E-book

Guide d'achat sur la prévention des menaces

Trouvez la solution de protection qui vous convient le mieux contre les menaces avancées et basées sur les fichiers.

Contenu

Repenser la sécurité pour le paysage des menaces actuelles **3**

La sécurité basée uniquement sur le périmètre est trop risquée pour le monde numérique moderne 3

Les adversaires profitent de la vague de migration vers le cloud 3

Une évolution vers une protection contre les malwares de type « zero day » est nécessaire **4**

Configuration requise pour le cloud sandboxing **5**

Déchiffrement et inspection à grande échelle 6

Gestion centralisée des politiques et des règles 7

Alignement des politiques sur la tolérance au risque et les attentes en matière de performances 7

Analyse intelligente et renseignements sur les menaces 8

Moteur de prévention des malwares optimisé par l'IA 8

Flux de travail SOC avec informations sur les menaces 8

Améliorer votre SOC avec le cadre MITRE ATT&CK 9

Questions à se poser avant d'acheter 10

Zscaler Cloud Sandbox et Protection avancée contre les menaces **11**

Il est temps de disposer d'une véritable solution de sandbox inline cloud native 11

Repenser la sécurité pour le paysage des menaces actuelles

La sécurité basée uniquement sur le périmètre est trop risquée pour le monde numérique moderne

Le passage au travail hybride et les applications hébergées dans le cloud ont changé la façon d'accéder aux ressources de l'entreprise. Les utilisateurs emploient des appareils non gérés sur des réseaux non sécurisés comme le Wi-Fi public pour rester productifs à distance ou en déplacement, faisant d'Internet le nouveau réseau d'entreprise. Le périmètre en est alors considérablement élargi, de sorte que l'approche cloisonnée de la sécurité devient totalement inappropriée pour protéger vos utilisateurs, vos applications et vos données. Continuer à se fier uniquement aux contrôles basés sur le périmètre introduit des risques car les défenses centrées sur le réseau sont contournées pour bénéficier d'un accès direct à Internet et d'une plus grande facilité d'utilisation.

La nouvelle génération de cyberattaques se joue facilement des contrôles de sécurité traditionnels. Il est temps de rapprocher la sécurité des utilisateurs et de passer de la protection du périmètre à la sécurisation des utilisateurs, des charges de travail et des systèmes OT/IOT.

Les adversaires profitent de la vague de migration vers le cloud

Prises entre le marteau et l'enclume, les équipes de sécurité ont fait de leur mieux pour adapter les contrôles de sécurité traditionnels au monde moderne, axé sur le mobile et le cloud. Cette inadéquation a été une victoire pour les adversaires. Alors que les entreprises s'efforcent de protéger les différentes périphéries du réseau, les portes sont involontairement laissées ouvertes aux malwares, comme en témoignent les conclusions de Zscaler ThreatLabz :

- Les attaques par ransomware ont **augmenté de 80 %** d'une année sur l'autre.[1]
- Les techniques d'extorsion à multiples facettes sont en hausse, et les ransomwares à double extorsion ont augmenté de **117 %**.[1]
- Les attaques par phishing **ont augmenté de 29 %** en 2021 par rapport à 2020.[2]
- **85 %** des entreprises ont subi une cyberattaque victorieuse en 2021.[3]
- **63 %** des victimes de ransomwares ont payé des rançons en 2021, ce qui encourage les cybercriminels à intensifier leurs attaques.[3]

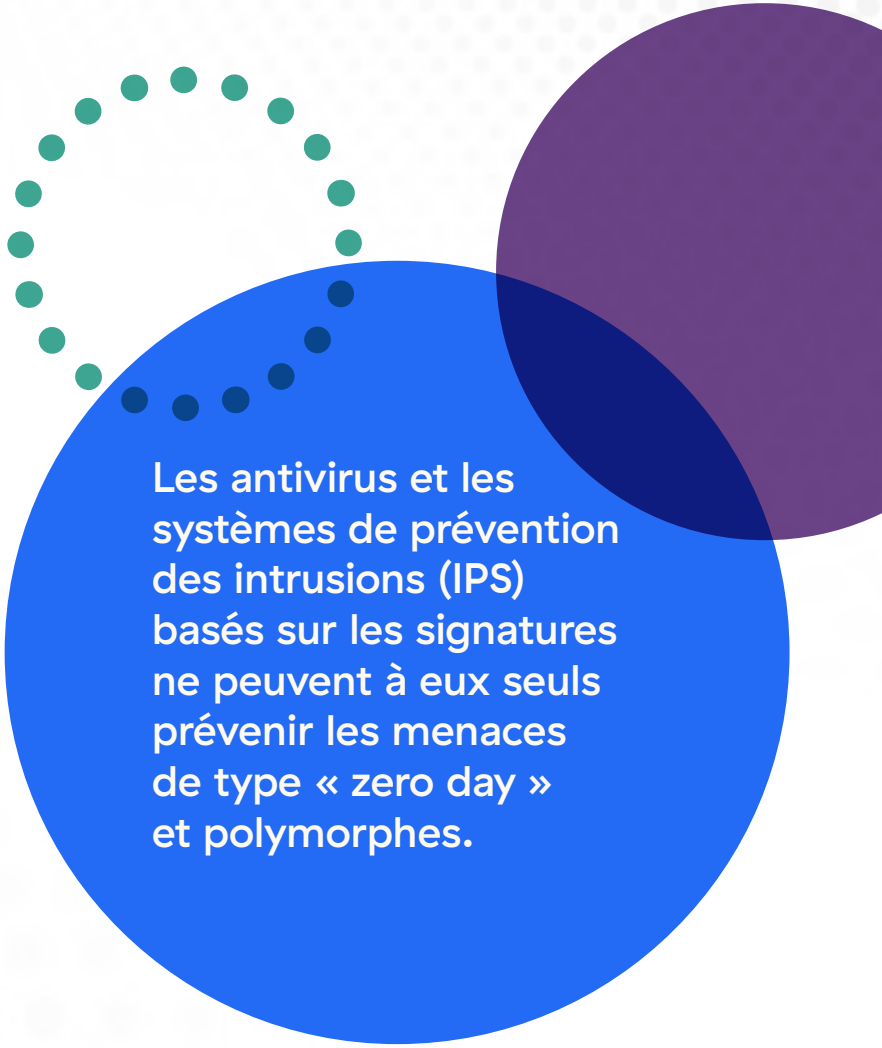
1. https://www.zscaler.fr/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.fr/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

Une évolution vers une protection contre les malwares de type « zero day » est nécessaire

Les adversaires disposent de deux avantages : **vitesse** et **prolifération**. Les développeurs de malwares créent des menaces plus rapidement que les défenseurs ne peuvent les cerner, se propageant et changeant de forme pour échapper à la détection.

Le phishing au moyen de pièces jointes ou de liens malveillants demeure actuellement le mécanisme de diffusion le plus courant. Les menaces se cachant dans le trafic chiffré, vous devez inspecter tout le trafic Web et non Web, y compris les protocoles de transfert de fichiers et SSL/TLS : à défaut, vous pouvez involontairement laisser entrer des malwares dans votre réseau et permettre à des adversaires d'exfiltrer des données sensibles ou de demander une rançon.

En tant que fonction critique dans la pile de sécurité, les sandbox sont des mesures préventives contre les fichiers malveillants et les exécutions de code. Ils sont conçus pour être la dernière ligne de défense, et le premier point de détection pour les enquêtes, contre les menaces inconnues. Malheureusement, les appliances sandbox traditionnelles sont hors bande et exigent des dispositifs complémentaires pour le déchiffrement et l'inspection SSL. Étant donné que la protection est appliquée une fois que le malware a déjà atteint l'utilisateur ou l'appareil, il est impossible de réaliser le Zero Trust.



Configuration requise pour le cloud sandboxing

Jusqu'à présent, les adversaires ont eu le dessus en exploitant l'architecture changeante de l'environnement cloud.

Le choix du bon cloud sandbox est essentiel pour prévenir les infections de type « zero day » et bloquer l'accès des menaces persistantes avancées à votre réseau.

La section suivante est destinée à vous aider à comprendre les exigences spécifiques à prendre en compte lors de la sélection d'un cloud sandbox.

Déchiffrement et inspection à grande échelle

Le chiffrement est devenu une tendance prometteuse en matière de sécurité, permettant de protéger et de sécuriser les communications privées et les informations sensibles. Malheureusement, les cybercriminels profitent du trafic chiffré pour cacher des charges utiles malveillantes.

Pratiques plus récentes, le déchiffrement et l'inspection du trafic sont des processus gourmands en ressources de calcul. Les sandbox traditionnels dotés d'une architecture passthrough permettent involontairement aux malwares de se faufiler parmi le trafic non inspecté. Les dispositifs d'inspection SSL dédiés ajoutés peuvent être utiles, mais comme toutes les appliances, ils n'ont pas la capacité de s'adapter, ce qui cause une accumulation de dispositifs coûteux alors que les infections de type patient zéro continuent de s'infiltrer dans les réseaux.

Lorsque vous évaluez une solution moderne de sandboxing, il est important de sélectionner des fournisseurs capables de fournir un déchiffrement et une inspection inline illimités et sans latence.

Les menaces sur HTTPS ont augmenté de plus de 314 % d'une année sur l'autre, avec une croissance de plus de 250 % pour la deuxième année consécutive.[4]

Liste de contrôle d'achat :

- ☐ Ne requiert aucun matériel supplémentaire ni installation de machine virtuelle (VM) pour déchiffrer le trafic SSL.
- ☐ Inspecte et analyse les types de fichiers suivants, sans latence ni limite de capacité :

EXE	DOC(X)	TAR
DLL	XLX(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	Fichiers script et fichiers ZIP
SWF	BZ2	

4. *https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks-fr*

Liste de contrôle d'achat :

- ☐ Application immédiate des politiques à tous les utilisateurs avec une protection identique, aussi bien sur le réseau de l'entreprise qu'en dehors
- ☐ Règles et capacités de quarantaine avancées pour tous les fichiers provenant de destinations suspectes
- ☐ Gestion centralisée des politiques
- ☐ Contrôles granulaires pour les fichiers greyware et adware

Gestion centralisée des politiques et des règles

Évitez la gestion incorrecte des règles et la configuration manuelle des sandbox à chaque passerelle grâce à une gestion centralisée des politiques et des règles fournies dans le cloud. Envisagez des solutions dotées de politiques adaptatives et dynamiques qui suivent les principes de Zero Trust énoncés par la norme **NIST 800-207**. En établissant des politiques d'accès et de sécurité basées sur le contexte, notamment le rôle et l'emplacement de l'utilisateur, la posture de l'appareil et les données demandées, le Zero Trust minimise les surfaces d'attaque. Les solutions fournies dans le cloud comportent des avantages supplémentaires qui peuvent vous permettre de bloquer les menaces pour tous les utilisateurs de l'entreprise une fois qu'une menace a été identifiée. Cela signifie que le traitement rétroactif de fichiers est supprimé (par exemple, les inspections hors bande et les protections appliquées après coup) pour fournir une sécurité davantage synchronisée.

Les contrôles granulaires vous permettent d'aligner les politiques sur la tolérance au risque et les attentes en matière de performance de votre entreprise.

Alignement des politiques sur la tolérance au risque et les attentes en matière de performances

Une solution de cloud sandbox doit contrôler les risques et appliquer des politiques en répondant aux besoins uniques de votre entreprise. Commencez par déterminer si vous êtes affecté par les éléments suivants :

- **Faible tolérance pour les fichiers malveillants :** les entreprises qui souhaitent éviter les risques peuvent choisir « Quarantine for First-Time Action » (mise en quarantaine en tant que première action) pour les fichiers inconnus ou suspects.
- **Faible tolérance pour la mise en quarantaine des fichiers :** les entreprises tolérantes au risque qui souhaitent éviter les retards et les interruptions peuvent choisir « Allow and Scan for First-Time Action » (Autoriser et analyser en tant que première action). Pour une protection supplémentaire, envisagez d'intégrer les capacités d'isolation du navigateur cloud pour restituer le fichier sous forme d'image et éviter la fuite de données et la diffusion de menaces actives.

Peu importe vos besoins spécifiques, les politiques doivent être faciles à appliquer à tous les utilisateurs, groupes, départements, emplacements et groupes d'emplacements à partir d'une plateforme unique.

Analyse intelligente et renseignements sur les menaces

Les adversaires sont connus pour réutiliser les attaques qui réussissent. Il est donc essentiel de partager les protections avec la communauté de sécurité pour arrêter rapidement les menaces dans leur lancée. Les cloud sandbox jouent un rôle important à cet égard en capturant les données de télémétrie et en partageant les informations sur les menaces nouvellement identifiées avec la communauté de la sécurité et les flux de menaces.

Moteur de prévention des malwares optimisé par l'IA

Les sandbox fournis dans le cloud sont en mesure de gérer des modèles AI/AA à forte charge de calcul pour assurer une protection supérieure.

Recherchez un sandbox qui identifie, met en quarantaine et prévient intelligemment les menaces inconnues ou suspectes en ligne à l'aide d'une IA/AA avancée, sans devoir réexaminer les fichiers inoffensifs.
Cela garantit :

- **Des verdicts de fichiers plus rapides :** en acheminant immédiatement les fichiers inoffensifs et en analysant les fichiers suspects ou inconnus, vous réduisez le travail manuel.
- **Prévention zero day :** en mettant en quarantaine les menaces inconnues sans autre intervention, vous pouvez empêcher que les menaces de type « zero day » ne deviennent plus importantes pour votre environnement.

Flux de travail SOC avec informations sur les menaces

Les analystes peuvent passer plusieurs heures par jour à rechercher une seule menace.
Optez pour un cloud sandbox qui réduit cette charge et accélère l'investigation et la réponse en partageant des informations comportementales et des renseignements sur les charges utiles malveillantes. Assurez-vous que les flux de menaces s'intègrent à vos outils de sécurité en place. Ils doivent inclure : un contexte actualisé sur les URL signalées, des indicateurs de compromission (IoC) extraits et des tactiques, des techniques et procédures (TTP) qui s'alignent sur les cadres de cybersécurité tels que MITRE ATT&CK®.

Liste de contrôle d'achat :

- ☐ Capacités AA/IA qui s'intègrent étroitement au processus d'analyse
- ☐ Fonctionnalités de quarantaine basées sur l'IA qui peuvent exploiter l'AA/IA pour retenir les fichiers potentiellement malveillants, les analyser et émettre des verdicts à la vitesse de la machine
- ☐ Contribution autonome aux protections quotidiennes contre les menaces, partagée entre les utilisateurs et les réseaux, quel que soit leur emplacement
- ☐ Capacité de partager des données analytiques détaillées et des verdicts de fichiers via une plateforme
- ☐ Intégration des flux de menaces avec les outils de sécurité existants

Veillez à choisir un sandbox qui peut fournir plus qu'un score de menace. Envisagez un sandbox qui peut décrireles techniques de contournement utilisées, telles que :

- Retarder l'exécution du code pour éviter la détection de la sandbox
- Capturer et visualiser le trafic lors de son passage sur le réseau
- Ouvrir des ports pour permettre une connectivité à distance
- Tenter un mouvement latéral pour découvrir des cibles de plus grande valeur
- Tenter de prendre le contrôle à distance

Rapports

Les solutions de sécurité proposant des rapports ne sont utiles que dans la mesure où ils sont exploitables. Les rapports sur les cloud sandbox devraient comporter les caractéristiques suivantes :

- À même d'inclure l'ensemble du cycle de vie des attaques malveillantes
- Simples à utiliser et à exploiter
- Facilement assimilables
- Disponibles via une interface de programmation d'applications (API) afin de pouvoir être corrélés avec les journaux existants
- Faisant partie d'une plateforme plus large qui prend également en charge les rapports de conformité

Améliorer votre SOC avec le cadre MITRE ATT&CK

Lorsque vous évaluez les capacités de reporting, pensez aux informations du sandbox qui peuvent être mises en correspondance avec le **cadre ATT&CK de MITRE**. Grâce à cette capacité, les équipes SOC peuvent exploiter les informations fournies pour élaborer des défenses tactiques dans d'autres parties de la pile de sécurité. Ainsi, le sandbox fait partie intégrante des flux de travail des opérations de sécurité.

En fonction de votre degré de compréhension du framework, vous pouvez utiliser le reporting de plusieurs manières :

- Réduire la charge de l'étiquetage en utilisant la taxonomie fournie
- Visualiser les techniques furtives qui peuvent échapper à votre solution de détection et de réponse des terminaux (EDR)
- Comparer et opposer d'autres contrôles
- Vous concentrer sur les TTP les plus courants ciblant votre entreprise au lieu de prévenir sans discernement toutes les tactiques et techniques
- Effectuer un rapport d'ingénierie inverse

Questions à se poser avant d'acheter

Pour vous orienter dans votre processus de décision, voici un récapitulatif des principales questions que vous devez poser et pourquoi vous devez les poser :

La solution couvre-t-elle tous les utilisateurs et leurs appareils, quel que soit leur emplacement ?

Vos utilisateurs peuvent accéder aux ressources de l'entreprise en déplacement, sur leurs propres appareils ou sur des réseaux non sécurisés. Il est indispensable de sécuriser tous les appareils qui sont essentiels à leur travail.[5]

La solution fonctionne-t-elle inline ou en mode point d'accès de test (TAP) ?

Les solutions qui fonctionnent inline peuvent identifier les menaces et les bloquer directement sans avoir à créer de nouvelles règles via des dispositifs tiers tels que des pare-feu.

Le sandbox examine-t-il le trafic de tous les protocoles HTTP, HTTPS, FTP et FTP sur HTTP ? Y a-t-il des limitations ?

Il est important d'examiner le trafic pour déceler les malwares furtifs. Un sandbox fourni dans le cloud peut mieux convenir pour inspecter tout le trafic sans créer de latence.

Est-il conforme aux lois et réglementations en vigueur, y compris aux exigences de Zero Trust ?

Les règlements de conformité peuvent avoir des exigences strictes sur la façon dont le sandboxing est géré et sur les questions de conservation des fichiers et de confidentialité. Une solution qui fonctionne uniquement en mémoire et qui supprime les informations identifiables pendant l'analyse vous aide à répondre à ces exigences. En outre, vérifiez si les solutions adhèrent aux principes de Zero Trust tels que définis par les normes mondiales NIST 800-207 et utilisez-les comme guide pour réduire les surfaces d'attaque et protéger les données.

Avec quels autres modules de sécurité le sandbox collabore-t-il ?

Aucun produit ne peut à lui seul assurer une protection totale contre les menaces avancées persistantes (APT). Au contraire, une approche multicouche de prévention, d'atténuation, de détection et de réponse aux menaces est indispensable. Le sandboxing est une couche intégrale et, en tant que tel, il doit parfaitement collaborer avec d'autres solutions et modules.

La solution complète-t-elle les sandbox proposés par les fournisseurs ou le sandboxing EDR ?

Une véritable stratégie de défense en profondeur peut exiger des solutions complémentaires et une protection en couches pour perturber de manière adéquate la chaîne d'élimination des malwares susceptibles de ruiner votre entreprise. Si un niveau de votre écosystème échoue, vous pouvez compter sur un autre. Les contrôles des terminaux, du réseau et des politiques doivent collaborer harmonieusement pour stopper l'ennemi.

5. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox et Protection avancée contre les menaces

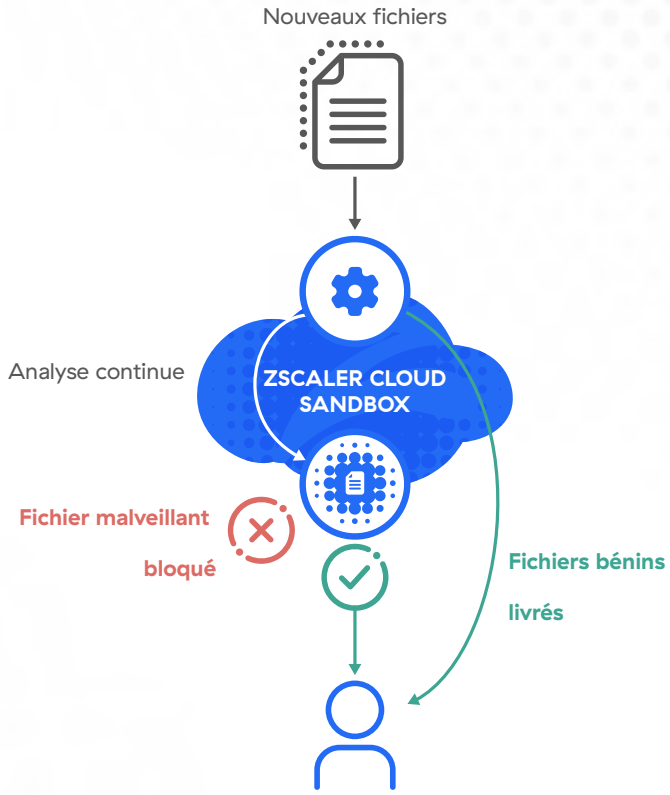
Il est temps de disposer d'une véritable solution de sandbox inline cloud native

Alors que les entreprises sont confrontées à un élargissement de leurs surfaces d'attaque et que les adversaires profitent des lacunes de la pile de sécurité existante, le moment n'a jamais été aussi propice pour choisir une véritable solution de sandbox inline cloud native. Zscaler Cloud Sandbox est spécialement conçu pour intercepter et stopper les menaces modernes tout en assurant une protection contre les malwares de type « zero day » pour tous les utilisateurs, sur tous les emplacements.

Construit sur une architecture cloud native basée sur un proxy, Zscaler Cloud Sandbox est le premier moteur de prévention des malwares piloté par l'IA au monde qui détecte, empêche et met en quarantaine les menaces inconnues et les fichiers suspects inline, le tout de manière automatique et intelligente. L'inspection illimitée et sans latence sur le Web, assortie des protocoles de transfert de fichiers (FTP), y compris SSL/TLS, permet au cloud sandbox d'effectuer une analyse dynamique approfondie en temps réel, garantissant qu'aucun fichier inconnu ne parvient à l'utilisateur du fait du téléchargement d'un fichier malveillant.

La quarantaine optimisée par l'IA arrête les malwares inconnus

Protection inline avec livraison instantanée des fichiers bénins, défense contre les infections de type patient zéro et contrôles des politiques granulaires



Réduction de la complexité et des coûts

- Facile à déployer, aucun matériel ni logiciel à gérer
- Suppression des produits ponctuels redondants et dissociés
- Élimination du backhauling du trafic Internet sur MPLS ou VPN

Protection immédiate et adaptative pour tous les utilisateurs et tous les emplacements

- Définition des politiques globales dans une console unique et centralisée
- Application immédiate des changements de politique
- Identification des menaces une seule fois pour les bloquer immédiatement et définitivement pour tous les clients

Détection des menaces cachées

- Prévention des infections de type patient zéro provenant de menaces connues et émergentes grâce à la quarantaine pilotée par l'IA
- Chargement des fichiers pour analyse (portail Filecheck)

Service de plateforme intégré

- Pré-filtrage de toutes les menaces connues à l'aide d'antivirus, de listes de blocage de hachage, de règles de classification YARA des malwares, de détections automatisées d'empreintes JA3 et de modèles d'AA/AI
- Les flux CIF (Collective Intelligence Framework) permettent à Zscaler d'intégrer plus de 60 flux de menaces, en plus du flux de menaces propre à Zscaler, alimenté par des milliards de transactions de sa base de clients.
- Superposez un cloud sandbox avec une solution EDR pour augmenter l'efficacité de la sécurité et limiter l'accès initial, l'exécution et les tactiques persistantes.

Une étude de validation des avantages économiques d'ESG a révélé que Zscaler Zero Trust Exchange a permis de réduire de 90 % le nombre d'appliances de sécurité.[6]

- Analyse statique, dynamique et secondaire, y compris l'analyse du code et des charges utiles secondaires
- Inspection SSL illimitée et sans latence
- Protection du trafic entrant et sortant
- Amélioration des enquêtes et des réponses en matière de sécurité grâce à des données analytiques détaillées, notamment sur l'utilisateur, l'origine géographique, les tactiques de contournement, etc.

Zscaler Cloud Sandbox est une fonctionnalité entièrement intégrée de Zscaler Internet Access, qui fait partie de Zscaler Zero Trust Exchange.

Pour plus d'informations, rendez-vous sur **zscaler.fr/custom-product-demo.**

6. https://info.zscaler.com/resources-industry-report-esg-economic-validation-fr

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. (siège) • 120 Holger Way • San Jose, CA 95134

zscaler.fr