FICHE TECHNIQUE

Zscaler Internet Access

Protection optimisée par IA pour tous les utilisateurs, applications et sites

Zscaler Internet Access™ : un accès Internet et SaaS sûr et rapide, adossé à une plateforme Zero Trust très efficace.

La sécurité réseau traditionnelle n'est plus efficace dans un monde qui fait la part belle au cloud et à la mobilité
Les architectures traditionnelles en étoile étaient efficaces lorsque les utilisateurs travaillaient principalement au siège ou sur un site d'entreprise, que les applications étaient exclusivement hébergées dans le data center d'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 sur la chaîne collaborative et d'autres menaces avancées parviennent à percer les défenses traditionnelles du réseau. Le moment est venu de trouver une solution globale de sécurité cloud native capable de maîtriser les risques et la complexité tout en offrant la flexibilité nécessaire au bon déroulement des projets d'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 du 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 SaaS évolutive à partir du plus vaste cloud de sécurité au monde, cette solution remplace les outils de sécurité réseau traditionnels afin de neutraliser les attaques avancées et de prévenir les

Avantages :

- **Prévention des cybermenaces et de 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 IA et enrichis par des mises à jour en temps réel issues de 500 000 milliards de signaux quotidiens de menace en provenance 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 doper votre productivité et l'agilité de votre entreprise.

pertes de données, grâce à une approche Zero Trust intégrale qui offre les avantages suivants :

Sécurité optimale pour les collaborateurs hybrides modernes : 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 ultrarapide sans infrastructure à déployer : la connectivité Direct-to-Cloud (accès local et direct vers Internet et le cloud) garantit une expérience utilisateur rapide et transparente, éliminant tout backhauling, améliorant les performances et l'expérience utilisateur, et simplifiant l'administration du réseau. Et ce, sans infrastructure physique.

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

Gestion simplifiée : votre équipe peut se consacrer aux objectifs stratégiques de votre entreprise en utilisant notre solution de sécurité cloud native optimisée par IA, sans matériel à administrer, et avec des workflows simplifiés et des politiques créées spécifiquement pour votre entreprise.

*Magic Quadrant de Gartner dédié au Security Service Edge, 10 avril 2023, Charlie Winckless et al.

Services intégrés et optimisés par IA pour la sécurité des données

Zscaler Internet Access propose une suite complète de services de sécurité et de protection des données, optimisée par IA et destinée à vous aider à déjouer les cyberattaques et prévenir les pertes de données. En tant que solution SaaS entièrement fournie depuis le cloud, vous pouvez activer rapidement de nouvelles fonctionnalités sans déployer aucun matériel supplémentaire. Les modules proposés par Zscaler Internet Access sont les suivants :

- **Cloud Secure Web Gateway (SWG) :** cette passerelle de sécurité Web assure une expérience Web sûre et rapide qui élimine les ransomwares, les malwares et autres attaques avancées, grâce à une analyse et un filtrage des URL en temps réel, optimisés par 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) :** ce service cloud de prévention des pertes de données protége les données en transit à l'aide d'une fonction d'inspection inline et de fonctionnalités sophistiquées comme la correspondance exacte des données (Exact Data Match, EDM), la reconnaissance optique des caractères (OCR) et l'apprentissage automatique.

- **Zscaler Firewall & cloud IPS :** étendez une protection optimale à tous les ports et protocoles, et remplacez vos pare-feu edge et sur sites distants par une plateforme cloud native.
- **Zscaler Sandbox :** déjouez les malwares furtifs et inconnus qui utilisent les protocoles Web et de transfert de fichiers. Bénéficiez d'une mise en quarantaine basée sur IA, et assurez une protection en temps réel, cohérente et globale pour tous les utilisateurs.
- **Cloud Browser Isolation :** cette fonction d'isolation du navigateur tire parti de l'IA pour déjouer les attaques Web et prévenir toute perte de données, en cloisonnant virtuellement (« air-gap ») les utilisateurs, le Web et les applications SaaS.
- **Digital Experience Monitoring :** maîtrisez vos coûts informatiques et traitez plus rapidement vos demandes de support grâce à une visibilité unifiée sur les indicateurs de performances liées aux applications, aux chemins d'accès au cloud et aux terminaux. Vous simplifiez ainsi vos analyses et les opérations de dépannage.
- **Connectivité Zero Trust pour les sites distants :** maîtrisez les risques et la complexité grâce à une connectivité pour les sites distants et data centers, capable de prendre en charge les utilisateurs, les serveurs et les dispositifs IoT/OT.
- **Sécurité des 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 instances

Avec Zscaler Internet Access, éliminez les risques qui pèsent sur les instances cloud accédant à Internet ou au SaaS. Les instances n'ont plus besoin d'accéder à Internet par le biais d'outils réseau traditionnels, tels que les VPN, les pare-feu (y compris les pare-feu virtuels) ou les technologies WAN. Vous pouvez prévenir les intrusions et le déplacement latéral des menaces sans devoir recourir à un mix hétérogène d'outils de sécurité. En appliquant aux instances la suite complète des fonctionnalités de sécurité et de protection des données de ZIA, vous offrez une sécurité Zero Trust pour vos utilisateurs et vos instances, à l'aide de cette plateforme unifiée et intégrée.

En associant ZIA à Zscaler Private Access, vous élargissez la protection à vos applications et instances privées, que ces dernières résident dans le cloud public ou dans un data center privé.

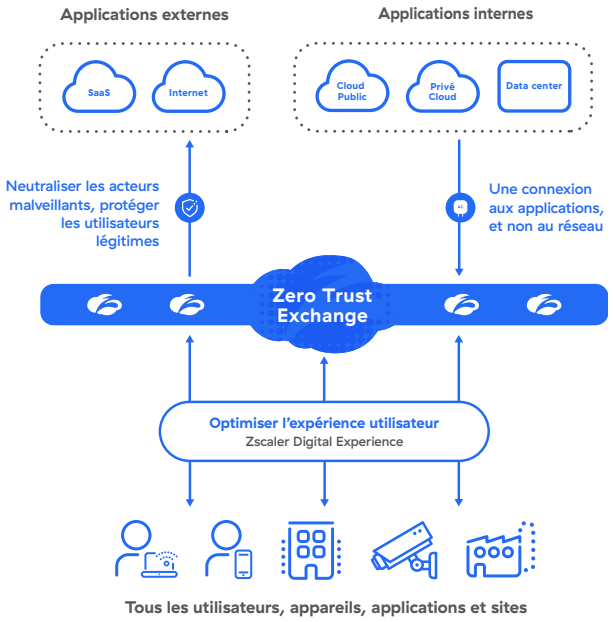

Illustration 1 : Zero Trust Exchange

Cas d'utilisation

Protection contre les cybermenaces et les ransomwares

Migrez d'une sécurité réseau traditionnelle vers l'architecture révolutionnaire Zero Trust de Zscaler qui prévient les intrusions, élimine la surface d'attaque, neutralise le déplacement latéral de menaces et protège les données.

En savoir plus ➞

Sécurisation des collaborateurs hybrides

Permettez aux collaborateurs, partenaires, clients et fournisseurs d'accéder en toute sécurité aux applications Web et aux services cloud, où qu'ils se trouvent, depuis n'importe quel appareil, et assurez-leur une expérience digitale de qualité.

En savoir plus ➞

Protection des données

Prévenez les pertes de données au niveau des utilisateurs, des applications SaaS et de l'infrastructure de cloud public, des pertes qui résultent d'une exposition fortuite à des risques, d'un détournement 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, rapide et sécurisé au cloud qui dispense de déployer des pare-feu sur l'edge ou sur les sites distants.

En savoir plus ➞

Écosystème de Zscaler Zero Trust Exchange

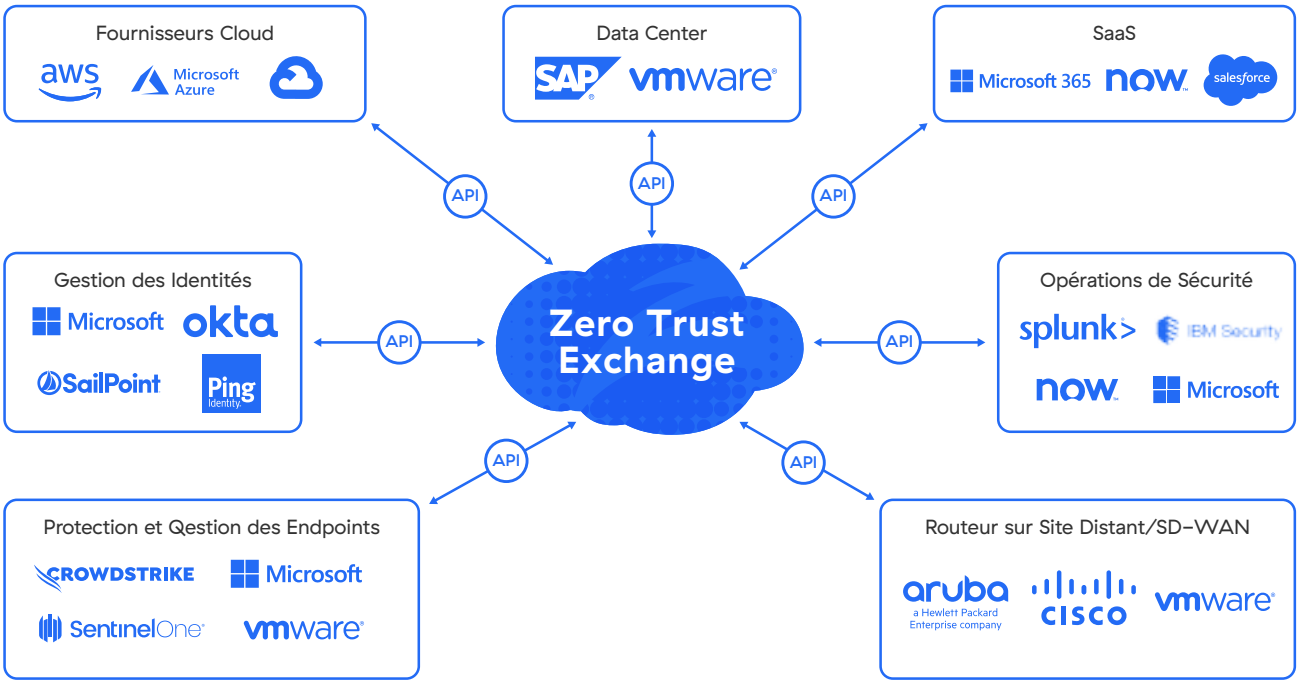

Illustration 2 : Écosystème des partenaires de Zscaler Internet Access

TABLEAU 1 : FONCTIONNALITÉS ET CAPACITÉS DE ZSCALER INTERNET ACCESS	
FONCTIONNALITÉ	**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 contrer les menaces Web et garantir la conformité aux politiques de l'entreprise.
Inspection SSL	Bénéficiez d'une inspection illimitée du trafic TLS/SSL pour identifier les menaces et tentatives d'exfiltration des données qui se dissimulent dans le trafic chiffré. Spécifiez les catégories ou applications Web à inspecter en fonction des exigences de confidentialité ou réglementaires.
Sécurité DNS	Identifiez et acheminez les connexions suspectes de type C&C (Command & Control) vers les moteurs Zscaler de détection de menaces pour une inspection complète du contenu.
Contrôle des fichiers	Bloquez ou autorisez le téléchargement/téléversement de fichiers vers ou depuis des applications, en fonction de l'application, de l'utilisateur ou d'un groupe d'utilisateurs.
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 à usage récréatif.
Protection contre les menaces avancées	Déjouez les cyberattaques avancées telles que les malwares, les ransomwares, les attaques sur la chaîne collaborative ou encore le phishing, grâce à une protection propriétaire contre les menaces avancées. Définissez des politiques granulaires en fonction de la tolérance au risque de votre entreprise.
Protection inline des données (données en transit)	Utilisez des fonctionnalités de forward proxy et d'inspection SSL pour contrôler en temps réel les flux d'informations sensibles vers des destinations Web et des applications cloud à risque, afin de neutraliser les menaces internes et externes qui ciblent les données. Une protection inline sophistiquée est assurée pour toutes les applications, qu'elles soient autorisées ou non, sans faire appel aux logs des dispositifs réseau.
Protection hors bande des données (données au repos)	Utilisez des intégrations par API pour analyser les applications SaaS, les plateformes cloud et leur contenu afin d'identifier les données sensibles au repos et les protéger automatiquement, notamment 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 collaborent en toute transparence avec les fonctions de pare-feu, de sandbox, de DLP et de CASB.
Politique de sécurité et d'accès dynamique basée sur les risques	Adaptez automatiquement votre politique de sécurité et d'accès aux risques liés aux utilisateurs, aux appareils, aux applications et au contenu.
Capture de trafic	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, grâce à l'IA et l'apprentissage automatique (AA) qui neutralisent les attaques de type patient zéro.
Filtrage de DNS	Contrôlez et bloquez les requêtes DNS vers des destinations connues et malveillantes.
Isolation Web	Déjouez les menaces Web en restituant du contenu actif sous forme d'image dans 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. Bénéficiez d'une visibilité sur le score des menaces, les ressources affectées, le niveau de 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.
Monitoring de l'expérience digitale	Dans le cadre de vos analyses et opérations de dépannage, obtenez une visibilité unifiée sur les indicateurs de performances des applications, des chemins d'accès au cloud et des terminaux.
Connectivité Zero Trust sur les sites distants	Modernisez la connectivité sur les sites distants avec Zero Trust Exchange en éliminant la surface d'attaque et en empêchant toute propagation de menaces en interne.
Protection des communications entre les instances et Internet	Prévenez toute compromission et les déplacements latéraux pour les communications entre les instances et Internet. Tirez parti de l'inspection SSL, de l'IPS, du filtrage d'URL et de la protection des données pour toutes vos communications.
Visibilité sur les dispositifs IoT	Bénéficiez d'une visibilité complète sur les dispositifs IoT, les serveurs et les appareils personnels de vos utilisateurs, grâce à un processus automatisé d'identification, un monitoring permanent, une classification optimisée par IA/AA et des fonctionnalités d'étiquetage automatique de ces équipements.

FONCTIONNALITÉ	DESCRIPTION
Fonctionnalités de la plateforme	
Flexibilité des options de connectivité	• **Zscaler Client Connector (ZCC) :** acheminez le trafic vers Zero Trust Exchange via cet agent léger compatible avec Windows, macOS, iOS, iPadOS, Android et Linux. • **Tunnels GRE ou IPsec :** utilisez des tunnels GRE et/ou IPsec pour acheminer le trafic vers Zero Trust Exchange pour les appareils qui ne disposent pas de Zscaler Client Connector. • **Isolation du navigateur :** connectez de manière transparente tous les appareils BYOD (appareils personnels utilisés à des fins professionnelles) ou non gérés, grâce à la fonction Cloud Browser Isolation. • **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. • **Fichiers PAC :** acheminez le trafic vers Zero Trust Exchange avec des fichiers PAC pour les appareils qui ne disposent pas de Zscaler Client Connector.
Services fournis depuis le cloud	Plateforme 100 % cloud et services fournis en tant que SaaS. Pour des cas d'utilisation spécifiques, des Services Edges privés et virtuels sont disponibles.
Confidentialité et conservation des données	Lors de la mise en log des données, le contenu n'est jamais écrit sur disque. 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, assurer l'anonymisation/l'obscurcissement du nom d'utilisateur, et offrir des droits d'accès différenciés par département ou fonction, conformément aux principales réglementations de conformité en vigueur. Les données sont conservées pendant une période renouvelable de six mois ou moins, selon le produit. Vous pouvez investir dans des capacités de stockage supplémentaire pour conserver les données aussi longtemps que vous le souhaitez.
Principales certifications de conformité	Ces certifications sont : • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C Accédez à la liste de nos certifications de conformité ici.
Compatibilité avec les API	Nous assurons des intégrations API REST avec de nombreux fournisseurs de service d'identité, de réseau et de sécurité. Vous pouvez, par exemple, partager vos journaux depuis Zscaler vers votre SIEM basé dans le cloud ou sur site (Splunk, par exemple). En savoir plus
Peering direct	Le peering direct avec les principaux fournisseurs d'Internet et de SaaS, et avec les environnements de cloud public garantit un routage ultrarapide du trafic.
Accords de niveau de service (SLA)	
Disponibilité	99,999 %, disponibilité mesurée selon le nombre de transactions perdues
Latence du proxy	< 100 ms, y compris lorsque l'analyse antimalware et l'analyse DLP sont activées
Identification de virus	100 % des virus et malwares connus
Plateformes et systèmes compatibles	
Client Connector	Compatible avec : • iOS 9 ou versions ultérieures • Android 5 ou versions ultérieures • Windows 7 et versions ultérieures • Mac OS X 10.10 et versions ultérieures • CentOS 8 • Ubuntu 20.04 En savoir plus
Branch Connector	Compatible avec : • VMware vCenter ou vSphere Hypervisor • Centos • Redhat

Éditions Zscaler Internet Access

	Capacités	Essentials	Business	Transformation	Unlimited
Services de la plateforme		Filtrage de contenu, antivirus inline, inspection SSL, Nanolog Streaming Service (NSS)	(+) Certificat SSL privé	(+) Cloud NSS, récupération des logs NSS, accès étendu au data center, tunnel IPSec, alertes contextuelles, ZIA Virtual Private Service Edge (8)	(+) Ancrage de l'IP source, environnement de test, catégorisation des priorités, serveur ZIA Virtual Private Service Edge (32) et protection de l'IoT (1 Go/10 utilisateurs)
Protection contre les menaces	**Protection contre les menaces avancées (comprenant une détection optimisée par IA du phishing et des communications C&C)** Protection contre les menaces connues et inconnues (URL, antivirus, botnet/C2, phishing)	Oui	Oui	Oui	Oui
	Sandbox cloud Prévention des attaques de type « zero-day » via une analyse des fichiers suspects et une mise en quarantaine optimisée par IA	Module complémentaire	Module complémentaire	Oui	Oui
	Isolation – Protection contre les cybermenaces Protection contre les attaques de type « zero day » issues de contenus Web suspects . Isolation optimisée par IA, selon le niveau de risque	Module complémentaire	Module complémentaire	Isolation – Protection contre les cybermenaces : Standard (100 Mo/utilisateur/mois)	Isolation – Protection contre les cybermenaces : Standard (1,5 Go/utilisateur/mois)
	Informations corrélées sur les menaces Accélère les enquêtes et renforce la réactivité grâce à une veille contextuelle sur les menaces	–	Oui	Oui	Oui
	Politique dynamique basée sur le risque Recommande automatiquement des politiques de sécurité en fonction de divers facteurs de risque	–	–	Oui	Oui
	Technologie de leurre Renforce votre posture de sécurité Zero Trust en leurrant les assaillants actifs, ces derniers étant amenés à se révéler	–	–	Standard[1]	Standard[1]
Transformation du réseau	**Résolution et filtrage DNS** Résolveur DNS de confiance pour une résolution DNS géolocalisée et optimale	Jusqu'à 64 règles	Jusqu'à 64 règles	Oui	Oui
	Détection des tunnels DNS Détection et prévention des attaques sur les DNS et de l'exfiltration de données via des tunnels DNS	–	–	Oui	Oui
	Contrôle de bande passante Contrôle du trafic et priorisation de la bande passante, limitation du débit pour le trafic Web		Oui	Oui	Oui
	Pare-feu cloud Sécurité du télétravail pour tous les utilisateurs et le trafic (Web et non-Web) avec inspection SSL illimitée	Réseau, services applicatifs, sites, FQDN jusqu'à 10 règles	Réseau, services applicatifs, sites, FQDN jusqu'à 10 règles	(+) Utilisateurs et sites de télétravail, inspection DPI des applications	(+) Utilisateurs et sites de télétravail, inspection DPI des applications
	Protection contre le trafic non authentifié Protection des réseaux avec une sécurité de fiabilité opérateur entièrement automatisée et avec des seuils de limite	0,5 Go/utilisateur/mois	1 Go/utilisateur/mois	1,5 Go/utilisateur/mois	2 Go/utilisateur/mois

	Capacités	Essentials	Business	Transformation	Unlimited
Protection des données et prévention des pertes de données	**Contrôle des applications cloud + restrictions sur le Tenant** Identification d'applications à risque ou non autorisées (Shadow IT) et contrôle de leur utilisation	Oui	Oui	Oui	Oui
	Isolation – Protection des données (SaaS) Prévention des pertes de données des applications SaaS vers des appareils personnels (BYOD) ou non gérés (sans agent client)	Module complémentaire	Module complémentaire	Module complémentaire	Isolation pour la protection des données (SaaS) : Standard (100 Mo/utilisateur/mois)
	DLP, CASB, Inline Web Essentials, API SaaS (1 application) Prévention des pertes de données sensibles sur Internet ; Analyse d'une application SaaS pour détecter le partage à risque de données sensibles ou de malware	–	Protection des données : Standard (DLP et CASB Essentials)	(+) Rétro-analyse des API SaaS	Oui
	API SaaS, sécurité de la chaîne collaborative SaaS, appareils non gérés, classification, gestion des incidents Avantages de la protection des données de l'édition Standard plus : contrôle des risques liés aux appareils BYOD en diffusant les données sous forme d'image ; analyse de plusieurs applications SaaS pour détecter les partages à risque et les malwares ; personnalisation de la DLP avec fonctions EDM, IDM et OCR ; outils de gestion des incidents et d'automatisation des workflows	Module complémentaire	Module complémentaire	Module complémentaire	Oui
Monitoring de l'expérience digitale	Surveillance des expériences digitales des utilisateurs finaux afin d'optimiser les performances et de résoudre rapidement les problèmes liés aux applications, au réseau et aux appareils	–	Standard	Standard	Standard
Premium Support Plus		Module complémentaire	Module complémentaire	Module complémentaire	Oui

Modèle de licence

Toutes les éditions/versions de Zscaler Internet Access sont facturées selon le nombre d'utilisateurs. Pour certains produits de votre version, la tarification peut varier en fonction 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 permet des connexions rapides et sécurisées tout en permettant à vos collaborateurs de travailler d'où ils le souhaitent, en utilisant Internet comme réseau d'entreprise. Avec pour fondement le principe du Zero Trust et l'accès sur la base du moindre privilège, cette solution fournit une sécurité complète grâce à une gestion contextuelle des identités et à l'application des politiques.

> « Lorsque d'autres entreprises sont victimes d'attaques de ransomware, leurs systèmes sont paralysés par milliers, sans compter les lourdes conséquences liées au paiement d'une rançon. Quand ce type d'événement fait la une des journaux, je reçois des appels inquiets de mes dirigeants, et je suis heureux de pouvoir leur dire que tout va bien pour nous. »
>
> **Ken Athanasiou,** vice-président et RSSI, AutoNation

zscaler™ | Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, résilience et sécurité. 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. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

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