zscaler™

E-book

Guide d'achat des solutions de prévention des menaces

Identifiez votre solution idéale pour contrer les menaces sophistiquées utilisant des fichiers.

Sommaire

Réinventer la sécurité face aux menaces actuelles

La sécurité périmétrique, à elle seule, est trop risquée dans le monde digital moderne

La généralisation du travail hybride et l'utilisation d'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 (Wi-Fi public par exemple) pour rester productifs, lorsqu'ils travaillent à distance ou sont en déplacement : Internet est devenu le nouveau réseau d'entreprise. Votre périmètre réseau s'étend donc, ce qui remet en cause la capacité d'une sécurité cloisonnée, basée sur plusieurs produits distincts et non intégrés, à protéger vos utilisateurs, vos applications et vos données. Compter uniquement sur des fonctions de sécurité actives sur le périmètre réseau introduit des risques. En effet, une ligne de défense orientée réseau peut être contournée pour un accès direct à Internet et une utilisation plus simple.

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 réseau à la sécurisation des utilisateurs, des instances et des systèmes OT/IOT.

Les assaillants tirent parti de l'adoption massive du cloud

Prises entre le marteau et l'enclume, les équipes de sécurité ont fait de leur mieux pour adapter les fonctions de sécurité traditionnelle à un monde moderne, qui fait la part belle à la mobilité et au cloud. Cette inadéquation est à l'avantage des assaillants. Alors que les entreprises s'efforcent de protéger les différents edges (périphéries) de leur réseau, des portes sont involontairement laissées ouvertes aux malwares, comme le souligne Zscaler ThreatLabz :

- Les attaques par ransomware ont **bondi de 80 %** d'une année sur l'autre.[1]
- Les techniques d'extorsion et leurs multiples facettes sont en hausse, tandis que les ransomwares à double extorsion ont progressé 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 réussie en 2021.[3]
- **63 %** des victimes de ransomwares ont payé des rançons en 2021, ce qui encourage les cybercriminels à intensifier leurs attaques.[3]

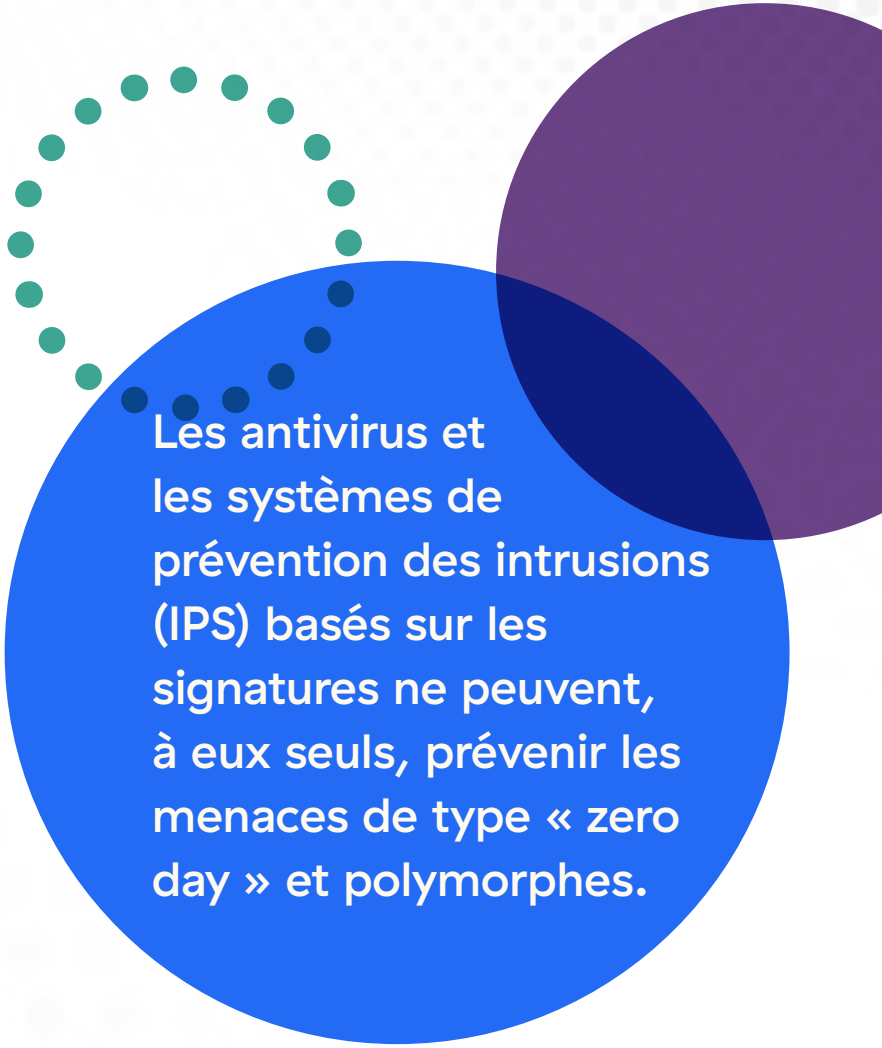
1. https://www.zscaler.fr/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.fr/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

Se protéger contre les malwares de type « zero day » est nécessaire

Les adversaires disposent de deux avantages : **vitesse** et **prolifération**. Les concepteurs de malwares créent des menaces plus rapidement et les défenseurs ne peuvent pas toujours les identifier. Ce malwares se propagent et mutent pour éviter de se faire détecter.

Le phishing au moyen de pièces jointes ou de liens malveillants demeure actuellement le mécanisme de diffusion le plus courant. Les menaces se dissimulant 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 l'arsenal de sécurité, les sandbox sont des mesures préventives contre les fichiers malveillants et l'exécution de logiciels malveillants. Ils sont conçus pour être une nouvelle ligne de défense, mais également le premier point de détection pour identifier les menaces inconnues. Malheureusement, les appliances sandbox traditionnelles opèrent en mode hors bande et exigent des dispositifs complémentaires pour déchiffrer et inspecter le protocole SSL. Étant donné que la sécurité s'applique une fois que le malware a déjà atteint l'utilisateur ou l'appareil cible, il est impossible de mettre en œuvre le Zero Trust.



Sandbox cloud : les prérequis

Jusqu'à présent, les adversaires étaient à leur avantage en tirant parti de la migration des infrastructures vers le cloud.

Le choix de la sandbox cloud la plus adaptée est essentiel pour prévenir les infections de type « zero day » et empêcher les menaces persistantes et avancées (APT) d'accéder à votre réseau.

La section suivante est destinée à vous aider à mieux comprendre les critères d'un choix éclairé d'une sandbox cloud.

Déchiffrement et inspection à grande échelle

Le chiffrement est une tendance positive 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 y dissimuler des objets malveillants.

Le déchiffrement et l'inspection du trafic sont des processus gourmands en ressources CPU. Les sandbox traditionnelles de type "passthrough" permettent involontairement aux malwares de se faufiler au sein du trafic non inspecté. Des dispositifs dédiés à l'inspection SSL peuvent être rajoutés, mais comme toutes les appliances, leur évolutivité est limitée, ce qui entraîne une prolifération de dispositifs coûteux qui n'empêche pas les infections de s'immiscer dans le réseau.

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

Les menaces via HTTPS ont bondi de plus de 314 % en un an, une croissance supérieure à 250 % pour la deuxième année consécutive.[4]

Checklist des critères d'achat :

- ☐ Aucun matériel supplémentaire ni installation de machine virtuelle (VM) requis pour déchiffrer le trafic SSL
- ☐ Inspection et analyse des types de fichiers suivants, sans latence ni limite en capacités :

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 de script et fichiers ZIP
SWF	BZ2	

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

Checklist des critères d'achat :

- ☐ Application immédiate des politiques à tous les utilisateurs avec un même niveau de protection pour les utilisateurs sur et hors du réseau
- ☐ Règles et mise en quarantaine 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 une gestion complexe des règles et la nécessité de configurer manuellement les sandbox présentes sur chaque passerelle, grâce à une gestion centralisée des politiques et des règles, assurée dans le cloud. Privilégiez des solutions dotées de politiques adaptatives et dynamiques, conformes aux principes du Zero Trust définis par la norme **NIST 800-207**. Le Zero Trust permet de restreindre la surface d'attaque, grâce à des politiques d'accès et de sécurité basées sur des éléments de contexte : rôle et l'emplacement de l'utilisateur, posture de l'appareil utilisé, données demandées, etc. Les solutions fournies depuis le cloud assurent des avantages supplémentaires, comme la possibilité de neutraliser une menace pour tous les utilisateurs, dès que cette menace est détectée. Cela signifie que les analyses répétées d'un même fichier suspect ne sont plus nécessaires (par exemple, les inspections hors bande et le déploiement d'une protection en aval de l'incident) pour assurer une sécurité plus pertinente.

Les contrôles granulaires vous permettent de définir des politiques adaptées à la tolérance au risque et aux objectifs de performance de votre entreprise.

Des politiques définies en fonction de la tolérance au risque et des objectifs de performances

Une solution de sandbox cloud doit maîtriser les risques et appliquer des politiques adaptées aux spécificités de votre entreprise. Commencez par déterminer si les principes suivants s'appliquent à votre entreprise :

- **Faible tolérance aux fichiers malveillants :** les entreprises qui souhaitent éviter tout risque peuvent choisir la mise en quarantaine en tant que première action (« Quarantine for First-Time Action ») pour les fichiers inconnus ou suspects.
- **Faible tolérance à la mise en quarantaine des fichiers :** les entreprises tolérantes au risque qui souhaitent éviter tout retard ou interruption de service peuvent choisir l'autorisation et l'analyse en tant que première action (« Allow and Scan for First-Time Action »). Pour une protection supplémentaire, vous pouvez envisager un isolement du navigateur, une fonction cloud qui restitue tout fichier sous forme d'image. Cette approche prévient les fuites de données et l'acheminement de menaces actives.

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

Analyse intelligente et veille sur les menaces

Les cybercriminels sont connus pour réutiliser les attaques qui réussissent. Il est donc essentiel de partager toute information pertinente avec la communauté de la sécurité au sens large, pour neutraliser rapidement les menaces en cours. Les sandbox cloud jouent un rôle important à cet égard en capturant des données de télémétrie et en partageant les informations sur les menaces nouvellement identifiées avec les flux d'information sur les menaces et la communauté de la sécurité.

Prévention antimalware optimisée par IA

Les sandbox cloud sont en mesure de gérer des modèles IA (Intelligence artificielle) et ML (Machine Learning) gourmands en ressources pour optimiser la protection.

Privilégiez une sandbox qui identifie, met en quarantaine et prévient intelligemment les menaces inconnues ou suspectes, en mode inline et à l'aide de fonctions IA/ML avancées, sans devoir réexaminer les fichiers inoffensifs. Cela garantit :

- **Des verdicts plus rapides sur les fichiers :** en acheminant immédiatement les fichiers sains et en analysant les fichiers suspects ou inconnus, les tâches manuelles sont moindres.
- **Prévention des menaces de type « zero day » :** en mettant en quarantaine les menaces inconnues sans autre intervention, vous pouvez empêcher que les menaces « zero day » ne se propagent au sein de votre environnement.

Workflows du SOC et veille sur les menaces

Les analystes peuvent consacrer plusieurs heures par jour à enquêter sur une seule menace. Optez pour une sandbox cloud accélère cette tâche et la prise en charge des menaces, en partageant des informations comportementales et des renseignements sur les objets malveillants. Assurez-vous que vos outils de sécurité en place bénéficient de flux d'informations sur les menaces. Ces informations doivent porter sur les URL suspectes, les indicateurs de compromission (IoC) recueillis, ainsi que les tactiques, techniques et procédures (TTP) telles que répertoriées par des frameworks de cybersécurité comme MITRE ATT&CK®.

Checklist des critères d'achat :

- ☐ Fonctions IA/ML étroitement intégrées au processus d'analyse
- ☐ Fonctionnalités de mise en quarantaine basées sur l'IA qui peuvent tirer parti de l'IA et du ML pour retenir des fichiers potentiellement malveillants, les analyser et statuer rapidement sur leur dangerosité
- ☐ Contribution autonome à la protection au quotidien contre les menaces, pour les utilisateurs et les réseaux, quel que soit leur emplacement
- ☐ Capacité de partager des données analytiques détaillées et les verdicts sur les fichiers via une plateforme
- ☐ Intégration des flux d'informations sur les menaces avec les outils de sécurité existants

Privilégiez une sandbox qui peut fournir plus qu'un score sur une menace, en décrivant les techniques de furtivité utilisées, telles que :

- Retarder l'exécution d'un logiciel pour éviter la détection par la sandbox
- Capturer et visualiser le trafic qui transite sur le réseau
- Ouvrir des ports pour permettre une connexion à distance
- Tenter de se déplacer en interne pour identifier des cibles de valeur
- Tenter de prendre le contrôle à distance

Reporting

Les solutions de sécurité proposant un reporting doivent s'assurer sa pertinence. Le reporting sur les sandbox cloud sandbox doit :

- Porter sur l'ensemble du cycle de vie des attaques malveillantes
- Être simple à utiliser et à exploiter
- Être compréhensible
- Être disponibles via une API afin de pouvoir être corrélés avec les logs existants
- Faire partie d'une plateforme plus large qui propose également un reporting de conformité

Améliorer votre SOC avec le cadre MITRE ATT&CK

Lorsque vous évaluez la pertinence d'un reporting, assurez-vous que les informations issues de la sandbox peuvent être mises en correspondance avec le **cadre ATT&CK de MITRE.** C'est à ce titre que les équipes SOC tireront parti des informations fournies pour élaborer des tactiques de défense utilisées par les autres fonctions de sécurité. La sandbox est alors étroitement intégrée aux workflows opérationnels de sécurité.

En fonction de votre degré de compréhension du cadre, vous pouvez utiliser la création de rapports de plusieurs manières :

- Faciliter les tâches de classification en utilisant la taxonomie fournie
- Visualiser les techniques furtives qui peuvent être utilisées pour contourner votre solution EDR (détection et réponse aux menaces)
- Comparer et évaluer l'efficacité d'autres fonctions
- Vous concentrer sur les TTP les plus courantes ciblant votre entreprise plutôt que de tenter de déjouer toutes les tactiques et techniques
- Réaliser un rapport de rétro-ingénierie

Questions à se poser avant d'acheter

Pour vous orienter dans votre processus de décision, voici un récapitulatif des principales questions à se poser et des raisons de se les poser :

- **La solution protège-t-elle tous les utilisateurs et leurs appareils, quel que soit leur emplacement ?**
  Lors de leur déplacement, vos utilisateurs peuvent accéder aux ressources d'entreprise, sur leurs propres appareils et via des réseaux non sécurisés. Il est indispensable de sécuriser tous les appareils utilisés dans le cadre du travail.[5]

- **La solution fonctionne-t-elle en mode inline ou en mode TAP (Test Access Point) réseau ?**
  Les solutions opérant en mode inline identifient les menaces et les neutralisent sans devoir créer de nouvelles règles, grâce à des dispositifs tiers tels que des pare-feu.

- **La sandbox examine-t-elle le trafic de tous les protocoles HTTP, HTTPS, FTP et FTP sur HTTP ? Quelles sont les contraintes ?**
  Il est important d'examiner le trafic pour déceler les malwares furtifs. Une sandbox opérant depuis le cloud permet d'inspecter tout le trafic sans induire de latence.

- **La sandbox est-elle conforme à la législation et aux réglementations en vigueur, y compris aux exigences du Zero Trust ?**
  Les règlements de conformité peuvent avoir des exigences strictes sur la façon dont le sandboxing est géré et sur les modalités de conservation des fichiers et de confidentialité. Une solution qui fonctionne uniquement en mode in memory et qui supprime les informations identifiables pendant l'analyse est conforme à ces exigences. En outre, vérifiez si les solutions adhèrent aux principes du Zero Trust tels que définis par les normes mondiales NIST 800-207 et utilisez-les comme guide pour réduire votre surface d'attaque et protéger vos données.

- **Avec quels autres modules de sécurité la 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, de détection et de réponse aux menaces est indispensable. Le sandboxing est une couche de sécurité qui doit collaborer avec d'autres solutions et modules.

- **La solution complète-t-elle les sandbox proposées par les fournisseurs ou le sandboxing EDR ?** Une véritable stratégie de défense en profondeur exige des solutions complémentaires et une protection multicouche pour neutraliser la kill chain des malwares susceptibles d'infecter votre entreprise. Si un des niveaux de votre écosystème de sécurité échoue, vous pouvez compter sur les autres. Les fonctions dédiées aux endpoints, au réseau et aux 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

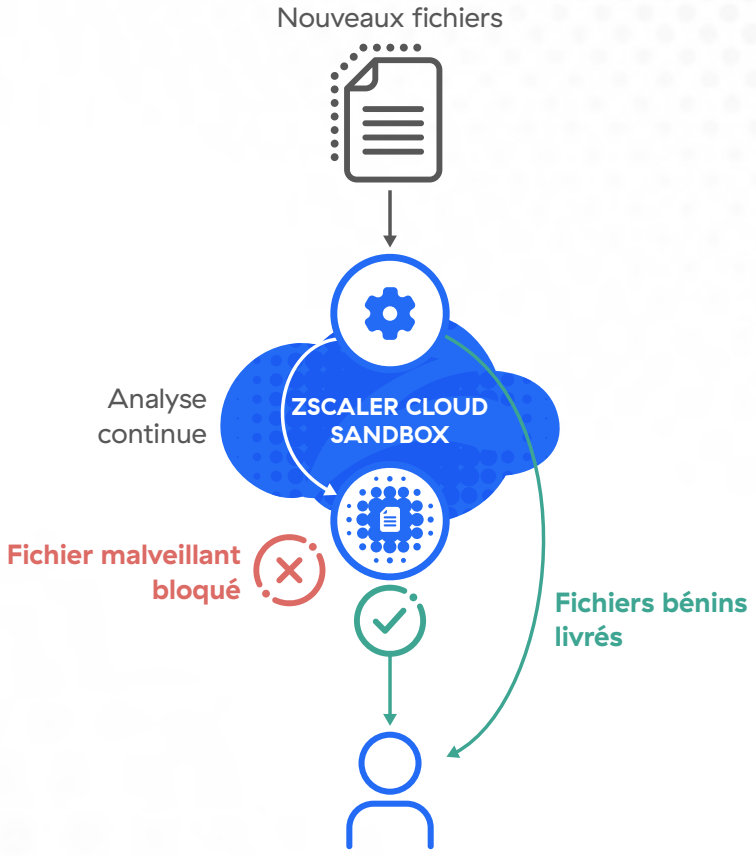
Il est temps de disposer d'une solution de sandbox inline et cloud-native

Alors que les entreprises sont confrontées à une expansion de leur surface d'attaque et que les adversaires tirent parti des failles de l'arsenal de sécurité en place, le moment n'a jamais été aussi propice pour choisir une véritable solution de sandbox inline et 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 sites.

Conçu sur une architecture cloud-native basée sur un proxy, Zscaler Cloud Sandbox est un moteur de prévention des malwares optimisé par IA. La solution détecte et met en quarantaine les menaces inconnues et les fichiers suspects, de manière automatique et intelligente. L'inspection illimitée et sans latence sur le Web et les protocoles de transfert de fichiers (FTP), y compris SSL/TLS, permet à la sandbox cloud d'effectuer une analyse dynamique approfondie et en temps réel, garantissant qu'aucun fichier inconnu ne parvient à l'utilisateur suite au 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



Maîtrise de la complexité et des coûts

- Facile à déployer, aucun matériel ni logiciel à gérer
- Suppression des produits autonomes, redondants et cloisonnés
- Pas de backhauling du trafic Internet via MPLS ou VPN

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

- Définition de politiques globales à partir d'une console unique et centralisée
- Application immédiate des modifications de politique
- Une menace identifiée une fois chez un client est immédiatement et définitivement neutralisée chez tous les autres clients

Détection des menaces dissimulées

- Prévention des infections du patient zéro par des menaces connues ou émergentes, grâce à une mise en quarantaine pilotée par l'IA
- Chargement des fichiers pour analyse (portail de vérification des fichiers)

Service de plateforme intégré

- Pré-filtrage de toutes les menaces connues à l'aide d'antivirus, de blocklists basés sur les hashs, de règles de classification YARA des malwares, de détections automatisées d'empreintes JA3 et de modèles AA/IA
- Des flux CIF (Collective Intelligence Framework) permettant à Zscaler d'intégrer plus de 60 flux d'informations sur les menaces, en plus du flux propre à Zscaler qui est alimenté par des milliards de transactions menées par ses clients.

Une étude de validation des avantages économiques, menée par ESG, révèle que Zscaler Zero Trust Exchange a réduit de 90 % le nombre d'appliances de sécurité.[6]

- Association d'une sandbox cloud et d'une solution EDR pour augmenter l'efficacité de la sécurité et prévenir l'accès initial d'un malware, son exécution et ses tactiques
- Analyse statique, dynamique et secondaire, y compris l'analyse de code et l'analyse d'objets secondaires
- Inspection SSL illimitée et sans latence
- Protection du trafic entrant et sortant
- Amélioration des investigations et des réponses de sécurité grâce à des analyses post-incident détaillées : utilisateur impacté, origine géographique, 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 des entreprises pour les rendre plus agiles, productives, résilientes et sécurisées. 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, quelle que soit leur localisation. Opérationnel sur plus de 150 data centers dans le monde, Zero Trust Exchange basé sur le 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