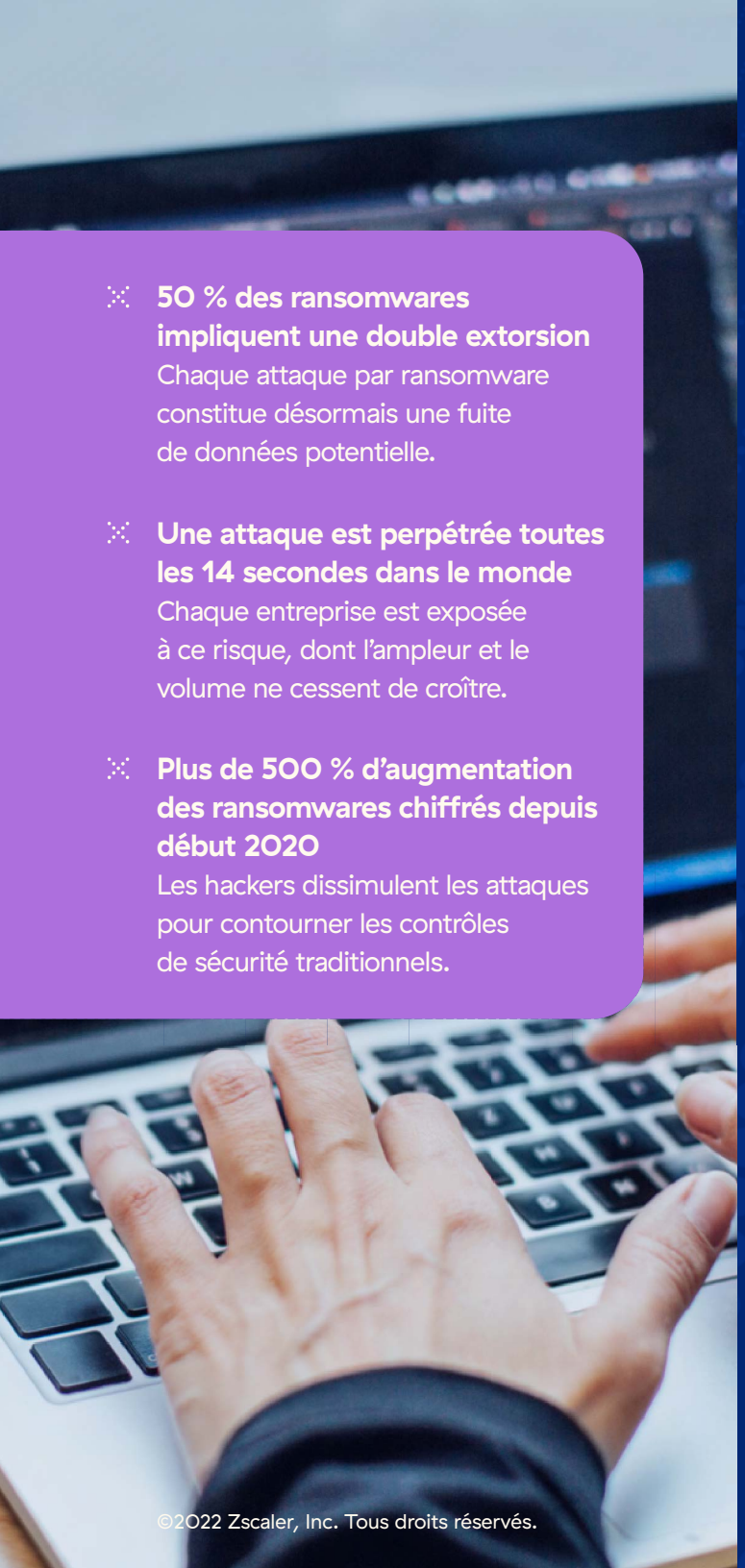
Livre électronique

10 moyens de se protéger des ransomwares grâce à une architecture Zero Trust



- **50 % des ransomwares impliquent une double extorsion**
  Chaque attaque par ransomware constitue désormais une fuite de données potentielle.
- **Une attaque est perpétrée toutes les 14 secondes dans le monde**
  Chaque entreprise est exposée à ce risque, dont l'ampleur et le volume ne cessent de croître.
- **Plus de 500 % d'augmentation des ransomwares chiffrés depuis début 2020**
  Les hackers dissimulent les attaques pour contourner les contrôles de sécurité traditionnels.

Les ransomwares sont la plus grande menace qui pèse sur l'économie digitale

Si les ransomwares existent depuis des décennies, leur fréquence a explosé au cours des dernières années. Ces attaques étaient autrefois perpétrées par des individus ; elles sont désormais lancées par des groupes d'affiliés en réseau qui achètent et vendent leurs compétences spécialisées et leurs boîtes à outils respectives. Autrefois, les attaques étaient peu ciblées et unidimensionnelles ; aujourd'hui, elles recourent à des tactiques ciblées, à plusieurs niveaux, contre lesquelles il est beaucoup plus difficile de se défendre et qui exigent des rançons beaucoup plus élevées. **Les ransomwares devraient représenter un préjudice de 42 milliards de dollars d'ici la fin de 2024.**[1]

La tendance la plus marquante des ransomwares modernes est sans doute l'avènement des attaques à double extorsion, qui consistent pour les hackers à dérober des données et à menacer de non seulement les chiffrer, mais également de les publier. Environ 50 % des attaques de ransomware incluent désormais des tentatives d'exfiltration de données.

Il n'existe qu'une seule stratégie sous-jacente qui maximise les chances d'une entreprise de réduire les conséquences d'une attaque de ransomware : Zero Trust.

La stratégie Zero Trust est une approche de la sécurité qui repose sur l'idée qu'une faille s'est déjà produite. Des architectures, des politiques de contrôle d'accès et des tactiques de surveillance et d'authentification sont mises en place pour limiter le degré et la gravité des dommages qu'un hacker peut causer.

Voici, en 10 points, comment une stratégie Zero Trust peut aider votre entreprise à se défendre contre les ransomwares.

[1] *Selon Cybersecurity Ventures, « les coûts mondiaux des préjudices causés par les ransomwares devraient dépasser 265 milliards de dollars d'ici 2031 ».*

Comprendre la séquence d'attaque des ransomwares

Au cours d'une attaque par ransomware, les pirates doivent remplir un certain nombre d'objectifs pour réussir. Ils doivent tout d'abord pénétrer dans votre environnement en réussissant à infecter un système avec un payload malveillant de ransomware. **La première étape pour arrêter une attaque consiste donc à mettre en place des contrôles préventifs qui réduisent vos vulnérabilités, minimisent votre surface d'attaque et vous permettent de bloquer, contrôler et inspecter le trafic.**

Les hackers effectuent ensuite une reconnaissance, pour localiser les actifs de grande valeur qu'ils pourront dérober et chiffrer. Pour ce faire, ils doivent être en mesure de se déplacer latéralement sur le réseau. **La deuxième étape permettant d'arrêter une attaque et de minimiser les dommages qu'un hacker peut causer consiste à limiter sa capacité à se déplacer latéralement.**

Lorsqu'ils entreprennent une attaque à double extorsion, les pirates dérobent des données et les retiennent en otage afin d'augmenter leurs chances de réussite et le montant de la rançon qu'ils réclameront. **La troisième étape de la défense contre une attaque par ransomware consiste à prévenir les pertes de données.**

Voyons comment la stratégie Zero Trust assure une protection efficace tout au long de la chaîne d'attaque.

#1

En rendant les applications invisibles aux hackers, une architecture Zero Trust minimise la surface d'attaque.

Lorsque l'identité d'une application, d'un utilisateur ou d'un appareil est ouvertement accessible sur Internet, cela équivaut à exposer publiquement vos informations les plus précieuses. Lorsque ces ressources sont visibles, les hackers peuvent facilement trouver et exploiter des vulnérabilités, telles qu'un logiciel de serveur Web non mis à jour ou un mot de passe faible qui peut être décodé par une attaque par force brute, et ainsi accéder immédiatement à votre environnement.

Une solution comme Zscaler Private Access™ permet aux applications de se connecter aux utilisateurs, et non aux utilisateurs de se connecter aux applications. Grâce à cette forme de connectivité interne, toutes les applications demeurent privées, et donc invisibles pour les hackers. En étendant cette approche à l'ensemble des appareils et des applications de votre environnement, il devient quasiment impossible aux hackers d'explorer votre environnement.

#2

Dans une architecture Zero Trust, tout le trafic, y compris le trafic chiffré, est soumis à une inspection approfondie et minutieuse.

La grande majorité du trafic Internet actuel fait appel au chiffrement, et le trafic malveillant ne fait pas exception. Plus de 90 % du trafic Internet est désormais chiffré, et le chiffrement des ransomwares est en hausse de plus de 500 % depuis le début de 2020. Les équipes de sécurité ne peuvent plus supposer aveuglément que tout le trafic chiffré par SSL est sans danger.

Cependant, maintenant que l'inspection de tout le trafic, chiffré ou non, est un élément essentiel d'une stratégie défensive robuste, les architectures reposant sur des pare-feu de nouvelle génération et d'autres défenses basées sur le périmètre ne sont plus adaptées. Il est tout simplement impossible, même pour les outils de sécurité sur site les plus avancés, d'inspecter l'ensemble du trafic chiffré par SSL sans créer une congestion qui nuit à la productivité. Une architecture basée sur un proxy dans le cloud, spécialement conçue pour détecter les logiciels malveillants chiffrés par SSL à grande échelle, protégera l'ensemble de votre trafic et éliminera les angles morts.

#3

Les stratégies Zero Trust incluent des contrôles permettant de détecter des menaces de ransomware inconnues avant qu'elles ne puissent causer des dommages.

Un nombre croissant d'attaques par ransomware s'appuie sur des programmes malveillants conçus sur mesure. Pour pouvoir vous défendre contre cette menace, vous devez être en mesure de détecter et de bloquer les nouvelles menaces. Grâce au sandboxing cloud natif et à la détection alimentée par l'IA, vous pouvez vous appuyer sur l'analyse comportementale pour découvrir des variantes de ransomwares inconnues jusqu'alors en mettant en quarantaine et en analysant intégralement les fichiers avant qu'ils ne soient transmis aux utilisateurs ou qu'ils ne puissent s'exécuter.

Avec une solution telle que Zscaler Cloud Sandbox, vous pouvez définir des politiques basées sur les utilisateurs, les groupes et les types de contenu, ce qui vous confère un contrôle granulaire sur les actions de mise en quarantaine. Cette solution faisant partie de Zscaler Zero Trust Exchange™, vous bénéficiez de verdicts de fichiers en temps quasi réel provenant d'une communauté mondiale, ce qui minimise l'impact sur les utilisateurs tout en maximisant la précision de la détection des programmes malveillants.

#4

Zero Trust simplifie les politiques de contrôle d'accès, renforce la visibilité et améliore l'efficacité.

La microsegmentation est un concept fondamental de Zero Trust. Elle consiste à restreindre l'accès aux applications et aux ressources afin que les hackers qui s'introduisent dans l'une d'elles ne puissent porter atteinte aux autres. Dans l'approche traditionnelle de la microsegmentation basée sur le réseau, les pare-feu appliquaient des règles en vérifiant les adresses réseau. Cette approche exigeait que les politiques soient redéfinies et mises à jour au fur et à mesure que les applications se déplaçaient et que les réseaux évoluaient. Ceci constituait déjà un réel challenge dans le data center sur site, mais le caractère éphémère du cloud a accru sa complexité au point de la rendre ingérable.

Les architectures proxy réduisent considérablement la complexité de la mise en œuvre de la microsegmentation, tout en assurant une protection plus robuste des charges de travail. Les politiques et les autorisations étant gérées sur la base des identités des ressources, elles sont indépendantes de l'infrastructure réseau sous-jacente et peuvent automatiquement s'adapter, quelle que soit la dynamique de l'architecture du réseau ou la rapidité de l'évolution des besoins de l'entreprise. Cela simplifie également la gestion : vous pouvez protéger un segment avec seulement quelques politiques basées sur l'identité au lieu de centaines de règles basées sur l'adresse.

#5

Une architecture Zero Trust protège les utilisateurs et les appareils où qu'ils se trouvent.

Lorsque la pandémie de COVID-19 a imposé la prise en charge du télétravail aux entreprises de tous les secteurs, beaucoup se sont tournés vers les réseaux privés virtuels (VPN) ou le Remote Desktop Protocol (RDP) pour permettre aux télétravailleurs de se connecter aux réseaux et aux ressources de l'entreprise. Malheureusement, les créateurs de ransomware ont rapidement suivi la voie tracée par ces entreprises, en lançant une nouvelle vague d'attaques basées sur le RDP et le VPN. À titre d'exemple, un VPN a été piraté lors de la désormais célèbre attaque de Colonial Pipeline, qui a interrompu le transport de près de la moitié de l'approvisionnement en carburant de l'est des États-Unis.

Dans une approche de sécurisation des utilisateurs distants basée sur la stratégie Zero Trust, chaque connexion bénéficie d'une protection identique, quel que soit l'endroit où se situent les utilisateurs. L'ajout de Zscaler Client Connector, un agent endpoint léger, à l'appareil de chaque utilisateur distant lui donne accès à l'ensemble de la sécurité, de l'application des politiques et des contrôles d'accès disponibles via Zscaler Zero Trust Exchange. Et puisque Zscaler est distribué dans 150 data centers à travers le monde, les utilisateurs bénéficient toujours d'une connexion rapide via un data center tout proche, ce qui élimine les désagréments liés à la latence des VPN.

#6

Une véritable architecture Zero Trust interdit aux hackers de se déplacer latéralement sur votre réseau.

Beaucoup trop d'équipes de sécurité se fient encore à la traditionnelle segmentation du réseau basée sur les pare-feu pour empêcher le trafic malveillant de s'infiltrer dans les réseaux d'entreprise. Ces stratégies sont non seulement complexes à déployer et à gérer, mais elles laissent également les ressources internes vulnérables. Si les hackers parviennent à forcer une application ou un pare-feu, ils peuvent toujours se déplacer latéralement dans l'environnement, ce qui leur permet de chiffrer et de dérober beaucoup plus de données qu'ils ne le pourraient autrement.

Une véritable approche Zero Trust connecte un utilisateur directement à l'application dont il a besoin via un segment 1:1, sans jamais rendre le réseau visible. Les équipes de sécurité peuvent recourir à une architecture proxy pour authentifier en permanence les utilisateurs et les connecter directement aux applications, plutôt que de faire confiance au trafic provenant d'un réseau ou d'un sous-réseau interne, éliminant ainsi le plus grand risque digital auquel sont confrontées les entreprises d'aujourd'hui. Et mieux encore, un proxy fonctionne quel que soit l'endroit où sont situés vos utilisateurs, vos appareils ou vos applications, assurant ainsi une connectivité sécurisée sur site et hors site.

#7

Une architecture Zero Trust empêche les hackers de tirer profit des charges de travail.

Dans une architecture Zero Trust, les politiques de sécurité sont appliquées en fonction de l'identité des charges de travail qui tentent de communiquer entre elles. Ces identités sont constamment vérifiées ; les charges de travail qui ne sont pas vérifiées ne peuvent tout simplement pas communiquer avec les autres. Cela signifie qu'elles ne peuvent pas interagir avec des serveurs de commande et de contrôle distants malveillants, ni avec des hôtes, utilisateurs, applications et données internes.

Une plateforme telle que Zscaler Zero Trust Exchange garantit automatiquement que tout le trafic, quelle que soit son origine, respecte les politiques de l'entreprise lorsqu'il accède à vos ressources. Elle appliquera ces politiques de manière totalement uniforme, que les ressources en question soient internes, externes ou des SaaS tiers. Cette approche de la microsegmentation du réseau est beaucoup plus simple que celle qui consiste à appliquer des politiques à plusieurs niveaux, mais elle se révèle également plus efficace.

#8

Zero Trust inclut des stratégies proactives destinées à battre les adversaires à leur propre jeu.

Les opérateurs de ransomware actuels sont des ennemis sophistiqués, capables de contourner la prévention initiale. C'est pourquoi l'un des aspects essentiels de la notion de Zero Trust réside dans l'utilisation de stratégies permettant de détecter et d'isoler les attaques avant qu'elles ne causent des préjudices. Seule plateforme Zero Trust au monde à intégrer des capacités de tromperie, Zscaler Deception™ utilise des tactiques de tromperie avancées pour attirer, détecter et intercepter les hackers, quels que soient le degré d'avancement et de ciblage de leurs stratégies.

Cette approche proactive de la défense consiste à doter votre environnement informatique de leurres, tels que de faux endpoints, répertoires, bases de données, fichiers et chemins d'accès utilisateur. Ces leurres imitent des ressources de production de grande valeur, mais demeurent cachés aux utilisateurs réels. Leur seul objectif est d'alerter votre équipe de sécurité de la présence d'un pirate lorsqu'ils sont impactés. Comme aucun trafic légitime n'est acheminé vers les leurres, les alertes sont extrêmement précises et fournissent des preuves tangibles de l'existence d'une menace ou d'une faille qui se démarquent du bruit des autres systèmes de détection. C'est un véritable avantage pour votre équipe de sécurité, qui lui permet de perturber les modes opératoires des pirates et de limiter les dégâts.

#9

Les architectures Zero Trust assurent une protection complète contre la perte de données.

La fréquence sans cesse croissante des stratégies d'attaque par ransomware à double extorsion oblige de considérer chaque attaque par ransomware comme une atteinte aux données. Des mesures empêchant l'exfiltration et la publication de vos données sensibles contribueront grandement à atténuer les conséquences les plus dévastatrices d'une attaque par ransomware.

Une solution CASB (Cloud Access Security Broker) vous permet d'appliquer des contrôles granulaires sur vos applications cloud, de protéger les données au repos au sein des plateformes SaaS et d'empêcher un sur-partage accidentel ainsi qu'une activité malveillante. Vous bénéficierez en outre d'une meilleure visibilité sur vos applications cloud, ce qui vous permettra de facilement identifier les vulnérabilités, les mauvaises configurations et l'informatique fantôme, c'est-à-dire l'utilisation d'applications cloud non autorisées. Grâce aux fonctionnalités de protection contre la perte de données (DLP), vous pourrez bloquer automatiquement l'exfiltration des données, et ainsi réduire la menace de double extorsion.

#10

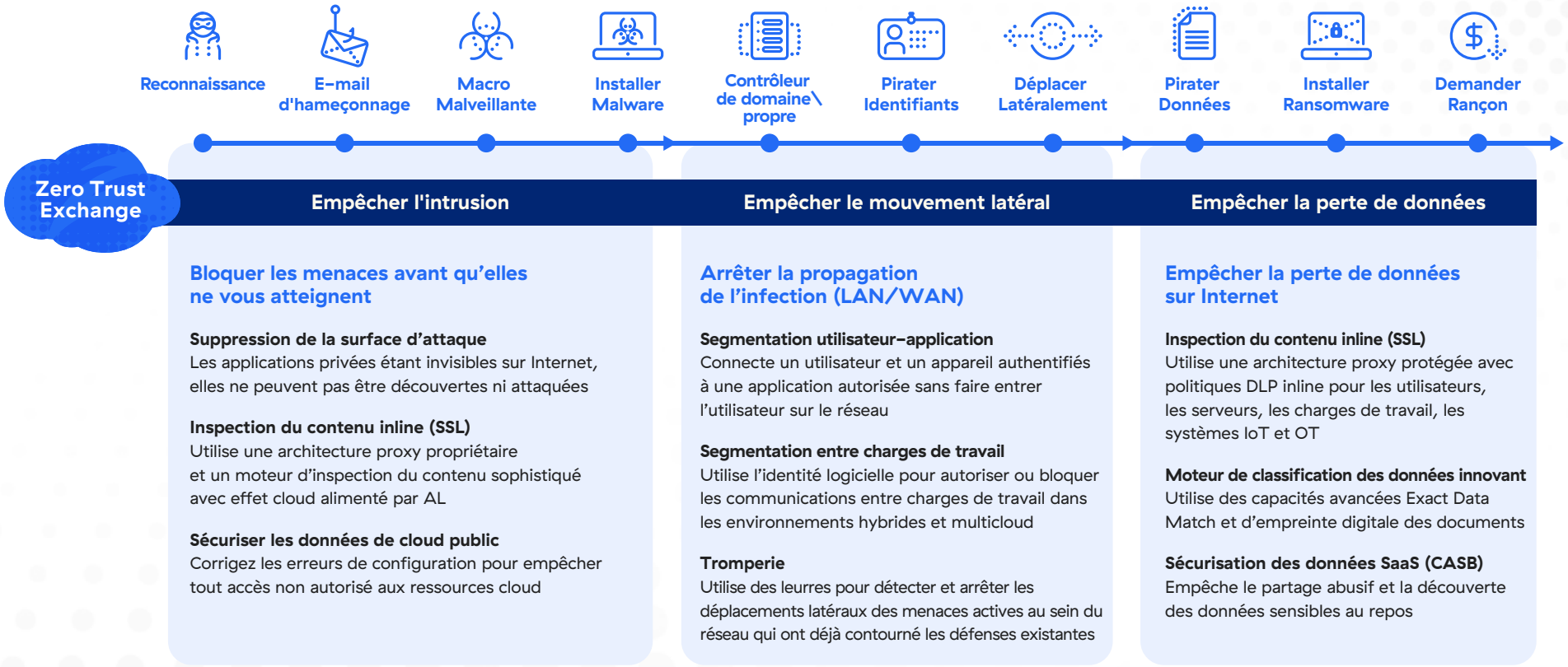
Avec son inspection inline complète de tout le trafic sortant, une architecture Zero Trust vous permet de mettre un terme au vol de données.

Si des acteurs frauduleux cachent des programmes malveillants dans le trafic entrant chiffré par SSL, ils peuvent utiliser la même stratégie — en exploitant le chiffrement — pour dissimuler le fait qu'ils exfiltrent de sensibles et précieuses données d'entreprise. Il est essentiel de pouvoir inspecter le trafic chiffré par SSL pour prévenir la perte de données et identifier les failles d'exfiltration de données de type « zero day ».

Une solution basée sur une architecture Zero Trust telle que Zscaler Zero Trust Exchange garantit que chaque connexion de votre environnement sera vérifiée et sécurisée individuellement, peu importe qu'elle soit entrante ou sortante. Avec une architecture proxy native du cloud, il est possible d'effectuer une inspection SSL à l'échelle sans affecter les performances ni engendrer de coûts excessifs. Cela supprime les failles de sécurité que les opérateurs de ransomware ont exploitées pour lancer de désastreuses attaques de double extorsion.

Appliquer une stratégie Zero Trust comme protection contre les ransomwares

Zscaler Zero Trust Exchange constitue la défense la plus complète contre l'ensemble des étapes que doivent suivre les hackers pour arriver à leurs fins. Découvrez comment Zscaler utilise la stratégie Zero Trust pour apporter une protection inégalée à votre entreprise.



Arrêter les attaques modernes implique une sécurité moderne.

Protégez votre entreprise avec la défense contre les ransomwares la plus complète du secteur.

En savoir plus

zscaler™ | 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. (HQ) • 120 Holger Way • San Jose, CA 95134
zscaler.fr