Zero Trust Cloud

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

FICHE TECHNIQUE

La transformation numérique stimule la création et l'utilisation de workloads dans un large éventail de data centers sur site, de clouds privés et publics. Votre entreprise dépend de ces workloads et il est donc essentiel de les protéger contre les cyberattaques et la perte de données.

Les architectures traditionnelles telles que les pare-feu et les VPN 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 entre les workloads et Internet, et entre les workloads, dans vos data centers sur site, vos clouds privés et publics.

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.

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 combinent les mesures suivantes :

- Configuration de solutions de sécurité natives proposées par les fournisseurs de services cloud
- Déploiement d'outils tiers tels que le pare-feu, l'inspection TLS, la DLP, etc.
- 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 :

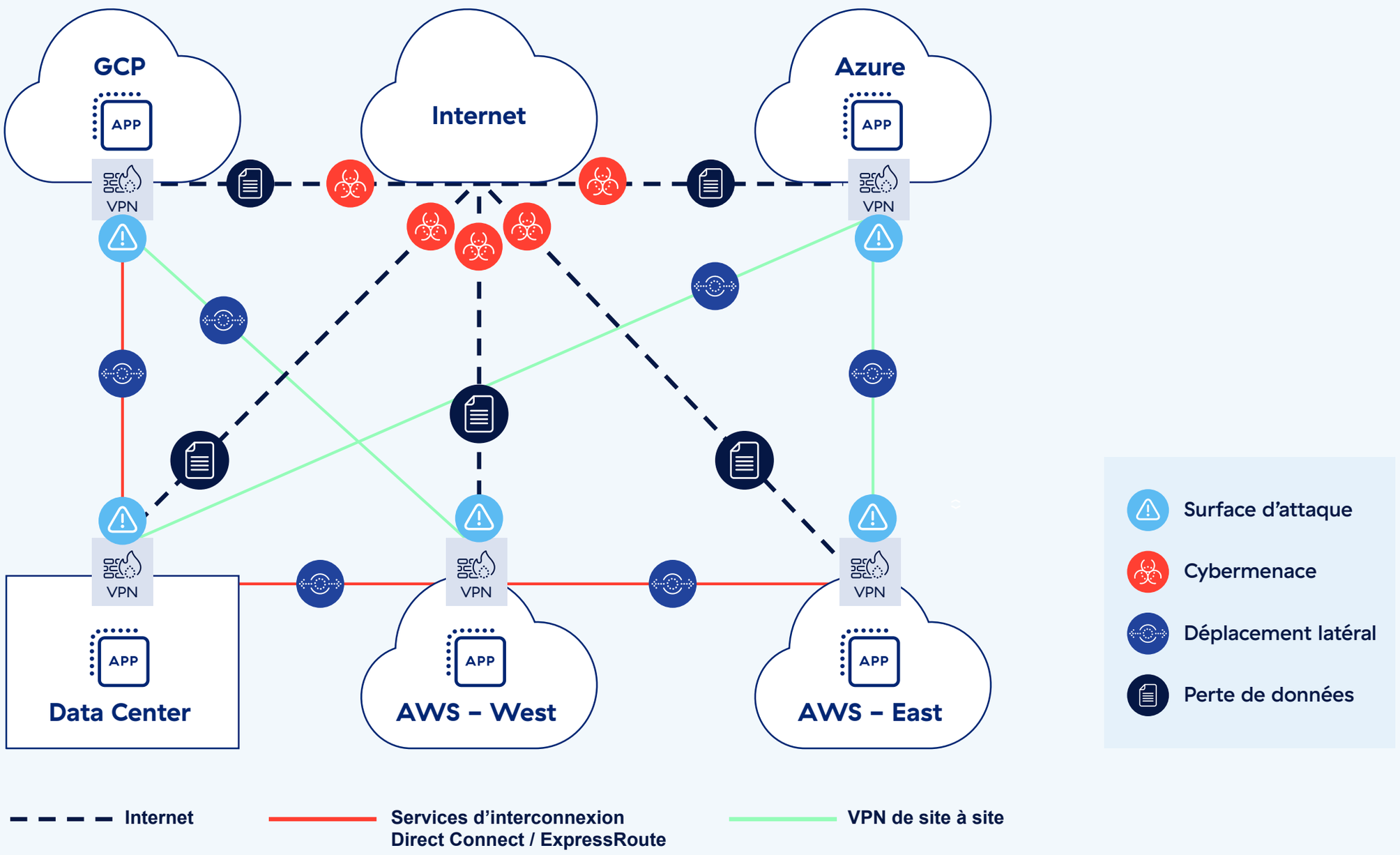
- **Augmentation de la surface d'attaque et des opportunités de déplacements latéraux.** Les solutions telles que les pare-feu étendent le réseau aux workloads, ce qui amplifie les risques de déplacements latéraux. Chaque pare-feu connecté à Internet élargit également la surface d'attaque. Cela peut 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. L'inspection TLS à grande échelle augmente également les coûts opérationnels et d'infrastructure.

- **Accroissement de la complexité et baisse des performances.** Les solutions traditionnelles de réseau et de sécurité ne sont pas 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 ponctuels de sécurité réseau traditionnels, tels que les pare-feu et les VPN, entraîne un surprovisionnement de l'infrastructure. Le déploiement d'outils de sécurité cloud natifs auprès de plusieurs fournisseurs de services cloud nécessite des ressources hautement spécialisées.

- **Stockage inefficace des journaux.** 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.



©2025 Zscaler, Inc. Tous droits réservés.

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

Zero Trust Cloud élimine la surface d'attaque du réseau en connectant vos 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 telles que les pare-feu et les VPN, 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 Zero Trust Exchange qui s'adapte à la fois verticalement et horizontalement. Avec Zero Trust Cloud, l'ensemble du trafic des workloads 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, telle qu'Internet, des applications SaaS ou d'autres workloads hébergés dans des data centers sur site, des clouds privés ou publics.

Avec Zero Trust Cloud, vous pouvez :

ACQUÉRIR UNE PROTECTION COHÉRENTE ET COMPLÈTE DES DONNÉES ET CONTRE LES MENACES

Appliquer des politiques de sécurité uniformes aux data centers sur site, clouds privés et publics

- Prévenir les attaques de type « zero day » grâce à une inspection TLS et à une protection contre les menaces 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 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

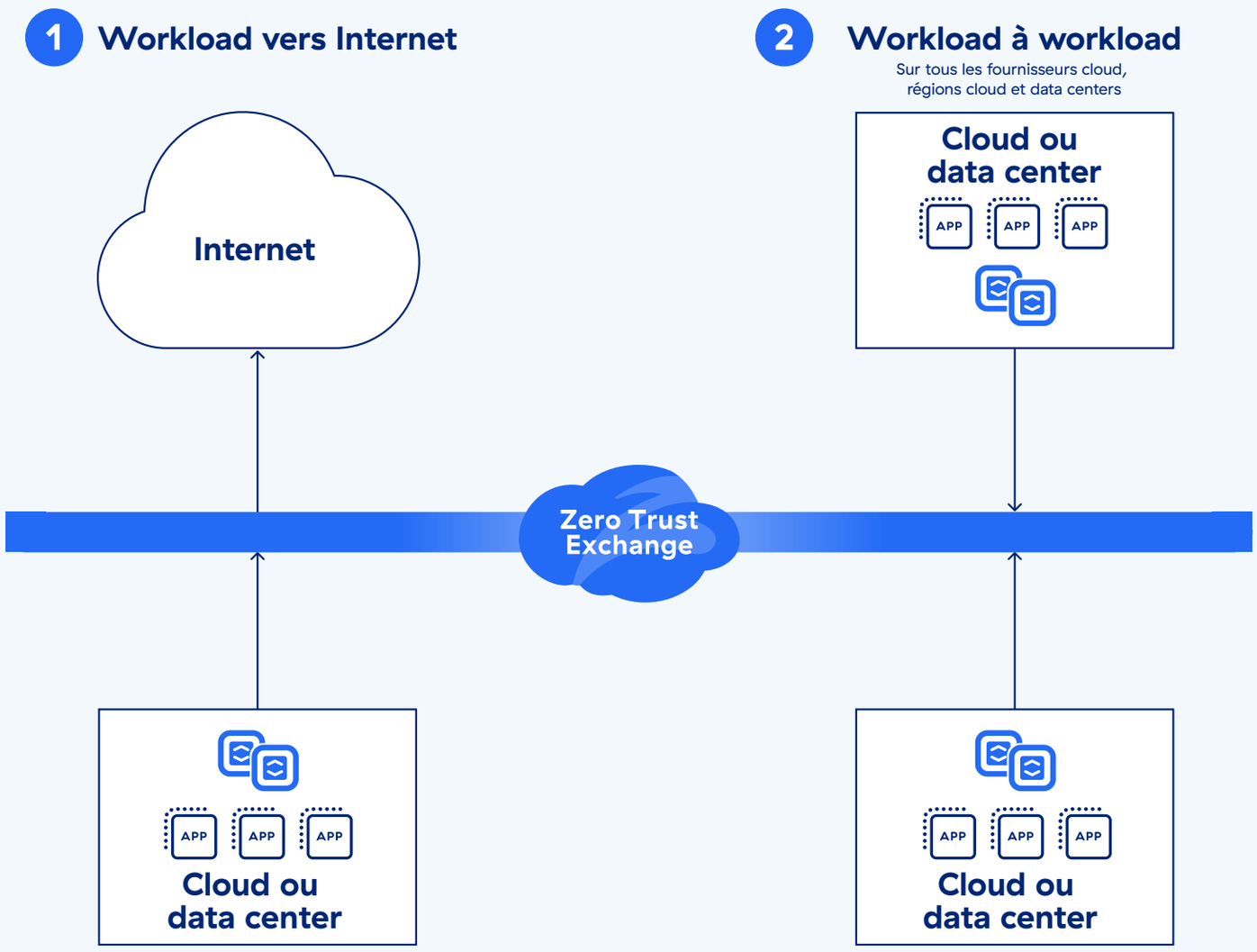
- Appliquer un accès sur la base du moindre privilège pour segmenter les workloads sur la base de différents critères (IP, FQDN, VPC, VNet, balises définies par l'utilisateur)
- Interconnecter les workloads via Zero Trust Exchange, éliminant ainsi la surface d'attaque du réseau
- Prendre en charge les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

RÉDUIRE LES COÛTS OPÉRATIONNELS ET LA COMPLEXITÉ

Utiliser une plateforme de sécurité unique pour protéger tous les workloads dans vos clouds

- 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, notamment les API Zscaler, Hashicorp Terraform et AWS CloudFormation
- Tirer parti des intégrations intégrées avec les CSP pour faire évoluer l'infrastructure, optimiser les chemins vers le cloud et simplifier les définitions de règles grâce aux métadonnées cloud

©2025 Zscaler, Inc. Tous droits réservés.



Protection cohérente des données et contre les menaces
Politiques de sécurité communes à tous les environnements

Élimine les déplacements latéraux et la surface d'attaque
Connexion aux applications et non aux réseaux, ressources indétectables

Simplifie la complexité opérationnelle et allège les coûts
Plateforme cloud unique pour sécuriser tous les 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 hautes performances 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 traitées chaque jour, offre une protection permanente et robuste contre les ransomwares, une prévention des menaces de type « zero day » et une défense 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.

©2025 Zscaler, Inc. Tous droits réservés.

Caractéristiques de Zero Trust Cloud

PLATEFORME ZSCALER ZERO TRUST CLOUD	
FONCTIONNALITÉS	**DÉTAILS**
Clouds privés, publics et sur site	Prend en charge la sécurisation des workloads dans AWS, Microsoft Azure, Google Cloud Platform et les data centers sur site. La solution prend en charge des régions spécifiques, notamment Microsoft Azure China et AWS China. De plus, elle est compatible avec AWS GovCloud et Microsoft Azure GovCloud, avec les certifications FedRAMP Moderate et High (niveau d'impact modéré et élevé).
Inspection TLS/SSL	Bénéficiez d'une inspection du trafic TLS/SSL à l'échelle du cloud 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 de diverses exigences en matière de confidentialité ou de réglementation.
Segmentation intra-régionale	Sécurisez les workloads grâce à la segmentation entre VPC ou entre sous-réseaux au sein d'une région cloud spécifique. Assurez la prise en charge des balises source et de destination dans la politique de transfert de trafic interne.
Diffusion des journaux	Regroupez les journaux des workloads et des serveurs à l'échelle mondiale dans un référentiel central défini par votre entreprise. Les administrateurs peuvent visualiser et exploiter les données de transaction des workloads cloud.
Infrastructure as Code	Automatisez les déploiements de sécurité via des interfaces programmables, notamment les API Zscaler, Hashicorp Terraform et AWS CloudFormation.
Prise en charge de la connectivité	Utilisez des connecteurs dédiés ou des offres de services gérés Zscaler pour diriger le trafic. Vous pouvez également exploiter vos tunnels IPsec ou GRE existants.

ZSCALER INTERNET ACCESS POUR LE TRAFIC DES WORKLOADS VERS INTERNET	
FONCTIONNALITÉS	**DÉTAILS**
Protection des communications des workloads vers Internet	Prévenez les cybermenaces et la perte de données pour les communications des workloads vers Internet. Comprend l'inspection TLS, les systèmes de prévention d'intrusions (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.

©2025 Zscaler, Inc. Tous droits réservés.

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 de fichiers vers/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 de 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	**DÉTAILS**
Segmentation workload à workload	Sécurisez la connectivité et les communications entre workloads au sein des environnements hybrides et multicloud.
Identification d'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 OWASP, ainsi que les vulnérabilités émergentes de type « zero day » qui peuvent contourner les fonctions traditionnelles de sécurité réseau.

©2025 Zscaler, Inc. Tous droits réservés.

ZSCALER DATA PROTECTION	
FONCTIONNALITÉS	**DÉTAILS**
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.
Correspondance de documents indexés (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	
NIVEAU DE FONCTIONNALITÉS	**CAPACITÉS**
Zero Trust for Workloads – Version Standard	• Abonnement annuel par Go (gigaoctet) de trafic mensuel pour Zero Trust for Workloads Standard : • Inclut le filtrage du contenu
Zero Trust for Workloads – Version Advanced	• Toutes les fonctionnalités disponibles dans la version Standard • Accès Internet pour l'inspection SSL/TLS, la protection contre les menaces avancées, Cloud NSS, l'ancrage IP source • Private Access for Workloads : segments d'application, sous-emplacement, journalisation et création de rapports LSS Standard • Data Protection for Workloads : Web inline (en mode moniteur uniquement) • Cyber Protection for Workloads : pare-feu standard • Segmentation interne
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

Zero Trust Cloud est disponible en deux modes de déploiement. Avec l'option Virtual Machine (VM), les clients bénéficient d'un contrôle complet de leur infrastructure cloud en déployant les composants Zero Trust sous forme de machine virtuelle. Avec Zero Trust Gateway, les clients peuvent utiliser les fonctionnalités comme un service cloud natif entièrement géré par Zscaler. Les deux modes de déploiement offrent les mêmes fonctionnalités. Zero Trust Gateway est disponible dans les versions Zero Trust for Workloads Advanced et Zero Trust for Workloads Advanced Plus.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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