FICHE TECHNIQUE

Zero Trust Cloud

Sécurisez le trafic de vos workloads cloud vers Internet et le trafic entre workloads grâce à la plateforme Zscaler Zero Trust Exchange™.

La transformation numérique stimule la création et l'utilisation de workloads au sein de multiples environnements déployés sur site, dans le cloud privé et dans le cloud public. Votre entreprise utilise ces workloads et il est donc essentiel de les protéger contre les cyberattaques et les risques de perte de données.

Les architectures traditionnelles ne sont plus adaptées : elles fournissent une protection incohérente des données et contre les menaces, étendent la surface d'attaque, permettent les déplacements latéraux et accentuent tant la complexité que les coûts opérationnels.

Zscaler Zero Trust Cloud simplifie radicalement la sécurité des workloads hybrides. Grâce à la puissance de la plateforme Zero Trust Exchange, cette solution sécurise le trafic sortant des workloads vers Internet et le trafic entre workloads dans les data centers de cloud public et sur site pour vos workloads et serveurs critiques.

Zero Trust Cloud fournit une protection cohérente des données et contre les menaces, élimine la surface d'attaque, prévient les déplacements latéraux, réduit la complexité et diminue les coûts opérationnels.

> « Grâce à Workload Communications de Zscaler, nous pouvons normaliser les politiques de sécurité pour les utilisateurs et les applications, où qu'ils se trouvent. »
>
> **Rui Cabeço,** responsable mondial du groupe Global Outbound Connectivity, Siemens

Défis liés à la sécurité traditionnelle des workloads et des serveurs

De nombreuses entreprises se contentent d'architectures traditionnelles pour sécuriser leurs workloads dans le cloud. La plupart d'entre elles combineront les mesures suivantes :

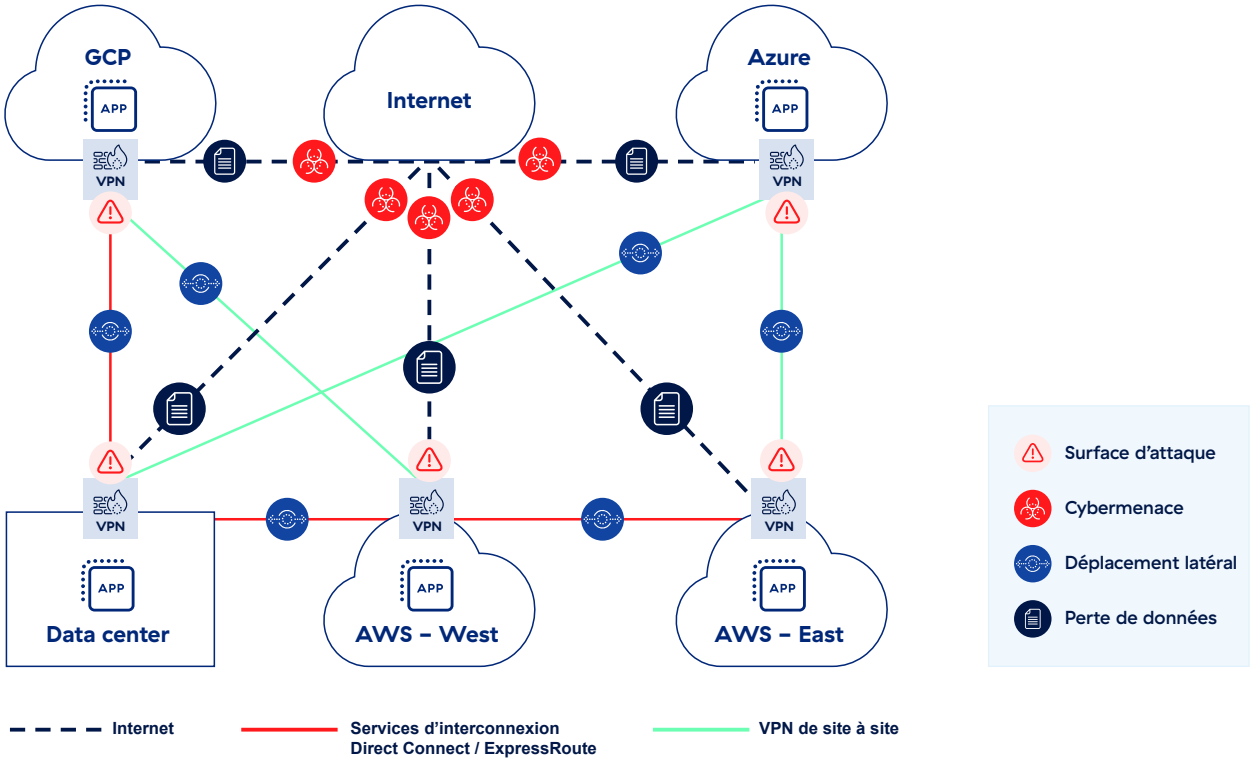
Configuration de solutions de sécurité natives proposées par les fournisseurs de services de cloud public

Déploiement de plusieurs outils (pare-feu, inspection TLS/SSL, DLP, etc.) en tant que couches de protection supplémentaires

Backhauling du trafic vers l'infrastructure de sécurité réseau sur site, à des fins d'inspection et de protection

L'utilisation de ces méthodes présente plusieurs défis, notamment :

- **Augmentation de la surface d'attaque et des opportunités des déplacements latéraux.** Les solutions telles que les pare-feu étendent le réseau aux workloads et aux serveurs, ce qui amplifie les risques de déplacements latéraux. Chaque pare-feu connecté à Internet élargit également la surface d'attaque. Cela peut étendre Internet à différents environnements cloud et locaux. De plus, un patchwork d'appliances virtuelles, d'outils opérationnels et de politiques non standard introduit des lacunes connues et inconnues dans la couverture de sécurité, ce qui accroît les risques de sécurité.
- **Lacunes en matière de visibilité sur le trafic TLS.** L'inspection TLS peut utiliser d'importantes ressources de calcul et engendrer des problèmes tels qu'une dégradation des performances lorsqu'elle est activée. La gestion des certificats distribués ou l'application d'exclusions aux workloads épinglés posent des problèmes opérationnels. En outre, ces éléments augmentent souvent les coûts de l'infrastructure de cybersécurité pour couvrir l'évolutivité.
- **Accroissement de la complexité et baisse des performances.** Les solutions traditionnelles de réseau et de sécurité n'ont pas été conçues pour les workloads dans le cloud. Des produits ponctuels tels que des pare-feu virtuels, des proxys et des passerelles NAT doivent par conséquent être intégrés. Certaines solutions peuvent utiliser des VM distinctes pour chaque fonction de sécurité, ce qui exige une inspection séquentielle de type chaîne de montage, et augmente la latence. Cela génère d'importantes complexités opérationnelles lorsque cette configuration est appliquée à des environnements multicloud.
- **Coûts élevés.** L'utilisation de produits de sécurité réseau traditionnels (pare-feu, IPS, routeurs, etc.), le surprovisionnement de l'infrastructure de sécurité réseau pour compenser le manque d'évolutivité et l'utilisation croissante de services cloud natifs contribuent tous à l'augmentation des dépenses d'investissement et d'exploitation.
- **Absence de journalisation commune.** Certaines obligations légales et réglementaires exigent des entreprises qu'elles stockent des journaux pendant de longues périodes. L'accès à ces journaux à partir de différents environnements cloud et leur stockage dans un SIEM central peuvent s'avérer complexes et coûteux.



Étendre l'architecture Zero Trust aux clouds publics et aux data centers sur site

Zero Trust Cloud élimine la surface d'attaque du réseau en connectant les workloads et serveurs à Internet et aux applications privées via une architecture Zero Trust. Cette approche simplifie considérablement la connectivité en réduisant la dépendance de votre entreprise à l'égard des solutions traditionnelles de type pare-feu, tout en rendant le transfert de trafic plus flexible et en simplifiant la gestion des politiques grâce au cadre de politiques éprouvé de Zscaler Internet Access™ (ZIA) et Zscaler Private Access™ (ZPA).

Tout cela est rendu possible par la plateforme hyperscale Zero Trust Exchange, qui peut gérer toute augmentation du trafic des workloads et des serveurs, grâce à une évolutivité horizontale et flexible. Avec Zero Trust Cloud, l'ensemble du trafic sortant des workloads et des serveurs est acheminé vers Zero Trust Exchange, où des politiques de sécurité sont appliquées pour une inspection TLS/SSL et un contrôle d'accès complets.

Le trafic sortant est ensuite transmis vers sa destination finale, qu'il s'agisse d'Internet, d'applications SaaS ou d'autres workloads et serveurs hébergés dans d'autres clouds publics ou data centers.

Avec Zero Trust Cloud, vous pouvez :

Acquérir une protection cohérente et complète des données et contre les menaces

Appliquer des politiques de sécurité communes sur tous les environnements

- Prévenir les attaques de type « zero day » grâce à une inspection TLS et à une protection contre les menaces évolutives, adaptées au cloud
- Prévenir les fuites de données grâce à une inspection DNS et à une protection inline des données
- Limiter le nombre de destinations auxquelles les workloads et les serveurs peuvent accéder grâce à des contrôles stricts

Éliminer la surface d'attaque et les déplacements latéraux

Connecter les applications et non les réseaux pour que les ressources deviennent indétectables

- Appliquer un accès sur la base du moindre privilège pour segmenter les workloads en fonction de différents critères (IP, FQDN, VPC, VNet, balises)
- Interconnecter les workloads via Zero Trust Exchange, éliminant ainsi la surface d'attaque du réseau
- Prendre en charge les connexions de cloud à cloud, de cloud au data center, de région à région

Réduire les coûts opérationnels et la complexité

Utiliser une plateforme cloud unique pour sécuriser tous les workloads

- Sécuriser les workloads sur les principaux fournisseurs de services cloud, notamment AWS, Azure et GCP, à l'aide d'une plateforme unifiée
- Automatiser les déploiements de sécurité via des interfaces programmables, à l'aide de modèles IaC (Infrastructure as Code)
- Utiliser les intégrations fournies par les fournisseurs de services de cloud public tels que l'équilibreur de charge de la passerelle AWS, les balises définies par l'utilisateur d'AWS et la fonction d'auto scaling d'AWS

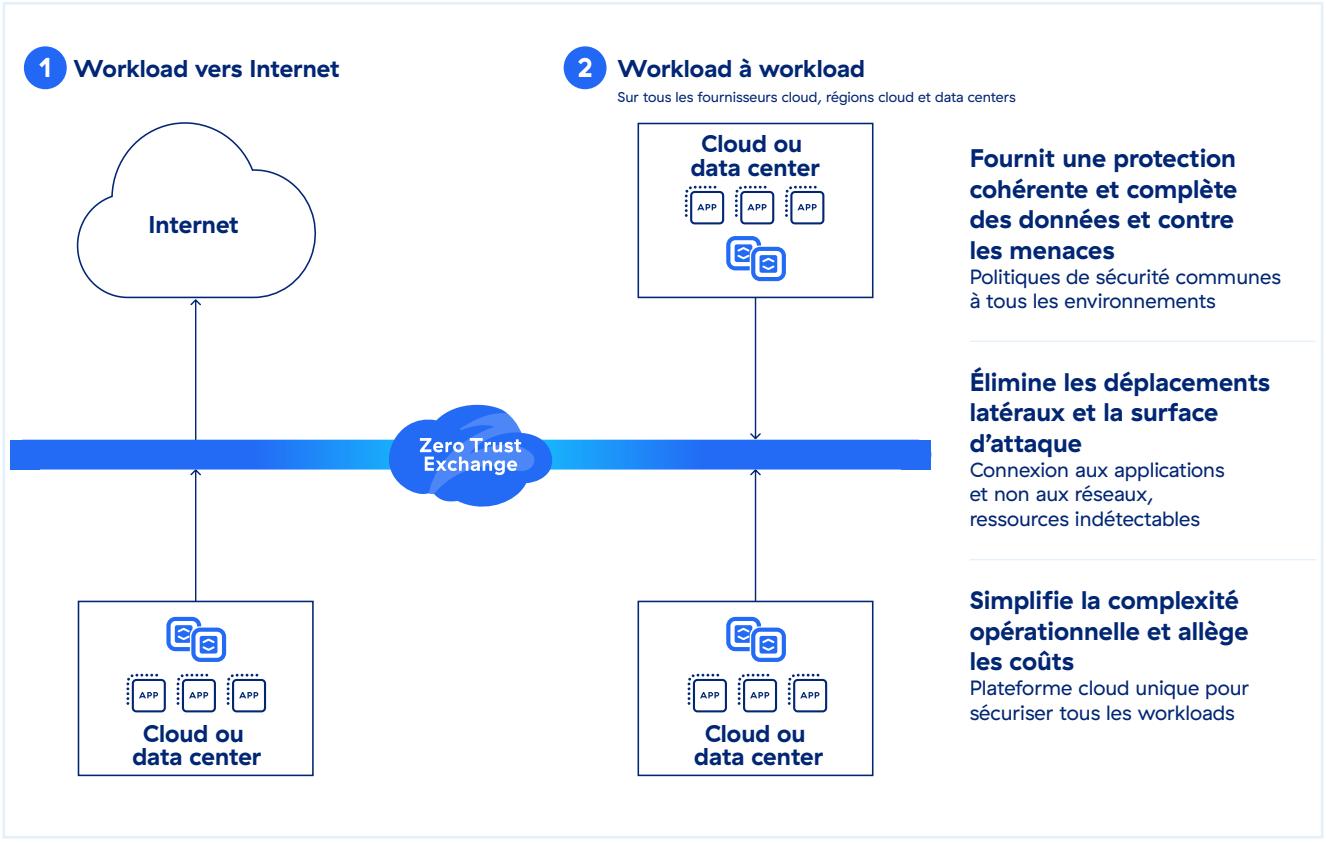


FIGURE : Zscaler Zero Trust for Workloads

Fonctionnalités de Zero Trust Cloud

Zero Trust Cloud Repose sur Zero Trust Exchange, une plateforme qui connecte en toute sécurité les utilisateurs, les appareils et les applications à l'aide de politiques d'entreprise, sur n'importe quel réseau et sur n'importe quel cloud, à grande échelle.

Architecture proxy Zero Trust : notre architecture de proxy dédiée et multi-entité inline connecte en toute sécurité les sources et les destinations tout en offrant une visibilité totale sur le trafic sortant.

Déchiffrement TLS à l'échelle du cloud : l'inspection de haute performance s'effectue par une architecture « Single-Scan, Multi-Action » conçue pour évoluer.

Segmentation granulaire d'application à application : un accès Zero Trust basé sur le moindre privilège pour tous les workloads et tous les serveurs simplifie l'application et la gestion des politiques d'entreprise.

Inspection bidirectionnelle des menaces : la protection contre les menaces optimisée par l'IA, alimentée par 500 000 milliards de signaux quotidiens et 320 milliards de transactions quotidiennes, offre une protection permanente sans faille contre les ransomwares, ainsi qu'une protection contre les menaces de type « zero day » et contre les malwares inconnus.

Protection des données inline : une inspection DLP hautes performances et évolutive est appliquée sur l'ensemble des canaux et des sites.

Plateforme commune, prête pour le multicloud : une plateforme unifiée assure la gestion des politiques, la surveillance du trafic et le suivi des journaux. Des politiques normalisées sont appliquées sur AWS, Azure, GCP et les data centers sur site.

Caractéristiques de Zero Trust Cloud

PLATEFORME ZSCALER ZERO TRUST CLOUD	
FONCTIONNALITÉS	**DESCRIPTION**
Couverture dans le cloud public et sur site	Sécurisez les workloads dans AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure China et AWS GovCloud. Les serveurs des data centers sur site sont également pris en charge. Certifié FedRamp pour AWS GovCloud.
Inspection TLS/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.
Diffusion des journaux	Consolidez les journaux de tous les workloads et serveurs, à l'échelle mondiale, dans un référentiel centralisé déterminé par votre entreprise, grâce à Zscaler Nanolog Streaming Service. Les administrateurs peuvent visualiser et exploiter les données de transaction des workloads cloud en temps réel.
Infrastructure as Code	Zscaler fournit des modèles Terraform qui automatisent le provisionnement et le déploiement des politiques de sécurité et des machines virtuelles Cloud Connector.
Prise en charge de la connectivité	Tirez parti d'IPsec, de tunnels GRE ou des Cloud Connectors pour diriger le trafic sortant des workloads vers Zero Trust Exchange. IPsec et GRE sécurisent le trafic des workloads vers Internet. Les Cloud Connectors sont utilisés pour sécuriser à la fois le trafic vers Internet et le trafic entre workloads.

ZSCALER INTERNET ACCESS POUR LE TRAFIC DES WORKLOADS VERS INTERNET	
FONCTIONNALITÉS	**DESCRIPTION**
Protection des communications entre les workloads et Internet	Prévenez les cybermenaces et les pertes de données pour les communications des workloads vers Internet. Cela comprend l'inspection SSL, l'IPS, le filtrage d'URL et la protection des données pour toutes les communications.
Filtrage d'URL	Autorisez, bloquez, surveillez ou cloisonnez l'accès des workloads à des catégories ou à des destinations Web spécifiques afin de neutraliser les menaces Web et garantir la conformité aux politiques de l'entreprise.
Protection contre les menaces avancées	Neutralisez les cyberattaques avancées telles que les malwares, les ransomwares, les attaques sur la chaîne d'approvisionnement, 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.
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.
Prévention d'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 workloads. Les systèmes de prévention d'intrusions (IPS) cloud et Web fonctionnent de manière transparente avec les pare-feu, le sandboxing et la DLP.
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.
Filtrage DNS	Contrôlez et bloquez les requêtes DNS vers des destinations connues et malveillantes.
Contrôle des fichiers	Bloquez ou autorisez le téléchargement/chargement de fichiers vers ou depuis des applications, en fonction de l'identité du workload ou de l'application.
Contrôle de la bande passante	Appliquez des politiques de bande passante et donnez la priorité aux applications stratégiques au détriment d'autres types de trafic à usage récréatif.
Politique de sécurité et d'accès dynamique basée sur les risques	Adaptez automatiquement votre politique de sécurité et d'accès aux risques liés aux workloads, aux serveurs, aux destinations Internet et au contenu.
Informations corrélées 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.
Filtrage du contenu et règles avec état	Le filtrage se base sur 6 classes, 101 catégories et 29 super-catégories. Tirez parti de la classification dynamique du contenu pour les URL inconnues et les recherches de type Safe Search. Appliquez une politique granulaire par adresse IP, groupes et identités hébergées.

ZSCALER PRIVATE ACCESS POUR LE TRAFIC ENTRE WORKLOADS	
FONCTIONNALITÉS	**DESCRIPTION**
Segmentation workload à workload	Sécurisez la connectivité et les communications entre workloads au sein des environnements hybrides et multicloud.
Identification des applications	Découvrez et répertoriez automatiquement les applications à l'aide de noms de domaine et de sous-réseaux IP spécifiques pour disposer d'informations granulaires sur votre écosystème d'applications privées et sur votre surface d'attaque potentielle.
Segmentation des applications optimisée par l'IA	Appliquez les recommandations de segmentation optimisées par l'AA et automatiquement fournies dans ZPA afin d'identifier rapidement et facilement les segments d'applications pertinents et élaborer des politiques d'accès appropriées. La segmentation optimisée par l'AA vous aide à minimiser votre surface d'attaque interne grâce à des modèles d'AA entraînés sur des millions de signaux provenant de clients et sur vos propres profils d'accès aux applications.
Protection des applications	Protégez les applications privées et l'infrastructure contre les principales attaques grâce à une inspection de sécurité performante et inline de l'ensemble des payloads des applications. Identifiez et maîtrisez les risques de sécurité Web connus, tels que les menaces du Top 10 de l'OWASP, ainsi que les vulnérabilités émergentes de type « zero day » qui peuvent contourner les fonctions traditionnelles de sécurité réseau.

ZSCALER DATA PROTECTION	
FONCTIONNALITÉS	**DESCRIPTION**
Protection des données inline (données en transit)	Pour le trafic des workloads vers Internet et le trafic entre workloads, utilisez les fonctionnalités de proxy de transfert et d'inspection SSL pour contrôler en temps réel les flux d'informations sensibles vers des destinations Web et des applications cloud à risque. Vous neutralisez ainsi les menaces internes et externes qui pèsent sur les données. Une protection inline avancée est fournie, qu'une application soit autorisée ou non, sans nécessiter de journalisation des périphériques réseau.
Exact Data Match (EDM)	Désigne la prise d'empreinte (« fingerprinting ») et la sécurisation des données d'entreprise.
Index Document Match (IDM)	Désigne la prise d'empreinte (« fingerprinting ») et la sécurisation des documents et formulaires spécifiés.
Reconnaissance optique de caractères (OCR)	Désigne la recherche et la protection contre la perte de données via des images et des captures d'écran.

(Les fonctionnalités énumérées ne sont pas exhaustives. La disponibilité des fonctionnalités et capacités peut varier selon les versions de Zscaler.)

ZSCALER ZERO TRUST CLOUD – VERSIONS	
NOM DE LA VERSION	**CAPACITÉS**
Zero Trust for Workloads – Version Standard	• Abonnement annuel à 1 Go de trafic mensuel pour la version Standard de Zero Trust for Workloads • Inclut le filtrage d'état et Cloud Connector
Zero Trust for Workloads – Version Advanced	• Toutes les fonctionnalités disponibles dans la version Standard • Internet Access for Workloads : inspection SSL/TLS, protection contre les menaces avancées, Cloud NSS, ancrage IP source • Private Access for Workloads : segments d'application, sous-emplacement, LSS Standard, journalisation et création de rapports • Data Protection for Workloads : Web inline (en mode moniteur uniquement) • Cyber Protection for Workloads : pare-feu standard, contrôle DNS
Zero Trust for Workloads – Version Advanced Plus	• Toutes les fonctionnalités disponibles dans la version Advanced • Data Protection for Workloads : protection des données inline et classification avancée • Cyber Protection for Workloads : Firewall Advanced for Workloads, Sandbox Advanced for Workloads

zscaler™ | Experience your world, secured.™

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 les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 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 Twitter **@zscaler**.

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