E-Book

Les principaux cas d'utilisation de la protection des données SSE

Comment stopper les violations de données dans le monde professionnel actuel avec Zscaler SSE

Contenu

E-Book

L’essor du SSE

Les utilisateurs et les applications des entreprises se trouvaient autrefois tous sur site. Cette configuration a débouché sur une sécurité cloisonnée via des appliances coûteuses qui constituaient des périmètres de réseau destinés à protéger les données en leur sein.

Avec le cloud, le Web et le télétravail, le périmètre a disparu, mais nombreux sont ceux qui s’appuient encore sur des architectures cloisonnées. Les empilements complexes des appliances ne peuvent hélas pas répondre aux besoins modernes de protection des données. Le backhauling du trafic induit également de mauvaises performances, limite l’évolutivité et entrave la productivité des utilisateurs.

De nombreux outils modernes de protection des données ne sont pas non plus à la hauteur, notamment lorsqu’ils se concentrent sur les menaces internes et négligent les menaces externes pesant sur les données. En d’autres termes, une bonne protection des données doit être assortie d’une sécurité robuste.

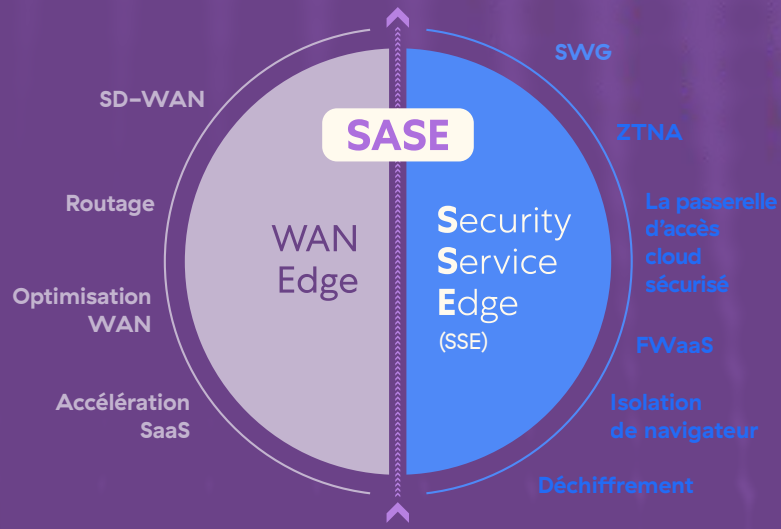
Le Security Service Edge (SSE) constitue la solution à ces défis. Il s’agit de plateformes complètes qui réduisent la complexité et comblent les lacunes de la protection moderne des données en intégrant CASB, SWG, ZTNA, et plus encore. Grâce à la sécurité fournie dans le cloud à la périphérie, le SSE apporte des performances, une évolutivité et une expérience utilisateur optimales.

Zscaler Zero Trust Exchange™, le plus grand cloud de sécurité au monde, a été conçu pour sécuriser toute transaction bien avant la création du SSE. Il bloque tous les risques liés aux données, qu’ils proviennent de l’intérieur ou de l’extérieur.

Poursuivez votre lecture pour découvrir les témoignages de clients qui utilisent notre SSE pour protéger leurs données.

Politique de sécurité cohérente

Protection des données et contre les menaces



Expérience utilisateur cohérente

Accès Zero trust

Assurer une sécurité Zero Trust

Les outils de sécurité traditionnels accordent un accès illimité au réseau dans son ensemble (et à toutes les données et applications qu'il contient). Mais cela facilite le déplacement latéral des menaces entre les ressources, ce qui peut amplifier les incidences des violations de données. Cela déroge également au principe de Zero Trust du moindre privilège, selon lequel les utilisateurs autorisés n'ont accès qu'aux ressources dont ils ont besoin, au moment où ils en ont besoin.

Zero Trust Exchange

Zero Trust Exchange adopte une approche fondamentalement différente et garantit une protection moderne des données basée sur le concept de Zero Trust. En agissant comme un tableau de distribution intelligent entre les utilisateurs, les applications SaaS, les applications privées, l'IoT/OT, et plus encore, Zscaler prolonge l'accès sécurisé uniquement aux ressources individuelles selon les besoins, tout en appliquant des mesures de prévention de la perte de données (DLP) pour une plus grande granularité.

Ce que Zscaler vous apporte

- Dissimule toutes les ressources informatiques derrière Zero Trust Exchange afin d'éliminer la surface d'attaque.
- Empêche le déplacement latéral des menaces en connectant les utilisateurs directement aux applications, et non au réseau.
- Empêche toute compromission en sécurisant l'ensemble des transactions utilisateur–application, application–application et machine–machine.

Prévenir la perte de données via le trafic chiffré

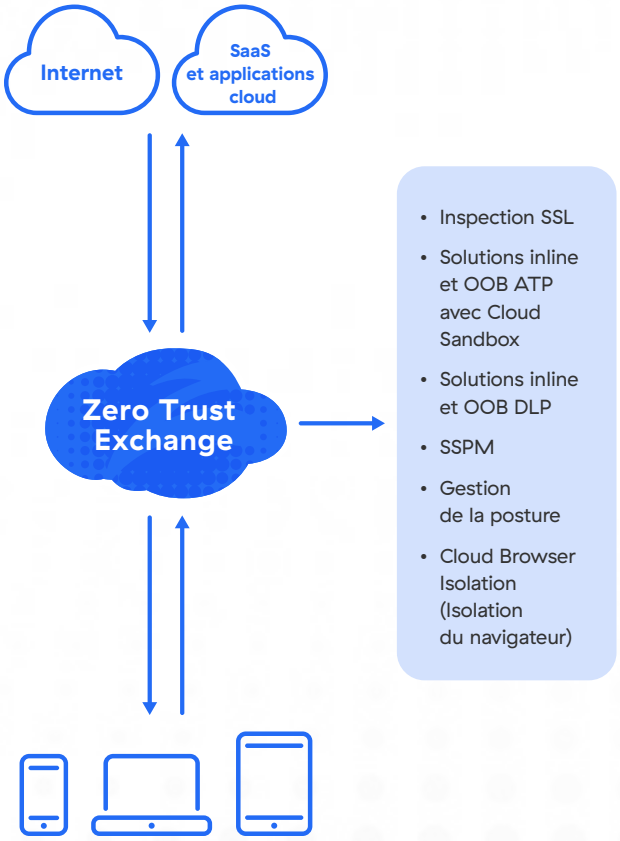
Les appliances de sécurité traditionnelles (qu'elles soient matérielles ou virtuelles) servent souvent à inspecter le trafic Web pour déceler les pertes de données. Cependant, elles disposent de capacités fixes pour desservir les utilisateurs, ne peuvent pas gérer le trafic chiffré à grande échelle et, par conséquent, n'assurent que peu ou pas d'inspection SSL. Plus de 95 % du trafic Web étant désormais chiffré, il s'agit d'une dangereuse faiblesse.

Une véritable architecture cloud

Reposant sur le plus grand cloud de sécurité au monde, le Security Service Edge de Zscaler se targue des performances nécessaires pour inspecter le trafic chiffré à l'échelle de sociétés internationales comptant des centaines de milliers d'utilisateurs. Cela garantit la détection et la correction en temps réel de toute perte de données potentielle dissimulée par SSL.

Ce que Zscaler vous apporte

- Un Security Service Edge doté d'une évolutivité et de performances inégalées qui traite plus de 200 milliards de transactions par jour
- Une plateforme construite sur une architecture inline éprouvée qu'utilisent plus de 25 % des sociétés du Global 2000 de Forbes
- Une présence mondiale de plus de 150 data centers qui assurent la sécurité à la périphérie pour une expérience utilisateur optimale



Stopper les ransomwares à double extorsion

Outre le chiffrement des appareils, les ransomwares à double extorsion dérobent des données et menacent de les divulguer faute de paiement d'une rançon. Ces menaces exploitent des cibles faciles (comme des données non sécurisées au repos et des applications mal configurées) pour proliférer et exfiltrer des données. Malheureusement, les appliances de sécurité traditionnelles ne peuvent s'y opposer dans notre monde cloud-first.

Protection complète des données et contre les menaces

Zscaler fournit une protection complète contre les menaces afin de bloquer les ransomwares en amont et au repos dans tout l'écosystème informatique. De plus, le DLP et le CASB examinent minutieusement tous les canaux de données dans le cloud pour arrêter les exfiltrations, tandis que la gestion de la posture et le SSPM détectent les mauvaises configurations des applications cloud susceptibles d'exposer les données.

Ce que Zscaler vous apporte

- Inspection SSL complète et évolutive destinée à identifier en temps réel l'exfiltration de données et les ransomwares en transit
- Technologie de cloud sandboxing destinée à bloquer les ransomwares de type zero-day inline et hors bande
- Puissance du plus grand cloud de sécurité au monde : des menaces découvertes et bloquées où qu'elles se trouvent

Sécuriser les applications SaaS

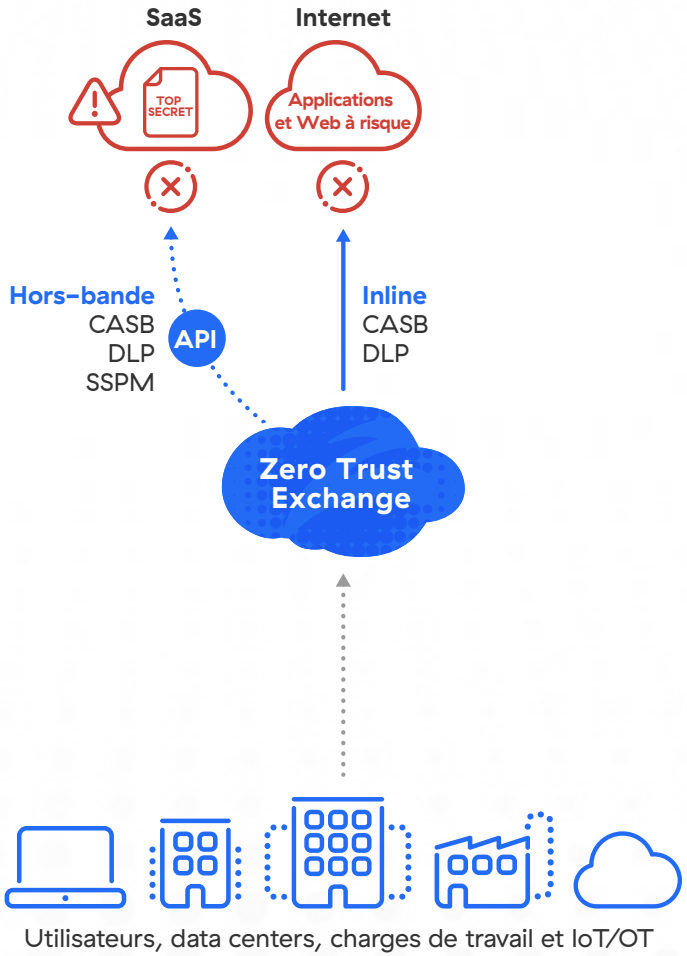
Les applications SaaS permettent une productivité et une flexibilité sans précédent, mais elles peuvent facilement être la cause de pertes de données si elles ne sont pas correctement sécurisées. Les utilisateurs téléchargent en effet régulièrement des données vers des applications non autorisées ; des fichiers au repos peuvent facilement être partagés avec des tiers non autorisés ; des configurations incorrectes peuvent compromettre la posture de sécurité des applications et exposer les données.

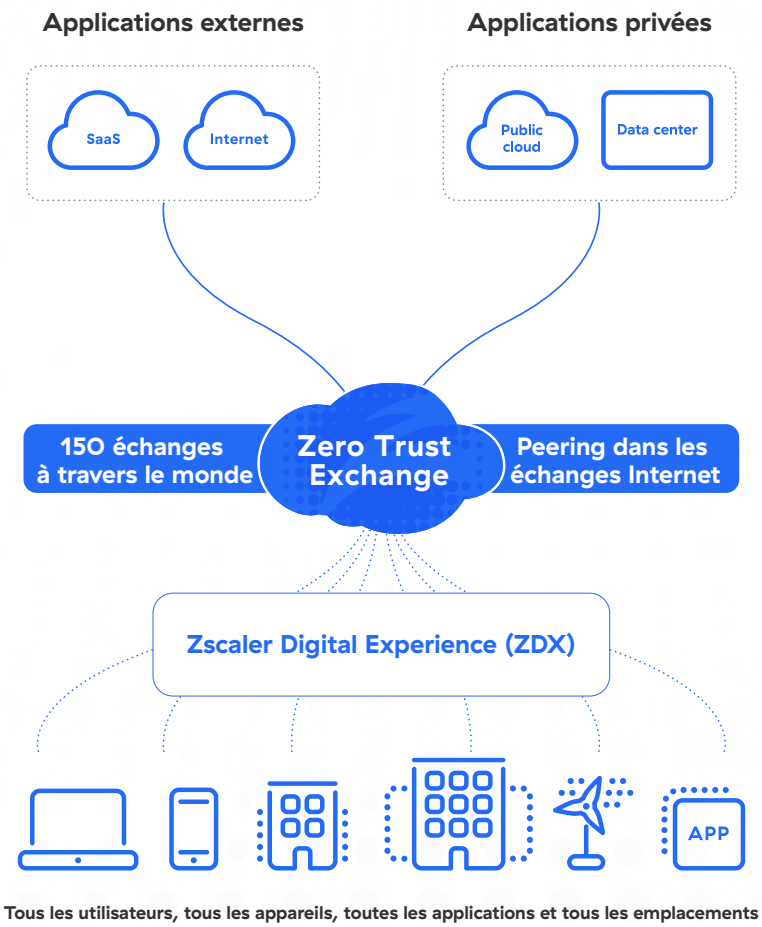
CASB avec DLP

Zscaler sécurise les applications SaaS en détectant automatiquement l'informatique fantôme, en contrôlant les téléchargements de données vers des applications cloud non approuvées et en sécurisant les données au repos dans les applications cloud approuvées. De plus, la gestion de la posture de sécurité SaaS analyse les applications à la recherche de mauvaises configurations susceptibles d'exposer les données ou de compromettre la mise en conformité.

Ce que Zscaler vous apporte

- Protection unifiée des données qui sécurise de manière cohérente tous les canaux de données SaaS et cloud à l'aide d'une politique unique
- Fonctionnalité CASB haute performance au cœur du Security Service Edge le plus éprouvé et le mieux intégré
- Cloud DLP complet avec des capacités avancées comme l'EDM et l'OCR pour protéger des valeurs spécifiques et des données sous forme d'images





Protéger les données des utilisateurs distants

Le télétravail est appelé à perdurer, mais la sécurité traditionnelle n'a pas été conçue pour ce nouveau style de travail. Le recours au VPN et au backhauling du trafic utilisateur vers les appliances de sécurité n'offrent pas une évolutivité suffisante, nuisent à la productivité des utilisateurs et ne répondent pas aux cas d'utilisation modernes de la protection des données auxquels les sociétés cloud-first doivent répondre.

Une sécurité à la périphérie fournie dans le cloud

Grâce au cloud de sécurité le plus important et le plus éprouvé au monde, Zscaler peut se targuer de disposer de l'ampleur et de l'expertise nécessaires pour défendre les données tout en facilitant le télétravail partout dans le monde. Zscaler est capable de sécuriser les utilisations de SaaS, IaaS, PaaS, le Web et les applications privées sans backhauling du trafic vers une appliance, assurant une protection globale des données avec un rendement maximal.

Ce que Zscaler vous apporte

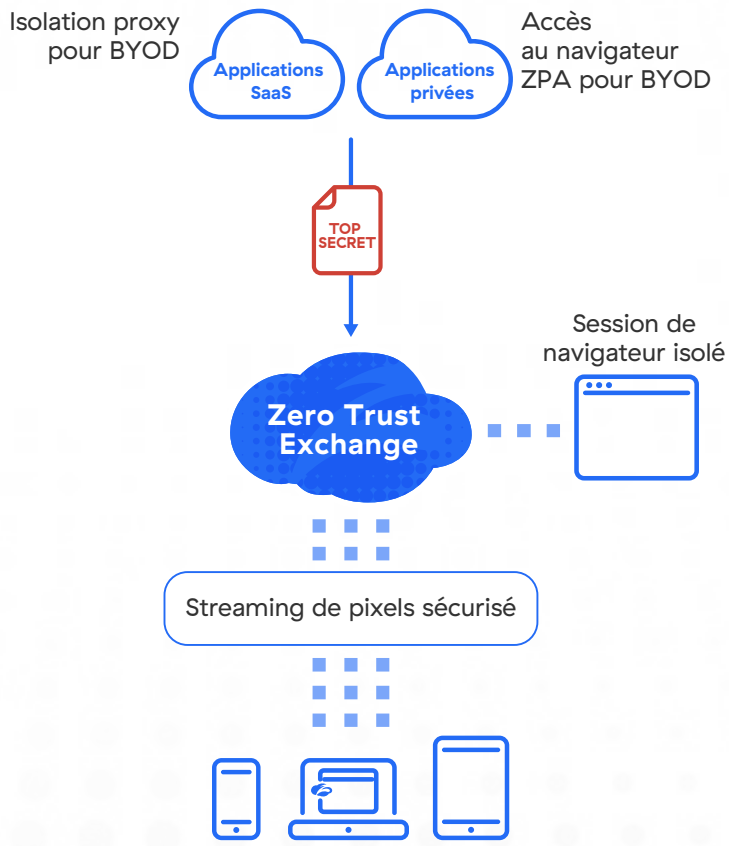
- Un cloud de sécurité mondial comptant plus de 150 data centers assure une sécurité des données extrêmement performante à la périphérie.
- Une offre de sécurité en tant que service élimine le besoin de backhauling vers les appliances matérielles et virtuelles.
- Une architecture à passage unique avec CASB, SWG, ZTNA et plus encore, assure une protection efficace et complète, partout.

Sécuriser les appareils BYOD et autres appareils non gérés

Les terminaux non gérés ou n'appartenant pas à l'entreprise, comme les appareils BYOD (appareils personnels utilisés à des fins professionnelles) et B2B, ont souvent de bonnes raisons d'accéder aux applications de l'entreprise, mais le service informatique perd le contrôle dès qu'ils téléchargent des données. Malheureusement, bloquer ces appareils perturbe la productivité, les installations d'agents logiciels sont généralement irréalisables et les proxys inversés se rompent fréquemment. Alors, que doit faire le service informatique ?

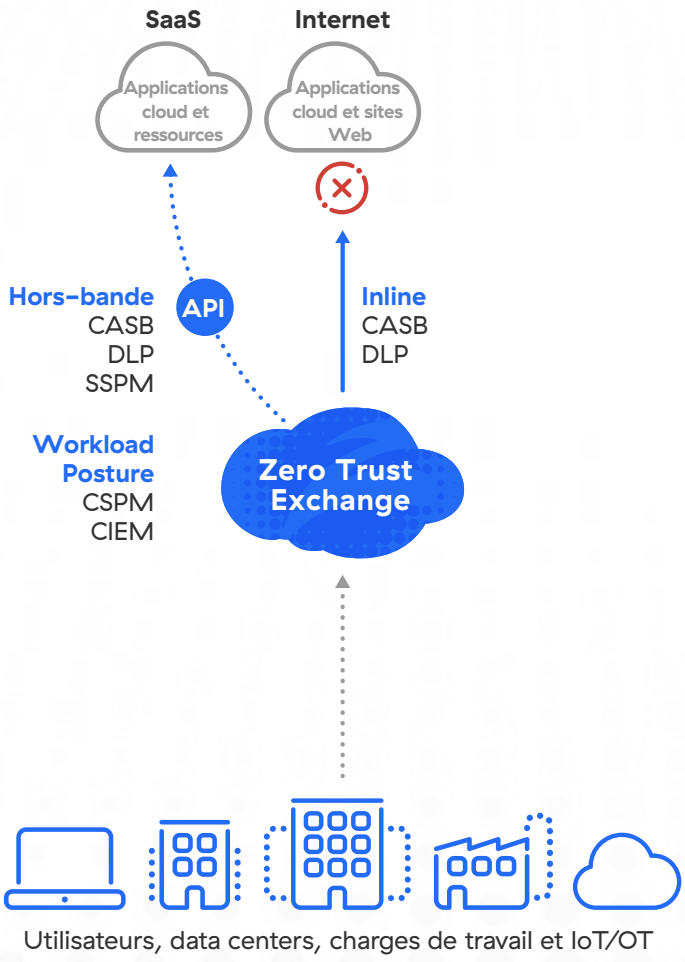
Isolation de navigateur cloud

Avec l'isolation du navigateur sans agent, Zscaler virtualise la session d'application d'un utilisateur dans un environnement isolé et ne transmet que des pixels au terminal, empêchant le téléchargement, le copier-coller et l'impression. Cela signifie que le service informatique peut autoriser l'accès à des appareils non gérés tout en préservant la sécurité des données et en contournant les défis posés par les agents et les proxys inversés. Cette fonctionnalité empêche également les téléchargements de fichiers infectés à partir de terminaux à risque.



Ce que Zscaler vous apporte

- Isolation du navigateur cloud basée sur le cloud de sécurité le plus important et le plus performant au monde
- Proxy d'isolation pour une sécurité sans agent sur n'importe quel appareil accédant à n'importe quelle application SaaS
- Accès au navigateur ZPA pour un accès sécurisé aux applications privées sans installation de logiciel côté client



Respecter la conformité réglementaire

Les données réglementées par le RGPD, l'HIPAA et autres migrent hors site avec le reste des informations sensibles de l'entreprise, mais les outils traditionnels sont incapables de les protéger et de maintenir la conformité dans le cloud. Ceci revêt une importance cruciale, car le non-respect des lois sur la protection de la vie privée comme le CCPA et des cadres de travail comme PCI DSS peut se traduire par des amendes, une perte de confiance des consommateurs et une baisse du chiffre d'affaires.

Une assurance de conformité sans faille

Nous avons conçu le Security Service Edge de Zscaler en tenant compte de la conformité réglementaire. La solution procure une visibilité et un contrôle complets sur l'ensemble de l'écosystème informatique afin de garantir que les données réglementées restent en sécurité, que les applications ne contiennent aucune vulnérabilité susceptible d'entraver la conformité et que les principes de Zero Trust sont appliqués partout.

Ce que Zscaler vous apporte

- Cloud DLP avec une fonctionnalité CASB multimode qui sécurise les données réglementées en mouvement et au repos
- Conformité préservée : aucun téléchargement de données effectué par Zscaler à des fins d'inspection, même pour des mesures telles que la correspondance exacte des données
- SSPM et gestion de la posture de Zscaler pour détecter et corriger les mauvaises configurations et les droits susceptibles d'induire une non-conformité

Acquérir une protection des données cohérente et gérable

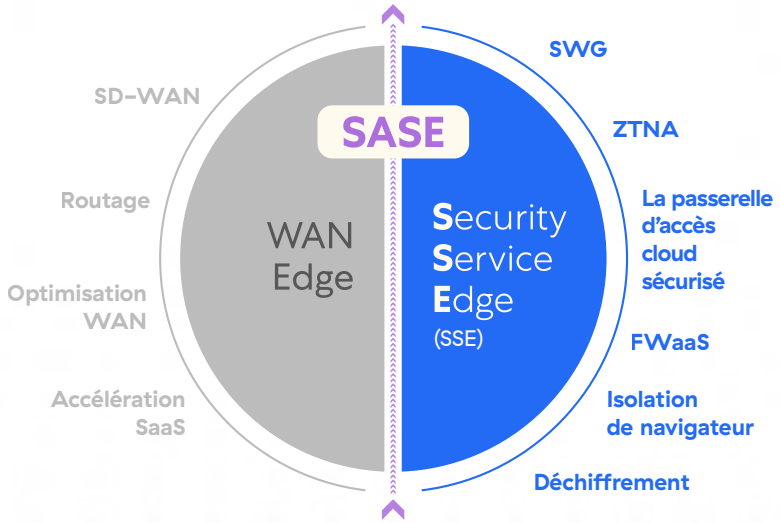
S'appuyer sur un patchwork de produits ponctuels décousus aux capacités disparates génère un certain nombre de défis. Cela engendre notamment une protection des données incohérente dans un écosystème informatique de plus en plus complexe. En outre, les administrateurs qui supervisent une multitude de solutions cloisonnées subissent une lourde charge de gestion.

Une plateforme tout-en-un

Zscaler SSE intègre des technologies de pointe capables de sécuriser n'importe quelle transaction et de protéger les données où qu'elles aillent, de manière cohérente et complète. Grâce à une offre cloud complète dotée d'une architecture à passage unique, l'entreprise peut également réduire la complexité informatique tout en allégeant la charge de gestion qui pèse sur les administrateurs.

Politique de sécurité cohérente

Protection des données et contre les menaces



Expérience utilisateur cohérente

Accès Zero trust

Ce que Zscaler vous apporte

- Protection cohérente des données pour toutes les applications SaaS, cloud, Web et privées
- Simplification de l'architecture qui permet de réduire le nombre de produits et d'appliances ponctuels
- Facilité de gestion regroupée qui dispense de dupliquer les politiques et fait gagner du temps aux administrateurs

Le cloud et la mobilité offrent d'innombrables avantages en termes de productivité et de flexibilité, mais pour en tirer parti sans compromettre la sécurité des données, vous devez adopter une autre approche de la cybersécurité. Le Security Service Edge de Zscaler donne à votre entreprise les moyens d'adopter la transformation digitale tout en protégeant vos données, où qu'elles aillent.

Découvrez ce que les clients pensent de Zscaler SSE

Lisez le Magic Quadrant pour le Security Service Edge

zscaler™ | **Experience your world, secured.™**

À propos de Zscaler

Zscaler (NASDAQ: ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.fr