# Zscaler Internet Access

## Protection optimisée par l'IA pour tous les utilisateurs, toutes les applications, tous les emplacements

FICHE TECHNIQUE

**Zscaler Internet Access™ définit un accès Internet et SaaS sûr et rapide avec la plateforme Zero Trust la plus complète et la plus fiable du secteur.**

### La sécurité réseau traditionnelle n'est plus efficace dans un monde axé sur le cloud et la mobilité

Les architectures en étoile traditionnelles étaient efficaces lorsque les utilisateurs travaillaient principalement au siège ou dans un site distant, que les applications étaient uniquement hébergées dans le data center de l'entreprise et que votre surface d'attaque était restreinte aux ressources contrôlées par votre entreprise. Nous vivons aujourd'hui dans un monde radicalement différent, dans lequel les ransomwares, les menaces chiffrées, les attaques de la chaîne d'approvisionnement et d'autres menaces avancées parviennent à franchir les défenses des réseaux traditionnels. Le moment est venu de trouver une solution de sécurité cloud native qui réduit globalement les risques et la complexité tout en offrant la flexibilité nécessaire à l'avancement des projets de l'entreprise.

### Zscaler Internet Access

La sécurisation de l'entreprise moderne, dans un contexte de cloud et de mobilité, exige une approche foncièrement différente, fondée sur le principe de Zero Trust. Zscaler Internet Access, composante de Zscaler Zero Trust Exchange™, est la plateforme SSE (Security Service Edge) la plus déployée au monde, et le fruit d'une décennie d'expertise en matière de passerelles Web sécurisées.

Fournie en tant que plateforme de sécurité cloud SaaS évolutive et résiliente, ZIA élimine les solutions de sécurité réseau traditionnelles pour neutraliser les attaques avancées et prévenir les pertes de données grâce à une approche Zero Trust intégrale, qui offre les avantages suivants :

**Sécurité optimale et cohérente pour les collaborateurs hybrides d'aujourd'hui :** lorsque vous migrez la sécurité vers le cloud, tous les utilisateurs, applications, appareils et sites bénéficient d'une protection permanente contre les menaces, basée sur le contexte et l'identité. Votre politique de sécurité s'applique à vos utilisateurs, où qu'ils se trouvent.

**Accès ultra-rapide sans aucune infrastructure :** l'architecture directe vers le cloud garantit une expérience utilisateur rapide et fluide. Elle élimine le backhauling, améliore les performances et l'expérience utilisateur, et simplifie l'administration du réseau, sans l'aide d'aucune infrastructure physique.

**Protection optimisée par l'IA depuis le plus vaste cloud de sécurité au monde :** une inspection inline de tout le trafic Internet et SaaS (et notamment un déchiffrement du trafic SSL), associée à une suite de services de sécurité cloud optimisés par l'IA, permet de neutraliser les ransomwares, le phishing, les malwares de type « zero-day » et les attaques avancées, sur la base de renseignements sur les menaces provenant de 500 000 milliards de signaux quotidiens.

**Gestion simplifiée :** votre équipe peut se consacrer aux objectifs stratégiques de l'entreprise en utilisant notre solution de sécurité cloud native optimisée par l'IA, en exploitant l'automatisation pour rationaliser les flux de travail et en appliquant des politiques créées spécifiquement pour l'entreprise, et ce, sans matériel à gérer.

## Services intégrés de sécurité et de protection des données optimisés par l'IA

Zscaler Internet Access comprend une suite complète de services de sécurité et de protection des données optimisée par l'IA et destinée à vous aider à mettre fin aux cyberattaques et à la perte de vos données. En tant que solution SaaS entièrement fournie dans le cloud, vous pouvez ajouter de nouvelles fonctionnalités sans aucun matériel supplémentaire ni longs cycles de déploiement. Les modules disponibles dans le cadre de Zscaler Internet Access sont les suivants :

- **Cloud Secure Web Gateway (SWG) :** assurez une expérience Web sûre et rapide qui élimine les ransomwares, les malwares et autres attaques avancées, grâce à une analyse et un filtrage d'URL en temps réel, optimisés par l'IA.

- **Cloud Access Security Broker (CASB) :** sécurisez les applications cloud avec un CASB intégré pour protéger les données, déjouer les menaces et garantir la conformité dans vos environnements SaaS et IaaS.

- **Cloud Data Loss Prevention (DLP) :** protégez les données en transit avec une inspection inline complète et des mesures avancées telles que la correspondance exacte des données (EDM), la reconnaissance optique des caractères (OCR) et l'apprentissage automatique.

- **Zscaler Firewall et Cloud IPS :** étendez une protection optimale à tous les ports et protocoles, et remplacez vos pare-feu de périphérie et de sites distants par une plateforme cloud native.

- **Zscaler Sandbox :** arrêtez les malwares inconnus et furtifs à travers le Web et les protocoles de transfert de fichiers avec une mise en quarantaine basée sur l'IA, et assurez une protection en temps réel, cohérente et globale pour tous les utilisateurs.

- **Navigateur Zero Trust optimisé par l'IA :** déjouez les attaques Web et prévenez toute perte de données, en cloisonnant virtuellement (« air-gap ») les utilisateurs, le Web et les applications SaaS.

### AVANTAGES :

- **Prévenez les cybermenaces et la perte de données grâce à l'IA :** protégez votre entreprise contre les menaces avancées grâce à des services de protection des données et de lutte contre les cybermenaces, optimisés par l'IA et enrichis par des mises à jour en temps réel issues de 500 000 milliards de signaux quotidiens liés aux menaces provenant du plus vaste cloud de sécurité au monde.

- **Bénéficiez d'une expérience utilisateur optimale :** profitez d'une expérience Internet et SaaS performante (jusqu'à 40 % plus performante que celle offerte par les architectures de sécurité traditionnelles) pour stimuler votre productivité et favoriser l'agilité de votre entreprise.

- **Réduisez les coûts et la complexité :** réalisez un retour sur investissement de 139 % avec Zscaler en remplaçant 90 % de vos appliances coûteuses, complexes et lentes par une plateforme Zero Trust entièrement cloud native.

- **Sécurisez votre personnel hybride :** permettez aux employés, aux clients et aux tiers d'accéder en toute sécurité aux applications Web et aux services cloud, où qu'ils se trouvent, sur n'importe quel appareil, avec une expérience numérique de qualité.

- **Unifiez les efforts SecOps et NetOps :** accélérez les résultats en matière de sécurité et favorisez une collaboration efficace grâce à des outils partagés tels que des analyses du trafic en temps réel, des intégrations axées sur les API et un contrôle d'accès granulaire basé sur les rôles.

- **Assurez une souveraineté totale sur les données et le contenu :** appliquez la conformité pour un accès sécurisé et localisé sans compromis sur les performances grâce à une passerelle NAT de sortie, au contenu géolocalisé et à la journalisation des données au niveau national.

- **Sécurisez l'IA dans votre environnement :** activez l'utilisation sécurisée de Microsoft Copilot et d'autres applications d'IA.

- **Protégez les environnements de développement à grande échelle :** automatisez l'inspection SSL/TLS de plus de 30 outils de développement tout en isolant le code et les fichiers inconnus ou volumineux dans un environnement de sandboxing, avec des verdicts instantanés générés par l'IA, le tout sans ralentir l'innovation.

- **Surveillance de l'expérience numérique :** réduisez les coûts opérationnels informatiques et accélérez le traitement des demandes d'assistance grâce à une visibilité unifiée sur les indicateurs de performances liées aux applications, aux chemins d'accès au cloud et aux terminaux, ce qui vous permet de simplifier ainsi vos analyses et les opérations de dépannage.

- **Connectivité Zero Trust pour les sites distants :** réduisez les risques et la complexité grâce à une connectivité non routable pour les sites distants et data centers, capable de prendre en charge les utilisateurs, les serveurs et les dispositifs IoT/OT.

- **Sécurité DNS :** optimisez la sécurité et les performances DNS pour tous les utilisateurs, dispositifs et applications, sur tous les ports et protocoles, partout dans le monde.

## Zscaler Internet Access pour les utilisateurs et les workloads

Éliminez les risques pour les workloads cloud accédant à toute destination Internet ou SaaS avec Zscaler Internet Access. Les workloads n'ayant plus besoin d'accéder à Internet par le biais d'outils traditionnels centrés sur le réseau, tels que les VPN, les pare-feu (y compris les pare-feu virtuels) ou les technologies WAN, vous pouvez prévenir les compromissions et arrêter les déplacements latéraux sans devoir recourir à un patchwork d'outils de sécurité. En appliquant aux workloads la suite complète de fonctionnalités de sécurité et de protection des données de ZIA, vous pouvez unifier la sécurité Zero Trust pour vos utilisateurs et vos workloads avec une plateforme unique et intégrée.

En associant ZIA à Zscaler Private Access, vous pouvez étendre la protection à vos applications et workloads privés, qu'ils résident dans le cloud public ou dans un data center privé.

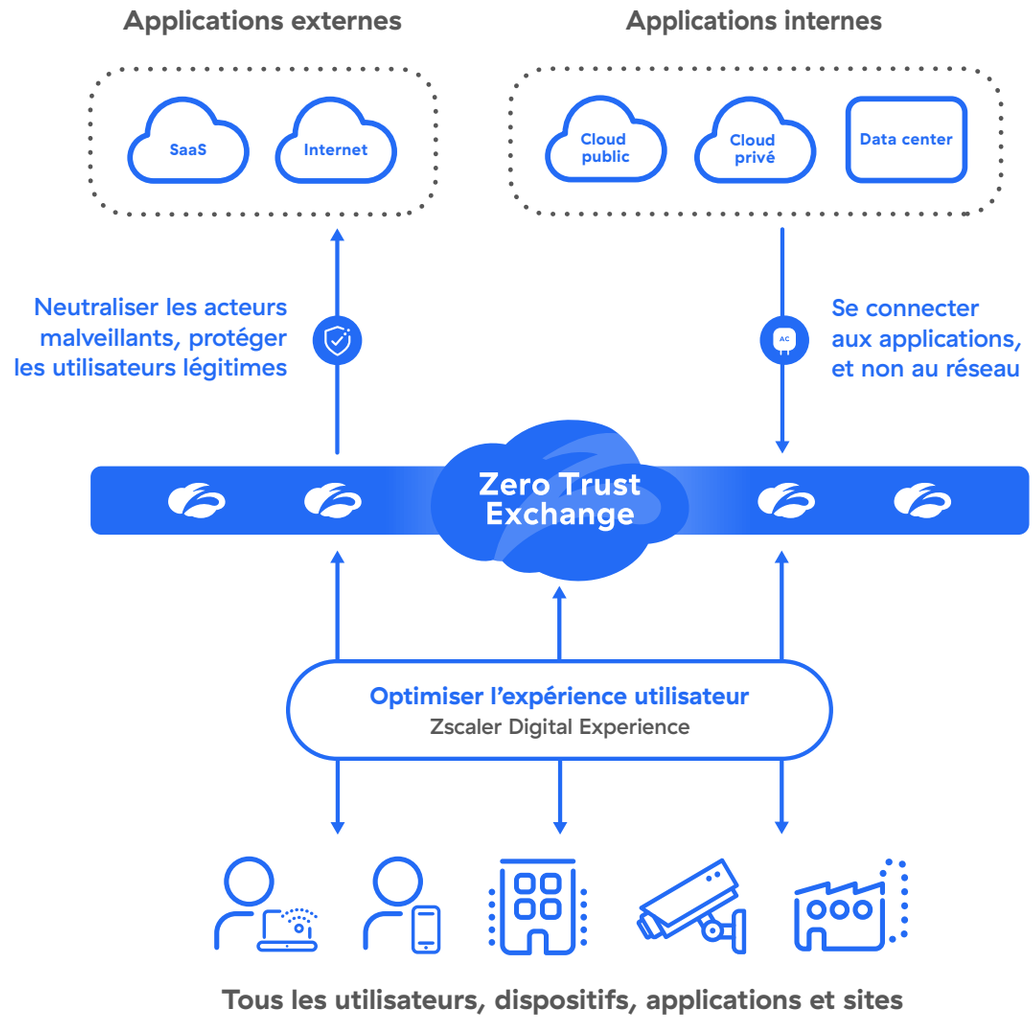



Illustration 1 : Zero Trust Exchange

*Gartner, Magic Quadrant pour le Security Service Edge, 15 avril 2024, Charlie Winckless et al.

Gartner n'approuve aucun fournisseur, produit ou service décrit dans ses publications de recherche, et ne conseille pas aux utilisateurs de technologie de sélectionner uniquement les fournisseurs ayant les cotes les plus élevées ou toute autre désignation. Les publications de recherche de Gartner se composent des opinions de l'organisation de recherche de Gartner et ne doivent pas être interprétées comme des déclarations de fait. Gartner décline toutes les garanties, exprimées ou implicites, à l'égard de cette recherche, y compris toute garantie de valeur marchande ou d'aptitude à un but particulier.



Gartner

Zscaler a été désigné parmi les leaders 2024 du Gartner® Magic Quadrant™ pour le Security Service Edge (SSE).

**EN SAVOIR PLUS**

## Cas d’utilisation

### PROTECTION CONTRE LES CYBER-MENACES ET LES RANSOMWARES

Passez de la sécurité réseau traditionnelle à l’architecture Zero Trust révolutionnaire de Zscaler qui empêche toute compromission, élimine la surface d’attaque, bloque les déplacements latéraux et préserve la sécurité des données.

En savoir plus

### SÉCURISATION DES COLLABORATEURS HYBRIDES

Permettez aux employés, partenaires, clients et fournisseurs d’accéder en toute sécurité aux applications Web et aux services cloud, où qu’ils se trouvent, sur n’importe quel appareil, et assurez une expérience numérique de qualité.

En savoir plus

### PROTECTION DES DONNÉES

Empêchez la perte de données des utilisateurs, des applications SaaS et de l’infrastructure de cloud public résultant d’une exposition accidentelle, d’un vol de données ou d’un ransomware à double extorsion.

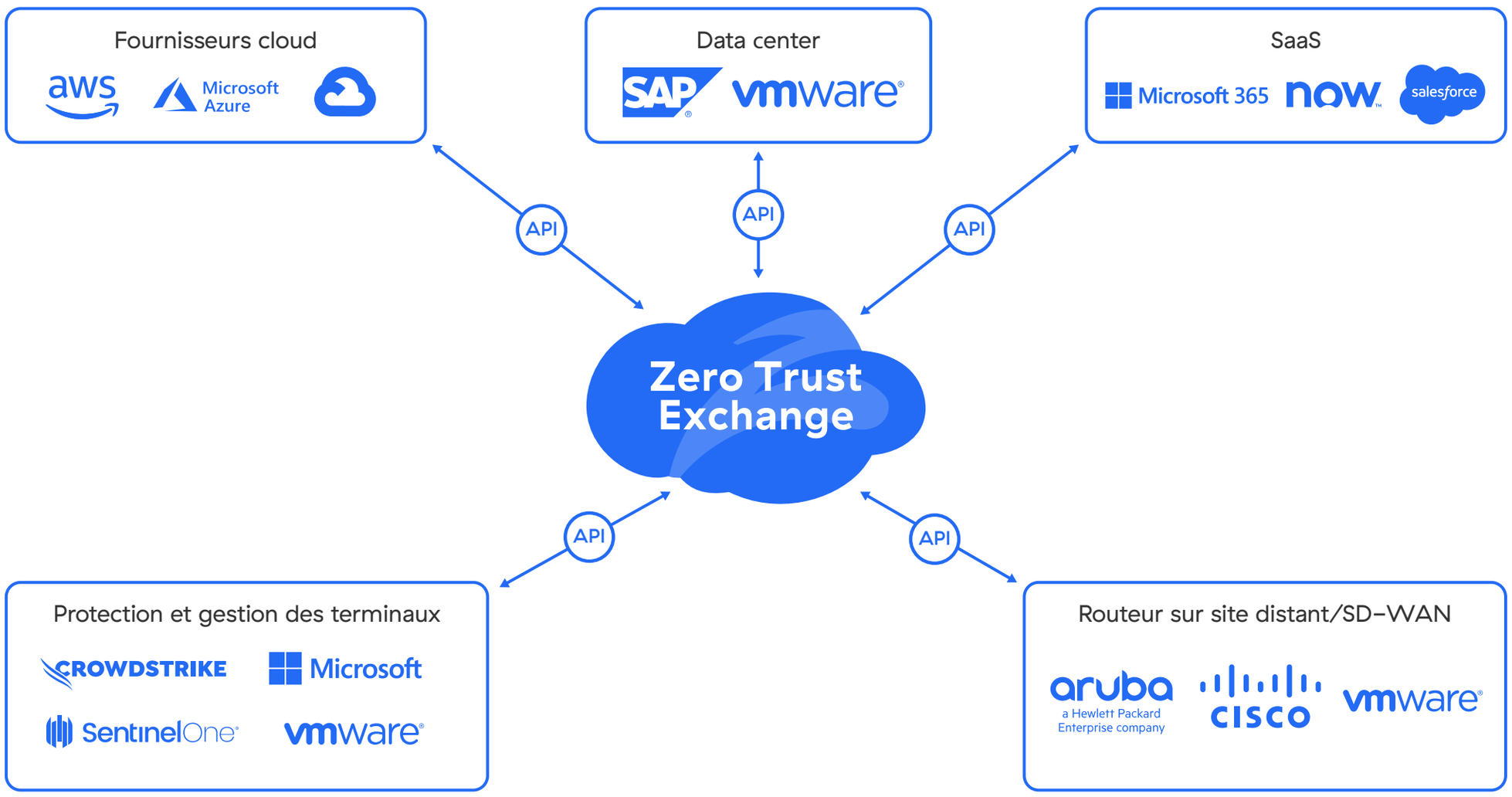
En savoir plus

### MODERNISATION DES INFRASTRUCTURES

Éliminez les réseaux complexes et coûteux grâce à un accès direct au cloud, rapide, fiable et sécurisé qui dispense de pare-feu en périphérie et dans les filiales.

En savoir plus

## Écosystème de Zscaler Zero Trust Exchange



| TABLEAU 1 : FONCTIONNALITÉS ET CAPACITÉS DE ZSCALER INTERNET ACCESS | |
|---|---|
| **FONCTIONNALITÉS** | **DESCRIPTION** |
| **CAPACITÉS** | |
| **Filtrage d'URL** | Autorisez, bloquez, surveillez ou isolez l'accès des utilisateurs à des catégories ou à des destinations Web spécifiques afin de mettre fin aux menaces Web et de garantir la conformité aux politiques de l'entreprise. |
| **Inspection SSL** | Bénéficiez d'une inspection illimitée du trafic TLS/SSL afin d'identifier les menaces et tentatives d'exfiltration des données qui se dissimulent dans le trafic chiffré. Spécifiez les catégories ou les applications Web à inspecter en fonction des exigences en matière de confidentialité ou de réglementation. Intégrez l'inspection à l'outil de développement pour sécuriser les flux de travail des développeurs. |
| **Sécurité DNS** | Identifiez et acheminez les connexions suspectes de type C&C (commande et contrôle) vers les moteurs de détection de menaces de Zscaler pour une inspection complète du contenu. |
| **IP dédiée** | Donnez accès aux applications qui autorisent les adresses IP avec des adresses IP dédiées à votre entreprise. Facilitez également la transition d'une architecture traditionnelle vers le Zero Trust. |
| **Contrôle des fichiers** | Bloquez ou autorisez le téléchargement/chargement de fichiers vers ou depuis des applications, en fonction de l'application, de l'utilisateur ou d'un groupe d'utilisateurs. |
| **Bring Your Own IP (Utilisation d'une adresse IP personnelle)** | Maintenez la cohérence et le contrôle de votre identité réseau, et assurez aux applications tierces ou à l'infrastructure dépendante que le trafic provient exclusivement de votre entreprise. |
| **Gestion de la bande passante** | Appliquez des politiques de bande passante et donnez la priorité aux applications stratégiques au détriment d'autres types de trafic lié au divertissement. |
| **Journalisation par pays** | Stockez et gérez les journaux en fonction des frontières d'un pays spécifique afin de respecter les exigences de souveraineté des données qui imposent que les données relatives aux citoyens soient traitées conformément aux lois locales. |
| **Protection contre les menaces avancées** | Arrêtez les cyberattaques avancées telles que les malwares, les ransomwares, les attaques de la chaîne d'approvisionnement, le phishing et bien d'autres encore grâce à une protection propriétaire contre les menaces avancées. Définissez des politiques granulaires en fonction du niveau de tolérance au risque de votre entreprise. |
| **Protection inline des données (données en transit)** | Utilisez les fonctionnalités de proxy de transfert et d'inspection SSL pour contrôler en temps réel le flux d'informations sensibles vers des destinations Web et des applications cloud à risque afin de stopper les menaces internes et externes qui ciblent les données. Une protection inline avancée est fournie, qu'une application soit autorisée ou non, sans nécessiter de journalisation des périphériques réseau. |
| **Protection des données hors bande (données au repos)** | Utilisez des intégrations API pour analyser les applications SaaS, les plateformes cloud et leur contenu afin d'identifier les données sensibles au repos et les corriger automatiquement, par exemple en empêchant les partages à risque ou vers l'externe. |

| | |
|---|---|
| **Prévention des intrusions** | Bénéficiez d'une protection complète contre les botnets, les menaces avancées et les menaces de type « zero-day », ainsi que d'informations contextuelles sur les utilisateurs, les applications et les menaces. Les systèmes de prévention d'intrusions (IPS) cloud et Web fonctionnent de manière transparente avec les composants Firewall, Cloud Sandbox, DLP et CASB. Déployez des signatures de menaces personnalisées à l'aide du composant Cloud Custom IPS pour détecter et bloquer les attaques ciblées. |
| **Politique de sécurité et d'accès dynamique basée sur les risques** | Adaptez automatiquement la politique de sécurité et d'accès aux risques liés aux utilisateurs, aux appareils, aux applications et aux contenus. |
| **Capture de trafic** | Grâce à la capture transparente des paquets, la capture du trafic déchiffré s'effectue aisément à l'aide de critères spécifiques des moteurs de politiques Zscaler, ce qui permet d'effectuer des analyses expertes de sécurité sans recourir à des appliances supplémentaires. |
| **Analyse des malwares** | Détectez, prévenez et mettez en quarantaine les menaces inconnues qui se dissimulent dans des payloads malveillants inline, grâce à des fonctions d'IA/AA avancées qui neutralisent les attaques de type patient zéro. |
| **Filtrage de DNS** | Contrôlez et bloquez les requêtes DNS vers des destinations connues et malveillantes. |
| **Navigateur Zero Trust (isolation Web)** | Déjouez les menaces Web en restituant du contenu actif sous forme de flux de pixels inoffensifs vers le navigateur de l'utilisateur final. |
| **Corrélation des informations sur les menaces** | Accélérez les enquêtes et les délais de réponse grâce à des alertes contextualisées et corrélées avec des informations sur le score de la menace, la ressource affectée, la gravité, etc. |
| **Isolation des applications** | Accordez un accès sécurisé et sans agent aux applications SaaS, cloud et privées en contrôlant précisément les actions de l'utilisateur (copier/coller, charger/télécharger, imprimer, etc.) pour déjouer toute perte de données sensibles. |
| **Surveillance de l'expérience numérique (ZDX)** | Obtenez une vue unifiée sur les indicateurs de performances des applications, des chemins d'accès au cloud et des terminaux pour faciliter vos analyses et opérations de dépannage. |
| **Connectivité Zero Trust des sites distants** | Modernisez la connectivité sur les sites distants avec Zero Trust Exchange en éliminant la surface d'attaque et en empêchant tout déplacement latéral des menaces. |
| **Protection des communications entre les workloads et Internet** | Prévenez toute compromission et empêchez les déplacements latéraux pour les communications du workload vers Internet. Cela comprend l'inspection SSL, l'IPS, le filtrage d'URL et la protection des données pour toutes les communications. |
| **Visibilité sur les dispositifs IoT** | Bénéficiez d'une visibilité complète sur tous les dispositifs IoT, les serveurs et les appareils d'utilisateurs non gérés dans votre entreprise grâce à une découverte automatisée, une surveillance continue, une classification optimisée par l'IA/AA et des fonctionnalités optimales et automatiques d'étiquetage. |
| **Contrôle d'accès basé sur les rôles (RBAC)** | Bénéficiez d'autorisations adaptées pour contrôler ce que les administrateurs peuvent modifier et afficher dans les rapports sur les politiques et les analyses au sein de la plateforme Zscaler afin d'éviter les conflits et d'améliorer la gouvernance. |

| FONCTIONNALITÉS | DESCRIPTION |
|---|---|
| **FONCTIONNALITÉS DE LA PLATEFORME** | |
| **Flexibilité des options de connectivité** | • Zscaler Client Connector (ZCC) : transférez le trafic vers Zero Trust Exchange via un agent léger qui prend en charge Windows, macOS, iOS, iPadOS, Android et Linux.<br>• Tunnels GRE ou IPsec : utilisez des tunnels GRE et/ou IPsec pour envoyer le trafic vers Zero Trust Exchange pour les appareils sans ZCC.<br>• Isolation du navigateur : connectez de manière transparente tous les appareils BYOD ou non gérés grâce à l'isolation du navigateur Zero Trust intégrée.<br>• Chaînage de proxy : Zscaler prend en charge le transfert du trafic d'un serveur proxy à un autre. Ceci n'est toutefois pas recommandé en environnement de production.<br>• Fichiers PAC : envoyez du trafic vers Zero Trust Exchange avec des fichiers PAC pour les appareils sans ZCC. |
| **Déploiement dans le cloud** | Plateforme entièrement cloud native fournie en tant que service SaaS. Des Services Edges privés et virtuels sont disponibles pour la planification de la continuité d'activité et d'autres cas d'utilisation spéciaux. |
| **Confidentialité et conservation des données** | Lors de la journalisation des données, le contenu n'est jamais écrit sur le disque et des contrôles granulaires permettent de déterminer où la journalisation a lieu exactement. Utilisez le contrôle d'accès basé sur les rôles (RBAC) pour fournir un accès en lecture seule, l'anonymisation/obfuscation du nom d'utilisateur et des droits d'accès distincts par département ou fonction, conformément aux principales réglementations de conformité.<br><br>Les données sont conservées pendant une période renouvelable de six mois ou moins, selon le produit. Vous pouvez acheter un stockage supplémentaire qui conserve les données aussi longtemps que vous le souhaitez. |
| **Principales certifications de conformité** | Ces certifications sont :<br>• FedRAMP<br>• ISO 27001<br>• SOC 2 Type II<br>• SOC 3<br>• NIST 800-63C<br>La liste complète de nos certifications de conformité est disponible ici. |
| **Prise en charge granulaire des API** | Nous assurons des intégrations API REST avec de nombreux fournisseurs d'identité, de réseau et de sécurité. Vous pouvez, par exemple, partager vos journaux depuis Zscaler vers votre SIEM basé sur le cloud ou sur site (Splunk, par exemple).<br><br>En savoir plus |
| **Peering direct** | Le peering direct avec les principaux fournisseurs d'Internet et de SaaS, et les destinations de cloud public garantit le trajet du trafic le plus rapide possible. |

| FONCTIONNALITÉS | DESCRIPTION |
|---|---|
| **ACCORDS DE NIVEAU DE SERVICE (SLA)** | |
| **Disponibilité** | Disponibilité de 99,999 % mesurée selon le nombre de transactions perdues |
| **Latence du proxy** | < 100 ms, y compris lorsque l'analyse des menaces et l'analyse DLP sont activées |
| **Identification de virus** | 100 % des virus et malwares connus |
| **PLATEFORMES ET SYSTÈMES COMPATIBLES** | |
| **Client Connector** | Compatible avec :<br>• iOS 9 ou versions ultérieures<br>• Android 8 ou versions ultérieures<br>• Windows 8 et versions ultérieures<br>• Mac OS X 10.14 et versions ultérieures<br>• CentOS 9<br>• Ubuntu 20.04<br>En savoir plus |
| **Branch Connector** | Compatible avec :<br>• VMware vCenter ou vSphere Hypervisor<br>• Centos<br>• Redhat |

## Zscaler Internet Access : plusieurs options pour démarrer

| | PLATEFORME ESSENTIALS<br><br>Commencez votre parcours Zero Trust avec un accès Internet sécurisé et fiable, ainsi qu'un accès privé limité grâce à d'autres innovations Zscaler. | PLATEFORME ZSCALER<br><br>Libérez la puissance de la solution SASE/SSE complète, y compris l'accès complet à Internet, l'accès privé et la protection des données. |
|---|---|---|
| **SERVICES DE LA PLATEFORME** | | |
| Transfert de trafic – Client Connector, GRE, PAC, chaînage de proxy, IPsec | Oui | Oui |
| Fournisseurs d'identités multiples (IdP), accès API, posture de l'appareil | Oui | Oui |
| Authentification – SAML, protocole LDAP sécurisé, Kerberos | Oui | Oui |
| Environnement de test ZS | – | – |
| Accès aux data centers publics de Zscaler | Oui | Oui |
| Accès aux data centers publics de Zscaler à coût élevé (Australie, Nouvelle-Zélande, Dubaï (non réglementé), Amérique du Sud, Afrique, Corée du Sud, Taïwan et Chine continentale) | – | Oui |
| China Premium / Accès réglementé au data center du Moyen-Orient | – | – |
| **ACCÈS INTERNET** | | |
| Filtrage du contenu | Oui | Oui |
| Contrôle du type de fichier | Oui | Oui |
| Inspection TLS/SSL | Oui | Oui |
| Certificat SSL privé | Oui | Oui |
| Contrôle de la bande passante | Oui | Oui |
| Diffusion vers SIEM sur site (service de diffusion en continu Nanolog avec gestion en direct) | Oui | Oui |
| Cloud NSS (pour > 500 utilisateurs) | Oui | Oui |
| Ancrage de l'IP source | – | Oui |
| ZIA Private Service Edge — Appliance virtuelle | – | Oui |
| Matériel : ZIA Private Service Edge – 3 instances, 5 instances | – | – |

| | | |
|---|---|---|
| **PROTECTION CONTRE LES CYBERMENACES** | | |
| Cyberthreat Protection (version Standard) : Advanced Threat Protection, Sandbox (version Standard), Zero Trust Firewall (version Standard), Zero Trust Browser (version Standard) | Oui | Oui |
| Logiciels antivirus et anti-spyware inline | Oui | Oui |
| Sandbox – Version Advanced | – | – |
| Zero Trust Firewall – Version Advanced | – | – |
| Zero Trust Browser – Version Advanced (1,5 Go de trafic/ utilisateur/mois, mesuré pour tous les utilisateurs de Zero Trust Browser) | – | – |
| Zero Trust Browser – Version Unlimited (aucune limite d'utilisation du trafic) | – | – |
| **ACCÈS PRIVÉ (ZPA)** | | |
| Accès sécurisé aux applications privées (dans le cloud, les data centers) : diffusion des journaux, ancrage IP source, IdP multiples, surveillance de l'état de santé | 1 utilisateur pour 20 utilisateurs abonnés (min : 500 utilisateurs abonnés) | Oui |
| App Connectors | Autant que nécessaire (jusqu'à la capacité maximale du système) | Autant que nécessaire (jusqu'à la capacité maximale du système) |
| **PROTECTION DES DONNÉES** | | |
| Data Protection – Version Standard : contrôle des applications cloud, rapport sur l'informatique fantôme, restriction d'entité, Web inline (mode surveillance), API SaaS (1 application), sécurité de l'IA générative | Oui | Oui |
| DLP Web inline et IA générative, toutes les applications (Internet et accès privé) | – | Oui |
| **GESTION DES RISQUES** | | |
| Norme de gestion des risques : Deception – Version Standard | – | Oui |
| **ZERO TRUST FOR WORKLOADS** | | |
| Zero Trust for Workloads – Version Standard : filtrage avec état, DNS, inspection TLS | 1 Go de trafic de workload mensuel par utilisateur abonné | 2 Go de trafic de workload mensuel par utilisateur abonné |
| **EXPÉRIENCE NUMÉRIQUE (ZDX)** | | |
| ZDX – Version Standard : fonctionnalité prédéfinie | Oui | – |
| ZDX – Version Standard | – | Oui |
| **ASSISTANCE** | | |
| Support – Version Standard | Oui | Oui |
| Support – Version Plus | – | – |

## MODÈLE DE LICENCE

Toutes les éditions de Zscaler Internet Access sont facturées par utilisateur. Pour certains produits inclus dans votre édition de plateforme, les tarifs peuvent varier indépendamment du nombre d'utilisateurs. Pour plus d'informations sur la tarification, contactez votre interlocuteur Zscaler.

## Composante de la solution globale Zero Trust Exchange

Zero Trust Exchange facilite des connexions rapides et sécurisées tout en permettant à vos employés de travailler partout en utilisant Internet comme réseau d'entreprise. Avec pour fondement le principe Zero Trust de l'accès sur la base du moindre privilège, cette solution fournit une sécurité complète en utilisant l'identité basée sur le contexte et l'application des politiques.

L'avantage de Zscaler est qu'il offre tout ce dont nous avons besoin dans une plateforme Zero Trust : une inspection évolutive du trafic SSL, d'autres fonctionnalités de prévention des menaces et une protection efficace des données.

**NITIN NEGI**

Responsable principal de l'ingénierie et des opérations de cybersécurité, Micron Technology

### À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications,quel que soit leur emplacement. Distribué dans plus de 160 data centers dans le monde, Zero Trust Exchange, basé sur le SSE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.



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

zscaler™

**Zero Trust Everywhere**