LES 7 PIÈGES À ÉVITER LORS DE LA SÉLECTION D'UNE SOLUTION SSE

Construire le security service edge (SSE) sur un modèle Zero Trust

Par :

Sanjit Ganguli
VP Stratégie de Transformation / Field CTO Zscaler

Nathan Howe
VP Technologie émergente et 5G Zscaler

Sponsorisé par :

zscaler™

Les 7 pièges à éviter lors de la sélection d'une solution SSE

Table des matières

SSE : de quoi s'agit-il et pourquoi devrais-je m'en préoccuper ?

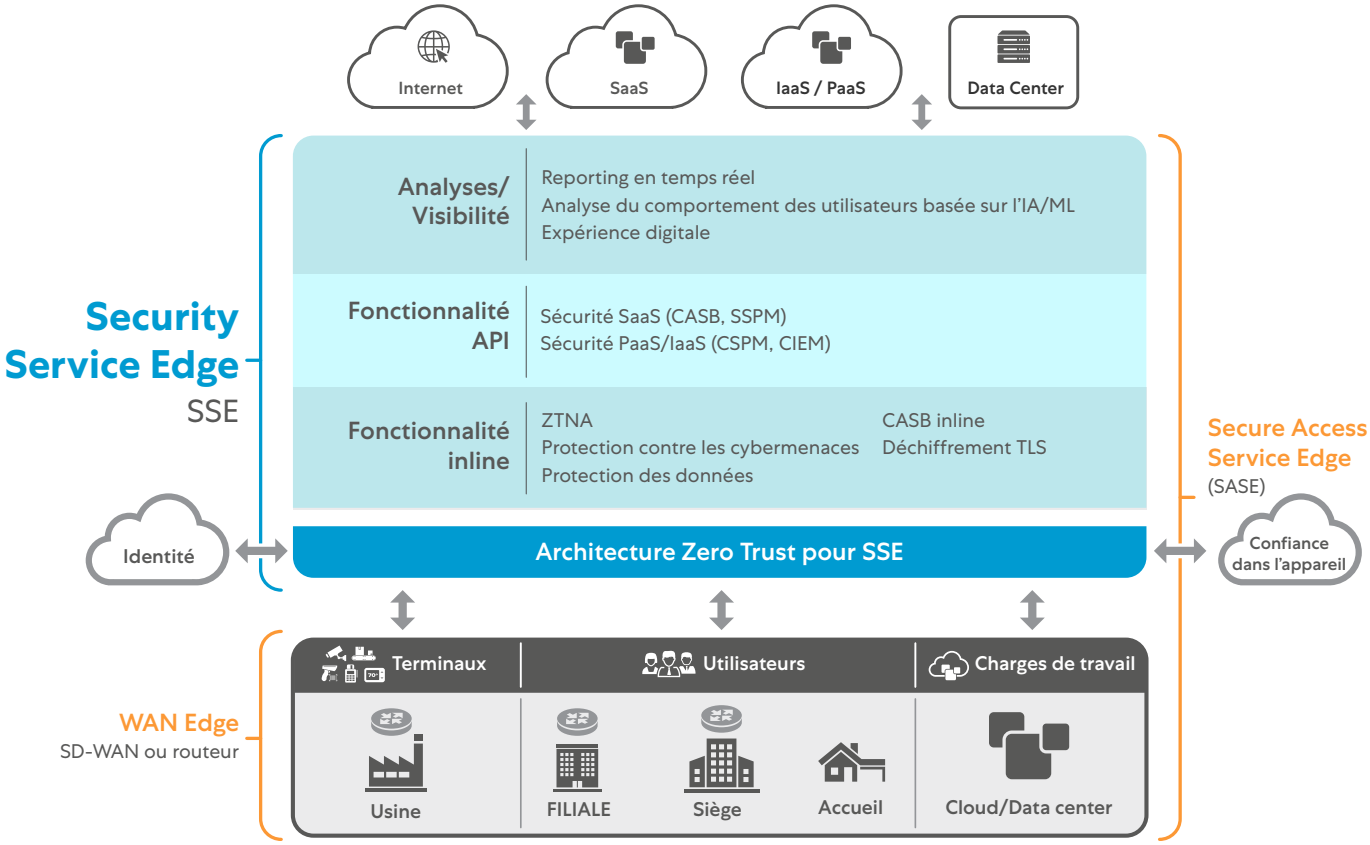

Figure 1 : Le cadre SASE (Secure Access Service Edge) inclut le SSE pour la prise de décision et l'application des politiques. Le SASE requiert l'utilisation de solutions de connectivité dédiées entre l'entité requérante et la périphérie sécurisée (ou security edge) où la politique est appliquée.

Le Security Service Edge (SSE) est l'appellation de Gartner pour la prise de décision et l'application de politiques en tant que composants du cadre Secure Access Service Edge (SASE). Le SSE promet une sécurité et une connectivité regroupées, simplifiées et fournies par le cloud.

La simplicité architecturale est toujours un avantage pour une entreprise, surtout lorsque cette simplicité minimise la dette technique et favorise l'activité commerciale. Cependant, de nombreuses entreprises considèrent la sécurité comme un handicap, un obstacle qui crée des congestions, une barrière qui limite l'agilité ou une entrave à la réussite de l'entreprise. Le SSE va à l'encontre de ces stéréotypes. Dans un environnement SSE, la sécurité assure protection et contrôle tout en étant un facteur de progrès pour l'entreprise.

Un peu de contexte : présenté en 2019, le cadre SASE vise à guider les entreprises dans leur parcours digital, un parcours principalement motivé par l'adoption du cloud et de la mobilité. SASE fait converger l'accès au réseau et la sécurité, et sert les deux à partir de la périphérie du cloud (hautement distribuée) **(voir la figure 1)**. Le SASE garantit ainsi que la sécurité n'est plus centralisée et que des connexions sécurisées peuvent être établies vers et depuis n'importe quel emplacement.

Pensez à la façon dont un téléphone mobile se connecte à divers réseaux cellulaires et sans fil. Il n'existe pas de solution de routage réseau dédiée, mais l'utilisateur a besoin de contrôles de sécurité pour le trafic entre la source et la destination. De même, la périphérie, le réseau ou l'emplacement auquel l'utilisateur se connecte ne devrait pas être important pour la protection du trafic d'entreprise. C'est ce qu'apporte le SSE.

Les sociétés de cybersécurité ont rapidement pris le train du SASE en marche. Certains spécialistes du marketing se sont cyniquement appropriés le terme à des fins d'image de marque, en laissant entendre que l'« accès » au SASE les rendait conformes au SASE (ou les concurrents non conformes) : « J'ai une fonction réseau, donc je suis SASE ; vous ne construisez pas de routes réseau, donc vous n'êtes pas SASE ».

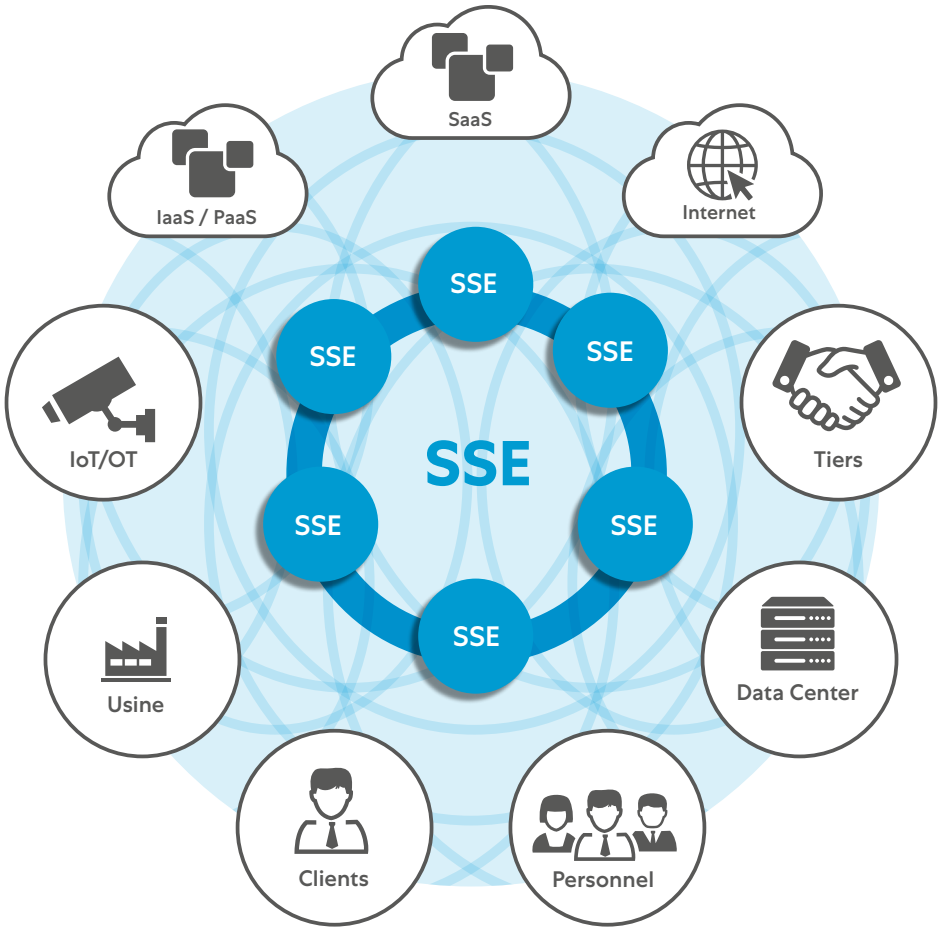

Figure 2 : Fournir un accès d'entité à entité validé et basé sur des politiques à la périphérie pour un monde axé sur le mobile et le cloud. Le SSE vous permet d'apporter la sécurité à l'utilisateur à la périphérie, sans compromis sur les performances, tout en supprimant tous vos pare-feu et VPN.

SSE fait référence à la suite de services SASE utilisés pour protéger le trafic de l'entreprise. Le SSE garantit que le bon utilisateur (ou charge de travail) bénéficie d'un accès aux applications et services appropriés, en toute sécurité et sous le contrôle du service informatique de l'entreprise. Ces services peuvent être des charges de travail dans un IaaS ou PaaS, des applications SaaS ou des services Internet comme LinkedIn ou YouTube. L'accès aux services doit être accordé conformément aux contrôles Zero Trust Access (ZTA), décrits de manière beaucoup plus détaillée dans le **deuxième piège à éviter**.

Pour répondre à ces objectifs ambitieux, un fournisseur de solutions SSE doit proposer une solution mondiale, hautement disponible, évolutive et indépendante du réseau, qui fournit une politique cohérente, un accès Zero Trust et une expérience digitale rapide.

Sans cette fonctionnalité et cette disponibilité, les solutions SSE ne peuvent pas assurer une protection et une disponibilité universelles **(voir figure 2).** Contrairement au SASE, le SSE ne prescrit aucune méthode de connexion ou d'accès. Le SSE est censé fonctionner sur n'importe quel réseau et fournir des contrôles à tout service autorisé, où qu'il se trouve.

L'idéal du SASE est de fusionner connectivité et protection, mais dans un contexte d'entreprise. Cette association ne fonctionnera que si elle est transparente pour les employés utilisateurs finaux. La connectivité est directe, que ce soit d'un utilisateur à une application, d'une application à une autre, d'une charge de travail à une autre, d'un service à un autre. Les utilisateurs ne doivent jamais se dire : « Ah, je dois me connecter au réseau avant de pouvoir travailler ». Au contraire, ils devraient se dire : « Je vais pouvoir travailler sans attendre ».

Cet idéal intégré ne peut tout simplement pas être concrétisé dans des environnements d'entreprise dépendant d'une infrastructure réseau et de sécurité traditionnelle. Dans cet ancien modèle d'architecture, la sécurité est centralisée et le trafic de données doit d'abord être connecté et acheminé via le réseau d'entreprise vers (et à travers) l'emplacement physique des contrôles de sécurité matériels basés sur les appliances, quel que soit l'emplacement (par exemple, distant ou filiale), quelle que soit la source (par exemple, utilisateur, application ou charge de travail) et quelle que soit la destination (par exemple, Internet, cloud, data center).

La véritable valeur économique de la transformation digitale induite par le SSE

L'adoption du SSE peut exiger une transformation digitale considérable de l'entreprise. Mais adhérer à ce changement peut avoir un impact tangible :

Contrôle :

Le SSE se construit de zéro. Le SSE valide chaque personne, machine, charge de travail, réseau et périphérie. Sans une identification correcte, associée à un contexte fourni par l'analyse comportementale, aucun accès n'est accordé, ce qui permet à l'entreprise d'avoir le contrôle total sur qui ou quoi accède aux services au sein de l'entreprise.

Connectivité directe :

L'application des politiques SSE se fait en ligne entre l'entité d'origine et le service de destination. Les décisions d'accès sont prises au niveau de chaque application, et non au niveau du réseau.

Sécurité axée sur les entreprises :

Les politiques déterminant quelles entités peuvent se connecter à quels services sont définies sur la base du principe du moindre privilège. Les utilisateurs, les machines, les charges de travail, etc., ne peuvent se connecter qu'à ce à quoi ils sont autorisés à se connecter, et rien de plus. Aucune autre connectivité n'est disponible, et tout autre accès est bloqué.

Exécution globale :

Le SSE doit être doté d'une exécution globale afin que toute entité puisse faire appliquer des contrôles sur le chemin d'accès en fonction du contexte fourni par la politique, les moteurs d'analyse et les connaissances externes (surveillance des menaces, tromperie, etc.). Cette exécution globale doit être adaptée aux besoins de votre entreprise.

Complet :

Le SSE fournit une évaluation complète et in-line pour inspecter le trafic à grande échelle et en profondeur. Le SSE fournit une protection contre les menaces avancées, défend les ressources de l'entreprise (cloud et au-delà), empêche la perte de données et assure un contrôle in-line. Le cas échéant, la solution doit permettre de contrôler le contenu stocké dans les services cloud.

Invisible :

Le SSE empêche tout accès indésirable et l'exposition des ressources de l'entreprise en supprimant la surface d'attaque. Il n'est pas possible d'attaquer ce qui n'est pas accessible.

De n'importe où :

Le SSE apporte cette connectivité à toutes les composantes de l'entreprise, où qu'elles se trouvent. Le SSE protège et connecte une base d'utilisateurs flexible tout en garantissant que les charges de travail, les objets et les machines puissent être déplacés, relocalisés et transformés sans perdre le contrôle.

Le SSE peut être un catalyseur de changement dans une entreprise, simplement en sécurisant l'entreprise de manière remarquablement complète. Mais toutes les solutions ne sont pas créées égales. Les responsables informatiques désireux d'adopter le SSE doivent évaluer et sélectionner la bonne solution, celle qui permet à leur entreprise de simplifier la sécurité.

Il existe sept pièges à éviter sur le chemin de la transformation digitale de l'entreprise vers le SSE. En évitant ces écueils, les responsables informatiques pourront choisir le bon ensemble de services, d'architecture et de fonctions pour concrétiser la proposition de valeur que du SSE. Ce parcours doit permettre de rompre avec les « anciennes méthodes de travail », telles que l'ancrage aux réseaux ou l'autorisation d'un accès généralisé aux services, qui limitent la capacité de transformation et de réponse aux besoins des entreprises.

Piège n° 1 :
Choisir une solution SSE qui n'a pas fait ses preuves en termes de performance et de disponibilité sur une plateforme cloud mondiale évolutive

Piège n° 2 :
Choisir une solution SSE qui ne repose pas sur une architecture Zero Trust

Piège n° 3 :
Choisir une solution SSE qui promet une protection contre les menaces avancées et une DLP avancée, mais qui ne peut pas inspecter le trafic chiffré à grande échelle

Piège n° 4 :
Choisir une solution SSE universelle qui ne prend pas en charge des solutions de déploiement et de gestion flexibles, évolutives et variées

Piège n° 5 :
Choisir une solution SSE qui apporte une expérience utilisateur (UX) médiocre en n'optimisant pas la connectivité des applications ou en ne diagnostiquant pas les dégradations de l'UX

Piège n° 6 :
Choisir une solution SSE dont l'intégration et l'orchestration avec un écosystème de fournisseurs tiers sont limitées

Piège n° 7 :
Choisir une solution SSE qui ne peut pas facilement démontrer sa valeur dans un environnement de production pilote

À qui s'adresse ce document ?

Passer au SSE n'est pas seulement une question de transformation de la sécurité et ne concerne pas seulement les **architectes de la sécurité**. Les bonnes pratiques décrites dans cet e-book s'adressent aux **architectes de la sécurité**, **aux architectes réseau**, **aux architectes d'entreprise**, **aux architectes du cloud** et **aux architectes d'application**.

#1 Piège

Choisir une solution SSE qui n'a pas fait ses preuves en termes de performance et de disponibilité sur une plateforme cloud mondiale évolutive.

Envisagez plutôt les solutions SSE qui présentent les avantages suivants :

- Offrent un ensemble diversifié et mondial d'application des politiques au niveau des services publics avec des performances, une disponibilité, un débit et une fonction garantis par des accords de niveau de service (SLA). La solution applique des politiques localement sur les sites des clients.
- Sont créées dans le cloud avec la meilleure résilience, infrastructure, diversité géographique, capacités fonctionnelles de leur catégorie et une expérience utilisateur optimale. Fournissent des services SSE in-line dans des data centers indépendants des opérateurs, et non comme un service exécuté par-dessus un cloud de destination géré ou un fournisseur de data center.
- Présentent des antécédents éprouvés et transparents en termes d'évolutivité, de croissance et de livraison, confirmés par des références clients, des rapports historiques, des certifications tierces et des référentiels de données open source externes (https://www.peeringdb.com/org/12297).

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Construire et exécuter une plateforme SSE multi-entités pour des milliards de transactions est bien plus que du simple calcul et n'est pas une chose aisée. **La solution SSE sera chargée de la protection, de la connectivité et de la capacité de votre entreprise**. Elle doit donc fournir l'ensemble des services de SSE de manière uniforme et opportune à toutes les parties prenantes de l'entreprise.

La bonne solution SSE fournira des services à votre entreprise par le biais d'un service distribué à l'échelle mondiale. D'un point de vue architectural, le mode de fourniture le plus efficace est un service basé sur un proxy. Non lié à l'état du réseau, un service proxy se concentre sur la mise en place du SSE au niveau de l'accès à l'application, ce qui permet une meilleure compréhension sans nécessiter le déchargement sur des plateformes supplémentaires pour des informations telles que l'inspection à grande échelle **(voir le piège n° 3)**.

Il convient de souligner qu'une véritable architecture proxy nécessite des efforts considérables en matière de recherche et de développement, ainsi que de nombreuses années de perfectionnement pour répondre aux exigences d'évolutivité de l'entreprise moderne. La bonne solution SSE disposera d'un grand nombre d'exemples de déploiements importants où l'architecture proxy a démontré sa capacité à évoluer.

Ce service doit être fourni par le biais d'un ensemble uniforme de politiques appliquées à la périphérie où toutes les fonctions de transmission de données de votre entreprise sont protégées ; il ne doit pas s'agir uniquement du nombre de nœuds, mais plutôt du nombre de sites garantis par des accords de niveau de service qui offrent les services requis par le client. Le fournisseur de SSE ne doit pas fournir de PoP public s'il ne peut pas garantir l'accord de niveau de service dans cette région en raison d'un mauvais peering ou pour d'autres raisons.

Adopter le SSE implique que vous allez regrouper, dynamiser et partager la responsabilité de la sécurité, de la connectivité et du contrôle de votre entreprise avec un fournisseur de sécurité de confiance. Ce modèle partagé simplifiera les moyens par lesquels vous assurez la protection et la connectivité de vos utilisateurs, charges de travail, services et filiales, entre autres. Le fournisseur de SSE doit respecter un ensemble d'accords de niveau de service définis et éprouvés pour garantir le fonctionnement de votre entreprise, tout en assurant sa protection.

Lorsque votre service d'entreprise se connecte, il a besoin d'un chemin efficace pour exploiter la fonction de destination. Cela ne peut se faire que par le biais d'une solution SSE dotée d'un peering très efficace au sein de data centers indépendants des opérateurs. C'est pourquoi les contrôles doivent être appliqués en ligne, entre la source et la destination, indépendamment de l'emplacement de la source et/ou de la destination.

Les solutions qui hébergent le service de sécurité dans des clouds centraux, souvent au sein d'hyperscaleurs, et qui disposent de passerelles d'entrée, comme le montre la Figure 3 (souvent appelées services on-ramp), s'appuient sur des périphéries d'entrée distribués, mais traitent le contrôle des politiques et l'application de manière centralisée, ce qui introduit une latence indésirable et se traduit par une piètre expérience utilisateur.

Les fournisseurs de SSE doivent disposer d'une plateforme cloud complète, étendue et évolutive. Au-delà des accords de niveau de service, la plateforme SSE doit également apporter des preuves d'évolutivité, de stabilité, de disponibilité, de déploiement géographique, etc. Pour valider cet aspect, consultez les données historiques fournies publiquement et discutez avec des clients existants pour comprendre leurs expériences.

Application uniforme de la politique appliquée à la périphérie

L'ensemble des service edges d'un fournisseur de SSE doit garantir l'application des politiques. Il ne peut s'agir de connexions en périphérie à un réseau plus vaste, basé sur le cloud, dans le seul but de router ou d'acheminer « on-ramp » votre trafic vers l'infrastructure centrale d'application. De tels systèmes vont à l'encontre de l'objectif de fournir des services extrêmement performants et à faible latence

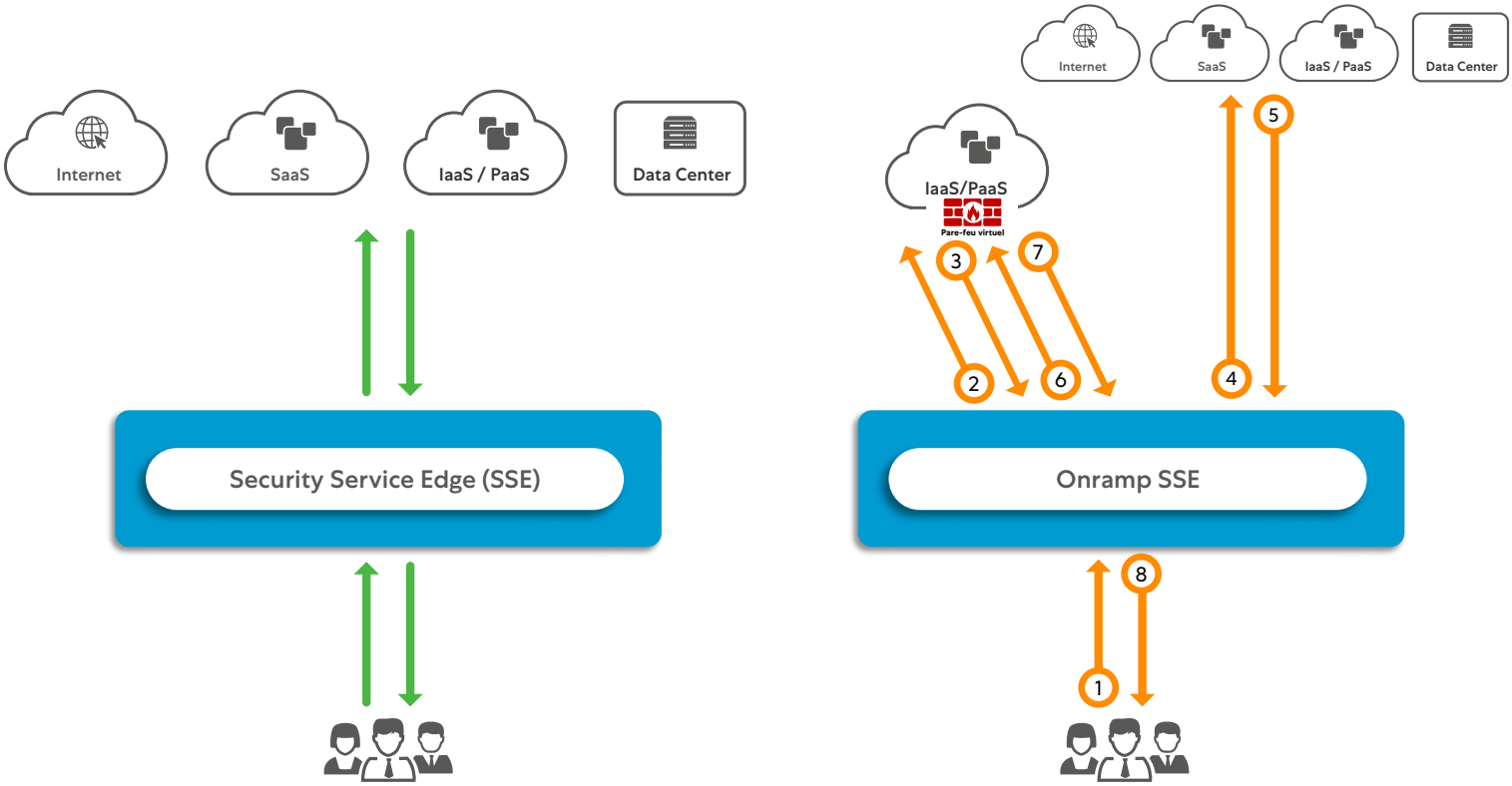

Figure 3 : Les services SSE in-line (à gauche) appliquent des contrôles de sécurité au trafic en ligne. Les contrôles de sécurité on-ramp (à droite) fournissent des passerelles d'entrée à la périphérie, pour ensuite transmettre le trafic à un contrôle centralisé hébergé dans le cloud, ce qui ajoute de la latence, nuit à l'efficacité et offre une piètre expérience utilisateur.

Le fournisseur doit prendre en compte les considérations de conception suivantes, en veillant à ce que les service edges proposent les avantages suivants :

- Être hébergés dans des emplacements de peering vitaux au sein de data centers indépendants des opérateurs, ce qui garantit une latence minimale entre la source et la destination. Lors de l'évaluation d'un fournisseur SSE, vérifiez les statistiques des références publiques comme PeeringDB et les déploiements de partenaires **(voir le piège n° 6 concernant les informations sur l'intégration des partenaires)**.
- Être soutenus par un SLA valide. Cela assurera la stabilité des fonctions de l'entreprise et indiquera que le fournisseur SSE travaille dans les mêmes zones qu'elle pour garantir les accords de niveau de service.
- Être déployés de manière privée, par client, dans les endroits où les conditions locales exigent des déploiements plus nuancés, par exemple sur site ou dans un nœud de calcul en périphérie **(voir le piège n° 4 pour plus de détails)**.
- Démontrent un historique de croissance du débit.
- Offrent une tolérance aux pannes déployée en mode actif-actif pour garantir la disponibilité et la redondance. (Le fournisseur surveille et maintient ses service edges public pour assurer une disponibilité continue).
- Promeuvent la confidentialité des données afin de garantir que le trafic des clients n'est transmis à aucun autre composant de l'infrastructure et qu'aucune donnée n'est jamais stockée sur disque.
- Fournissent des contrôles uniformes pour les ressources de l'entreprise sur tous les service edges et ne routent pas ou n'acheminent pas « on-ramp » le trafic des service edges distants vers les emplacements centraux.
- Appliquent une protection à l'échelle mondiale afin de protéger tous les services de l'entreprise dès qu'une menace est détectée.

⚠ À quoi dois-je être attentif ?

- Aux service edges publics qui n'assurent pas l'exécution. Ils acheminent plutôt le trafic vers des data centers d'application plus importants où des ressources informatiques sont disponibles.
- À la revendication de centaines de service edges publics sans partage de la fonction et de la capacité de chaque service.
- Aux service edges sans accords de niveau de service sur la disponibilité, le débit et la résilience.
- Aux service edges qui ne sont pas multi-entité et qui forcent le trafic via un cheminement on-ramp/un routage vers d'autres sites.
- Aux services SSE qui n'ont pas fait la preuve de leur déploiement auprès de gros clients.
- Aux services sans information publiquement disponible sur la stabilité et la disponibilité du service.

Résultats :

La sélection d'une solution SSE qui s'adapte à votre entreprise aujourd'hui et, plus important encore, à vos objectifs futurs, est un investissement crucial. L'évolutivité n'est pas simplement le mécanisme qui permet de vous développer, mais surtout de répondre aux besoins de votre entreprise sans sacrifier la fonction, la stabilité et la protection de votre entreprise. Choisissez une solution qui présente les avantages suivants :

- Fournit des preuves en toute transparence quant à son déploiement mondial et diversifié.
- A documenté et validé des SLA (accords de niveau de service) pour la perte ou la dégradation des services SSE.
- A réalisé le déploiement d'un grand nombre de clients de taille et de complexité similaires à celles de votre entreprise.
- Dispose d'informations publiques et consultables pour chaque PoP en utilisant des outils publics (par exemple, PeeringDB).
- Fournit toutes les fonctions critiques sur tous les sites sans hairpinning du trafic.
- Fournit une protection in-line entre la source et la destination.
- Est conçue pour l'infrastructure et la résilience opérationnelle et fonctionnelle.
- Peut être utilisée sous plusieurs formes sur plusieurs sites.

#2 Piège

Choisir une solution SSE qui ne repose pas sur une architecture Zero Trust

Envisagez plutôt les solutions SSE qui présentent les avantages suivants :

- N'autorisent l'accès qu'aux identités validées contextuellement, indépendamment de l'emplacement/du réseau. Ce modèle basé sur le moindre privilège s'applique à tous les services, pas seulement aux utilisateurs. En connectant les sources autorisées par le biais des contrôles SSE appropriés à des destinations valides et rien de plus, les entreprises suppriment les déplacements latéraux, qui sont souvent exploités par les acteurs des menaces.
- Concentrez-vous uniquement sur la connexion d'un accès dynamique, par session. Zero Trust n'est pas fourni avec des pare-feu, SD-WAN et autres services réseau. Il doit s'agir d'une superposition indépendante du réseau.
- N'exposez jamais les ressources de l'entreprise à une source non autorisée, afin de réduire la surface d'attaque et de garantir que des contrôles corrects sont appliqués à tous les services.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Zero Trust pour toutes les communications d'entreprise implique qu'aucun accès n'est accordé à une source quelconque (y compris les utilisateurs, les tiers, les réseaux, etc.) à une destination quelconque sans autorisation et approbation explicite.

L'instauration de Zero Trust au sein d'une entreprise a toujours été difficile en raison du contexte de réseau partagé qui relie la source à la destination, en s'appuyant sur un chemin de réseau physique ou logique pour interconnecter les deux entités. La figure 4 décrit ces préoccupations physiques communes. Il n'est pas possible de construire ou d'ajouter une stratégie Zero Trust avec des SD-WAN ou des pare-feu.

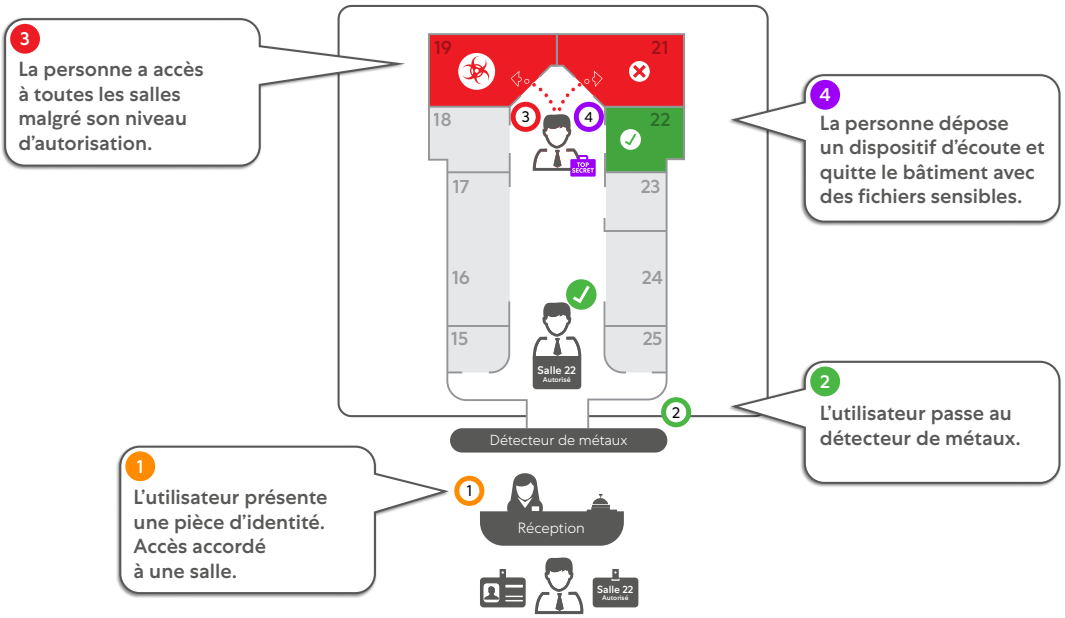

Figure 4 : Comment ne pas permettre l'accès ou l'analogie du vieux monde de la sécurité du réseau. Connecter des utilisateurs à votre réseau d'entreprise équivaut à laisser des visiteurs non accompagnés se promener dans votre siège social, avec le risque qu'ils dérobent des données sensibles.

Le SSE peut vous aider à appliquer des restrictions d'accès et d'utilisation à l'échelle de l'entreprise pour vos charges de travail. En étendant ces contrôles au-delà des employés, vous pouvez protéger votre entreprise contre des risques tels que l'exposition d'une surface d'attaque ou le déplacement latéral des menaces.

Entre autres choses, l'architecture Zero Trust applique des contrôles granulaires, garantissant que chaque demandeur communique avec la bonne destination sur une base par session, comme l'illustre la Figure 5. De telles règles nécessitent la connaissance des entités source et destination et c'est pourquoi la plupart des entreprises commencent leur parcours Zero Trust (et SSE) par leur base d'utilisateurs. Les utilisateurs se voient souvent attribuer une identité, ce qui leur permet de se différencier des autres services. Cependant, les réseaux étant plats, exposés et ouverts, le risque qu'un utilisateur ait accès à davantage d'informations simplement parce qu'il a partagé un réseau constitue une préoccupation majeure pour la stabilité des entreprises.

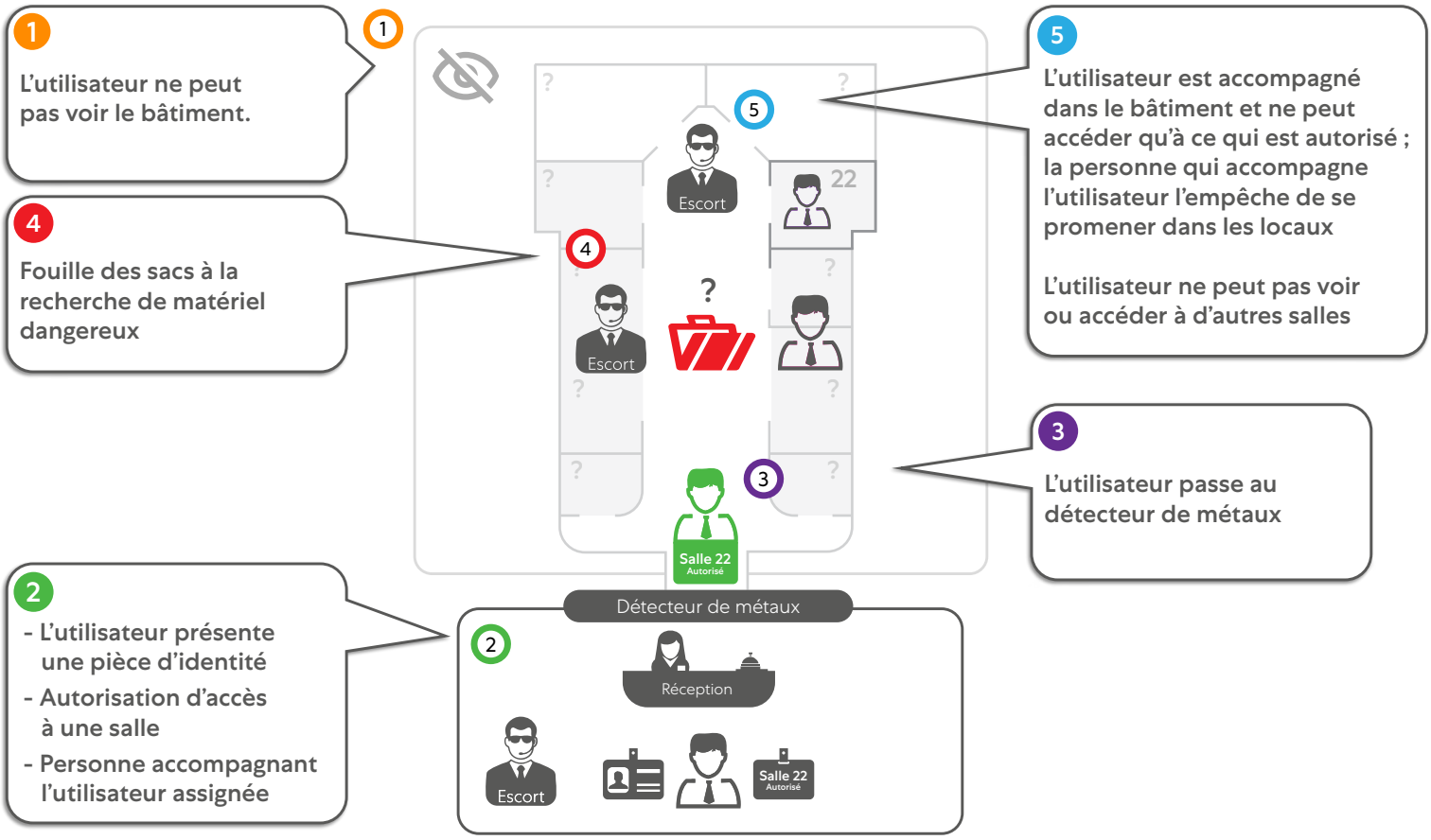

Figure 5 : La façon correcte de fournir un accès est le contrôle de bout en bout. Un accès Zero Trust, c'est comme escorter un visiteur aux yeux bandés à une réunion à votre siège social, puis l'escorter à la sortie. Le visiteur ne peut pas se promener dans vos locaux ni dérober des données.

Tenez compte de tous les cas d'utilisation commerciale, comme la protection des utilisateurs et des actifs commerciaux clés, et appliquez des contrôles SSE à l'ensemble du trafic. Établissez des connexions après avoir examiné de manière dynamique et contextuelle le risque que représentent les quatre valeurs de connexion suivantes (voir Figure 6) :

Initiateur de la connexion

Quelle est l'identité et la confiance dont bénéficie l'utilisateur/le dispositif/le réseau ? Comment cette identité différencie-t-elle l'accès pour cette source et dans quelles conditions ?

Exemple : Sarah des RH doit accéder au système RH hébergé dans le cloud ainsi qu'au système de dépenses hébergé en interne. L'accès est accordé par la plateforme SSE tant que son identité et son appareil de confiance disposent des droits définis pour obtenir l'accès.

Contrôle de la politique

Où, comment et quels contrôles seront appliqués ? Les critères de contrôle incluent l'efficacité du chemin, le risque et la confiance de l'initiateur, la fonction de la destination demandée et la politique de l'entreprise.

Exemple : Pierre dispose d'une identité valide pour accéder à Salesforce, mais sa société souhaite uniquement qu'il consulte, et non qu'il télécharge ou manipule des données. La solution SSE autorise donc Pierre à accéder uniquement au contenu de l'application en mode lecture et rien de plus.

Destination de la connexion

À quel service le demandeur accède-t-il ? S'agit-il d'un SaaS public ou d'une charge de travail interne ? Quels contrôles doivent-ils être appliqués ? L'accès peut changer en fonction du contexte de la politique d'identité et de contrôle.

Exemple : un initiateur légitime peut avoir l'autorisation d'accéder à un service PaaS cloud spécifique, et s'il s'agit d'un service cloud, le SSE inspectera la charge de travail pour s'assurer qu'elle ne divulgue pas de secrets d'entreprise. Ce même initiateur peut ensuite s'adresser à un service interne avec une confiance similaire, établissant ainsi simplement une connexion entre l'initiateur et le service, sans contrôle supplémentaire.

Établissement de la connexion

Enfin, en partant des entrées précédentes, des informations conditionnelles sur les charges de travail, les capacités du réseau ou de la périphérie, la politique définie par l'entreprise, etc. sont validées avant que l'accès ne soit établi. La solution SSE doit reconnaître les variations, par exemple un changement d'emplacement, et orienter l'accès vers le meilleur chemin possible.

Exemple : une fois la source, le contrôle et les destinations validés, la connexion sera établie, pour cette session et rien de plus. Le flux de bout en bout de l'application par session est décrit dans la Figure 6.

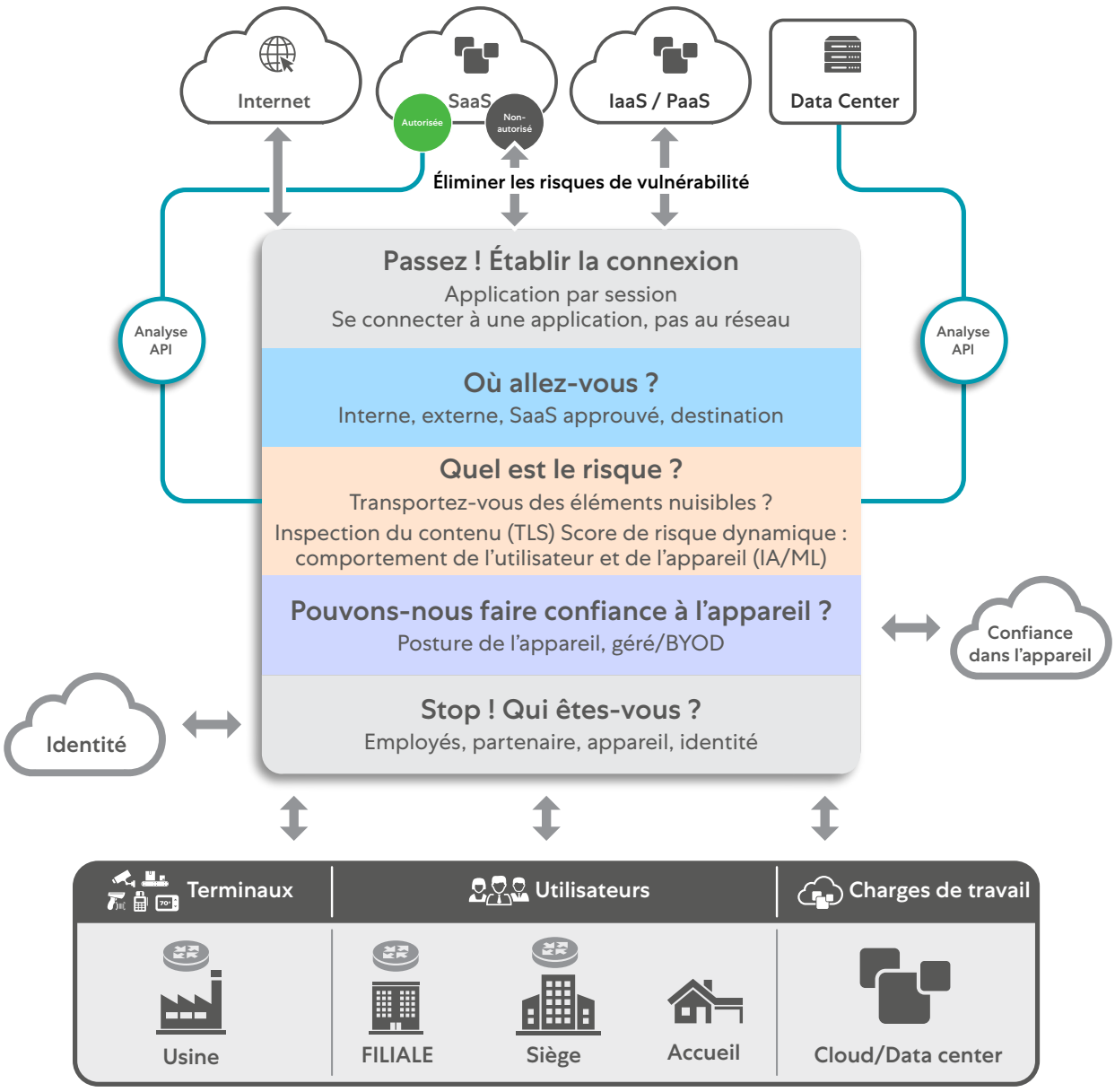

Figure 6 : Étapes d'une architecture Zero Trust, montrant le contrôle et l'application de la politique à chaque étape.

La définition des contrôles de connexion au sein d'une solution SSE **garantit que seule la bonne source peut accéder à la bonne destination**, via la bonne solution SSE. Cette utilisation du SSE sur la base du moindre privilège offre de nombreux avantages à l'entreprise, notamment :

- Les contrôles SSE appropriés sont appliqués à la source appropriée.
- Les services protégés par le SSE ne sont pas exposés à des sources non autorisées, ce qui réduit les risques de cybersécurité.
- Une réduction du gaspillage est observée, par exemple ne pas autoriser un serveur Linux à se connecter à un système de correctifs Windows.
- Une visibilité granulaire et une connaissance des flux sont mises en évidence, par demande d'accès, pas de réseau IP à IP.
- L'accès est consolidé en fonction de l'identité et non du réseau, ce qui permet de rationaliser la fonction (et l'infrastructure) des réseaux.

Parcours progressif du SSE avec Zero Trust :

En choisissant une solution SSE qui procure le contrôle dans tous les cas d'utilisation suivants, et uniquement un contrôle basé sur l'utilisateur, vous pouvez étendre la protection à toutes vos fonctions d'entreprise (voir Figure 7) :

Utilisateur à charges de travail

Permettre l'accès des utilisateurs aux charges de travail signifie que vous pouvez supprimer le contexte réseau de l'accès des utilisateurs, tout en obtenant simultanément une visibilité sur les charges de travail auxquelles les utilisateurs accèdent. Cette combinaison est généralement celle qui porte le plus rapidement ses fruits.

Envisagez un contrôle granulaire pour les utilisateurs sur l'ensemble du paysage des applications. Par exemple, des services Internet tels que YouTube peuvent être limités à l'équipe de relations publiques d'une entreprise.

Vous pouvez permettre un développement large de la gamme des services de l'entreprise et autoriser des règles plus granulaires telles que l'accès à des plateformes isolées d'OT et de R&D, sans jamais exposer l'ensemble de l'écosystème à la base d'utilisateurs.

Accès par des tiers

Appliquer un accès Zero Trust pour les partenaires tiers supprime le risque de connectivité au réseau et d'exposition de la surface d'attaque qui accompagne l'accès des partenaires traditionnels. Le contrôle basé sur le moindre privilège de Zero Trust vous permet de contrôler l'accès des partenaires à partir d'appareils non fiables ou personnels à des applications spécifiquement désignées, et rien de plus, tout en offrant une meilleure visibilité sur ce à quoi ils accèdent.

Les contrôles tiers de la solution SSE doivent fournir plusieurs mécanismes de contrôle d'accès. Au nombre des options figurent l'accès client autorisé à partir de plusieurs fournisseurs d'identité, par le biais d'applications spécifiques, l'accès isolé par navigateur uniquement, ou l'isolation complète de l'accès par une image de synthèse présentée au tiers (diffusion de pixels sur l'appareil de l'utilisateur, comme dans le cas du BYOD).

Charges de travail à charges de travail

Les contrôles de charge de travail à charge de travail sont des demandes d'accès à des applications et des services. En général, une machine Windows demandera des correctifs Windows, pas Linux. Il est donc essentiel pour une entreprise de catégoriser ce à quoi les systèmes devraient avoir accès.

Comme pour les utilisateurs, les contrôles de la charge de travail doivent fournir une identité valide pour utiliser un service. Si la charge de travail utilise des ressources publiques telles que des services IoT/OT basés sur le PaaS, la couche de sécurité doit valider et comprendre son contexte et bloquer toute tentative d'utilisation abusive.

À l'inverse, si la charge de travail accède à un service local et privé, cela ne peut se faire que par le biais de contrôles SSE en ligne, après approbation de l'identité, conformément à une validation Zero Trust.

Emplacement à emplacement

À mesure que l'accès et le contrôle évoluent dans votre entreprise, envisagez de recourir au Zero Trust pour la connectivité inter-site. Vous devez isoler un ensemble de services sur un réseau, un site, un VPC, etc. La connexion entre l'emplacement et le site connu ne doit pas passer par un réseau partagé. Zero Trust permet à un emplacement valide de se connecter à un ensemble valide de charges de travail au sein d'un autre emplacement. Zero Trust n'utilise pas l'accès à la couche de liaison du réseau ; il demande une connectivité d'application à application de manière uniforme à travers tout site, VPC, VLAN, etc.

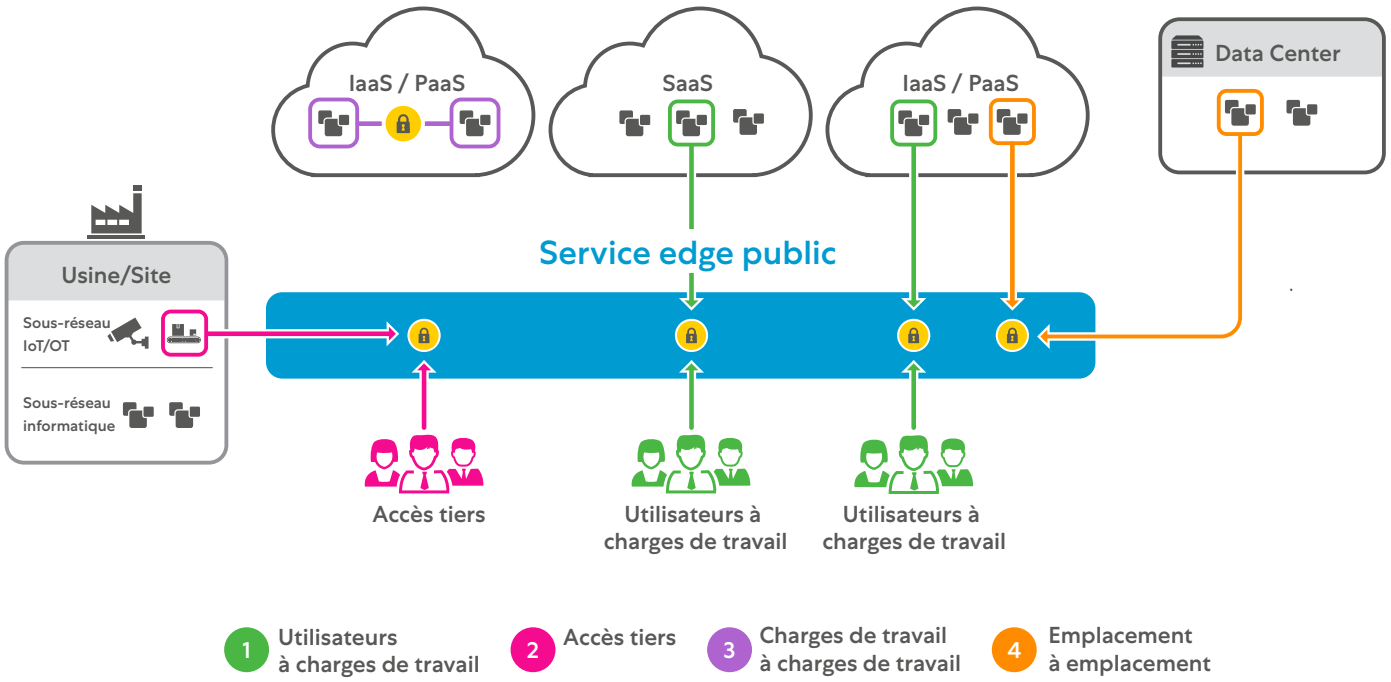

Figure 7 : Une approche suggérée pour la segmentation des entreprises. Permettre une approche progressive de contrôle, d'apprentissage, de segmentation et d'isolation supplémentaires dans le cadre d'une mise en œuvre de Zero Trust.

À titre d'exemple récent, lorsque des chercheurs en sécurité ont découvert la vulnérabilité de type « zero-day » de Log4j, chaque client utilisant l'utilitaire de journalisation vulnérable basé sur Apache Java risquait d'être victime d'une exécution complète du code à distance. Cependant, ceux qui ont adopté une architecture Zero Trust ont rendu leurs applications internes complètement invisibles sur Internet, ce qui signifie que les attaquants ne pouvaient ni les trouver ni les attaquer, protégeant même les versions sensibles d'Apache Log4j de cette vulnérabilité et de celles à venir. Cela aurait été impossible avec les services traditionnels exposés, comme les VPN et les pare-feu. **Zero Trust garantit que seuls les utilisateurs autorisés peuvent accéder aux applications ; ce modèle empêche les déplacements latéraux grâce à la microsegmentation utilisateur-application et application-application, et il peut inspecter le trafic entrant et sortant**.

C'est ce qui s'est produit lors de l'attaque de Colonial Pipeline, au cours de laquelle des informations d'identification VPN dérobées (dont la fonction MFA n'était pas activée) ont permis aux hackers de se déplacer latéralement sur le réseau et d'accéder à des données sensibles. Une architecture Zero Trust, qui ne connecte que les utilisateurs autorisés aux applications, et non aux réseaux, empêche les déplacements latéraux en segmentant les communications d'utilisateur à application et d'application à application

À quoi dois-je être attentif ?

- Évitez les services SSE qui ne suivent pas les principes de l'architecture Zero Trust, tels que la publication spéciale 800-207 du NIST.
- Assurez-vous que le service SSE offre des contrôles Zero Trust à toutes les ressources de l'entreprise, et pas uniquement aux utilisateurs.
- Zero Trust n'est ni un pare-feu ni un SD-WAN. Zero Trust est indépendant du réseau. Un SSE d'un fournisseur dépendant du réseau peut vous exposer à une déficience architecturale de Zero Trust.
- Assurez-vous que les contrôles de Zero Trust commencent par la confiance zéro ; aucune ressource de l'entreprise ne doit être accessible avant avoir été validée.
- Traitez tous les aspects de votre entreprise. Ne limitez pas vos contrôles Zero Trust à un seul secteur de l'entreprise.

Résultats :

La protection d'une entreprise et de ses utilisateurs doit être abordée d'une manière qui assure l'accès sur la base du besoin de savoir et du moindre privilège. **Zero Trust doit être le contrôle fondamental lors de la sélection d'une solution SSE.** En conséquence :

- Le fournisseur SSE protège tous les services de l'entreprise et valide l'identité des entités avant d'autoriser l'accès ; tout le reste doit être bloqué.
- Il convient d'éviter les solutions qui forcent la connectivité du réseau ; de plus, l'accès doit être indépendant du réseau, partout.
- Le service SSE garantit une surface d'attaque nulle pour vos services d'entreprise privés.

#3 Piège

Choisir une solution SSE qui promet une protection contre les menaces avancées et une DLP avancée, mais qui ne peut pas inspecter le trafic chiffré à grande échelle.

Envisagez plutôt les solutions SSE qui présentent les avantages suivants :

- Fournissent une inspection SSL/TLS du trafic à l'échelle de la production avec un impact minimal sur les performances. Ceci demande une architecture de proxy évolutive.
- Saisissent et analysent les connaissances approfondies acquises lors de l'inspection permettant d'appliquer une protection contre les menaces avancées pour le trafic chiffré et des politiques de classification avancées des données pour la prévention de la perte de données.
- Inspectent tout le trafic, y compris le trafic chiffré, provenant des utilisateurs, des objets, des charges de travail, etc.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Les fournisseurs de SSE ne peuvent pas prétendre offrir une protection contre les menaces avancées et une prévention des pertes de données de premier ordre s'ils ne sont pas en mesure d'inspecter tout le trafic à l'échelle de la production, y compris le trafic chiffré.

Méfiez-vous des affirmations des fournisseurs de SSE dans ce domaine, car tout dépend de l'architecture sous-jacente de la solution. Les fournisseurs de SSE qui ont conçu leur proxy dans le cloud dès le départ ont un avantage certain dans ce domaine.

La grande majorité (estimée à environ 85 %) du trafic Internet étant chiffrée, les fournisseurs SSE doivent inspecter ce trafic à grande échelle et en profondeur pour assurer une protection adéquate contre les menaces et la prévention des pertes de données requises face à la croissance exponentielle des risques de sécurité posés par les canaux chiffrés. Pourquoi le déchiffrement SSL/TLS à grande échelle est-il si important (voir Figure 8) ?

- Le chiffrement SSL/TLS peut dissimuler des contenus dangereux tels que des virus, des logiciels espions et d'autres programmes malveillants.
- Les attaquants construisent leurs sites Web avec le chiffrement TLS et SSL ou injectent du contenu malveillant dans des sites SSL et TLS connus et fiables.
- Le SSL/TLS peut masquer des fuites de données, telles que la transmission de documents financiers sensibles d'une entreprise.
- Le SSL/TLS peut masquer la navigation sur des sites Web appartenant à des catégories de responsabilité légale.
- La capacité de contrôler et d'inspecter le trafic en provenance et à destination des services en ligne utilisant le protocole HTTPS est devenue un élément important du dispositif de sécurité d'une entreprise.

Figure 8 : L'architecture pass-through utilisée par certains fournisseurs ne permet pas l'inspection du trafic chiffré à grande échelle, comme un contrôle de sécurité de base qui permet à une voiture de passer sans vérifier si son coffre contient des marchandises illicites.

Compte tenu de ces risques, l'architecture d'un fournisseur de SSE doit évoluer pour fonctionner comme un mandataire intermédiaire SSL/TLS qui fournit une analyse complète du contenu entrant et sortant et bloque immédiatement toute menace détectée n'importe où dans le cloud.

Les hackers continuent de faire évoluer leurs outils, techniques et procédures pour cibler les entreprises, notamment en utilisant des fournisseurs de services de stockage légitimes tels que Dropbox, Box, OneDrive et GDrive pour héberger des charges utiles malveillantes. Ces connexions utiliseront les certificats SSL/TLS génériques de ces fournisseurs réputés afin de diffuser les charges utiles malveillantes, qui, si elles ne sont pas inspectées, permettront la réussite de l'attaque. Les charges utiles malveillantes (exécutables, documents de bureau, etc.) sont également polymorphes par nature, l'objectif étant d'échapper aux détections d'empreintes digitales de base. L'architecture des fournisseurs SSE doit permettre l'extraction complète des charges utiles de ces connexions chiffrées SSL/TLS et doit être capable de décompresser et de démasquer ces fichiers pour une détection précise (voir Figure 9).

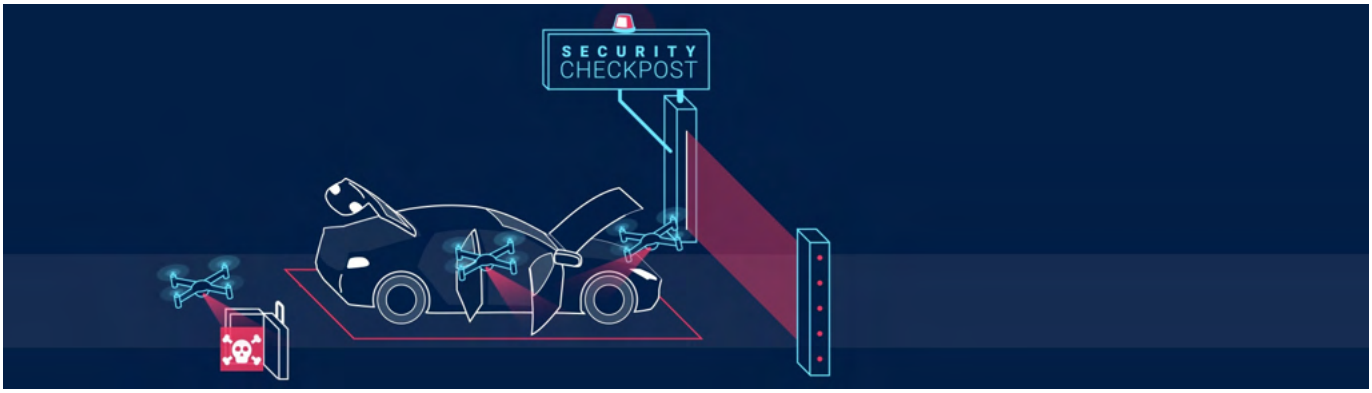

Figure 9 : Le fournisseur SSE de droite fournit une inspection SSL/TLS complète de tout le trafic à l'aide d'une architecture proxy, comme une voiture qui est arrêtée et entièrement inspectée avant d'être autorisée à passer le poste de contrôle de sécurité.

Cette protection contre les menaces doit s'appuyer sur de nombreux flux de menaces sectoriels provenant de sources ouvertes, commerciales et privées, ainsi que sur des mises à jour de sécurité fréquentes.

Outre le blocage des menaces, l'inspection à grande échelle permet une prévention avancée de la perte de données. **Les fournisseurs de SSE doivent être évalués sur leurs capacités de classification des données**. Celles-ci devraient inclure des expressions régulières (regex) comme mécanisme de base, mais trouver et classer rapidement les données sensibles sur tous les canaux de données du cloud est une condition essentielle pour protéger les données personnelles, sanitaires et confidentielles contre la perte. Cette classification nécessite une inspection SSL/TLS et permet des capacités avancées telles que :

- **Correspondance exacte des données**. Le SSE utilise des modèles d'index pour identifier un enregistrement d'une source de données structurée qui correspond à des critères prédéfinis.
- **Empreinte digitale des documents**. Lors de l'évaluation du trafic sortant, le SSE utilise un référentiel de documents pour identifier ceux qui correspondent entièrement ou partiellement.
- **OCR (reconnaissance optique de caractères)**. Le SSE détecte les données sensibles dans un fichier image, dans les images intégrées, dans les captures d'écran et dans les textes manuscrits, et ferme tous les canaux d'exfiltration de données basés sur le cloud.
- **Apprentissage automatique**. Des algorithmes pré-entraînés prennent des décisions sur le niveau de confidentialité des données.

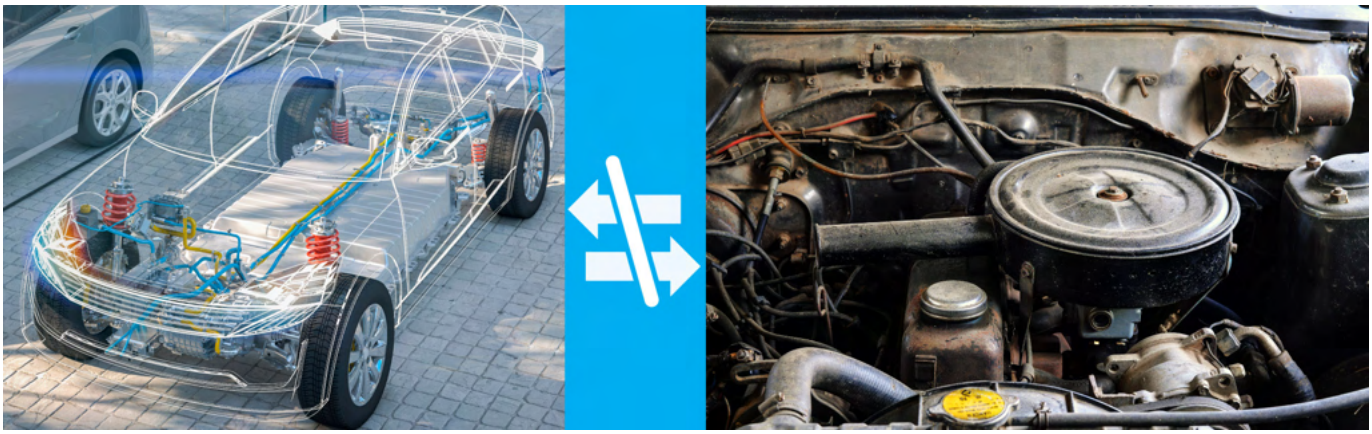

Figure 10 : Tout comme un moteur à combustion interne ne peut pas être modifié pour fonctionner comme un véhicule électrique, méfiez-vous des fournisseurs qui ajoutent des capacités telles que l'inspection SSL/TLS à leurs architectures existantes.

Le SSE comprend une fonctionnalité CASB (Cloud Access Security Broker) pour surveiller et appliquer les politiques entre les utilisateurs et les applications de services cloud, et la possibilité d'inspecter le trafic chiffré in-line présente un certain nombre d'avantages dans ce contexte. L'inspection peut se faire « hors bande », c'est-à-dire en analysant les API des fournisseurs de SaaS pour protéger les données au repos, ou « in-line », c'est-à-dire en analysant les données en mouvement. Accordez une attention particulière à ce dernier point, car l'inspection in-line empêche le téléchargement de données vers des applications non autorisées, le téléchargement de données vers des appareils non autorisés et le téléchargement de contenu malveillant. Le fournisseur SSE doit également permettre un contrôle d'accès granulaire basé sur un ensemble élaboré de définitions d'applications cloud, de contrôles de types de fichiers et d'attributs de risque.

Avec l'adoption de centaines de milliers d'applications cloud, les données sensibles des entreprises sont aujourd'hui largement disséminées. Les deux principaux canaux d'exfiltration de données sont les applications de bureau cloud et les applications personnelles de messagerie électronique. Un bon fournisseur SSE doit fournir une visibilité contextuelle et une mise en application complètes lorsque des utilisateurs mal intentionnés chargent des données sensibles sur leurs applications personnelles Box, Dropbox et autres bureaux cloud. Ils doivent également empêcher l'exfiltration de données sur des services de messagerie Web personnels et non agréés tels que Gmail et Hotmail.

Les fournisseurs de SSE se différencient clairement par leur capacité à déchiffrer et à inspecter le trafic SSL/TLS de manière évolutive en fonction de la demande de trafic, et par leur capacité à fournir ce niveau d'inspection sans que les performances en soient affectées, ce qui n'est possible qu'avec une solution SSE basée sur un proxy et conçue dès le départ dans un souci d'évolutivité (voir Figure 10).

Il est important de se pencher sur la manière dont le fournisseur SSE réalise ces objectifs. Pour maintenir une latence minimale pour chaque inspection de paquets, le fournisseur doit employer une architecture à passage unique où le paquet est placé une fois en mémoire et où les services d'inspection, chacun avec des ressources de processeur dédiées, sont capables d'effectuer leurs analyses simultanément. Les fournisseurs qui associent ces inspections à des applications physiques et virtuelles sérialisées subissent à chaque saut une surcharge de traitement et courent le risque de voir chaque paquet affecté par une latence excessive.

Ces avantages architecturaux doivent être appliqués aux dernières normes telles que la norme TLS 1.3, où une véritable architecture proxy présente l'avantage d'être in-line avec deux connexions distinctes au client et au serveur. Comme cela permet de réassembler et d'analyser l'objet entier, il est possible d'appliquer la protection contre les menaces avancées, la DLP et le sandboxing. Assurez-vous que les versions de TLS et les mises à niveau de chiffrement sont gérées de manière transparente par le fournisseur au sein de son cloud : certains fournisseurs de matériel peuvent forcer le rafraîchissement des appliances pour gérer la charge supplémentaire liée à la prise en charge de nouveaux chiffrements.

La gestion des certificats doit également être prise en compte, étant donné la complexité potentielle qui peut être induite. Les fournisseurs SSE doivent autoriser l'utilisation de leurs certificats ou l'utilisation des vôtres, et permettre la rotation entre les deux via l'API. Les certificats doivent être automatiquement répliqués entre les différents service edges.

Méfiez-vous des fournisseurs SSE qui pourraient ajouter des capacités d'inspection SSL/TLS aux pare-feu de nouvelle génération (NGFW) existants, lesquels présentent des problèmes d'évolutivité inhérents. Cela concerne même les fournisseurs qui déplacent des NGFW dotés de capacités d'inspection dans des instances virtuelles sur des nœuds de calcul de FSC.

⚠ À quoi dois-je être attentif ?

Lorsque vous évaluez la capacité d'un fournisseur SSE à inspecter le trafic SSL/TLS, assurez-vous que la latence encourue est acceptable. Malheureusement, les architectures qui ne sont pas cloud natives peuvent induire des baisses de performances considérables, en particulier lors de l'utilisation de TLS 1.2 ou de versions antérieures. **La confidentialité des données peut également constituer une source de préoccupation ; il est donc important de comprendre les contraintes réglementaires et la manière dont le fournisseur les gère**. Les fournisseurs SSE devraient permettre d'exclure facilement certains types de données afin de respecter les contraintes de confidentialité. Les fournisseurs SSE ne devraient jamais stocker les données des utilisateurs dans le cloud.

Méfiez-vous des fournisseurs SSE qui pourraient ajouter des capacités d'inspection SSL/TLS aux pare-feu de nouvelle génération (NGFW) existants, lesquels présentent des problèmes d'évolutivité inhérents. Cela concerne même les fournisseurs qui déplacent des NGFW dotés de capacités d'inspection dans des instances virtuelles sur des nœuds de calcul de FSC. Méfiez-vous également des fournisseurs qui combinent des capacités CASB hors bande avec une inspection limitée du trafic in-line. La sécurisation des données au repos et des données en mouvement est cruciale.

Évaluez la manière dont le fournisseur SSE gère les certificats, et sachez que l'épinglage de certificat peut poser problème.

La mise en œuvre de l'inspection du trafic SSL/TLS a toujours constitué un défi pour l'entreprise et ce, pour diverses raisons. **Le fournisseur SSE devrait être le principal expert de confiance et devrait fournir des conseils, des explications et assurer la mise en œuvre lors de l'activation de l'inspection SSL/TLS. L'inspection SSL/TLS** n'est pas négociable dans le monde du SSE, où il ne faut en aucun cas sacrifier la sécurité au profit de la vitesse.

Résultats :

L'inspection SSL/TLS à grande échelle avec une latence minimale augmente considérablement la capacité à bloquer les menaces en tirant parti de la puissance du cloud pour identifier et sécuriser les données sensibles. Seuls les fournisseurs SSE dotés de la bonne architecture cloud native sont en mesure de fournir :

- Une inspection SSL/TLS de tout le trafic à l'échelle de la production avec un impact minimal sur les performances pour une protection approfondie des données contre les menaces.
- Une architecture d'analyse à mémoire unique offrant des avantages d'évolutivité exceptionnels pour un déchiffrement à grande échelle.
- L'expérience pour guider les clients tout au long des étapes et des défis de l'inspection SSL/TLS.

#4 Piège

Choisir une solution SSE universelle qui ne prend pas en charge des solutions de déploiement et de gestion flexibles, évolutives et variées

Envisagez plutôt les solutions SSE qui présentent les avantages suivants :

- Proposent des modèles de déploiement flexibles pour protéger les utilisateurs et les applications quel que soit l'endroit où l'application est hébergée, y compris le data center, le cloud public, le cloud privé, le nœud de calcul en périphérie et sur site.
- Assurent la protection des utilisateurs accédant aux applications sur des appareils ou des objets gérés ou non gérés.
- Étendent ces mêmes protections contre les cybermenaces et des données pour sécuriser toutes les autres communications de charge de travail à charge de travail au sein d'un même cloud ou entre plusieurs clouds.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Les évaluateurs de solutions SSE doivent analyser l'état de préparation de leur environnement pour comprendre comment appliquer au mieux les protections SSE. Pour prendre en charge les différents scénarios de déploiement, les fournisseurs de SSE doivent prévoir à la fois les service edges publics et les service edges privés.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Les évaluateurs de solutions SSE doivent analyser l'état de préparation de leur environnement pour comprendre comment appliquer au mieux les protections SSE. Pour prendre en charge les différents scénarios de déploiement, les fournisseurs de SSE doivent prévoir à la fois les service edges publics et les service edges privés.

La plupart des utilisateurs se connecteront au SSE via le service edge public d'un fournisseur. Il s'agit de passerelles Internet sécurisées et complètes et de courtiers d'applications privés qui proposent une sécurité intégrée. Ils inspectent tout le trafic de manière bidirectionnelle à la recherche de programmes malveillants et appliquent des politiques de sécurité, de conformité et de pare-feu. Ils doivent gérer des centaines de milliers d'utilisateurs simultanément avec des millions de sessions simultanées. Ainsi, quel que soit l'endroit où se trouvent vos utilisateurs, ils peuvent y accéder à partir de n'importe quel appareil :

- Internet avec les service edges publics protégeant le trafic et appliquant vos politiques d'entreprise
- Applications internes avec des politiques d'accès et de ré-authentification basées sur les bonnes pratiques de votre entreprise

Figure 11 : Un fournisseur de SSE doit proposer des solutions de service edges publics et privés, qui doivent également fonctionner en harmonie avec une gestion centralisée.

Il est important de veiller à ce que ces service edges publics disposent d'importantes capacités de tolérance aux pannes et soient déployés en mode actif-actif pour garantir la disponibilité et la redondance. Le fournisseur doit surveiller et entretenir ses service edges afin de garantir une disponibilité continue. Pour garantir la confidentialité des données, le trafic des clients ne doit être transmis à aucun autre composant de l'infrastructure et aucune donnée ne doit jamais être stockée sur disque.

Il peut toutefois arriver que le service edge public ne réponde pas aux besoins et que le fournisseur de SSE doive alors proposer des solutions de service edge privé (voir Figure 11). Cette option permet d'étendre l'architecture et les capacités du service edge public aux locaux d'une entreprise ou à un emplacement privé et de tirer parti de la même politique contrôlée de manière centralisée que celle des service edges publics.

Pour un accès sécurisé à Internet, les service edges privés peuvent être installés dans le data center d'une entreprise et sont dédiés à son trafic, mais ils doivent être gérés et entretenus par le fournisseur de SSE, avec une intervention quasi nulle de l'entreprise. Ce mode de déploiement profite généralement aux entreprises qui ont certaines exigences géopolitiques ou qui utilisent des applications qui requièrent que l'adresse IP source soit celle de l'entreprise.

Pour l'accès aux applications internes, le service edge privé assure une gestion similaire des connexions entre l'utilisateur et l'application, et applique les mêmes politiques que le service edge public, le service étant hébergé soit sur site, soit dans le cloud public, mais là encore géré par le fournisseur de SSE. Ce modèle de déploiement permet une confiance zéro (Zero Trust) « entre les quatre murs », car il est utile de réduire la latence d'une application lorsqu'une application et un utilisateur se trouvent au même emplacement (et le fait de se rendre au service edge public ajouterait une latence supplémentaire). Cette option fournit également une couche de survie en cas de perte de la connexion à Internet. Le fournisseur de SSE doit distribuer des images pour un déploiement dans les data centers d'entreprise et les environnements cloud privés locaux.

Afin de fournir une protection Zero Trust aux applications internes, les fournisseurs de SSE doivent proposer un moyen de créer une interface sécurisée et authentifiée entre vos serveurs d'applications et les service edges publics et privés afin de protéger les applications internes. **Ce mécanisme doit être disponible sous plusieurs formes** : une image de machine virtuelle (VM) standard ou un déploiement conteneurisé dans les data centers d'entreprise, des environnements de cloud privés locaux tels que VMware, ou des environnements de cloud publics tels que EC2 d'Amazon Web Services (AWS), et les paquets qui peuvent être installés sur les distributions Linux prises en charge.

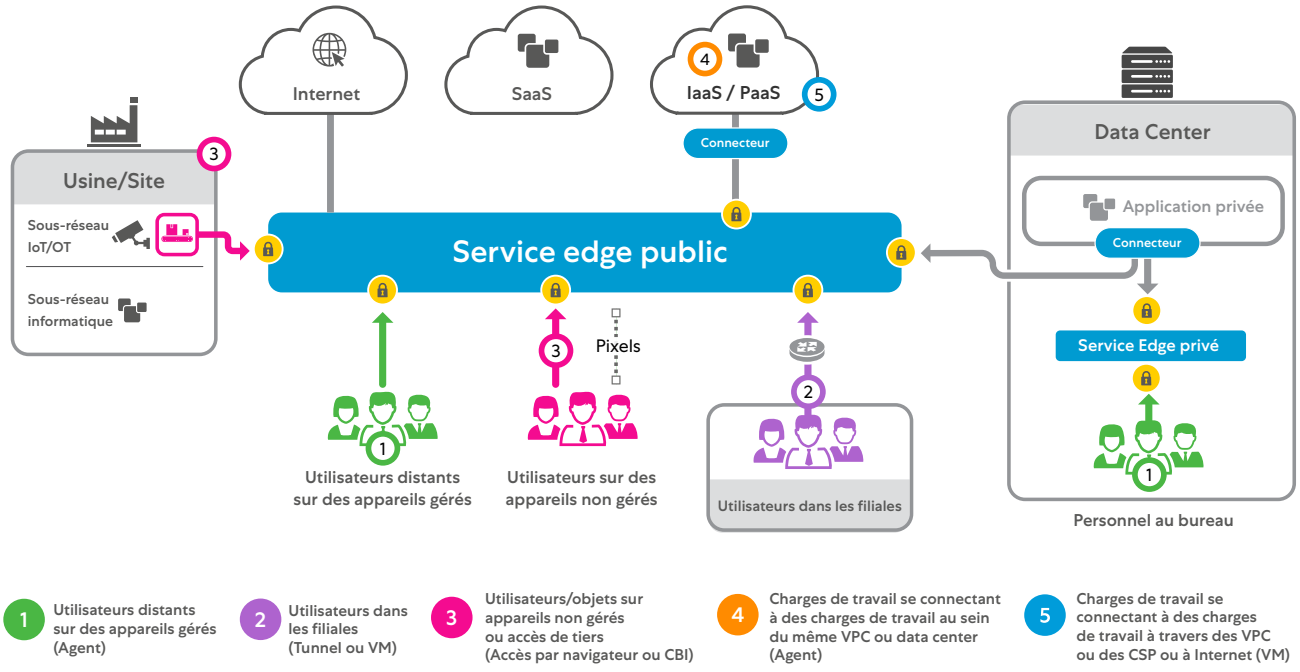

Figure 12 : Le fournisseur de SSE doit prendre en charge un certain nombre de modes de déploiement et de gestion, en tenant compte des utilisateurs distants, des utilisateurs dans les filiales, des utilisateurs au siège, des charges de travail communiquant avec les charges de travail, etc. via des agents et des VM.

Une fois que l'emplacement depuis lequel les politiques SSE seront administrées et mises en œuvre a été déterminé, il convient d'analyser comment les utilisateurs et les charges de travail bénéficieront de cette protection. Il est important d'envisager différents scénarios (voir la figure 12) :

Pour les utilisateurs distants utilisant des appareils gérés, le fournisseur de SSE doit proposer un agent unifié unique qui achemine le trafic vers le service edge pour un accès Internet sécurisé. L'agent doit également fournir un accès granulaire, basé sur des politiques, aux ressources internes. Tout cela doit être automatisé grâce à l'intelligence intégrée à l'agent. Il doit également protéger le trafic mobile de vos utilisateurs sur les réseaux Wi-Fi ou cellulaires. L'agent transmet le trafic utilisateur au service SSE, qui applique les politiques de sécurité et d'accès de votre entreprise partout où les utilisateurs accèdent à Internet, et établit un transport sécurisé pour accéder aux applications et services de l'entreprise. Assurez-vous que cet agent peut détecter la connexion d'un utilisateur à un réseau de confiance et, si l'agent doit désactiver son service, comme déterminé par la politique, quand il détecte un réseau de confiance. Assurez-vous que ces agents prennent en charge une large gamme de systèmes d'exploitation, notamment Windows, MacOS, Linux, iOS et Android.

Pour les utilisateurs d'une filiale, une méthode courante de transfert du trafic vers le service edge consiste à utiliser un tunnel GRE ou IPSec. Cependant, le fournisseur de SSE devrait proposer une approche alternative. Une machine virtuelle installée dans la filiale peut simplifier la complexité et l'administration continue de ces tunnels, et éliminer le déplacement latéral des menaces en supprimant le réseau routable géré par le client. Le déploiement doit être automatisé et inclure des politiques flexibles d'orientation du trafic vers le service edge avec une surveillance des SLA (accords de niveau de service) et un basculement intégrés. Cette solution convient bien aux moyennes et grandes filiales, et à celles qui fournissent des services locaux.

L'option précédente, qui consiste à traiter chaque utilisateur comme un utilisateur distant, doit être envisagée pour les petites filiales qui ne proposent pas de services locaux (pensez au modèle du café). Compte tenu de la manière dont les récents événements ont modifié l'importance de la filiale, cette option est souhaitable, car elle ne permet à personne d'accéder au réseau de l'entreprise et empêche tout risque de déplacement latéral.

Pour les utilisateurs/objets sur des appareils non gérés ou pour l'accès de tiers aux applications Web internes, les fournisseurs de SSE doivent être en mesure d'assurer une protection SSE similaire sans avoir à installer un agent. Ces utilisateurs utilisent alors un navigateur Web pour l'authentification de l'utilisateur, navigateur qui fournit ensuite une protection Zero Trust en publiant un CNAME spécifique à l'application dans votre zone DNS afin de pouvoir automatiquement rediriger ces requêtes. Le fournisseur de SSE doit également disposer d'une fonction intégrée d'isolation du navigateur dans le cloud (CBI) pour une sécurité sans agent de tout appareil non géré, où qu'il se trouve. Ceci a pour avantage de contourner complètement le besoin d'un reverse proxy fragile.

Avec le CBI, les administrateurs configurent le paramètre SSO d'une ressource cloud autorisée pour la rediriger vers le fournisseur de SSE. Après quoi, lorsque les utilisateurs tentent d'accéder à la ressource cloud à partir d'un dispositif personnel ou tiers, leur trafic est automatiquement envoyé à CBI, sans aucune installation de logiciel. Il pixelise le contenu envoyé aux appareils des utilisateurs, empêchant ainsi le téléchargement, la copie, le collage et l'impression. Les utilisateurs peuvent ainsi effectuer leurs tâches professionnelles à partir d'appareils non gérés, sans risque de fuite de données et de téléchargement de programmes malveillants, tout en respectant les exigences réglementaires.

Pour les charges de travail se connectant à des charges de travail au sein d'un même VPC ou data center, la segmentation traditionnelle du réseau était la solution. Bien que cela soit logique de façon théorique, la réalisation de la segmentation du réseau dans la pratique constitue un défi. Les fournisseurs de SSE doivent donc étendre leurs protections utilisateur-application aux communications entre charges de travail. Grâce à l'installation d'un agent sur la charge de travail elle-même, le fournisseur de SSE doit déterminer le risque et appliquer une protection basée sur l'identité à vos charges de travail, sans aucune modification du réseau. Il doit également disposer de politiques qui s'adaptent automatiquement aux changements d'environnement.

Pour les charges de travail se connectant à des charges de travail sur des VPC ou des CSP ou sur Internet, les fournisseurs de SSE doivent à nouveau étendre à ces charges de travail une protection SSE similaire à celle offerte aux utilisateurs. À ce titre, les fournisseurs de SSE doivent proposer un mécanisme, généralement via une machine virtuelle (disponible dans les clouds publics ou les hyperviseurs sur site), qui simplifie la transmission du trafic vers le service edge. Il en résulte une protection des données et une protection contre les cybermenaces pour les charges de travail qui se connectent à Internet, ainsi qu'une protection Zero Trust pour les charges de travail d'un cloud qui accèdent à des charges de travail d'un autre cloud. Grâce à cette approche, les fournisseurs de SSE peuvent regrouper plusieurs produits (par exemple, les proxys Web, les pare-feu, les passerelles NAT, le filtrage d'URL, etc.) en une seule solution.

Pour sécuriser les données au repos dans des environnements IaaS et SaaS, le fournisseur de SSE doit également fournir des solutions dans le domaine du CASB, de la gestion des droits d'accès à l'infrastructure cloud (CIEM) et de la gestion de la posture de sécurité cloud (CSPM), afin de permettre une analyse basée sur les API avec des applications SaaS et IaaS populaires. Cela permet d'identifier et de corriger les mauvaises configurations et les autorisations inappropriées dans les environnements cloud, ainsi que d'auditer et d'analyser les plateformes SaaS et IaaS pour sécuriser les données et les protéger contre les menaces. Un fournisseur de SSE doit proposer ces fonctionnalités hors bande en parfaite adéquation avec ses fonctionnalités in-line pour appliquer des politiques cohérentes aux données au repos et en mouvement.

L'avantage d'un fournisseur de SSE unique fournissant cette vaste panoplie de protection est qu'elle peut être gérée à partir d'un plan de contrôle central, les politiques de l'entreprise étant appliquées de manière uniforme et dynamique à toutes les communications entre utilisateurs/objets et applications et entre charges de travail.

⚠ À quoi dois-je être attentif ?

Le déploiement de la technologie SSE dépend largement de la complexité de l'environnement de l'entreprise. **Il est donc très important de bien connaître l'emplacement, le comportement et les besoins d'accès des utilisateurs, de même que les besoins des applications**. En outre, certains pays comme la Chine présentent des défis uniques en matière de performances en raison des contrôles de l'Internet que même des modèles de déploiement flexibles ne peuvent résoudre. Le fournisseur de SSE doit proposer des solutions innovantes pour relever ces défis.

Résultats :

Déployées correctement, ces options flexibles, diversifiées et évolutives offriront à votre entreprise tous les avantages du Security Service Edge, quel que soit l'endroit où se trouve l'utilisateur ou l'objet, ou l'endroit où l'application est hébergée, et étendront même cette protection au sein de l'application elle-même :

- L'avantage d'un fournisseur de SSE unique proposant une large gamme de protection est que cette dernière peut être gérée à partir d'un panneau de contrôle central, les politiques de l'entreprise étant appliquées de manière uniforme et dynamique à toutes les communications entre utilisateurs/objets et applications et entre charges de travail.
- L'extension de la même protection des appareils gérés aux appareils BYOD (appareils personnels utilisés à des fins professionnelles) et tiers non gérés apporte une plus grande flexibilité aux prestataires et aux employés.
- La sécurité de charge de travail à charge de travail procure aux ingénieurs DevOps et CloudOps les mêmes protections Zero Trust pour leurs applications accédant à d'autres charges de travail, d'autres clouds ou à Internet.

#5 Piège

Choisir une solution SSE qui apporte une expérience utilisateur (UX) médiocre en n'optimisant pas la connectivité des applications ou en ne diagnostiquant pas les dégradations de l'UX.

Privilégiez plutôt les fournisseurs de SSE qui présentent les avantages suivants :

- Sont transparents, faciles à authentifier et toujours actifs, garantissant que les utilisateurs finaux de leur plateforme SSE bénéficient d'une excellente expérience utilisateur sur la base de mesures objectives.
- Établissent une corrélation entre une mauvaise expérience de l'utilisateur final et ses causes sous-jacentes, qu'il s'agisse de l'appareil, du réseau, des applications ou de la pile de sécurité.
- Exploitent des partenariats avec des fournisseurs de SaaS populaires tels que Microsoft 365 pour minimiser la latence entre le service edge public et le réseau du fournisseur d'applications.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

Les points de présence du fournisseur de SSE dans le monde entier et les relations d'échange de trafic Internet avec les fournisseurs et les vendeurs d'applications offrent une alternative puissante au backhauling et au hairpinning imposé par les piles de sécurité traditionnelles.

Au-delà de ces avantages architecturaux, les fournisseurs de SSE sont particulièrement bien placés pour mesurer et analyser l'expérience de l'utilisateur final grâce à leur présence sur les appareils des utilisateurs et sur le chemin des données des applications. Ces avantages permettent aux fournisseurs de SSE de comprendre l'expérience de l'utilisateur du point de vue de son appareil et de fournir des diagnostics plus approfondis et une plus grande échelle en exploitant l'infrastructure du service edge public.

Privilégiez les fournisseurs de SSE qui ont intégré une solution de surveillance (communément appelée **Digital Experience Monitoring** ou DEM) à leurs agents existants et leur infrastructure cloud. Les fournisseurs qui proposent des solutions nécessitant des agents supplémentaires ou des acquisitions vaguement intégrées ne fourniront pas le même niveau de visibilité et de diagnostic.

La solution DEM proposée par les fournisseurs de SSE doit être large. Elle doit offrir une visibilité et un dépannage de bout en bout des problèmes de performance de l'utilisateur final pour chaque utilisateur ou application, quel que soit leur emplacement. Elle doit en outre permettre une surveillance continue pour les équipes chargées du réseau, de la sécurité, des postes de travail et du service d'assistance, avec un aperçu des problèmes de performance des appareils, du réseau et des applications de l'utilisateur final. Enfin, elle doit permettre à la fois des flux de travail réactifs pour aider à résoudre les problèmes signalés par les employés, ainsi que des flux de travail proactifs pour aider à identifier les macro-problèmes (comme les pannes locales des FAI ou les indisponibilités des applications au niveau mondial) avant que les utilisateurs ne s'en rendent compte. **Cela doit être rendu possible par des algorithmes d'évaluation basés sur l'apprentissage automatique, permettant de distinguer les expériences normales et anormales des utilisateurs par utilisateur, par application, par bureau ou par emplacement géographique**.

Cette surveillance doit s'effectuer à plusieurs niveaux, notamment au niveau de la couche 7 pour fournir des informations sur les temps de réponse des applications Web et au niveau de la couche 3 pour comprendre le comportement du réseau, y compris les informations saut par saut sur le chemin, la latence et la perte de paquets. Cette analyse doit également inclure l'auto-diagnostic du cloud du fournisseur de SSE afin d'identifier si et quand le saut SSE induit un retard anormal. Enfin, la solution doit fournir un aperçu de l'état de santé de l'appareil de l'utilisateur et identifier les événements de l'appareil responsables de baisses de score **(voir Figure 13)**.

Les fournisseurs de SSE sont particulièrement bien placés pour mesurer et analyser l'expérience de l'utilisateur final grâce à leur présence sur les appareils des utilisateurs et sur le chemin des données de l'application.

Surveillance et dépannage de la qualité des performances de Microsoft Teams et Zoom

Teams et Zoom devenant les principales plateformes de collaboration et de communication de nombreuses entreprises, la mesure et le diagnostic des problèmes de qualité audio/vidéo revêtent une importance encore plus grande. Les solutions de DEM proposées par le fournisseur de SSE doivent être en mesure de s'interfacer avec des applications UCaaS populaires telles que Zoom et Microsoft Teams afin de collecter des mesures de qualité audio et vidéo et de les combiner avec une analyse approfondie, saut par saut, du réseau et des appareils. En combinant ces ensembles de données, la solution DEM doit identifier ceux qui ont des problèmes de qualité et proposer une cause profonde du problème.

En outre, la solution DEM devrait tirer parti de l'échelle du cloud du fournisseur de SSE, en l'utilisant pour servir de proxy aux tests de télémétrie et les mettre en cache, de sorte que des données granulaires puissent être collectées auprès de chaque utilisateur final, toutes les quelques minutes, avec un impact minimal sur les applications.

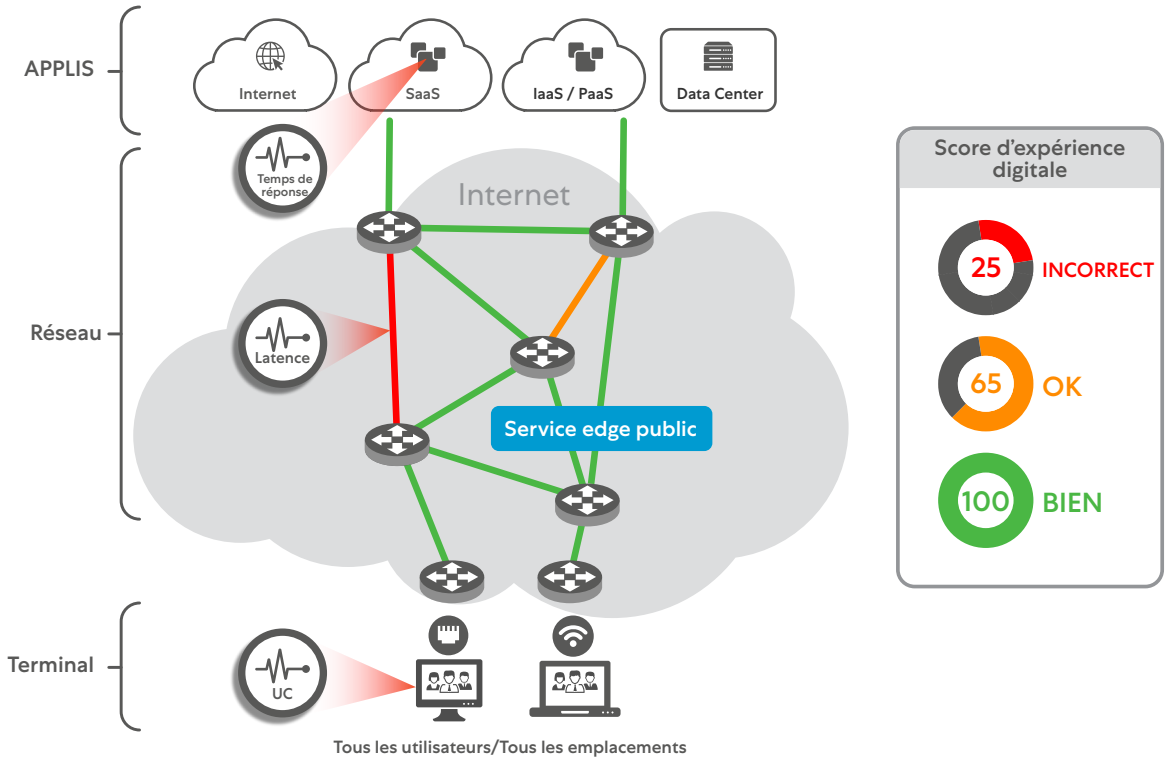

Figure 13 : Une solution de DEM intégrée à la plateforme SSE devrait fournir une visibilité unique sur la qualité de l'expérience utilisateur du point de vue de l'utilisateur final, en révélant les problèmes liés aux appareils, au réseau et aux applications.

Méfiez-vous des outils de surveillance traditionnels qui adoptent une approche de surveillance centrée sur le data center et qui collectent les métriques à partir d'emplacements fixes plutôt que directement à partir de l'appareil de l'utilisateur. Cette approche ne fournit pas une vue unifiée des performances en fonction de l'appareil utilisateur, du chemin d'accès au réseau ou de l'application, et offre une visibilité limitée lorsque les utilisateurs et les applications ne se trouvent pas dans le data center ou sur le réseau de l'entreprise. Ces outils créent des cloisonnements d'informations et ne partagent aucun contexte, ce qui se traduit par une visibilité fragmentée de l'expérience utilisateur et un allongement du temps de dépannage. Les outils de surveillance ponctuels optimisés pour les data centers laissent des lacunes en matière de visibilité pour détecter, dépanner et diagnostiquer les problèmes de performance des utilisateurs finaux sur Internet, alors qu'une solution moderne de DEM intégrée à une plateforme SSE fournit un large éventail de données pour analyser les causes profondes (voir Figure 14).

La solution DEM doit identifier ceux qui ont des problèmes de qualité et proposer une cause profonde du problème.

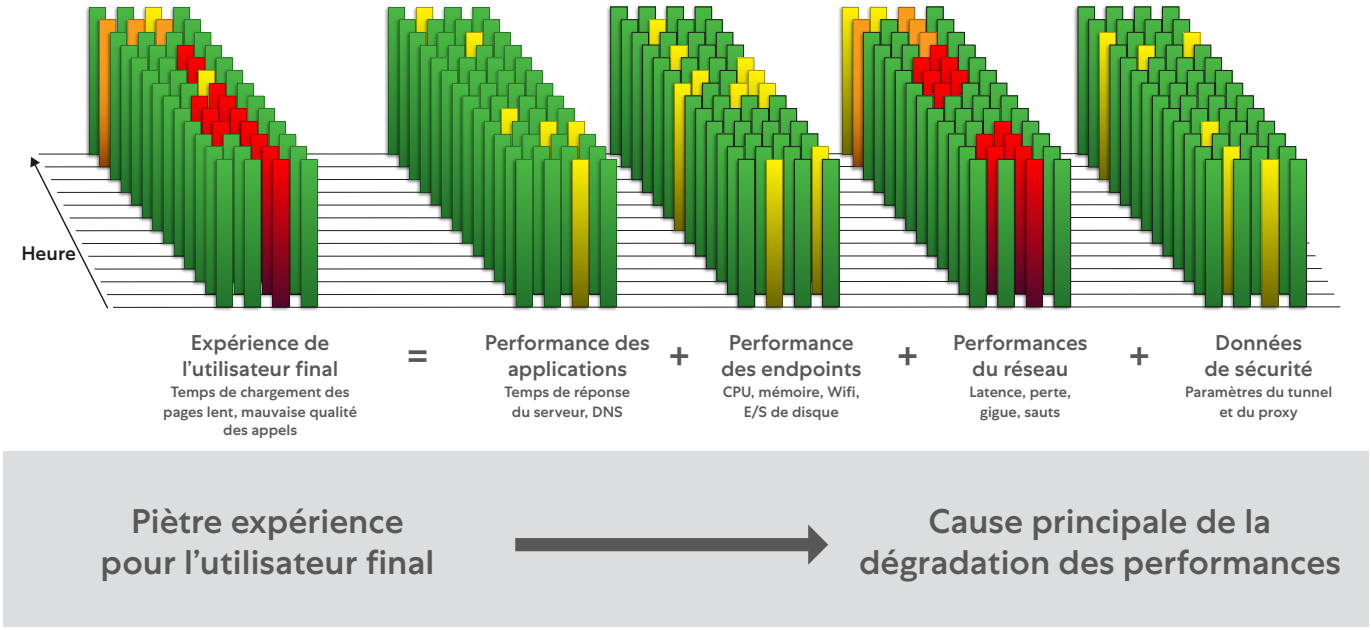

Figure 14 : Une solution de DEM intégrée à la plateforme SSE devrait fournir une visibilité unique sur la qualité de l'expérience utilisateur du point de vue de l'utilisateur final, en révélant les problèmes liés aux appareils, au réseau et aux applications.

Optimiser l'expérience utilisateur de M365

Un SSE complet peut aller au-delà de la mesure et du diagnostic de l'expérience de l'utilisateur final pour optimiser les performances d'applications SaaS populaires comme Microsoft 365. La difficulté réside dans le fait que la plupart des entreprises acheminent le trafic de manière centralisée via des réseaux en étoile et des connexions ExpressRoute. En outre, le trafic utilisateur de M365 augmente de 40 % l'utilisation du réseau. Les infrastructures de sortie Internet de la plupart des sociétés ne sont tout simplement pas adaptées à la tâche, et l'expérience utilisateur en est affectée. Microsoft recommande des connexions Internet directes et une architecture de fournisseur de SSE permettant des sorties Internet locales pour apporter des performances et un coût optimaux.

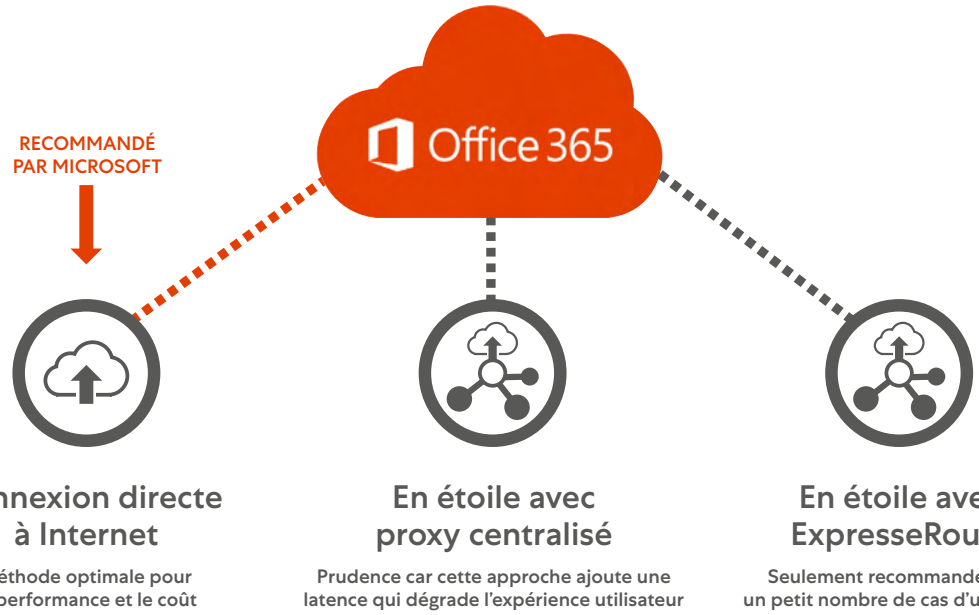

Figure 15 : Microsoft recommande une connexion Internet directe comme méthode optimale en termes de performances et de coûts, conformément aux principes du SSE (source : microsoft.com).

Cependant, l'architecture a son importance. Les points de présence du fournisseur de SSE dans le monde et les relations de peering avec les fournisseurs et les vendeurs d'applications doivent rapprocher la périphérie des utilisateurs pour une connectivité rapide et un accès à faible latence. Recherchez des fournisseurs de SSE qui s'appuient sur une fibre directe vers Microsoft 365 dans la plupart des principaux centres d'échange afin de réduire la latence à environ 1-2 ms aller-retour, de s'adapter au nombre élevé de connexions à longue durée de vie, de permettre un téléchargement rapide de fichiers et de fournir une résolution DNS rapide avec moins de sauts (voir la figure 15).

Il est particulièrement important de sécuriser les transactions M365 avec votre solution SSE, car l'inspection d'applications comme OneDrive et SharePoint est profitable pour la prévention de la perte de données sensibles. Cela fournit également une piste d'audit complète de chaque communication vers et depuis les applications M365. Cependant, sachez que certaines applications M365, comme Teams, ne doivent pas nécessairement être inspectées, étant donné que la majeure partie de ce trafic est constituée de voix/vidéo via UDP.

⚠ À quoi dois-je être attentif ?

Compte tenu de l'essor du mode de travail à distance, il existe de nombreux maillons faibles dans le processus de fourniture de bonnes performances applicatives sur le réseau mondial de réseaux câblés et sans fil. L'optimisation de l'expérience utilisateur est une tâche difficile, même avec une architecture de bonne qualité et des outils dédiés à la mesure et au diagnostic des problèmes d'expérience utilisateur. Il est essentiel de fixer des attentes raisonnables aux utilisateurs finaux sur ce qui constitue une expérience utilisateur acceptable des applications critiques. Il est ensuite vital de se fonder sur ces attentes pour établir des lignes de base à surveiller et à gérer.

Diagnostiquer les problèmes d'expérience utilisateur est plus un art qu'une science. Cela exige d'excellents outils et une excellente architecture, mais cela dépend également des compétences nécessaires pour interpréter les données et agir en conséquence. Alors que les outils DEM proposés par les fournisseurs de SSE mettront en évidence la plupart des causes des problèmes (problèmes de Wi-Fi, de FAI, de backbone, d'appareil ou de DNS), un sous-ensemble nécessitera une augmentation et des ensembles de données supplémentaires. Par exemple, des journaux et des suivis de paquets peuvent être nécessaires pour trouver la cause première. Et il y aura également un sous-ensemble de problèmes qui ne seront pas du tout résolus, ce qui est tout à fait normal.

Méfiez-vous des fournisseurs qui procèdent au hairpining du trafic. Les data centers d'un fournisseur de SSE doivent tous être capables d'effectuer des calculs et des inspections, ce qui assure une expérience utilisateur plus rapide et de meilleure qualité. L'architecture cloud native ne doit pas procéder au hairpining du trafic à quelques emplacements centralisés à des fin d'inspection du trafic. Par exemple, si un utilisateur se connecte à Melbourne, l'inspection du trafic doit se faire localement avec des services de prévention des menaces et de protection des données, et non pas être renvoyée vers d'autres zones comme Sydney ou Singapour. Les fournisseurs de SSE qui font fonctionner leur cloud sur des hyperscalers finissent souvent par procéder au hairpining du trafic utilisateur. Un hyperscaler peut avoir 120 points d'accès, mais 80 % d'entre eux sont probablement de type « on-ramps » qui acheminent le trafic vers un plus petit nombre de data centers hyperscalers où le contrôle de la politique SSE peut être appliqué. Il est important de comprendre combien de data centers sont de type « on-ramps » et combien de data centers peuvent réellement appliquer la politique.

Résultats :

Le succès de toute transformation, qu'elle soit digitale, de réseau ou de sécurité, est conditionné par l'expérience de l'utilisateur final. L'objectif ultime de tout projet SSE est d'améliorer l'expérience de l'utilisateur final tout en réduisant l'exposition aux menaces et en protégeant les données sensibles. Par conséquent, le résultat idéal serait que la capacité d'un fournisseur de SSE à améliorer l'UX puisse être mesurée à l'aide de la capacité DEM. Ce devrait être une tâche aisée, puisque l'abandon du hairpinning au profit d'un data center ou l'abandon des VPN sont des moyens couramment admis pour améliorer l'expérience utilisateur :

- La solution SSE doit moderniser l'expérience utilisateur et mettre à jour l'expérience du service d'assistance. En adoptant une approche proactive de l'expérience utilisateur, le service d'assistance peut réagir avant que les utilisateurs ne se plaignent.
- La solution SSE doit fournir un aperçu des performances audio et vidéo en temps réel pour les plateformes de collaboration comme Teams et Zoom.
- La solution SSE doit collecter des mesures à partir de l'application, de l'appareil et des couches réseau afin de trouver des anomalies et d'en déterminer la cause profonde.
- Le fournisseur de SSE doit fournir un nombre restreint de sauts entre son cloud et des destinations populaires telles que Microsoft 365.

#6 Piège

Choisir une solution SSE dont l'intégration et l'orchestration avec un écosystème de fournisseurs tiers sont limitées

Privilégiez plutôt les fournisseurs de SSE qui présentent les avantages suivants :

- S'intègrent via des API robustes avec les principaux acteurs de l'écosystème (comme les CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) pour garantir une protection et une expérience utilisateur optimales.
- Exploitez ces intégrations pour faciliter l'automatisation et l'orchestration et réduire la complexité opérationnelle et les frais généraux.
- N'alourdissez pas la dette technique en bricolant un portefeuille de solutions dont l'intégration est limitée, tant au sein du portefeuille qu'avec des tiers.

Comment les bons fournisseurs de SSE atteignent ces objectifs :

La plupart des entreprises aux prises avec une dette technique réalisent qu'une grande partie de celle-ci est due à l'acquisition au fil des ans de technologies qui ne sont pas interopérables.

Pire encore, la soi-disant « plateforme » proposée par un seul fournisseur qui n'est pas vraiment intégrée, mais qui est constituée d'une collection de produits ponctuels acquis sans véritable intégration au-delà d'un tableau de bord. Souvent, ces technologies de fournisseurs exigent des compétences spécialisées pour fonctionner et pour maintenir une coexistence fragile avec les technologies qui les accompagnent. Le SSE peut éliminer une grande partie de cette dette technique grâce à une plateforme de sécurité unifiée dans le cloud proposée par un fournisseur unique. Compte tenu de cette vision, le SSE réside toujours au sein d'un écosystème de technologies complémentaires, et les fournisseurs doivent considérer l'interopérabilité avec cet écosystème comme un objectif primordial **(voir Figure 16)**. Cet écosystème se compose essentiellement d'autres solutions de sécurité, de réseau et de cloud.

Figure 16 : Ne vous retrouvez pas perdu avec un fournisseur qui ne dispose pas d'un riche écosystème d'intégrations tierces, car cela engendre une dette technique, une interopérabilité limitée et une pile de sécurité fragile (non agile).

Pour garantir un déploiement et une intégration rapides, faciles et sûrs, le fournisseur de SSE doit proposer des intégrations avec les leaders des domaines suivants :

- Fournisseurs de services cloud (CSP), tant IaaS/PaaS que SaaS
- Détection et réponse aux terminaux (EDR)
- SD-WAN
- Gestion de l'identité et de l'accès (IAM)
- Gestion de l'information et des événements de sécurité (SIEM)/Orchestration de la sécurité, automatisation et réponse (SOAR)
- Outils d'orchestration

Ces intégrations doivent permettre l'orchestration entre le fournisseur de SSE et les fournisseurs adjacents afin de réduire la complexité, le coût total de possession et d'améliorer la posture de sécurité (voir Figure 17).

Fournisseurs de services cloud (IaaS/PaaS et SaaS)

Pour les applications internes qui se déplacent vers le cloud ou qui sont construites nativement dans le cloud, le fournisseur SSE doit intégrer les principaux fournisseurs IaaS/PaaS tels que AWS, GCP et Azure pour fournir une connectivité d'accès à distance sécurisée Zero Trust à ces applications. Ainsi, ces applications ne sont jamais exposées sur Internet, ce qui les rend totalement invisibles pour les utilisateurs non autorisés, qui se connectent au moyen d'une connectivité de l'intérieur vers l'extérieur basée sur des politiques, au lieu d'étendre le réseau jusqu'à elles.

Cette approche garantit un accès direct au cloud sans passer par un accès distant VPN, avec la possibilité d'exploiter les avantages d'échelle du fournisseur de cloud sans ajouter aucune complexité de segmentation du réseau. Elle ne repose sur aucune appliance virtuelle ou physique et offre les avantages de Zero Trust pour éliminer la surface d'attaque.

Pour les applications SaaS les plus populaires, les fournisseurs de SSE doivent proposer des intégrations en un clic. Dans le cas de Microsoft 365, l'intégration du fournisseur de SSE doit mettre en correspondance toutes les plages d'adresses IP et tous les domaines Microsoft pour les applications M365 répertoriées, ce qui permet de transférer de manière transparente le trafic des utilisateurs finaux vers leur cloud. En outre, l'appairage avec Microsoft 365 réduit le temps d'aller-retour, améliore l'évolutivité et permet des téléchargements de fichiers et une résolution DNS plus rapides.

L'intégration SSE avec d'autres fournisseurs de SaaS comme ServiceNow peut améliorer la protection des données. En analysant les données ServiceNow nouvelles et existantes, le fournisseur de SSE doit identifier les données sensibles sur la base des politiques DLP et bloquer le téléchargement sortant de fichiers contenant des données sensibles. L'intégration avec ServiceNow Security Incident Response peut orchestrer les actions de réponse, y compris la mise à jour des listes de blocage personnalisées. Les adresses IP, domaines et URL risqués peuvent être bloqués sans intervention manuelle, tandis que les erreurs de configuration du cloud peuvent être clôturées pour aider à réduire le risque de violation.

Détection et réponse des endpoints

Le fournisseur SSE doit s'intégrer à divers partenaires de sécurité des endpoints afin de partager la télémétrie, d'améliorer la visibilité mutuelle et d'orchestrer les réponses. Une telle intégration permet une défense en profondeur pour une mise en œuvre efficace de Zero Trust.

Cette intégration doit permettre d'évaluer l'identité de l'utilisateur, son emplacement et la position de l'appareil afin de mettre automatiquement en œuvre les politiques d'accès conditionnel appropriées. En outre, la corrélation et le flux de travail multiplateforme peuvent accélérer l'enquête et la réponse. Cela implique les actions suivantes :

- Évaluer l'intégrité des appareils et mettre automatiquement en œuvre les politiques d'accès appropriées
- Identifier les menaces de type zero-day et établir une corrélation avec la télémétrie des endpoints afin d'identifier les appareils touchés et mettre en œuvre des réponses rapides grâce à un flux de travail de mise en quarantaine multiplateforme
- Examiner les menaces en tenant compte du contexte des endpoints et du réseau pour une détection et une prise de décision efficaces

SD-WAN

Le fournisseur de SSE doit s'intégrer aux fournisseurs SD-WAN pour simplifier l'acheminement du trafic depuis la filiale et faciliter l'établissement de points d'accès Internet locaux sécurisés.

Une solution conjointe SSE/SD-WAN peut permettre un accès sécurisé et basé sur des politiques à Internet et aux applications critiques pour l'entreprise, et fournir une protection identique à tous les utilisateurs, indépendamment du lieu et du moment où ils se connectent aux applications cloud et à Internet. Les solutions SD-WAN peuvent être intégrées au SSE par le biais d'une intégration API. Avec cette solution combinée, les filiales des entreprises peuvent gérer l'augmentation du trafic Internet et cloud, sans backhauling de la DMZ centralisée du data center, en utilisant une architecture WAN hybride pour la transformation du réseau et une sécurité renforcée.

Il faut souligner que tout fournisseur de SSE doit être indépendant vis-à-vis du réseau et ne pas être lié exclusivement à une solution de réseau sous-jacente. En réalité, bon nombre des avantages du SD-WAN proviennent de ses capacités « définies par logiciel », mais pas nécessairement du WAN, qui par nature étend le réseau de l'entreprise et permet le déplacement latéral des menaces. Les décideurs du SSE doivent soigneusement évaluer les raisons de continuer à étendre le réseau de l'entreprise à la filiale et envisager d'autres approches (comme uniquement Internet) qui sont plus sûres.

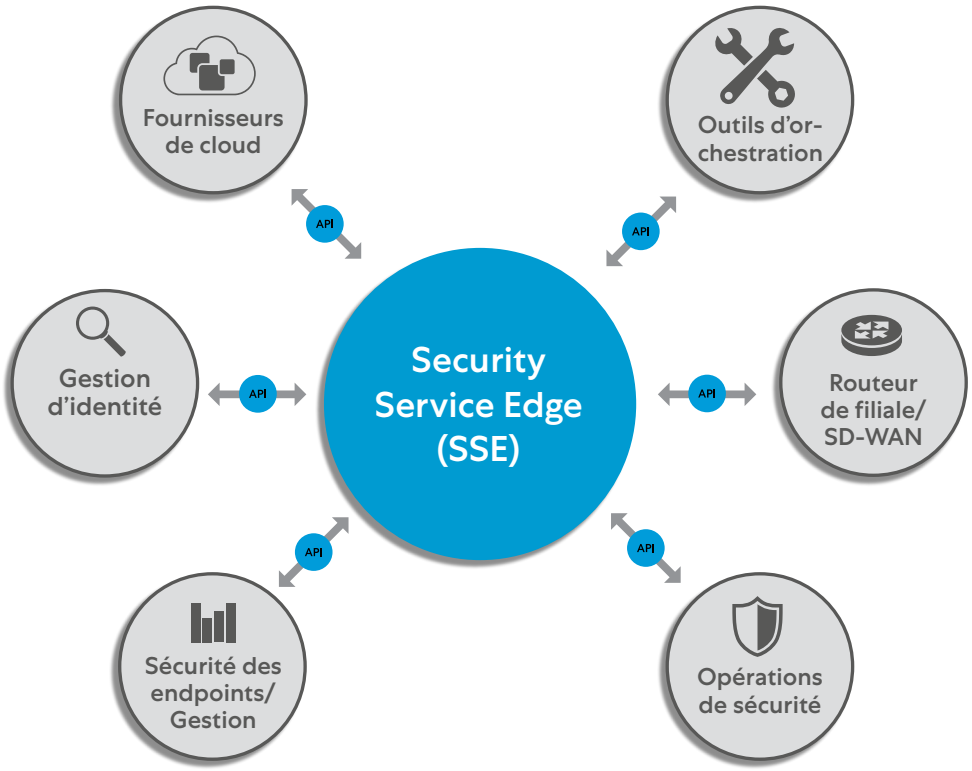

Figure 17 : Les fournisseurs de SSE devraient s'intégrer avec les meilleurs acteurs du marché pour diverses fonctions.

Gestion de l'identité et de l'accès

Les fournisseurs de SSE devraient proposer des intégrations avec les IAM afin de mettre en œuvre un accès Zero Trust basé sur la posture du dispositif et une protection plus efficace contre les menaces à l'échelle de l'entreprise.

Le déploiement de l'intégration devrait être simple grâce à des normes telles que SAML (Security Assertion Markup Language). Les utilisateurs devraient pouvoir s'authentifier et sécuriser l'accès aux applications Internet et internes. L'IAM gère l'accès de l'utilisateur final aux applications par une combinaison d'authentification unique (SSO) et d'authentification multi-facteur (MFA), tandis que le fournisseur SSE sécurise la connexion. La prise en charge du protocole SCIM (System for Cross-domain Identity Management) permet de synchroniser toutes les informations relatives aux utilisateurs entre les deux systèmes, y compris les changements de groupe d'utilisateurs ou de rôle et la suppression des comptes des utilisateurs qui quittent la société.

SIEM et SOAR

Les fournisseurs SSE doivent prévoir des intégrations avec les fournisseurs SIEM et SOAR afin de permettre une gestion efficace des risques et de la conformité grâce à l'enrichissement et à l'automatisation des informations.

Les fournisseurs de SSE doivent être en mesure d'envoyer des données de journalisation en temps quasi réel à des solutions SIEM/SOAR sur site et dans le cloud pour faciliter la corrélation des journaux provenant de plusieurs sources, permettant ainsi aux entreprises d'analyser les modèles de trafic sur l'ensemble de leurs réseaux. En outre, les entreprises doivent être en mesure d'exploiter les données des journaux dans le SIEM pour effectuer des analyses historiques étendues (> 6 mois). Cela garantit le respect des obligations réglementaires grâce à l'archivage local des journaux.

Outils d'orchestration

Comme l'infrastructure en tant que code (IaC) et DevSecOps forcent les équipes de sécurité à effectuer un « Shift-Left » (travail plus en amont), les fournisseurs SSE doivent fournir les API pour l'orchestration. Ici, l'accent est mis sur les applications internes où l'instanciation de l'accès Zero Trust fait partie du cycle de vie de livraison de l'application, activé par des scripts d'orchestration (tels que Ansible ou Terraform), en particulier pour les paramètres de segmentation utilisateur-application ou charge de travail-charge de travail. Ce type d'orchestration permet aux capacités de Zero Trust de s'aligner sur les méthodes agiles utilisées par les développeurs de logiciels.

Comme l'infrastructure en tant que code (IaC) et DevSecOps forcent les équipes de sécurité à effectuer un « Shift-Left », les fournisseurs SSE doivent fournir les API pour l'orchestration.

⚠ À quoi dois-je être attentif ?

Les décideurs du SSE doivent évaluer la profondeur des intégrations d'API, la fréquence des mises à jour et surveiller les changements sur le marché susceptibles d'entraver les intégrations futures (par exemple, un fournisseur qui devient un concurrent). Soyez conscient de la pénurie éventuelle de compétences au sein de votre entreprise, car la mise en œuvre de ces intégrations, en particulier avec les outils traditionnels, nécessitera des qualifications spécialisées.

Résultats :

Les fournisseurs de SSE qui proposent des intégrations tierces étoffées, basées sur des API, apportent des gains d'efficacité opérationnelle découlant de la capacité à orchestrer les meilleures solutions du marché et réduisent les risques de dépendance vis-à-vis des fournisseurs :

- Les fournisseurs de SSE qui intègrent les principaux acteurs de l'écosystème (comme les CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) pérennisent leur technologie et réduisent la dette technique.
- Un écosystème orchestré de fournisseurs intégrés réduit la complexité opérationnelle, les frais généraux et peut diminuer les erreurs des opérateurs.
- Les fournisseurs SSE qui bricolent un portefeuille de solutions par le biais d'acquisitions ont tendance à prendre du retard dans l'innovation des produits et manquent souvent d'interopérabilité avec des tiers.

#7 Piège

Choisir une solution SSE qui ne peut pas facilement démontrer sa valeur dans un environnement de production pilote.

Privilégiez plutôt les fournisseurs de SSE qui présentent les avantages suivants :

- Pilotent leur solution de manière transparente avec un seul agent unifié, un accès à un ensemble global de services (à proximité de l'utilisateur), avec une interface utilisateur centralisée et conviviale.
- Pilotent les nombreux aspects de la plateforme SSE avec des exigences de déploiement supplémentaires minimales.
- Donnent l'assurance que leur solution fonctionnera comme prévu lors du déploiement complet, avec un minimum de travail après-vente.

Figure 18 : Veillez à ce que le fournisseur de SSE effectue ses pilotes avec la vraie solution et non avec une réplique. Seul un essai pilote dans un environnement de production peut prouver la valeur de la solution du fournisseur de SSE.

Comment les bons fournisseurs de SSE assurent cela :

En adoptant une plateforme SSE, vous devez repenser votre architecture de sécurité. La sélection d'un fournisseur de SSE ne doit donc pas être prise à la légère. Il est donc essentiel d'appréhender la capacité réelle du fournisseur de SSE à travailler dans votre environnement de production. La facilité de mise en œuvre est représentative de l'architecture de la plateforme.

Lorsque vous évaluez les fournisseurs de SSE, comprenez les étapes nécessaires à l'exécution d'un pilote. Pour les bons fournisseurs de SSE, le processus devrait consister à trouver un moyen de transférer le trafic vers le service edge du SSE, après quoi le propre cloud du fournisseur de SSE prend le relais. L'administrateur du SSE ne devrait avoir qu'un minimum d'étapes à suivre, outre l'établissement d'un mécanisme de transfert, la configuration des politiques de base, l'authentification et le reporting. Il va de soi que les configurations de politiques avancées prendront plus de temps.

Le pilote doit répondre à un ensemble de résultats commerciaux et impliquer des membres de diverses équipes, notamment la sécurité, le réseau et le bureau (pour l'installation des agents d'endpoint, par exemple). Cependant, l'implication active de ces équipes doit être minimale : après tout, elles cherchent à acquérir une solution SaaS. Les fournisseurs de SSE qui requièrent une implication importante, en particulier de la part des équipes de mise en réseau pour gérer des scénarios de routage complexes dans un pilote, doivent vous mettre sur vos gardes.

Adoptez une approche séquentielle qui reflète vos objectifs commerciaux lors de la planification d'un pilote complet de solution SSE :

1. Examinez la posture de sécurité existante, les politiques en vigueur, l'infrastructure réseau et les exigences des applications, la technologie d'authentification, les options de transfert de trafic et la capacité.
2. Identifiez un ensemble d'utilisateurs/services sources et un ensemble d'applications de destination sur lesquels exécuter le pilote.
3. Activez la redirection du trafic pour ces utilisateurs, le plus souvent avec un agent unique, mais notez que la création de tunnels à partir d'une filiale est également possible ; déployez une ou plusieurs machines virtuelles devant les applications privées choisies.
4. Paramétrez l'authentification des utilisateurs en provisionnant l'intégration du fournisseur d'identité.
5. Paramétrez la prévention des menaces et de la perte de données à l'aide de modèles standard, notamment la protection contre les menaces, les politiques de sandbox, les politiques de contrôle du navigateur, les politiques d'URL, les politiques d'applications cloud, le contrôle du type de fichier, l'intégration des API pour les SaaS et les politiques de pare-feu.
6. Paramétrez la découverte du serveur pour les applications privées et la politique d'accès pour ces applications. Il peut s'agir d'une politique *.* pour les besoins du pilote.
7. Paramétrer l'inspection SSL/TLS, les politiques avancées et les capacités supplémentaires telles que CBI, DEM ou CSPM.

Toutes les étapes ci-dessus doivent être simples et réalisables par le fournisseur de SSE en peu de temps (en général quelques jours) et sans modification majeure du routage ni de la configuration. Alors que le déploiement complet réel exigera d'autres étapes, des paramètres de politique avancés, la gestion de divers types d'applications et d'endpoints, tout comme des intégrations et une coexistence avec d'autres agents/technologies, le fournisseur de SSE doit être en mesure de démontrer la valeur de la plateforme par le biais d'un pilote simple, mais bien exécuté.

Au cours de ce pilote, le fournisseur de SSE doit être en mesure de prouver ce qui suit, en s'alignant sur les six pratiques précédentes détaillées dans ce document :

- **Une infrastructure de cloud mondial avec une latence minimale pour l'utilisateur final, qui garantit une disponibilité et des performances élevées.** Le fournisseur doit démontrer sa capacité à exploiter ce cloud à grande échelle et à démontrer l'effet du basculement.
- **Zero Trust pour chaque session utilisateur**, depuis la protection des applications privées, des applications publiques et même des communications entre charges de travail (si le pilote le prévoit).
- **Une protection contre les menaces avancées et une DLP avancée en accédant au trafic chiffré**. La gestion des certificats peut nécessiter quelques étapes supplémentaires dans le pilote, mais démontrer la capacité du fournisseur à effectuer une inspection SSL/TLS avec une latence minimale constitue un excellent moyen de différencier un fournisseur SSE d'un autre.
- **Des options de déploiement flexibles**. Bien que cela ne fasse pas partie du pilote, le fournisseur de SSE doit fournir un plan de protection de tous les utilisateurs, indépendamment de leur emplacement ou de l'application. Cela peut exiger une compréhension du déploiement de service edges privés ou de CBI pour les entrepreneurs. Le point essentiel à vérifier est la capacité du fournisseur de SSE à répondre aux besoins d'un personnel et d'applications distribués avec ses modèles de déploiement.

- **Une expérience utilisateur optimale**. Cette métrique comprend aussi bien la facilité d'utilisation (comment l'utilisateur final s'interface-t-il avec son agent, par exemple) que l'expérience générale de l'utilisateur qui accède aux applications publiques et privées sur sa plateforme SSE. Le fournisseur doit être capable de mesurer et de diagnostiquer un large éventail de problèmes de performance de l'utilisateur final (Wi-Fi, FAI, CPU, etc.). Cette capacité de mesure/diagnostic doit être intégrée directement dans la plateforme SSE sans qu'il soit nécessaire de déployer de nouveaux agents.
- **L'intégration de fournisseurs tiers**. Bien que cela ne fasse pas non plus partie du pilote, le fournisseur doit proposer des méthodes d'intégration des données de journalisation dans un outil SIEM externe ou une intégration avec un outil EDR en place. Le fournisseur de SSE doit analyser l'écosystème d'outils existant et fournir des recommandations pour l'intégration une fois le déploiement commencé.

Privilégiez les fournisseurs de SSE qui imposent le moins moyens additionnels, étant donné la pénurie de compétences et de personnel à laquelle le secteur est confronté.

L'avantage de s'adresser à un fournisseur de sécurité SaaS est de pouvoir lui confier des tâches qui incombent généralement aux équipes en interne. Le pilote devrait donner une indication claire de la quantité de moyens nécessaires pour déployer, gérer et mettre à jour la solution SSE.

⚠ À quoi dois-je être attentif ?

- Les pilotes ne peuvent pas tester toutes les possibilités, et des problèmes imprévisibles peuvent survenir lors d'un déploiement concret.
- Vérifiez que le fournisseur de SSE est centré sur le client et qu'il manifeste la volonté de surmonter les problèmes de déploiement qui se présentent.
- Rappelez-vous que vous ne verrez probablement pas l'évolution dans un pilote et que vous ne verrez peut-être pas les choses se détériorer. Les fournisseurs de SSE peuvent éviter les problèmes de réseau ou de routage pendant le pilote, problèmes qui pourraient n'apparaître qu'au moment du déploiement. Le bon fournisseur de SSE doit être celui qui ne dépend d'aucune route de réseau pour fonctionner.
- Tenez compte de la charge de travail imposée par la gestion : qu'est-ce qui vous appartient et qu'est-ce qui appartient au fournisseur de SSE ? Calculez le travail nécessaire pour un déploiement de production, ainsi que pour la maintenance continue de la solution.
- Certains fournisseurs de SSE peuvent ne pas être de véritables SaaS. Assurez-vous que la gestion de la solution de SSE présente le coût total de possession le plus bas, ce qui est particulièrement important compte tenu de la pénurie de compétences à laquelle sont confrontées la plupart des entreprises informatiques.

Résultats :

Un pilote efficace prouvera que la solution SSE est facile à déployer, qu'elle fonctionne dans votre environnement de production et qu'elle répond à vos objectifs.

- Les fournisseurs de SSE qui peuvent piloter leur solution de manière transparente sont un bon signe pour les déploiements complets. L'objectif étant un faible coût total de possession, un agent unifié unique, l'accès à un ensemble global de service edges, ainsi qu'une interface utilisateur centralisée et facile à utiliser, sont autant d'éléments qui facilitent la maintenance continue de la solution. Tout déploiement à grande échelle nécessitera du temps et des moyens, mais l'objectif devrait être de travailler avec le fournisseur qui réduira ces facteurs.
- L'architecture et la conception d'un SSE doivent permettre d'ajouter facilement des fonctionnalités avec un minimum d'exigences supplémentaires en matière de déploiement (comme par exemple des agents ou des VM supplémentaires). Ainsi, les acheteurs peuvent adopter une approche progressive du SSE, conscients que le passage d'une phase à l'autre ne nécessitera pas de lourds investissements.
- En fin de compte, l'objectif est de pouvoir compter sur le fournisseur de SSE pour un déploiement fluide dans un environnement de production et de le savoir à vos côtés en cas de problèmes inévitables. Les fournisseurs orientés client et dotés d'une architecture éprouvée sont vos meilleurs indicateurs de la performance de votre investissement dans la transformation de la sécurité et du réseau.

Ne nous croyez pas sur parole.

Les périodes de rupture qui permettent aux entreprises d'investir brusquement dans une nouvelle voie sont très rares. C'est pourquoi les entreprises doivent envisager une approche réfléchie du SSE. Le champ d'application du SSE en entreprise (tel que partagé publiquement sur https://trust.zscaler.com), qui concerne tous les utilisateurs, serveurs, appareils, etc. possibles, est décrit dans le Piège n° 2. Vous trouverez ci-dessous comment vos homologues ont abordé l'adoption du SSE :

Référence A :

Le client a déployé la plateforme SSE de Zscaler pour un contrôle Zero Trust de :

- L'accès granulaire de l'utilisateur final aux services privés.
- La sécurité Internet de l'utilisateur final, y compris l'inspection en ligne et la protection des données.
- La transformation du réseau avec des utilisateurs totalement retirés du réseau.
- La protection des charges de travail, d'Internet et de l'accès privé.
- Le contrôle limité de l'accès des tiers.

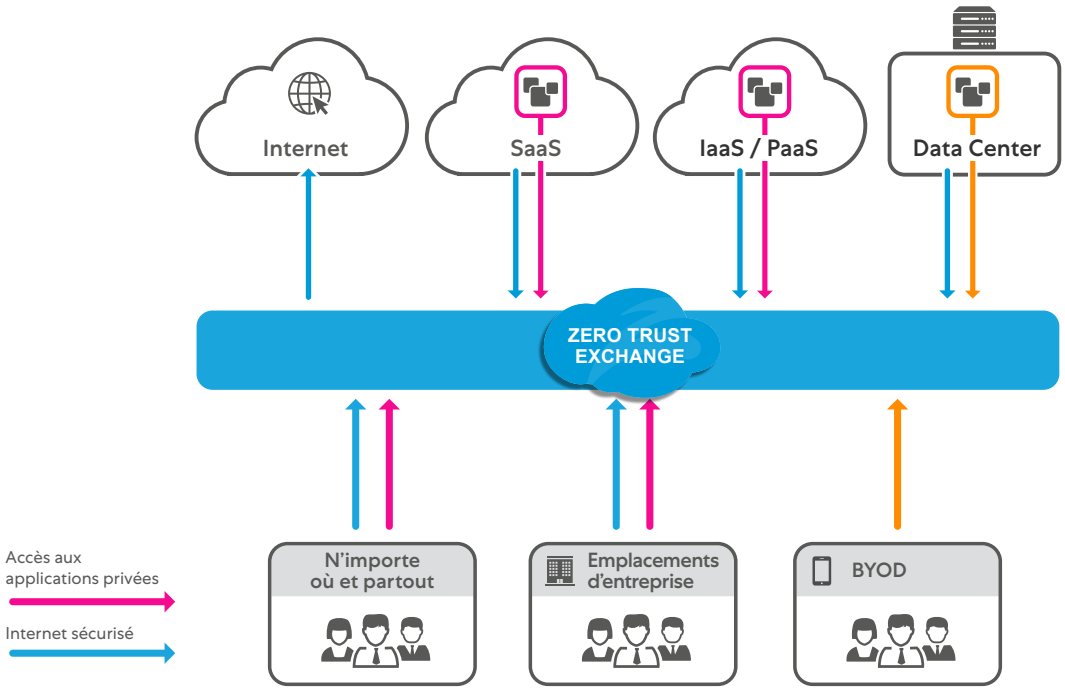

Figure 19 : Représentation détaillée de la connectivité déployée par l'entreprise avec Zscaler.

« En moins de cinq jours, nous avons effectué une transition en douceur, en toute sécurité et à moindre coût de 20 000 employés vers le télétravail en remplaçant les VPN par la solution d'accès réseau Zero Trust (ZTNA) de Zscaler. »

Michael Alvmarken, directeur de service pour la cybersécurité et la technologie, groupe Sandvik

« L'exploitation de l'infrastructure cloud de Zscaler et des intégrations natives avec ZIA et ZPA nous a apporté de meilleures informations sur nos utilisateurs finaux. »

John Dawes, directeur de l'architecture d'entreprise, Reckitt Benckiser

« En passant directement par Internet au lieu de faire un backhauling de notre trafic, nous espérons réduire nos coûts de 70 %. »

Frederik Janssen, vice-président du portefeuille d'infrastructures informatiques mondiales, SIEMENS.

Référence B :

- Le client a déployé la plateforme SSE de Zscaler pour :
- Une visibilité complète de l'accès à tous les services Internet (cloud et au-delà).
- Un contrôle in-line complet pour limiter la perte de propriété intellectuelle de l'entreprise.
- La surveillance de l'expérience digitale de l'accès des utilisateurs durant le télétravail.

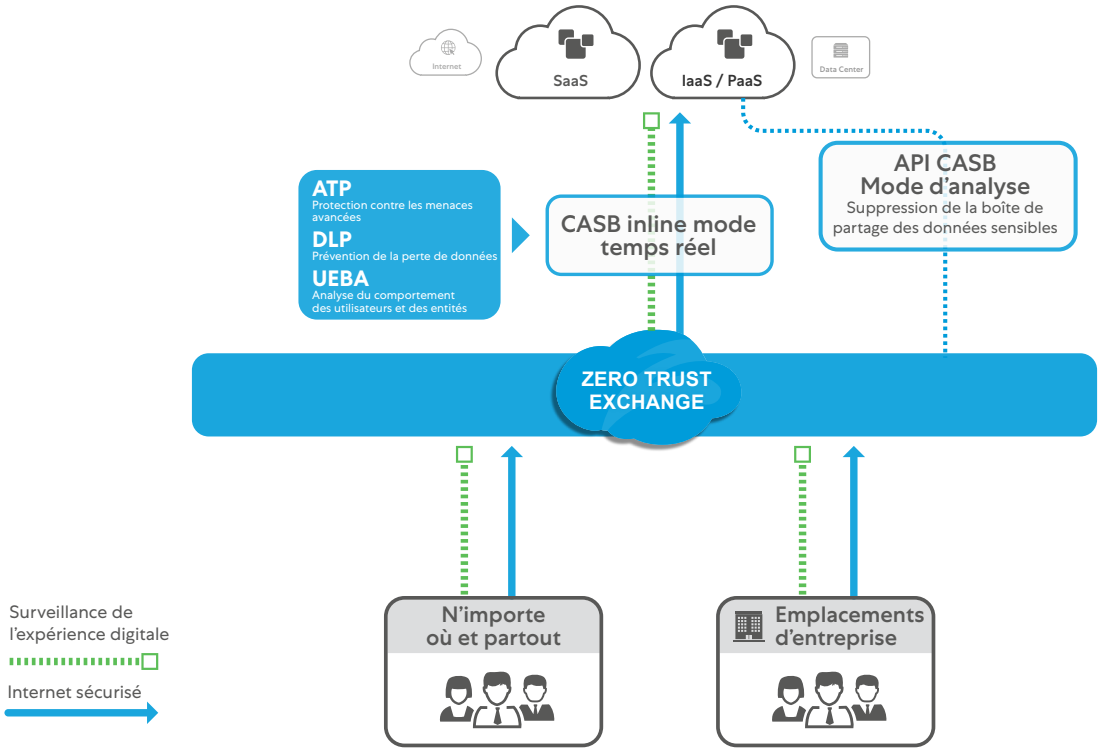

Figure 20 : Exemple de contrôle in-line et de surveillance de l'expérience avec Zscaler.

ciena

« Nous considérons Zscaler Digital Experience comme un service essentiel pour permettre une expérience productive de télétravail. Dans le passé, nous étions heureux de résoudre 25 % des problèmes des utilisateurs. Désormais, avec ZDX, nous sommes capables de résoudre tous nos problèmes d'expérience utilisateur, et nous pouvons en identifier la cause profonde dans 95 % des cas. »

Ed DeGrange, architecte principal de la sécurité, Ciena

SIEMENS

« Qu'il s'agisse d'un problème de commerce ou de fraude, un incident sur le site Web ou une fraude interne, tout a un impact financier, et c'est pourquoi la sécurité est indispensable. »

Frederik Janssen, vice-président du portefeuille d'infrastructures informatiques mondiales, SIEMENS.

BOMBARDIER

« Avec Zscaler Advanced Cloud Sandbox, il n'y a pas de lourde charge pour le service informatique, ce qui est crucial car de nos jours, le marché des talents est si restreint que le recrutement devient extrêmement difficile. »

Mark Ferguson, RSSI, Bombardier

Référence C :

Le client a assuré la protection granulaire de services non informatiques à l'aide de la plateforme Zscaler :

- Zero Trust pour la technologie d'exploitation (OT), tant pour les employés que pour les tiers.
- OT vers charge de travail
- Du cloud à la charge de travail.

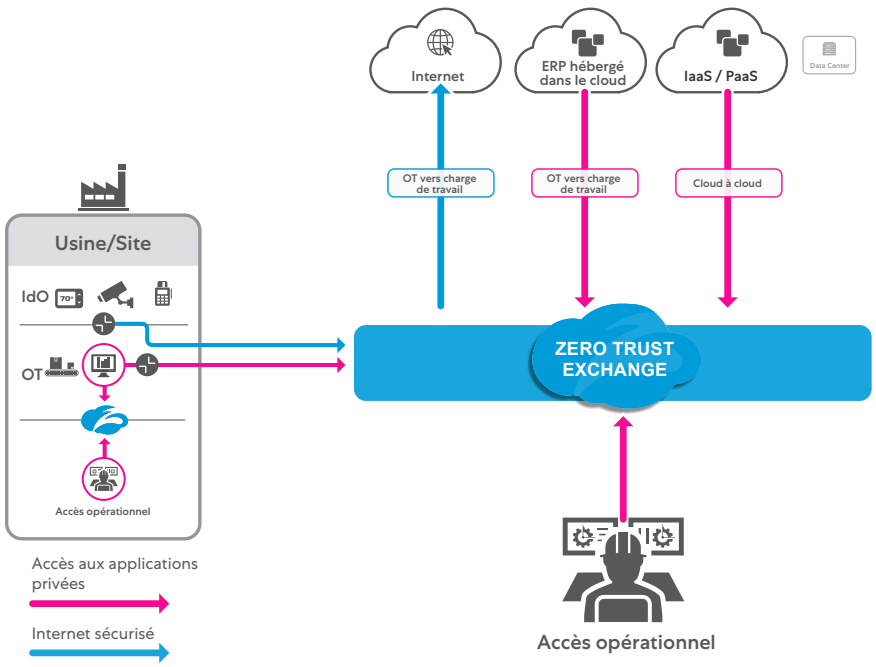

Figure 20 : Exemple de contrôle in-line et de surveillance de l'expérience avec Zscaler.

Points importants à retenir

- ☐ Le fournisseur SSE doit proposer un accord de niveau de service documenté basé sur la perte ou la dégradation du service.
- ☐ La solution SSE doit proposer une mise en application sur tous les sites : in-line, à l'échelle mondiale et au sein de points d'échange neutres vis-à-vis des opérateurs, garantissant le chemin le plus efficace aux clients.
- ☐ Le fournisseur de SSE doit proposer des contrôles Zero Trust pour tous les utilisateurs, charges de travail et appareils autorisés de l'entreprise, quel que soit le protocole.
- ☐ La solution SSE doit fournir un service de manière indépendante sur n'importe quel réseau.
- ☐ Le fournisseur SSE doit fournir son inspection in-line par le biais d'une architecture cloud proxy garantissant une latence minimale et permettant une visibilité totale sur l'ensemble du trafic Web (jusqu'à et y compris TLS 1.3).
- ☐ La solution SSE doit fournir différents contrôles de sécurité par le biais d'une architecture unique d'analyse de la mémoire afin de bénéficier d'avantages exclusifs en matière d'évolutivité pour le déchiffrement à grande échelle.
- ☐ Le fournisseur SSE doit proposer sa solution sous une forme gérée de manière centralisée et pouvant être déployée de différentes manières afin de tenir compte de l'emplacement du client, de sa région, de sa localité et de la personnalisation des fonctions.
- ☐ La solution SSE doit être étendue de manière à fournir une protection des BYOD (appareils personnels utilisés à des fins professionnelles) non gérés, tiers et partenaires avec le même niveau de contrôle granulaire que pour les employés.
- ☐ Le fournisseur SSE doit optimiser l'expérience utilisateur en surveillant et en diagnostiquant les problèmes de performance des services d'entreprise (Teams, Zoom, etc.).
- ☐ La solution SSE doit recueillir des mesures à partir des chemins d'application, des endpoints et des couches réseau afin d'identifier les anomalies et fournir des informations aux équipes d'assistance.
- ☐ Le fournisseur SSE doit s'intégrer avec les meilleurs acteurs de l'écosystème (tels que les CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.), apportant un contrôle et une sécurité complets et approfondis à l'ensemble du paysage de l'entreprise.
- ☐ La solution SSE doit être intégrée à ces fournisseurs afin de fournir une orchestration qui réduira au minimum les coûts opérationnels.
- ☐ Les fournisseurs de SSE doivent pouvoir piloter de manière transparente les fonctions et les emplacements nécessaires à la production de l'entreprise.
- ☐ La solution de SSE doit être aisément extensible sans nécessiter de matériel ou d'agents supplémentaires, ce qui permet aux entreprises de développer leur utilisation du SSE par une approche progressive.

Pour en savoir plus sur le SSE, consultez Zscaler SSE 2022

À propos des auteurs

Sanjit Ganguli (VP, Stratégie de transformation/Directeur technique de terrain) et Nathan Howe (VP, Technologie émergente et 5G), dont les carrières se sont déroulées dans le monde entier au sein d'entreprises telles que Gartner, Nestlé, Riverbed et Verizon, apportent un leadership et une vision innovante sur le cloud, la sécurité, la transformation et les technologies émergentes.