorer l'avenir de la sécurité
- Comprendre comment les transformations numériques affectent la sécurité
- Découvrir comment créer l'oasis de sécurité que nous voulons tous atteindre

Chapitre 1
Comment le contexte et l'intégration accélèrent la transformation de la sécurité

Les organisations se tournent vers les applications cloud pour tirer parti des avantages commerciaux évidents que procure le cloud en termes de rapidité, d'efficacité et de visibilité. Pour protéger réellement les données, les personnes et les applications cloud, la sécurité ne peut plus se borner à de simples décisions binaires, d'acceptation ou de refus, qui s'appliquaient à l'époque où le réseau régnait en maître et où la plupart des employés se trouvaient au même endroit. La sécurité doit devenir plus intelligente grâce à un contexte détaillé permettant d'élaborer exactement la protection qu'il faut à votre organisation, quel que soit l'emplacement de vos employés. La sécurité doit suivre les données où qu'elles aillent, et elle doit être facile à appliquer pour ne pas ralentir l'activité.

L'avenir de la sécurité

C'est le moment idéal pour se plonger dans le sujet de la sécurité. La puissance et la qualité de la technologie de la cybersécurité font des progrès étonnants. Jamais les professionnels de la sécurité n'ont eu à faire face à autant de changements aussi rapidement, et jamais ils n'ont eu l'occasion, comme aujourd'hui, de faire de la sécurité un outil stratégique pour l'entreprise. Les données, les applications et les employés ont migré vers le cloud. La sécurité doit donc suivre.

Les entreprises qui adoptent une posture de sécurité basée sur le cloud pour assurer leur transformation digitale innoveront plus rapidement et plus sûrement que les entreprises dont la politique de sécurité reste ancrée dans le passé. Nous envisageons une nouvelle ère dans laquelle les professionnels de la sécurité prendront enfin de l'avance sur les cybercriminels et soutiendront leurs entreprises alors que la transformation digitale alimentée par le cloud passe à la vitesse supérieure.

Les efforts visant à imposer les systèmes de sécurité existants dans le cloud ne sont pas couronnés de succès. Dans un cadre appelé Secure Access Service Edge (SASE), la sécurité se transforme pour s'adapter au lieu de travail hybride basé sur le cloud.

ATTENTION

Les produits et services de sécurité de pointe du passé ne sont pas utiles dans le cloud. Il en va de même pour la modernisation d'une ancienne technologie de sécurité ou sa requalification comme étant « compatible avec le cloud ».

Les fournisseurs de technologies de sécurité proposent au contraire de nouveaux produits et services « cloud native » pour assurer la protection lorsque les données sont stockées et les applications exécutées sur une infrastructure que les entreprises ne contrôlent pas elles-mêmes. Les nouvelles technologies de sécurité doivent protéger non seulement l'*accès* aux données, mais aussi l'*utilisation* de ces données.

Il est utile d'envisager la sécurité « prête pour le Cloud » en fonction de quatre idées fondamentales :

- Le **SASE** est le cadre de mise en œuvre d'une infrastructure convergente basée sur le cloud pour les fonctions réseau et de sécurité. Le SASE combine plusieurs concepts, notamment Zero Trust, SD-WAN et Security Service Edge (SSE), pour nous guider vers une politique de sécurité et de mise en réseau qui protège et régit le cloud et le nouvel environnement de travail à distance. Les analystes reconnaissent que cette nouvelle architecture offre une sécurité complète pour un monde centré sur le cloud. (Voir *Conception d'une architecture SASE pour les Nuls* de Netskope pour une présentation complète.)
- Le **SSE** est la manière dont tous les services de sécurité nécessaires au SASE (qui étaient auparavant des applications, des produits ou des services distincts, émanant souvent de fournisseurs différents) sont réunis sous une forme unifiée et intégrée qui offre une capacité et une efficacité accrues, et réduit la complexité et les coûts. Le SSE représente des capacités de sécurité profondément intégrées qui sont conscientes les unes des autres, fonctionnent bien ensemble et proviennent d'un seul fournisseur. Netskope définit en

outre un ensemble de capacités étendues que nous appelons le SSE authentique (voir le chapitre 3).

- Le **contexte** détermine comment les capacités de sécurité intégrées du SSE sont appliquées comme mécanisme de contrôle pour assurer la sécurité des données, des applications et des personnes à tout moment. Le contexte ou la compréhension approfondie de *l'identité* de la personne, de *ce qu'elle essaie de faire* et de la *raison* pour laquelle elle essaie de le faire (le qui, le quand et le pourquoi) permet également d'appliquer des politiques de sécurité adaptatives pour atténuer les risques en temps réel. Auparavant, les seules options possibles étaient l'autorisation ou le blocage. Désormais, le contexte enrichi prend en charge des nuances de contrôle d'accès, et permet des autorisations sous certaines conditions, afin de fournir une sécurité sûre sans perturber la productivité. La qualité et l'étendue du contexte constituent un facteur de différenciation essentiel entre les éditeurs de services de sécurité.
- Les principes **Zero Trust** différencient les politiques véritablement adaptatives de la simple authentification conditionnelle basée sur la familiarité. L'objectif n'est pas seulement de fournir l'accès et l'autorisation dont chaque personne a besoin pour effectuer une tâche donnée, en fonction du niveau de confiance dérivé d'une évaluation en temps réel de l'identité de l'employé et de la méthode d'accès. L'accès adaptatif nécessite de comprendre ce qui se passe *après* la connexion, notamment les signaux environnementaux qui varient dans le temps, le comportement historique et actuel, et les caractéristiques des données elles-mêmes. Chez Netskope, nous considérons le Zero Trust comme le point de départ (aucune confiance au début de chaque interaction) et visons l'objectif d'une *confiance adaptative continue*, avec un degré de confiance qui est proportionnel au niveau de confiance déterminé et aux signaux environnementaux.

Ce livre explique comment ces concepts se rejoignent dans une mise en œuvre efficace du SSE pour créer une nouvelle oasis de sécurité (voir le chapitre 3). Les entreprises vont enfin pouvoir bénéficier d'une sécurité basée sur le cloud offrant tout ce qui est nécessaire pour protéger une myriade de données et d'applications accessibles par des employés qui sont, et resteront, répartis et souvent éloignés du site de l'entreprise.

Imposer la transformation de la sécurité

Des innovations dans plusieurs domaines de la transformation digitale sont en train de remodeler le monde des affaires. La transformation de la sécurité est essentielle pour atteindre et maintenir le succès des efforts de transformation digitale.

RAPPEL

Les technologies comme le cloud, l'Internet des objets (IoT), le Machine Learning/l'intelligence artificielle (ML/IA) et l'analyse améliorent considérablement les résultats des entreprises. Si la sécurité ne peut pas suivre, ces progrès sont menacés.

- **L'explosion des données :** d'ici 2025, IDC prévoit qu'il existera 175 zettaoctets (Zo) de données dans le monde (soit 25 fois plus qu'en 2010). Les gros titres des journaux en témoignent que les cybercriminels volent les données des entreprises à des fins malveillantes : pour les vendre, les modifier de manière malveillante ou obtenir une rançon. Netskope Threat Labs a découvert que le cloud est un terrain de jeu pour les pirates, avec 68 % des logiciels malveillants diffusés via le cloud en 2021 (contre moins de la moitié en 2020). L'explosion des données accessibles à partir du cloud génère davantage de cibles pour les cybercriminels et de défis pour les défenseurs.
- **L'explosion du cloud :** les entreprises adoptent des infrastructures et des applications cloud pour gagner en rapidité, en flexibilité et en souplesse. Selon Netskope Threat Labs, une entreprise moyenne est abonnée à plus de 800 applications SaaS (Software-as-a-Service) différentes. Dans 97 % des cas, il s'agit d'applications de type Shadow IT, c'est-à-dire non gérées par les services informatiques internes (et, dans de nombreux cas, invisibles pour leurs yeux). En outre, les paramètres de sécurité par défaut de nombreuses applications cloud sont très ouverts, une autre raison pour laquelle les pirates trouvent que le cloud est une cible particulièrement lucrative.
- **L'explosion du nombre d'appareils :** les estimations varient considérablement quant au nombre de devices connectés à l'Internet qui se profilent à l'horizon, allant de 25 milliards en 2025 à 75 milliards peut-être en 2030. L'augmentation du nombre d'appareils et le surcroît de connectivité créent un domaine technologique plus vaste, et une surface d'attaque plus importante. Néanmoins, cette explosion d'appareils est un accélérateur pour l'innovation.

RAPPEL

La transformation de la sécurité consiste à créer une nouvelle manière de gérer tous ces évolutions afin que l'entreprise puisse faire ce dont elle a besoin pour réussir.

Les entreprises qui ne parviennent pas à s'engager dans une transformation de la sécurité basée sur le cloud sont confrontées à des risques croissants. Le paysage actuel de la sécurité est devenu trop complexe et coûte aux entreprises des sommes importantes en dépenses d'investissement (CapEx), en dépenses opérationnelles (OpEx) et en heures de

travail, alors même que son efficacité diminue. Les fournisseurs doivent par conséquent refondre les fonctions dans des systèmes qui collaborent.

Création d'une oasis de la sécurité

Les entreprises qui planifient leur avenir en matière de sécurité doivent envisager ce à quoi ressemble une oasis de la sécurité, tant dans les grandes lignes que dans les moindres détails. Ce sont des conseils pratiques, et non pas du marketing, qui doivent guider leurs décisions.

D'un point de vue global, voici comment cette transition pourrait se produire :

1. **Transformez le réseau.**

   Le réseau doit déplacer les données aussi efficacement que possible entre tous les points, y compris les services cloud et le datacenter, sans sacrifier la performance et l'expérience des employés au profit de la sécurité. Le trafic est acheminé à travers un réseau conçu pour prendre en charge le SSE et composé de points de présence (PoP) répartis dans le monde entier. Le personnel au bureau, en télétravail ou au café bénéficie d'une sécurité et de performances de haut niveau, et les données de l'entreprise restent protégées.

2. **Consolidez les services de sécurité.**

   Une suite unifiée, proposée par un seul fournisseur et offrant un SSE complet, remplace le patchwork d'anciennes appliances de sécurité. Les capacités fusionnées simplifient la gestion et l'administration, garantissent une application cohérente des politiques et rationalisent le traitement du trafic.

3. **Étendez l'utilisation du SSE et mettez en œuvre des services de sécurité avancés.**

   Une fois le SSE en place, les équipes de sécurité peuvent introduire des fonctions puissantes, comme l'isolation des activités de navigation web au sein d'un environnement cloud (RBI), la gestion de la politique de sécurité du cloud (CSPM) et la gestion de la politique de sécurité du SaaS (SSPM). Les fonctionnalités avancées comme la protection contre la perte des données (DLP) et la protection contre les menaces avancées (ATP) sont plus performantes que dans les anciens modèles, entravés par une intégration minimale et une visibilité limitée.

4. **Protégez les données stockées dans le cloud et les appareils de l'entreprise.**

   Le même fournisseur du SSE doit également proposer un pare-feu en mode service (FWaaS) pour protéger les applications basées sur le cloud, les appareils appartenant à l'entreprise et les référentiels de données.

5. **Traitez le datacenter comme une autre destination.**

   Le datacenter traditionnel de l'entreprise, qui était autrefois la seule destination par laquelle tout le trafic était réacheminé, devient une destination supplémentaire vers/à partir de laquelle le SSE achemine le trafic. L'élimination du hairpinning réduit les coûts, la complexité et renforce les performances.

6. **Appliquez les principes Zero Trust pour atteindre un état de confiance adaptative continue.**

   Comme le SSE surveille constamment le trafic après l'octroi de l'accès, les professionnels de la sécurité peuvent effectuer une analyse contextuelle approfondie de la session, prendre des décisions fondées sur des renseignements sur les risques fournis par des tiers, détecter les changements dans les profils de risque et neutraliser les actions dangereuses. Les notifications peuvent inciter les employés à améliorer leurs habitudes de sécurité.

7. **Améliorez la gestion des risques dans l'ensemble de l'entreprise avec une visibilité accrue.**

   La possibilité de voir, de guider et de contrôler l'activité de chaque personne dans l'entreprise améliore considérablement la connaissance et la détection des risques. L'équipe de sécurité peut se concentrer sur les zones à haut risque et déployer plus rapidement des politiques optimisées dans le SSE pour réduire les risques. Les responsables de la sécurité peuvent participer à des conversations sur les risques et la stratégie commerciale qui leur permettent d'occuper des positions vitales à la table des décideurs.

La transformation de la sécurité n'est pas une mince affaire. Le chapitre 4 montre comment les principes Zero Trust permettent de passer progressivement à une mise en œuvre complète de la sécurité basée sur le cloud. Le chapitre 5 met en évidence les erreurs courantes et les principes de réussite et décrit un parcours représentatif que de nombreuses entreprises suivront si elles abordent le SSE, le Zero Trust et, en fin de compte, le SASE correctement.

DANS CE CHAPITRE

- **Découvrir l'histoire du pare-feu**
- **Pourquoi le cloud n'est pas prêt de disparaître**
- **Accepter les limites des outils à usage spécifique**
- **Explorer comment la sécurité doit être intégrée et suivre les données**
- **Apprécier le rôle que joue le SSE dans les besoins en matière de sécurité**

Chapitre 2
Comment le cloud a remis en cause le modèle de sécurité traditionnel

Il y a dix ans, peu de dirigeants ont prédit la rapidité avec laquelle toutes les formes de solutions cloud allaient s'imposer dans les entreprises. Selon Netskope Threat Labs, les entreprises utilisent aujourd'hui, en moyenne, plus de 800 applications SaaS (Software-as-a-Service).

Le cloud et l'edge computing poussent de plus en plus de charges de travail de l'entreprise en dehors du datacenter. Les initiatives de travail à distance, accélérées par la pandémie de COVID-19, ont incité davantage de personnes, de devices, d'applications, de services et de données à s'échapper des limites traditionnelles du datacenter de l'entreprise. Le cloud est désormais essentiel à la productivité des entreprises. Mais à mesure que de nouveaux risques se matérialisent, il nous oblige également à repenser la sécurité.

Pensez à la façon dont les parents protègent leurs enfants lorsqu'ils sont bébés ou tout-petits. Ils ajoutent chez eux des dispositifs de sécurité aux escaliers, aux prises électriques, aux armoires et aux sièges de toilette. Les parents protègent le périmètre intérieur grâce à une alarme qui les

prévient chaque fois qu'une porte s'ouvre. Ils protègent le périmètre extérieur avec une clôture dans l'arrière-cour. Après avoir envoyé leurs enfants à la crèche, à l'école et plus tard à l'université, l'objectif de protéger leurs enfants reste le même, mais le rôle des parents a changé.

De même, les objectifs de sécurisation du cloud impliquent de reconnaître que l'objectif de la sécurité (protéger les données, les applications et les individus) n'a pas changé. Ce qui a changé, c'est que les données, les applications et les individus ont quitté le « nid », ce qui réduit le rôle du pare-feu et le relègue loin derrière. Par ailleurs, les menaces qui se développent le plus rapidement se trouvent dans le cloud, et non dans votre datacenter. Résultat : les tactiques de sécurité doivent changer.

L'époque où le pare-feu régissait la sécurité

Il y a plusieurs années, le pare-feu était le dispositif central de sécurité le plus important et probablement le poste le plus coûteux de votre budget dans ce domaine. La plupart des entreprises ont conçu leur architecture de sécurité réseau autour du datacenter, entouré d'un périmètre bien défini. La sécurité passait avant tout par la sécurisation du réseau.

Cette approche avait du sens dans un monde qui ne connaissait pas encore le cloud. Le datacenter était, après tout, un lieu unique où une entreprise hébergeait ses précieux actifs numériques. Tout comme une maison protégée aujourd'hui par une alarme efficace, une entreprise se devait d'ériger un périmètre (presque) impénétrable autour de son datacenter. L'accès était étroitement limité par une puissante barrière composée d'appliances de sécurité. Comme un parent ayant installé des alarmes sur les portes et les fenêtres, vous exerciez un contrôle important sur la sécurité de votre entreprise dans ce monde antérieur au cloud.

Les collaborateurs évoluaient dans un réseau exclusif et privé qui les reliait aux zones dont ils avaient besoin pour leur travail. Les personnes se trouvant dans des succursales éloignées ou travaillant à distance parcouraient le réseau privé, tapaient le code d'alarme et obtenaient l'autorisation d'accéder non seulement aux applications et aux données internes, mais aussi à toutes les destinations externes connectées. Le renvoi du trafic des télétravailleurs via ce datacenter centralisé à l'intérieur du périmètre, puis vers l'extérieur, augmentait le coût et la complexité et réduisait fortement les performances.

La sécurité des pare-feux legacy consistait simplement à autoriser ou à refuser l'accès. Une fois l'accès accordé, la présence et les bonnes intentions d'un individu étaient considérées comme acquises. Dans ce type de sécurité basée sur le périmètre, les entreprises ont adopté des mesures pour contrecarrer les menaces individuelles ou des catégories de

menaces au fur et à mesure de leur apparition. Si elles détectaient une menace, il leur suffisait d'acheter du matériel supplémentaire. Dans le modèle sur site, une entreprise pouvait disposer d'une rangée de dix boîtiers de sécurité reliés par un fil.

Chaque boîtier devait effectuer une opération particulière : détection de malwares, comparaison des signatures et blocage des intrusions, filtrage du courrier électronique, recherche dans les données sensibles, prévention des attaques par résolution de noms ou encore blocage des ports et des protocoles à l'aide de listes de contrôle d'accès. Chaque fonction faisait son travail et acheminait ensuite les paquets vers la fonction suivante de la chaîne, ce qui ajoutait de la latence et de la complexité.

Le cloud a changé toutes ces hypothèses.

Comprendre comment le cloud bénéficie aux entreprises

Le cloud computing offre une flexibilité et une valeur commerciale si profondes qu'à ce stade, il est impossible de revenir en arrière. (Et vous pouvez ignorer les déclarations fanfaronnes de « rapatriement » dans les datacenters des entreprises. Sauf pour des scénarios rares et spécifiques, ce n'est tout simplement pas possible.) Le cloud est attrayant pour les PDG, les directeurs financiers, les directeurs informatiques et les entreprises en général, car la majeure partie de l'infrastructure est commercialisée clés en main. Le cloud évite de consacrer beaucoup de temps et d'argent à créer votre propre infrastructure. Vous vous abonnez à une solution cloud, vous l'activez, vous la personnalisez pour qu'elle réponde aux besoins uniques de votre entreprise et vous pouvez l'utiliser comme bon vous semble. À l'heure où les entreprises cherchent à accélérer la création de revenus et à devenir plus rentables, le passage au cloud computing est de toute évidence une réponse à cet objectif.

Le cloud est également apprécié par vos collaborateurs très occupés. En effet, les applications SaaS largement disponibles offrent des plateformes modernes et parfois agréables pour collaborer, communiquer, gérer les finances, conclure des ventes et gérer la relation client. Ces applications cloud proposées par des entreprises tierces sont plus performantes, plus rapides et plus efficaces que ce qu'offrent les anciennes applications métiers encombrantes dans les limites rigides du datacenter.

ATTENTION

Mais le hic est là ... et le danger : la majorité de ces applications cloud n'ont pas été autorisées et ne sont pas gérées par le service informatique de l'entreprise. Elles ne sont pas non plus sécurisées. Vous avez toujours le devoir de protection, mais vous n'avez plus les mêmes moyens de contrôle auxquels vous étiez habitués. Adopter le cloud, c'est comme envoyer ses enfants à l'école ou même à l'université : vous ne pouvez plus les voir et savoir ce qu'ils font.

À l'ère du cloud, le pare-feu n'est plus le contrôle de sécurité le plus important, car il ne protège pas complètement votre entreprise contre les menaces du cloud. Dans ce nouveau paysage très ouvert, sans sécurité adéquate destinée à protéger nos processus numériques, nos employés, nos clients et nos biens, les efforts d'accélération numérique seront risqués. Dans cette nouvelle ère, le rôle de la sécurité est de libérer la valeur commerciale créée par le cloud tout en gérant ses dangers.

Les outils à usage spécifique peuvent être utiles, mais ne résolvent pas les problèmes majeurs

À mesure que les employés ont quitté leur bureau pour un mode de travail hybride, les données et les applications ont été transférées dans le cloud. C'est à ce moment là, que les outils de sécurité traditionnels installés dans le datacenter sont devenus aveugles aux activités se déroulant au-delà du périmètre. Les applications SaaS nécessitaient des données provenant de l'intérieur des murs pour être utiles. Pourtant, les applications elles-mêmes se trouvaient à l'extérieur des murs, ce qui rendait les données qui y migraient incontrôlées et non protégées par la sécurité de l'entreprise.

Un changement s'imposait si les entreprises voulaient profiter en toute sécurité des applications cloud. Les entreprises ont configuré de nouveaux produits ponctuels étroitement ciblés sur leurs réseaux privés et le cloud afin de résoudre les problèmes de sécurité les plus urgents et les faiblesses liées à l'utilisation du cloud. Ces outils comprenaient :

- **des passerelles d'accès cloud sécurisées (CASB) :** les CASB permettent de gérer et de protéger les données d'entreprise stockées dans l'ordinateur d'un tiers, ce qui est une façon honnête de conceptualiser le cloud.
- **des passerelles Web sécurisées (SWG) :** les SWG protègent les employés et les organisations contre les menaces sur le Web, c'est-à-dire les pages qu'un employé visite lorsqu'il est en ligne et qu'il navigue sur des sites publics.

- **un accès « Zero Trust » au réseau (ZTNA) :** les produits ZTNA protègent les applications privées d'une entreprise contre le public et mettent simultanément ces applications à la disposition d'un ensemble de collaborateurs connus.

Ces outils représentaient une première génération de sécurité dans le cloud. Mais cette première génération était également dépourvue d'un élément essentiel : l'intégration.

L'intégration de la sécurité est une nécessité

Les produits de sécurité cloud de première génération provenaient souvent de différents fournisseurs et, par conséquent, n'étaient pas compatibles les uns avec les autres. Chaque produit offrait sa propre console et nécessitait la configuration de stratégies de duplication et de chevauchement (pensez à la prévention de pertes de données ou DLP dans ce cas). Chacun d'entre eux pouvait nécessiter un agent dédié, créant ainsi des problèmes de déploiement et d'acheminement du trafic. Et chacun nécessitait des négociations de contrat et des accords d'achat distincts.

C'était comme si vos sens – ouïe, odorat, goût, vue et toucher – étaient tous reliés à des cerveaux différents. Faute d'intégration, si vous voyez un incendie, sentez une odeur de brûlé ou entendez des flammes crépiter, vous ne savez pas quoi faire parce que votre cerveau visuel, votre cerveau olfactif et votre cerveau auditif ne partagent aucune information. Ils ne mettent pas en corrélation les données de tous vos sens.

Dans une telle infrastructure de sécurité, vous disposez de nombreux systèmes différents, chacun ayant son propre cerveau compétent dans son domaine particulier. Par exemple, le CASB est un cerveau qui se concentre principalement sur les employés qui essaient d'accéder à une application SaaS.

RAPPEL

Tout comme votre cerveau unique acquiert des informations de tous vos sens pour prendre des décisions sur votre comportement dans le monde, vos services de sécurité doivent être totalement intégrés pour prendre des décisions efficaces qui soutiennent votre stratégie cloud. Le SSE est le cerveau qui intègre des catégories de sécurité disparates. Au lieu de fonctionner séparément en séquence, le SSE permet à tous ces « sens » de sécurité de s'activer en parallèle. Résultat ? Une sécurité à la fois plus rapide et plus efficace. De plus, le SSE est beaucoup plus facile à acquérir, car toutes les capacités (CASB, SWG, ZTNA et connexes) sont achetées ensemble au cours d'une seule transaction.

La sécurité doit suivre les données

Comme nous l'expliquons au chapitre 1, le SASE (Secure Access Service Edge) décrit une vision dans laquelle le périmètre traditionnel de l'entreprise n'existe plus. Au lieu de cela, l'ensemble du portefeuille de fonctions réseau et de fonctionnalités de sécurité est transféré dans le cloud, où il est immédiatement proche des employés, des données stockées dans le cloud et des applications SaaS.

Le SASE permet d'ajuster notre perspective dans un monde où l'on travaille à partir de n'importe où et où l'ancienne notion de périmètre physique a disparu. Dans ce nouveau monde, la sécurité doit aller bien au-delà des limites du datacenter. La sécurité doit maintenant suivre l'atout le plus important d'une entreprise (ses données) avec un niveau de conscience contextuelle suffisant pour protéger ces données partout où elles se trouvent et quel que soit l'accès.

Pour offrir une sécurité adaptée au cloud, de nouvelles hypothèses et capacités de sécurité doivent être mises en place. La sécurité doit :

- suivre les données.
- être basée sur un contexte enrichi.
- s'adapter aux caractéristiques spécifiques du contexte d'un employé.

L'autre élément clé qu'un modèle SASE permet de résoudre est l'équilibre entre la sécurité et les performances du réseau. Nous ne pouvons pas compromettre l'une au profit de l'autre : nous avons besoin des deux. Les collaborateurs sont plus productifs lorsque leur expérience de la technologie se fait sans effort et de façon fluide. Lorsque les outils de sécurité ralentissent les réseaux, les performances se dégradent et la productivité en souffre. Pire encore, les employés tentent de contourner les contrôles de sécurité, ce qui crée un risque et une exposition considérables.

L'étape cruciale pour arriver à cet équilibre consiste, pour une entreprise, à déplacer ses capacités réseau et de sécurité essentielles vers le cloud tout en éliminant les appliances périmétriques et (préparez-vous à des réactions négatives) tous les anciens outils.

Une telle approche fournira un accès sûr et fiable aux services Web, aux applications et aux données, avec des principes Zero Trust appliqués tout au long pour obtenir un état de confiance permanente et adaptable à chaque interaction.

Le SSE : un guide des besoins de sécurité sur le parcours du SASE

Le SASE et le SSE représentent la façon dont la sécurité migre vers le cloud et devient plus efficace que toutes les solutions utilisées auparavant.

Le SASE est une vision globale de la transition des fonctionnalités réseau et de sécurité vers le cloud. Le SSE est le cerveau qui intègre, identifie et exécute un ensemble spécifique de services de sécurité nécessaires pour mettre en œuvre le SASE. L'ensemble des services intégrés devient le point de contrôle principal où l'inspection et le contrôle de sécurité sont appliqués de manière cohérente à tout le trafic. Le SSE ne remplace pas le pare-feu (vous en aurez toujours un), mais supplante la position de ce dernier comme fonctionnalité de sécurité centrale.

La CASB, le SWG, le ZTNA et d'autres services connexes ont certainement de la valeur, individuellement. La plupart des entreprises ont déjà déployé une solution de ce type, voire deux. Toutefois, pour exploiter pleinement la valeur du cloud, ces services doivent être intégrés et fonctionner ensemble.

Netskope estime que les fonctions essentielles du SSE peuvent être complétées par de nombreuses fonctionnalités actuellement absentes de la sécurité de l'entreprise, mais incontournables pour sécuriser de manière fiable les actifs numériques au-delà des limites du datacenter. Par exemple :

- **La classification :** identifie les informations sensibles, idéalement lorsqu'elles sont créées, mais également par le biais d'analyses périodiques des bases de données.
- **La protection contre la perte des données (DLP) :** surveille et contrôle activement le mouvement des informations sensibles.
- **La sensibilisation aux menaces et leur neutralisation (également connue sous le nom de protection contre les menaces avancées ou ATP) :** identifie les signes indiquant qu'un environnement a été compromis et prend des mesures pour réduire ou éliminer la probabilité d'une nouvelle attaque.
- **La gestion de la politique de sécurité du cloud (CSPM) :** évalue la configuration des infrastructures et des plateformes cloud et prend des mesures pour remédier aux erreurs de configuration susceptibles d'entraîner des violations.

- **La gestion de la politique de sécurité en mode SaaS (SSPM) :** évalue la configuration des applications SaaS et élimine les erreurs de configuration qui pourraient permettre l'exfiltration, l'usurpation d'identité ou d'autres types d'attaques.
- **La gestion de l'expérience numérique (DEM) :** analyse les données recueillies à des fins de sécurité ainsi que d'autres signaux de disponibilité et de performance pour mesurer l'expérience des employés et résoudre rapidement les problèmes.

RAPPEL

En combinant toutes ces fonctionnalités en un seul produit de sécurité intégré déployé dans le cloud où il est le plus proche des utilisateurs, des données et des applications, le SSE devient le point de contrôle le plus important pour protéger votre entreprise. (Nous examinons le SSE plus en détail au chapitre 3.)

Nous avons besoin d'une sécurité pour demain, pas pour hier

Nous devons déployer des outils qui prennent en charge le cloud, facteur clé de la création de valeur et de revenus pour l'entreprise. Nous devons déployer des outils qui résistent aux attaques des adversaires. Enfin, nous devons déployer des outils qui n'entravent pas les opérations. Ce concept revient en quelque sorte à envoyer un garde du corps invisible avec votre enfant à la crèche, à l'école et à l'université. Ce garde du corps portable, c'est le SSE.

DANS CE CHAPITRE

- Comprendre la nécessité du SSE
- Explorer les fonctionnalités et les exigences du SSE
- Évaluer les avantages du SSE

Chapitre 3
Security Service Edge : un plan pour l'avenir de la sécurité dans le cloud

Le SASE (Secure Access Service Edge) change notre point de vue sur la façon dont la sécurité est fournie dans un monde basé sur le cloud où les données peuvent être consultées de n'importe où. Lorsque les employés travaillent à distance, que les applications deviennent des logiciels SaaS et que les données se déplacent dans le cloud, les efforts de cybersécurité d'une organisation doivent également se déplacer dans le cloud. Correctement mis en œuvre, le SASE nous montre que la sécurité doit être aussi proche que possible de l'endroit où les données résident et sont consultées. Dans le SASE, la sécurité protégera les intérêts d'une organisation et fournira des contrôles cohérents, même éloignés et sans dégrader la connectivité réseau et l'expérience utilisateur.

La réalisation du SASE s'appuie en partie sur la consolidation et l'intégration de la sécurité : l'essence même du SSE.

Le SSE délocalise les points de contrôle et d'inspection stratégiques vers le cloud où votre entreprise exerce ses activités. Cette évolution place la sécurité à proximité de l'endroit où les données, les applications et les personnes opèrent, et là où se trouve le danger. Avec le SSE, des services

d'inspection et de contrôle pour le SaaS, le Web et les données, ainsi qu'une sensibilisation et une neutralisation sophistiquées des menaces, fonctionnent comme un système unique, cohérent et interopérable.

CONSEIL

Vous n'avez pas un problème de réseau. Vous avez un problème de sécurité dans le cloud. La seule conversation au sujet du réseau concerne l'adoption d'une architecture qui fait du SSE le principal point de contrôle dans le cloud.

Le SSE fournit des fonctionnalités qui transcendent ce que les pare-feux traditionnels peuvent faire. Un SSE correctement implémenté discerne également le contexte (le quoi, le comment et le pourquoi de la consultation des données), ce qui lui permet de prendre des décisions de sécurité nuancées en temps réel. Le SSE connecte tous vos « sens » de sécurité en un système nerveux qui interprète les données, comprend l'étendue des risques présentés et négocie le niveau d'accès approprié à tout moment, dans n'importe quel scénario.

Dans un premier temps, nous verrons comment fonctionne le SSE.

Raisons pour lesquelles nous avons besoin du SSE

L'ancienne approche de la sécurité consistait à établir un périmètre et à déployer un pare-feu pour tenter de repousser les hackers qui visaient le datacenter de votre entreprise. Mais comme aucune sécurité n'est infaillible, un hacker ayant réussi à franchir le périmètre était libre de se déplacer latéralement dans votre réseau, rendant vos données et vos applications sans défense.

Les architectures SASE reposent toujours sur la gestion des identités et des accès pour authentifier les employés et sur les plateformes de protection des terminaux pour protéger les appareils. Mais un SASE efficace met également en œuvre des principes Zero Trust qui accordent l'accès et contrôlent la confiance sur la base d'un ensemble complet de conditions. Dans le cloud, le contexte entourant la personne devient le périmètre.

Le Zero Trust est une philosophie basée sur trois propositions qui sont fondamentales pour le SSE et, par conséquent, pour le SASE :

- La confiance implicite présente dans les conceptions existantes a fait son temps. Le Zero Trust inverse ce principe de confiance pour vérifier l'identité des utilisateurs avant de leur faire confiance. Chaque personne ou action qui demande l'accès aux données doit

faire vérifier son identité et son contexte à chaque fois pour atteindre un certain niveau de confiance. Aucune exception.

- Ne fournir qu'un accès minimum, également appelé privilège minimal, approprié au niveau de confiance déterminé. L'accès est limité à une ressource spécifique et n'est pas transférable à d'autres ressources.
- Le contexte doit être constamment réévalué en fonction de signaux tels que l'identité de l'employé, l'identité de l'appareil, la politique de sécurité de l'appareil, l'heure de la journée, la géolocalisation, le rôle de l'entreprise et la sensibilité des données. Chaque changement de signal doit déclencher une nouvelle réévaluation. (Netskope appelle cela la *confiance permanente et adaptable*, thème que nous abordons plus en détail au chapitre 4)

Le SASE fournit un cadre pour un programme Zero Trust efficace englobant pleinement les environnements dans lesquels les personnes, les applications et les données sont omniprésentes. Mais, comme nous le verrons plus en détail au chapitre 4, le Zero Trust est un ensemble de principes, et non une architecture technique permettant de mettre en œuvre différentes fonctions de sécurité de manière unifiée.

Le SSE fournit cette architecture technique. Il unifie, intègre et coordonne de nombreux services de sécurité, améliore les fonctionnalités de sécurité et fournit des performances élevées aux employés et pour les besoins de l'entreprise, d'une manière intégrée et personnalisée en fonction du contexte. Pour obtenir les résultats souhaités, le SSE fournit les avantages suivants :

- Contexte détaillé, comprenant l'historique de l'employé, l'appareil, les données demandées, l'application, le réseau et même le motif de la demande.
- Informations sur les ressources auxquelles la personne est autorisée à accéder pour répondre à la demande, que le SSE peut extraire des données concernant les autorisations et les droits.
- Données granulaires qui classifient la sensibilité des différentes ressources de données (pour éviter la perte de données).
- Conseils et ensemble détaillé de politiques décrivant le résultat de sécurité souhaité en fonction de diverses combinaisons de personnes, de données, d'applications et d'autres informations contextuelles.

La difficulté réside dans le fait que de nombreux résultats en matière de sécurité, comme la DLP, la connaissance et la neutralisation des

menaces, nécessitent la collaboration de plusieurs composants de sécurité.


ATTENTION

La mise en œuvre de chaque service indépendamment entraîne la répétition d'une bonne partie des mesures de sécurité dans les consoles de chaque outil. Cette opération est fastidieuse et sujette aux erreurs lorsqu'une vente (ou une vie) est en jeu.

Le SSE élimine cette répétition. Lorsqu'il est correctement mis en œuvre, il combine ces services et leur permet de partager le contexte, les droits, les stratégies de sécurité, les renseignements sur les risques, l'isolement du navigateur, le chiffrement/déchiffrement des données, et plus encore. Cette cohésion permet aux services de sécurité de traiter les transactions en un seul passage afin de fournir rapidement l'accès approprié.

Découvrir comment le SSE rassemble les services de sécurité

Le SSE repose sur l'intégration de nombreux services de sécurité soutenus par de nombreuses fonctionnalités connexes. Il existe une bonne façon de concevoir une plateforme SSE … et de nombreuses autres complètement erronées.


ATTENTION

Alors que le terme SSE gagne en popularité, les communications sur le sujet ne sont pas toujours correctes. Une plateforme SSE mal conçue se reconnaît facilement à son manque d'intégration. Les approches qui se contentent de relier des processus distincts ou de mettre à jour de vieilles chaînes d'appareils sont la preuve de systèmes assemblés à partir de composants séparés, conçus avant l'apparition du cloud et éventuellement acquis auprès de plusieurs fournisseurs. Ce « patchwork » de systèmes introduit une latence significative, ne vous apportera pas les multiples avantages du SSE et ne fait pas partie des étapes significatives de votre parcours vers un SASE global.

Le SSE n'est jamais une séquence de processus individuels où les données sont susceptibles de passer par un moteur DLP, puis un évaluateur de liste de contrôle d'accès, puis une passerelle Web, et ainsi de suite. Néanmoins, il est utile de définir les éléments qui décrivent une plateforme SSE entièrement intégrée.

Analyse en un seul passage et par étapes


RAPPEL

Dans une plateforme SSE idéale, les services de sécurité intégrés fonctionnent en parallèle. Toutes les inspections ont lieu simultanément, en temps réel, que le trafic provienne du Web, du cloud ou de votre datacenter.

En général, un seul passage fournit un filtrage du trafic de plus en plus fin pour sécuriser les données et les applications. Commencez par imaginer que le trafic passe par un entonnoir.

Une plateforme SSE appropriée établit une distinction entre les applications d'entreprise (par exemple Salesforce, Workday), les applications personnelles (comme le compte Gmail d'un utilisateur) et les applications/services tiers (comme les instances de l'entreprise de Microsoft Office 365 ou Dropbox). Elle utilise ces informations pour initier les connexions appropriées nécessaires à la protection de chaque application ou service conformément à la stratégie.

Une plateforme SSE appropriée évalue le contexte, en ajustant l'accès en fonction, par exemple, du fait qu'un médecin (voir chapitre 4) utilise une tablette appartenant à l'hôpital dans la chambre d'un patient, son téléphone sur le réseau Wi-Fi du café ou la console de jeu dans la chambre de son enfant.

Une plateforme SSE appropriée impose des stratégies visant à empêcher la perte ou la fuite de données. Les contrôles peuvent empêcher le téléchargement de documents, la capture d'écran, la saisie de données dans des formulaires Web ou la publication sur les réseaux sociaux.

Une plateforme SSE appropriée offre une surveillance continue. Pendant que l'employé exerce ses occupations courantes, le SSE surveille les anomalies. Lorsque les objets de données sont classifiés, le SSE peut faire la distinction entre le contenu sensible et non sensible, en modifiant dynamiquement les autorisations d'accès et les activités autorisées. Le SSE peut déclencher une alerte, émettre des avis ou interroger l'employé pour obtenir plus d'informations afin de guider son activité en toute sécurité.

Optimisé par des services partagés

Toutes les fonctions de sécurité de haut niveau, y compris la DLP, la sensibilisation et la neutralisation des menaces, la gestion de l'expérience numérique (DEM), et bien d'autres encore, peuvent exploiter l'un ou l'ensemble des services et des techniques que nous décrivons ici pour obtenir les résultats de sécurité souhaités :

- **Contexte partagé :** tous les éléments SSE partagent une énorme quantité de métadonnées qui identifient la personne, l'appareil et l'emplacement. Le site Web, l'application ou le service de destination est identifié(e) et fait l'objet d'une évaluation des risques, et ses activités sont également évaluées. Toutes les données demandées ou créées par le collaborateur et l'application sont prises en compte. Le contexte SSE enrichi comprend une évaluation du comportement

des employés, allant jusqu'à analyser des interactions passées pour analyser l'activité en cours. Ce paysage contextuel constamment mis à jour informe les actions entreprises et les stratégies appliquées par tous les éléments du SSE. (Dans le SSE de Netskope, ce service est appelé Cloud XD.)

- **Confiance permanente et adaptable :** l'accès aux données et aux applications n'est pas une décision simple et binaire. L'accès doit être flexible en fonction de l'évolution des besoins et des contextes. Une plateforme SSE appropriée aligne le degré de confiance sur la valeur des actifs en cours d'accès, guidé par la grande richesse des signaux contextuels disponibles et le degré de tolérance au risque de l'organisation comme défini par la stratégie.
- **Sécurité basée sur des stratégies :** dans le cadre de la sécurité en un seul passage, une plateforme SSE appropriée comprend un cadre stratégique détaillé et partagé qui permet à l'organisation d'établir les limites de sa tolérance au risque et de définir clairement les résultats attendus en matière de sécurité. Cela représente une différence significative par rapport aux milliers de règles exécutées généralement par un pare-feu. Les composants du SSE consultent le référentiel de politiques pour contrôler les activités et les données dans l'ensemble des applications, catégories d'applications et services Web.

Le SSE : principaux avantages

Maintenant que nous avons décrit les composants sous-jacents du SSE, nous pouvons examiner ses fonctionnalités. Certaines seront semblables à celles que votre organisation a déjà déployées sous une autre forme. Il est donc probable que le SSE les remplacera au fil du temps.

RAPPEL

Le SSE vise à permettre aux personnes et à votre entreprise de travailler aussi rapidement que possible et en toute sécurité. En fonctionnant partout, le SSE met fin aux efforts inutiles pour étendre la sécurité dans votre datacenter afin de suivre les données, les applications et les personnes qui ont migré vers le cloud.

Le tableau 3-1 montre les caractéristiques minimums nécessaires pour qu'un produit soit décrit avec justesse comme SSE, selon différents analystes en 2021.

TABLEAU 3-1 **Caractéristiques minimums requises pour les fonctionnalités du SSE**

Fonctionnalité	Objectif	Améliorations apportées par le SSE
SWG	Contrôle l'accès et protège uniquement contre les menaces du Web.	S'attaque également aux menaces et aux risques liés aux données dans le cloud pour les instances personnelles des applications managées, des milliers d'applications informatiques virtuelles et des services cloud.
CASB	Point d'application de la stratégie de sécurité placé entre les consommateurs de services cloud et les fournisseurs de services cloud pour appliquer les stratégies de sécurité de l'entreprise lors de l'accès aux ressources basées sur le cloud. Évalue le comportement et connaît les fonctionnalités des applications SaaS afin de définir un accès approprié pour une personne donnée.	Élimine la duplication des stratégies (entre SWG et CASB), simplifie l'administration (agent unique pour le SWG, le CASB et le ZTNA) et offre une visibilité sur toutes les voies de trafic.
ZTNA	Applique le principe selon lequel personne ne jouit d'une confiance aveugle et n'est autorisé à accéder aux actifs de l'entreprise avant d'avoir été vérifié comme légitime et autorisé. Prend en charge la mise en œuvre de l'accès aux privilèges minimaux, qui accorde sélectivement l'accès uniquement aux ressources dont les personnes ou les groupes de personnes ont besoin, rien de plus.	Booste le ZTNA en lui donnant une capacité d'accès adaptable. Harmonise l'administration des stratégies et les décisions avec les autres composants de la plateforme SSE tout en assurant l'application répartie des stratégies.
Remote Browser Isolation (RBI)	Sépare les appareils des employés de l'acte de navigation sur Internet en hébergeant et en exécutant toute l'activité de navigation dans un conteneur distant basé dans le cloud. Ce « sandboxing » protège les données, les appareils et les réseaux contre toutes sortes de menaces provenant de sites Web malveillants.	Permet au RBI de tirer parti de la classification des données et du contexte des rôles. Ajoute l'isolement à l'éventail des mesures stratégiques du SWG et du CASB.

(suite)

TABLEAU 3-1 *(suite)*

Fonctionnalité	Objectif	Améliorations apportées par le SSE
Pare-feu en mode service (FWaaS)	Sécurité réseau sur tous les ports et protocoles sortants pour un accès sécurisé et direct à Internet via un agent sur les appareils managés ou via GRE et IPsec pour les bureaux. Un seul moteur de stratégie et une seule plateforme de sécurité, offrant une gestion simplifiée pour les employés et les succursales à l'aide d'une seule console.	Permet aux organisations d'agréger le trafic provenant de sources multiples, qu'il s'agisse de datacenters sur site, de succursales, d'employés mobiles ou d'infrastructures cloud. Fournit une application et une imposition cohérentes des stratégies de sécurité sur tous les sites et auprès de tous les employés tout en offrant une visibilité et un contrôle complets sur le réseau sans déployer d'appliances physiques.

Fonctionnalités du SSE : bientôt disponibles pour votre équipe de sécurité

De par son évolution, le SSE intégrera un plus grand nombre de fonctionnalités à mesure que les produits gagnent en maturité et que les projets cloud se multiplient. Une architecture SSE appropriée englobe bien plus de fonctionnalités que celles mentionnées dans la définition de base initiale, par exemple :

- Classification améliorée pour prendre en charge la DLP
- Gestion de la politique de sécurité pour le cloud et le SaaS
- Sensibilisation aux menaces et leur neutralisation
- Gestion des ressources numériques

Nous abordons chacune d'entre elles dans les sections suivantes.

Classification améliorée pour prendre en charge la DLP

DLP est un nom fourre-tout pour une fonctionnalité destinée à empêcher l'exfiltration intentionnelle et accidentelle des données par une mauvaise utilisation intentionnelle ou non intentionnelle. Cette stratégie détecte le mouvement des informations sensibles, empêche leur propagation vers des emplacements indésirables, interrompt les employés avec des fenêtres contextuelles éducatives pour arrêter

l'exposition involontaire, et incorpore le Machine Learning pour évaluer les scores de risque des employés.

CONSEIL

Le SSE améliore la DLP en identifiant et en classifiant activement les données, ce qui permet de suivre et d'appliquer plus précisément les règles relatives au mouvement des données sensibles.

Gestion de la politique de sécurité pour le cloud et le SaaS

La gestion de la politique de sécurité du cloud (CSPM) et la gestion de la politique de sécurité du SaaS (SSPM) révèlent et corrigent les erreurs de configuration entre les clouds (la forme la plus courante de défaillance de la sécurité dans le cloud). En utilisant le contexte fourni par le SSE, les contrôles activés par l'interface de programmation d'application (API) et l'évaluation en temps réel des déploiements de clouds publics, CSPM et SSPM atténuent les risques en analysant la configuration, en suggérant des changements qui réduisent, voire éliminent, la probabilité d'une attaque potentielle et en surveillant la conformité réglementaire.

CONSEIL

Dans le cadre de la mise en œuvre appropriée du SSE, CSPM et SSPM reconnaissent les menaces et prennent activement des mesures pour augmenter la sécurité de l'organisation.

Par exemple, certaines implémentations de CSPM et de SSPM peuvent identifier la non-conformité lorsque la stratégie d'une organisation exige le chiffrement par défaut de toutes les données dans le cloud. Il s'agit d'une position très ferme à adopter, car elle impose des contrôles d'accès qui doivent s'accorder : l'identité d'une personne doit figurer sur la liste de contrôle d'accès pour un objet chiffré et sur la liste associée des clés de chiffrement. Le CSPM et le SSPM reconnaissent quand une personne a accès à l'une, mais pas à l'autre et signalent l'incohérence.

Sensibilisation aux menaces et leur neutralisation

La sensibilisation aux menaces et leur neutralisation permettent de découvrir des preuves d'attaques réussies et de déclencher des alarmes afin de contenir le danger. Les preuves typiques comprennent une activité inhabituelle du réseau, des modifications de la configuration et la suppression des fichiers journaux. L'analyse forensique détermine si une menace active se trouve dans l'environnement. La neutralisation des menaces est un parfait exemple de service qui tire parti des fonctionnalités partagées de l'architecture SSE et y contribue.

Gestion de l'expérience numérique (DEM)

Un aspect émergent et puissant du SSE est sa capacité à évaluer l'expérience des employés et les performances des applications, d'autant plus que les limites du réseau s'étendent désormais au cloud et au-delà. Grâce à la surveillance continue de l'ensemble du trafic, les clients bénéficient d'une visibilité de bout en bout sur le comportement de leur réseau et de leurs applications, ainsi que d'informations exploitables en temps réel basées sur l'activité humaine réelle, afin de garantir que le SSE ne compromet pas les performances. Lorsque des problèmes surviennent dans les appareils, le réseau ou les applications, la DEM peut permettre d'identifier rapidement les causes profondes, accélérer la résolution des tickets d'assistance et fournir des mesures proactives pour éviter que les petits problèmes ne deviennent des événements majeurs ayant un impact sur l'activité.

La gestion réseau doit elle aussi évoluer

Jusqu'à présent, nous nous sommes concentrés sur les fonctionnalités et les capacités de sécurité que le SSE fournit pour un monde axé sur le cloud. Mais la sécurité doit subir une transformation encore plus profonde.

RAPPEL

L'accès au réseau doit être distribué pour permettre aux employés et aux organisations d'extraire toute la valeur des systèmes basés sur le cloud que le SSE protège, comme le montre la figure 3-1.

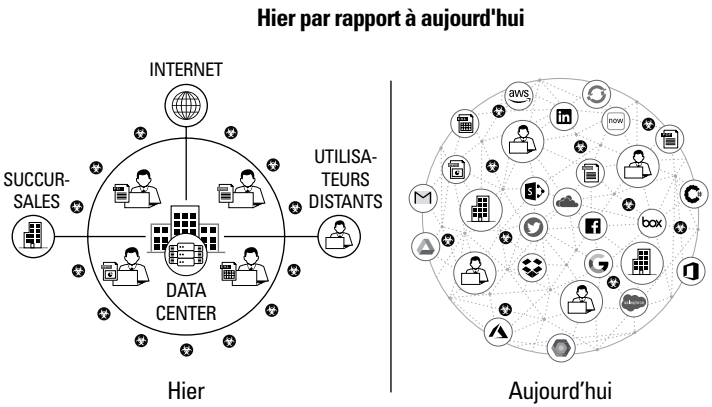

FIGURE 3-1 : L'ancien modèle d'accès était inefficace par rapport au nouveau modèle, qui permet un accès en tout lieu.

Dans l'ancien modèle d'accès, les employés étaient connectés à un réseau protégé par un périmètre bien défini. Les filiales géraient des connexions réseau privées coûteuses au datacenter. Cela est devenu un obstacle au fur et à mesure que les opérations commerciales se sont développées, d'abord sur le Web, puis dans le cloud. La seule option sûre était de détourner le trafic des employés et à travers la pile de sécurité du datacenter avant d'interagir avec le cloud et les ressources Web.

Mais, cette approche est inefficace. Permettre aux employés d'interagir directement avec les ressources cloud améliore considérablement les performances et la productivité, mais compromet la visibilité et le contrôle du datacenter. Persister à utiliser l'ancien modèle en concevant, en gérant et en surveillant des réseaux privés pour accéder à tout ce que le cloud peut offrir est compliqué, coûteux et ne peut tout simplement pas évoluer à une époque où la sécurité doit être une priorité absolue à tous les niveaux de l'entreprise, y compris pour le conseil d'administration.

Le nouveau modèle de réseau envisage une architecture conçue pour le travail à distance, dans laquelle les personnes se connectent de n'importe où et interagissent avec d'autres utilisateurs et informations, principalement dans le cloud. Pour optimiser les performances et l'expérience applicative, le réseau d'un prestataire SSE doit :

- Offrir de nombreuses connexions vers les destinations les plus importantes.
- Être constitué d'un nombre suffisant de points de présence équipés de toutes les ressources informatiques et répartis stratégiquement de manière à ce que les employés ne soient jamais loin.

CONSEIL

Pour obtenir des connexions rapides et sans effort, vous devez collaborer avec un fournisseur dont le réseau est très performant et qui offre de nombreuses connexions directes vers les destinations les plus importantes. Plus votre fournisseur offre de connexions, plus les performances sont élevées, plus la résilience est forte et plus les utilisateurs sont satisfaits.

RAPPEL

Un fournisseur bien connecté offre de meilleures performances, une plus grande résilience et des expériences agréables. L'expérience des employés est importante ! La transformation numérique réussit lorsque la sécurité et la mise en réseau fusionnent en un partenariat cohésif dès le premier jour. Une sécurité qui dégrade les performances du réseau ou qui oblige à faire un compromis dangereux entre sécurité et productivité n'est pas acceptable.

Comme tous les aspects de SASE et du SSE, la transformation du réseau est optimisée au fil du temps. Votre fournisseur de sécurité dans le cloud doit combler le fossé entre votre niveau de sécurité actuel et votre niveau de sécurité futur. Il doit fournir une solution SSE, ouvrir de nouvelles passerelles pour votre personnel remote et s'intégrer harmonieusement à l'infrastructure et aux processus réseau existants.

Le bénéfice du SSE pour la sécurité

En adoptant une architecture SASE basée sur les principes Zero Trust et en s'associant avec un fournisseur SSE capable de fournir des services de sécurité essentiels et distribués, une organisation peut s'attendre à bénéficier d'avantages importants :

- Confiance accrue lors de l'accès aux données et aux applications en dehors du datacenter
- Sécurité flexible basée sur la connaissance des risques, avec des politiques adaptables et un contrôle des activités spécifiques adaptées à chaque application
- Possibilité d'étendre les principes Zero Trust au-delà des applications privées pour couvrir les applications Web et SaaS
- Accès à des services de sécurité supplémentaires, notamment le RBI et la protection avancée contre la perte des données (DLP) en fonction du niveau de risque évalué ou de la confiance
- Surveillance continue des changements de contexte qui déclenchent automatiquement une réévaluation de la confiance et de l'accès
- Réduction de la surface d'attaque en éliminant l'exposition des protocoles et des services à l'Internet public
- Des clouds correctement configurés qui éliminent la forme la plus courante de défaillance de la sécurité dans le cloud.

Tous ces avantages représentent des aspects de l'oasis de sécurité que nous mentionnons au chapitre 1. Le chapitre 4 se penche sur l'avantage commercial d'une solution SSE appropriée et sur les étapes à suivre pour la concrétiser.

DANS CE CHAPITRE

- Instaurer un état de confiance permanente et adaptable à l'aide des principes Zero Trust
- Apprendre les quatre étapes de l'adoption du SSE
- Découvrir les bénéfices économiques du SSE

Chapitre 4
Utiliser le Zero Trust pour donner vie au SASE

Comme nous l'expliquons au chapitre 2, le transfert de la sécurité vers le cloud est important aujourd'hui, car le cloud est désormais un élément fondamental pour les entreprises. L'adoption du cloud est rapide, plus rapide que ne le prévoyaient même les organisations avant-gardistes il y a à peine cinq ans. Les entreprises se tournent vers le cloud pour bénéficier d'un développement rapide, d'un accès à des ressources à la demande, d'une mise à l'échelle élastique et d'une charge administrative beaucoup moins lourde, afin de pouvoir innover et créer de nouveaux produits et services en un temps record.

Les hackers ciblent le cloud parce que c'est là que les entreprises évoluent. Nous devons donc tous nous soucier de la sécurité de nos données, de nos applications et de des activités de nos employés dans le cloud.


ATTENTION

Si le cloud n'est pas protégé, ses avantages restent insaisissables.

Les experts dans l'entreprise doivent d'abord reconnaître que la protection du cloud est importante et ensuite que le SASE, le SSE et le rééquipement du réseau permettront une meilleure gestion des risques et réduiront les conflits en matière de sécurité. Les plans de projet doivent expliquer pourquoi ce changement en vaut la peine, prévoir les avantages économiques spécifiques et indiquer comment mesurer ces avantages en cours de route.

S'appuyant sur nos discussions relatives à la transformation de la sécurité, au SASE et au SSE, ce chapitre décrit la voie à suivre pour créer cette oasis de la sécurité que nous souhaitons tous atteindre : une voie dans laquelle nos données, nos applications et nos collaborateurs sont en sécurité dans le cloud et créent une valeur commerciale substantielle et incontestable. Cette voie passe désormais inexorablement par l'application des principes Zero Trust à l'architecture de notre sécurité.

Du Zero Trust à la confiance continue et adaptable

Une mise en œuvre réussie du SASE et du SSE ne se résume pas à un simple changement de technologie. Comme nous l'expliquons au chapitre 3, le Zero Trust remet en question certaines hypothèses de base sur le fonctionnement de la sécurité. Le modèle sur site, basé sur le réseau, part de l'hypothèse que le réseau est sécurisé et que nous devons vérifier l'identité d'une personne avant de lui accorder l'accès. Le paradigme typique accordait à l'utilisateur l'accès sur la base de tout ou rien : les seuls choix étaient le refus ou le blocage. Le Zero Trust change ce modèle de la façon suivante :

- **Lorsqu'une personne demande un accès, cette demande est évaluée en fonction de plusieurs conditions.** L'identité est l'une d'entre elles, mais le système tient également compte de l'endroit où se trouve la personne, de l'heure de la journée, de l'appareil, du type de connexion réseau et de nombreuses autres variables.
- **L'application à laquelle la personne est connectée fait partie de ce contexte.**
- **Le niveau de service souhaité est un facteur important.** S'agit-il d'une utilisation impérative d'une application ou d'un jeu vidéo pour se divertir ?
- **La façon dont le chemin d'accès réseau est protégé peut changer en fonction de l'application utilisée.** Si quelqu'un accède à son compte de messagerie personnel, une connexion Internet ordinaire est utilisée, avec une protection TLS (Transport Layer Security) négociée entre son serveur de messagerie et son client de messagerie. Si un médecin accède aux dossiers de ses patients, une session sécurisée, chiffrée et authentifiée est établi, quelles que soient les capacités du réseau ou de l'application sous-jacente.

Le niveau de confiance de la session d'une personne est déterminé en fonction de ce contexte. Quelqu'un qui demande l'accès à une application très sensible à un moment inhabituel et à partir d'un endroit

inhabituel (un cas de faible niveau de confiance) se heurtera probablement à un processus d'authentification en plusieurs étapes. L'accès accordé peut être limité à un petit ensemble de données et de fonctions, uniquement en mode lecture seule. Un employé qui accède à l'heure habituelle à partir d'un emplacement sécurisé (une instance avec un niveau de confiance élevé) peut obtenir un accès complet à toutes les données et capacités de l'application.

Prenons cet exemple d'un médecin accédant à des dossiers de santé électroniques, qui illustre les principes Zero Trust à l'œuvre dans le SSE.

> Un médecin transporte une tablette appartenant à l'hôpital alors qu'il traite un patient à l'hôpital. En fonction de l'identité du médecin, de sa localisation, de son appareil et d'autres facteurs, le SSE détermine qu'il est sûr de donner au médecin un accès complet aux dossiers du patient.
>
> Le docteur traverse la rue pour aller prendre un café. Il ouvre un ordinateur portable personnel, se connecte au réseau de la boutique et essaie d'accéder aux dossiers des patients. Le SSE reconnaît le médecin, mais repère que l'hôpital n'est pas propriétaire de l'ordinateur portable et que ce dernier se trouve sur un réseau inconnu. Le médecin est autorisé à consulter et à commenter les dossiers, mais il ne peut pas modifier les données.
>
> Le médecin dîne à la maison. Alerté d'une crise, il déconnecte son enfant de Minecraft pour utiliser le PC familial et accéder au dossier du patient. Le SSE reconnaît que cet ordinateur est moins sécurisé que la tablette de l'hôpital. Au lieu de refuser l'accès, le SSE affiche une série de messages qui permettent au médecin de vérifier davantage son identité et de définir la nature de la raison pour laquelle il a besoin d'un accès. Le SSE fournit alors au médecin un ensemble sécurisé de ressources pour répondre à l'urgence – par exemple, à l'intérieur d'une session de navigateur isolée sous le contrôle du SSE.

Vous connaissez peut-être l'expression « Zero Trust Network Access » (ZTNA). Le ZTNA est un excellent choix pour compléter votre réseau privé virtuel (VPN) afin de répondre à un plus grand nombre de scénarios d'accès à distance. Avec le ZTNA, les employés n'ont pas accès à toute une partie d'un réseau qui permettrait de se connecter à de nombreux services. Au lieu de cela, le ZTNA accorde à l'employé une connexion uniquement à l'application qu'il cherche à utiliser et (comme le montre notre exemple de médecin) seulement l'accès minimum nécessaire pour la tâche à accomplir.

Si nous examinons de plus près ce modèle et son fonctionnement dans sa forme la plus avancée, certaines idées importantes émergent et peuvent guider nos efforts :

- **Contexte :** avant le SASE, la sécurité du réseau était définie via le périmètre, une barrière qu'il fallait franchir pour y accéder. Un certain courant de pensée suggère que l'identité est le nouveau périmètre Zero Trust, car votre identité doit être validée pour obtenir un accès, mais ce concept est insuffisant. Une meilleure approche consiste à évaluer l'ensemble du contexte, y compris l'identité, mais aussi de nombreuses autres variables, pour déterminer le type d'accès à autoriser.
- **Moindre privilège :** le Zero Trust essaie toujours de n'accorder que l'accès minimum nécessaire pour permettre à la personne de faire son travail. La forme la plus avancée du Zero Trust tente également de découvrir en permanence si trop de privilèges ont été accordés et s'efforce de réduire cet excès de confiance du système.
- **Évaluation des risques :** le SSE constitue un historique d'activités lorsque les employés interagissent avec les applications. Il est possible d'analyser cet historique pour créer une représentation de l'activité normale et pour détecter les activités suspectes en temps réel. Cette analyse génère des scores de risque pour un employé, pour une application et pour un site Web. Ces scores fournissent un contexte supplémentaire pour déterminer le type d'accès à accorder.
- **Dissimulation de ressources :** l'accès basé sur le ZTNA n'expose pas les adresses IP publiques auxquelles tout le monde peut se connecter. La connectivité n'est possible qu'après l'évaluation du contexte. Par défaut, tout est caché. (Oui, l'obscurité a un rôle à jouer dans la sécurité, contrairement à ce qui est souvent enseigné dans les cours d'infosec)
- **Confiance permanente et adaptable (probablement la meilleure idée de cette liste) :** la confiance permanente et adaptable est la pratique qui consiste à surveiller une connexion et à ajuster constamment les autorisations en fonction des changements de contexte. Une personne utilisant normalement Salesforce essaie-t-elle d'accéder au système de trésorerie du directeur financier ? Signal d'alarme : réduisez l'accès et l'autorisation, augmentez le score de risque et alertez quelqu'un pour qu'il prenne des mesures. Une autre personne essaie-t-elle d'accéder à un site Web dangereux ? Affichez une fenêtre avec un avertissement avant d'accorder l'accès. L'objectif est de réagir constamment aux changements de contexte pour protéger correctement les données, les applications et les personnes.

RAPPEL

La mise en œuvre du SSE à l'aide des principes Zero Trust réduit la surface d'attaque et est beaucoup plus axée sur les données, ce qui améliore considérablement la politique de sécurité globale. Le niveau de risque présenté par une personne, une application ou un site Web est constamment réévalué. La sécurité s'adapte en temps réel en fonction des changements de contexte.

Maintenant que nous avons bien intégré le principe de confiance permanente et adaptable, nous pouvons nous pencher sur la meilleure manière de mettre en place le SSE.

Quatre étapes simples pour le SSE

Pour la plupart des organisations, la concrétisation du SSE implique de passer d'une sécurité basée sur les locaux, avec le réseau comme périmètre, à une sécurité basée sur le cloud, avec le contexte comme périmètre. Nous allons partir d'un point de départ qui reflète la situation actuelle de la plupart des entreprises : un pare-feu sur site qui comprend des VPN pour l'accès à distance, une appliance de passerelle Web sécurisée (SWG) sur site qui contrôle l'accès Web, et peut-être un abonnement à une passerelle d'accès cloud sécurisée (CASB) autonome qui protège l'utilisation des applications SaaS.

Étape 1 : migrez les employés mobiles pour retrouver de la visibilité

La première chose à faire est d'évaluer ce que font vos employés et de mesurer votre niveau de risque actuel. Le moyen le plus simple d'y parvenir est de commencer par votre groupe de collaborateurs mobiles, car ces employés présentent potentiellement plus de risques. Dirigez leur trafic Web et SaaS via les fonctionnalités SWG et CASB du SSE, configurées au plus près des stratégies existantes. Puis, regardez ce qu'il se passe.

Cet exercice permet d'obtenir une image plus complète de ce que font vos collaborateurs. Les entreprises qui n'utilisent pas déjà un CASB ou un SWG découvriront une quantité énorme (et potentiellement alarmante) d'activités. Celles qui utilisent déjà ces fonctionnalités en apprendront également davantage.

Vous constaterez sans doute que les collaborateurs mobiles accèdent à certaines applications et certains services sans que vous le sachiez. Vous apprendrez où ils travaillent et quels types de réseaux ils ont tendance à utiliser.

Pour conclure la première étape, il s'agit de migrer l'accès aux systèmes internes du datacenter des VPN vers le ZTNA du SSE. Vous améliorerez ainsi l'expérience des collaborateurs et renforcerez la sécurité par la même occasion. Imaginez qu'un plombier vienne chez vous pour réparer une fuite pendant que vous êtes au travail. Il a accès à l'ensemble de votre propriété lors de ses va-et-vient entre son camion et votre salle de bain. Peut-être qu'il laisse la porte d'entrée ouverte. Pendant tout ce temps, vous n'avez aucune idée de ce qui se passe. Le ZTNA, c'est comme s'armer d'un bouton de téléportation magique. Le plombier se présente, vous le téléportez de son camion jusqu'à la fuite et vice-versa, sans arrêt entre les deux. C'est le contrôle d'accès, perfectionné pour l'ère du cloud.

Étape 2 : migrez les collaborateurs au bureau et appliquez la classification des données à l'échelle de l'entreprise

La deuxième étape consiste à placer tous vos collaborateurs sur site sous la protection du SSE afin de contrôler l'accès aux applications et services cloud. Franchir cette étape pour que tous les collaborateurs, qu'ils soient sur site ou mobiles, soient protégés par le SSE transforme votre architecture réseau. Tous les collaborateurs traversent maintenant le point de présence le plus proche du fournisseur SSE, qui achemine ensuite le trafic vers la destination de manière optimale, souvent avec moins de rebonds que l'Internet public. Vous pouvez désormais simplifier le réseau et mettre hors service les réseaux privés coûteux qui ne sont peut-être plus nécessaires. Dans le cadre de cette transition du réseau, un SD-WAN (Software-Defined Wide-Area Networking) peut être introduit pour diriger sélectivement le trafic des filiales.

L'objectif est d'acquérir une compréhension complète des données, applications, sites Web et autres services qui intéressent nos collaborateurs. À ce stade, la capacité du SSE à capturer et à analyser l'activité augmente considérablement la portée et la profondeur du contexte. La politique de sécurité exprimée par vos stratégies SSE dans cette étape doit probablement être similaire à celle déjà présente dans les produits existants que le SSE remplace. Il est important de procéder par étapes d'ajouter de nouvelles fonctionnalités qui peuvent nécessiter une formation supplémentaire qu'une fois l'étape précédente est achevée.

Avec ce nouveau contexte en main, vous pouvez jeter les bases d'une meilleure sécurité en classant les données, les applications et les personnes en fonction du risque et du comportement. Une fois cette classification terminée, le système SSE peut utiliser des données internes et externes pour calculer les scores de risque en temps réel pour les collaborateurs, les applications et les sites Web. Il est maintenant possible de

remplacer une grande partie de l'ancienne infrastructure de sécurité et de passer à l'étape suivante où le SSE passe à un nouveau niveau de sécurité.

Étape 3 : aboutissez à une confiance permanente et adaptable et des services étendus

Jusqu'à présent, l'expérience des collaborateurs n'a pas beaucoup changé. À l'étape 3, l'expérience change considérablement, car la sécurité s'adapte en fonction du contexte.

RAPPEL

La confiance permanente et adaptable évalue le contexte pour équilibrer le risque par rapport à la confiance, en fournissant le type d'accès approprié à tout moment. Elle vous permet de définir des stratégies de sécurité beaucoup plus détaillées. En outre, elle émet plus fréquemment des avertissements ou des suggestions lorsque les utilisateurs sont sur le point de faire quelque chose de dangereux. Les collaborateurs sont ainsi guidés vers des actions approuvées.

Avec le SSE, les professionnels de la sécurité savent quelles données sont sensibles, et quelles applications et quels sites Web sont risqués. Une fois combiné avec des capacités comme la DLP, cela permet au personnel de sécurité de contrôler de façon précise les opérations des utilisateurs, et ce, à un niveau sans précédent dans le domaine de la sécurité. Au lieu d'une simple décision de blocage ou d'autorisation, l'accès se situe quelque part dans un continuum.

La confiance permanente et adaptable vous permet également d'ajouter d'autres services. Par exemple, imaginons qu'un médecin souhaite visiter un site Web considéré comme risqué. Après avoir reçu un avertissement, ce médecin souhaite tout de même le visiter. Le SSE peut alors transférer le médecin dans une session de Remote Browser Isolation (RBI), un navigateur qui fonctionne sur une machine virtuelle chez le fournisseur de SSE, ce qui réduit encore le risque. D'autres services avancés peuvent être ajoutés selon les besoins.

Étape 4 : gérez les risques de manière proactive grâce à l'analyse et la classification dynamiques

À l'étape 4, l'équipe chargée du SSE peut commencer le processus de détection proactive des risques et de leur élimination de l'environnement. Une méthode pour mesurer les progrès réalisés qui consiste à suivre les scores de risque des collaborateurs, des applications et des sites Web. L'objectif est de montrer une réduction de la fréquentation

des sites à risque et de la fréquence des actions à risque. Une autre méthode consiste à réduire les droits en suivant les habitudes d'utilisation et en éliminant les privilèges excessifs.

À ce stade, certains des contrôles de sécurité de niveau supérieur, comme la DLP et la neutralisation des menaces peuvent devenir primordiaux, augmentant les capacités CASB, SWG, ZTNA et pare-feu en mode service (FWaaS). Dans le SSE, ces contrôles fonctionnent mieux que dans leurs versions séparées sur site et offrent beaucoup plus de fonctionnalités. Par exemple, les modules de reconnaissance basés sur le Machine Learning permettent à la DLP d'identifier et de réagir aux documents sensibles en temps réel.

CONSEIL

La gestion de l'expérience numérique (DEM), la gestion de la politique de sécurité du cloud (CSPM) et la gestion de la politique de sécurité du SaaS (SSPM) améliorent davantage la gestion des risques. Elles ajoutent des méthodes avancées pour une disponibilité et des performances constantes permettant de détecter puis corriger les erreurs de configuration. Le SSE intégrera encore plus de ces services avancés à l'avenir.

RAPPEL

C'est votre situation unique qui dicte les détails des étapes à suivre. Mais d'un point de vue général, les étapes expliquent le processus que la plupart des entreprises suivront pour mettre pleinement en œuvre le SSE.

Transformer le réseau et le reste de la sécurité

CONSEIL

La mise en œuvre du SSE est un pas en avant important et non négociable pour le SASE. Mais pour atteindre l'oasis de sécurité que nous visons, le reste du paysage de la sécurité, au-delà du SASE, doit également évoluer pour que tous les éléments importants fonctionnent ensemble. La plupart des entreprises passent à un modèle de travail à distance dans lequel les avantages de la sécurité en tout lieu et à tout moment sont évidents. Cela permet de s'éloigner naturellement de la connectivité basée sur les VPN et les réseaux privés et de bénéficier de la simplicité et des avantages en termes de coûts du SSE.

Le point le plus important à garder à l'esprit est la façon dont, en adoptant le SSE (et le SASE), l'infrastructure technologique globale devient plus simple. Dans l'ancien modèle, les contrôles de sécurité destinés à empêcher les accès non autorisés étaient placés sur le réseau de l'entreprise parce que ce réseau était le seul chemin vers les données. Dans le nouveau modèle, les différents points de présence du fournisseur SSE deviennent les voies d'accès aux données, offrant non seulement un contrôle d'accès, mais aussi un contrôle complet du trafic. Le réseau

sous-jacent peut alors concentrer sa mission globale pour déplacer les bits rapidement et efficacement.

Les systèmes de gestion des identités et des accès (IAM) ont pour mission importante d'authentifier les collaborateurs. Nombre de ces systèmes sont déjà hautement configurables grâce à des interfaces de programmation d'applications (API). Ils sont également conçus pour s'intégrer à d'autres systèmes, une fonctionnalité nécessaire à toute implémentation du SSE. Les améliorations de la technologie IAM offrent encore plus de contexte, de surveillance et de fonctionnalités d'authentification avancées dont peuvent bénéficier le SASE et le SSE. Le SSE tire encore plus de bénéfices des plateformes de protection des terminaux (EPP). Celles-ci collectent des signaux importants (générant ainsi davantage de contexte), assurent une surveillance détaillée et incluent des mécanismes de contrôle du comportement et de la configuration de la sécurité. Synchronisez votre plan de mise en œuvre SSE avec une évolution EPP correspondante afin de tirer le meilleur parti de vos investissements en matière de sécurité.

Le SASE et le SSE accéléreront le changement de rôle du datacenter. Après la montée en puissance du cloud, le datacenter a perdu sa position de point central des activités liées à la sécurité. Le SSE fait sortir la sécurité du datacenter pour l'amener dans le cloud.

RAPPEL

Les datacenters continueront à jouer un rôle important dans la plupart des entreprises pour diverses bonnes raisons, notamment la pression des coûts, les exigences réglementaires, la gestion des risques et l'utilité de certains types d'infrastructures informatiques. Le datacenter sera désormais l'un des nombreux sites où des applications importantes sont hébergées et protégées par le SSE.

Avantages commerciaux du SSE

Le cyber risque est une priorité pour la plupart des conseils d'administration, mais comme nous l'expliquons clairement au chapitre 2, la sécurité n'est pas une fin en soi. Elle a pour mission de protéger la valeur commerciale créée par les systèmes qui soutiennent l'entreprise. Les entreprises ont migré vers le cloud parce que cela est logique pour elles. La mission d'une architecture SASE, y compris le SSE, est de protéger les applications, les données et les utilisateurs. Voici comment cela se traduit en valeur commerciale :

- **La sécurité ne fait plus obstacle à la productivité des entreprises.** L'agilité de l'entreprise peut être maintenue et les équipes de sécurité n'ont plus à jouer le rôle d'arbitre, car les opérations que

l'entreprise veut faire peuvent maintenant être correctement sécurisées. Les frictions liées à la sécurité sont réduites de façon spectaculaire. Les processus de développement et de maintenance des produits sont rationalisés, car la sécurité est plus facilement intégrée. Un SSE basé sur le cloud est parfaitement adapté à la sécurisation d'un environnement multi-clouds.

- **Le conseil d'administration a désormais beaucoup plus confiance dans le fait que les types de contrôle requis pour utiliser les ressources cloud en toute sécurité sont correctement examinés et gérés.** Le processus de gestion des risques liés aux utilisateurs, aux données et aux applications devient beaucoup plus sophistiqué, tout comme les mécanismes utilisés pour atténuer les risques. Avec le SSE, les risques peuvent être identifiés de manière proactive et systématiquement supprimés d'une entreprise. La sécurité au sens propre suit les données, ce qui rassure le conseil d'administration quant à la protection des actifs les plus importants.
- **L'équipe de sécurité devient beaucoup plus unifiée et axée sur l'activité.** Au lieu d'avoir une personne chargée du SWG, une seconde chargée du CASB et une troisième chargée du pare-feu, vous avez une équipe qui se concentre sur la situation dans son ensemble et qui dispose de plus d'informations pour être proactive.

RAPPEL

Concrétiser le SSE, c'est créer un monde doté d'une meilleure sécurité, et toutes les personnes impliquées dans l'entreprise en tireront un avantage.

Chapitre 5
Dix choses à faire ou à ne pas faire pour implémenter le SSE

Une grande partie du parcours vers un cloud sécurisé et agile consiste à reconnaître que votre organisation informatique actuelle n'a pas été conçue pour une telle destination. Il est naturel que l'organisation informatique reflète l'architecture technologique. Ainsi, si des personnes ou des équipes distinctes s'occupent de vos passerelles d'accès cloud sécurisées (CASB), de vos passerelles Web sécurisées (SWG), de vos réseaux privés virtuels (VPN) et de vos pare-feux, avec ou dans le cadre d'une équipe d'un centre d'opérations de sécurité (SOC) et d'une équipe de centre d'opérations réseau (NOC), vous serez confrontés à des réticences lorsque vous direz : « Hé, mettons maintenant en œuvre une nouvelle architecture intégrée SASE (Secure Access Service Edge) et SSE (Security Service Edge) qui converge également la sécurité et la gestion de réseau en une puissante brigade. » La résistance au changement est naturelle, elle est due en partie à la peur de perdre le contrôle d'un domaine que les personnes ont fini par maîtriser après des années de travail.

Le SASE et le SSE offrent des avantages tactiques qui améliorent la qualité de la sécurité et élargissent la portée des services de sécurité et des avantages stratégiques qui peuvent accélérer l'activité. Les sections suivantes fournissent un guide pour réussir l'adoption du SASE et du SSE. Tout d'abord, nous présentons quatre principes pour accélérer votre parcours. Ensuite, nous suggérons quatre erreurs à éviter.

Mettre les données au centre des préoccupations

Avec le SSE, la sécurité suit les données où qu'elles aillent. Ainsi, peu importe si vous créez des données dans Google Workspace et Microsoft 365, dans une application SaaS (Software-as-a-Service) ou sur le stockage d'objets cloud. Le SSE est toujours là pour protéger ces données.

Étant donné que le SSE devient un point de contrôle principal qui peut également faciliter la classification des données, il est important de déterminer le but et l'emplacement de toutes vos données. Utilisez ces connaissances pour donner la priorité à la protection et à la bonne utilisation des données sensibles, où qu'elles se trouvent, pour avoir la certitude d'avoir fait le travail le plus important en premier.

Adopter l'intégration

À chaque étape du cycle de réponse aux incidents, la création de compétences en matière d'automatisation et d'intégration est importante afin que vous puissiez faire converger vos composants de sécurité en une machine correctement optimisée. Le processus consiste à extraire des informations de plusieurs systèmes, à intégrer ces informations pour analyser ce qui se passe, à constituer la bonne équipe et à prendre des mesures automatisées lorsque cela est possible.

Le SSE intègre les services de sécurité cruciaux pour protéger le cloud, mais il fait partie d'un écosystème plus vaste de services de sécurité importants. Les systèmes de gestion des identités et des accès (IAM), les plateformes de protection des terminaux (EPP) et les outils de gestion des informations et des événements de sécurité (SIEM) sont quelques-uns des composants clés qui coopèrent avec les fonctions spécifiques au SSE pour fournir une sécurité complète, un diagnostic rapide et une réponse aux problèmes.

Rappelez-vous que les méchants sont aussi dans le cloud

Le SSE et le SASE représentent un grand bond en avant dans la portée et la qualité de la sécurité. Il est normal de se sentir satisfait une fois que les principes fondamentaux ont fonctionné. Mais rappelez-vous, les hackers utilisent le cloud pour augmenter leur force de frappe. Selon le rapport Cloud and Threat Report de Netskope (`www.netskope.com/blog/july-2021-netskope-cloud-and-threat-report`), le pourcen-

tage de malwares transmis via des applications cloud est passé de 50 % au deuxième trimestre 2020 à un niveau record de 68 % au deuxième trimestre 2021. Le SSE vous donne une longueur d'avance sur ces criminels, mais vous devez constamment apprendre et vous adapter pour garder une longueur d'avance.

Reconnaître que la sécurité est une composante essentielle de la stratégie commerciale

La sécurité doit dès le début faire partie de la discussion sur la stratégie commerciale. S'enthousiasmer pour les applications et le cloud n'a aucun sens si ces applications et les personnes qui travaillent avec ne peuvent pas être sécurisées. La bonne nouvelle, c'est que le SSE aidera les équipes de sécurité à devenir plus facilement un catalyseur pour les entreprises. Si l'équipe de sécurité comprend les objectifs de l'entreprise et leurs ramifications en matière de sécurité, elle peut dire « oui » plus souvent, car elle a plus de pouvoir pour protéger tout ce que l'entreprise veut faire.

CONSEIL

Pour que l'adoption du SASE et du SSE soit réussie, les promoteurs du programme doivent expliquer que les avantages de la sécurisation du cloud sont importants au niveau de la stratégie globale, à savoir le message que nous avons investi dans le cloud pour transformer notre activité et obtenir de meilleurs résultats. Maintenant, nous devons protéger cet investissement. L'enthousiasme à l'idée d'atteindre et de protéger ces résultats sera la meilleure motivation pour adopter avec élan le SASE et le SSE.

Ne pas penser aux silos

Le SASE et le SSE résolvent les problèmes épineux qui ont tendance à accompagner les projets de cloud. Évitez les tentatives de mise en œuvre CASB, SWG et ZTNA sous forme de projets indépendants, qui ajoutent encore des fournisseurs spécifiques promettant monts et merveilles. L'objectif est de protéger le cloud avec une plateforme intégrée tenant compte du contexte. Une certaine résistance au changement que le SASE et le SSE entraînent se fera ressentir.

ATTENTION

Une énorme erreur consiste à ralentir le processus en abordant le problème à partir des silos informatiques traditionnels. Ces « cylindres d'excellence » perpétuent les anciennes façons de penser dans le nouveau monde. La sécurité ne doit plus être considérée comme une simple question de réseau. N'ayez pas de conversation sur le réseau à propos

d'un problème de sécurité. Le SSE est maintenant devenu le point critique de visibilité et de contrôle de la sécurité dans le cadre d'une architecture SASE pleinement fonctionnelle.

Ne pas reporter les anciennes règles

Les équipes ont souvent peur de leurs pare-feux parce qu'ils ont accumulé des couches de règles créées par des personnes qui ont quitté l'entreprise il y a longtemps. Il en va de même pour d'autres technologies de sécurité qui nécessitent des règles et des paramètres de configuration complexes pour obtenir les résultats souhaités. Le SSE est différent. Si les règles et la configuration existent toujours, une grande partie du travail est accomplie en définissant des stratégies qui décrivent les résultats souhaités. Lorsqu'il est mis en œuvre efficacement, le SSE gère lui-même les détails des interactions entre les règles. Ne vous inquiétez donc pas de la configuration de votre ancienne technologie. Concentrez-vous plutôt sur les résultats que vous souhaitez obtenir en matière de sécurité et utilisez le SSE pour y parvenir.

La plupart des produits offrent également la gestion de la politique de sécurité du cloud et la gestion de la politique de sécurité du SaaS pour vous aider à bien faire les choses et à les maintenir.

Ne pas détester le datacenter

Maintenant que vous adoptez le SASE et le SSE, il est facile de penser que le datacenter traditionnel n'est pas important. Nous aurons toujours des datacenters sous une forme ou une autre. Après tout, le cloud n'est rien d'autre qu'une collection de datacenters auxquels on accède par le biais d'interfaces de programmation d'applications (API). La nouvelle vocation du datacenter est d'accueillir les charges de travail et les applications informatiques importantes. Le datacenter ne joue plus le rôle principal dans l'infrastructure de sécurité, mais il joue toujours un rôle de soutien important.

Ne pas avoir peur du changement

Ne laissez pas la peur du SASE et du SSE vous ralentir. Oui, il y a un changement d'architecture et de nouveaux produits à maîtriser, une tâche difficile car les produits interagissent avec tout le monde dans l'entreprise. Une mise en œuvre du SSE vous en apprendra davantage sur vos collaborateurs, vos données, vos applications, vos sites et applications tiers. Ces connaissances ouvriront donc la porte à une plus grande automatisation pour trouver les erreurs et mettre en œuvre des réponses efficaces. Par rapport à votre politique de sécurité actuelle, vivre dans le nouveau monde reviendra à vivre au bord d'une oasis.

Le SSE est la pile de sécurité qui déterminera la réussite d'une architecture SASE. Ce livre vous montre comment réaliser les promesses du SSE aujourd'hui.

L'aventure SASE nécessite des partenaires fiables disposant de plateformes véritablement intégrées. Ce livre est votre guide pratique pour le SSE et le SASE. Il explique notamment pourquoi ces deux concepts sont si fondamentaux pour créer les architectures de sécurité et de réseau du futur, centrées sur le cloud, et comment investir et concevoir aujourd'hui votre SSE (Security Service Edge).

À l'intérieur…

- Définition du SASE et du SSE
- Découvrez le rôle essentiel du Zero Trust
- Protégez les données stratégiques de l'entreprise dans le cloud
- Dynamisez vos employés travaillant remote
- Évitez les pièges de conception du SSE et du SASE

netskope

Les dirigeants de Netskope, **Jason Clark** (CSO et CMO) et **Steve Riley** (Field CTO), sont des autorités largement reconnues dans le domaine de la technologie du cloud, de la cybersécurité et des réseaux. À eux deux, ils combinent des décennies d'expérience au sein d'organisations internationales comme Gartner, Optiv, Riverbed et Websense.

Allez sur Dummies.com®
pour voir des vidéos, des tutoriels, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-119-89667-8

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.