E-Book

4 raisons pour lesquelles les pare-feux et les VPN exposent les entreprises à des cyberattaques

Les solutions obsolètes sont les problématiques d'aujourd'hui

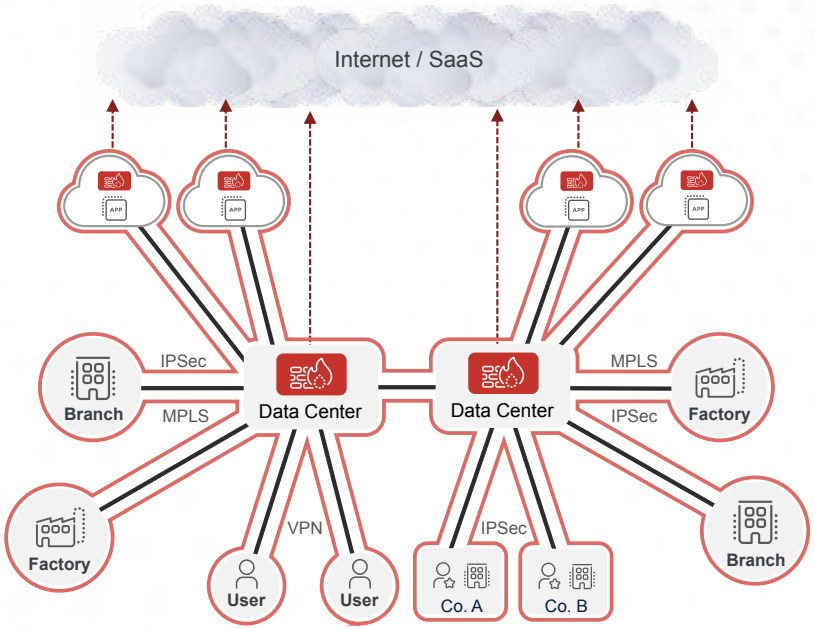
Les pare-feux et les VPN exposent les entreprises à des incidents de sécurité. Un paradoxe étant donné que ces deux outils de sécurité sont incontournables depuis des décennies. Mais c'est précisément là que réside le problème. Ils ont été conçus à une époque où le travail était très différent de ce qu'il est aujourd'hui. Autrefois, les utilisateurs et les applications résidaient sur site (au siège social ou sur un site distant) et les efforts de sécurité se concentraient sur l'établissement d'un périmètre de protection du réseau qui les connectait. En d'autres termes, un réseau en étoile était défendu par un modèle de sécurité cloisonnée, dit "castle-and-moat".

Ce modèle porte plusieurs appellations, qu'il s'agisse d'architecture basée sur le périmètre, d'architecture centrée sur le réseau ou d'architecture traditionnelle/héritée. Quelle que soit l'appellation utilisée, une telle architecture fait appel à des pare-feu et VPN, déployés pour tenter de protéger le réseau en gardant ce qui est malveillant à l'extérieur, et ce qui est légitime à l'intérieur.

Les entreprises ont rapidement évolué ces dernières années, et la pandémie de COVID-19 a été un coup d'accélérateur. En 2020, pour pérenniser leur productivité, elles ont dû accélérer leur transformation digitale, en généralisant l'utilisation d'applications cloud et le recours au télétravail. Cependant, cette évolution était incompatible avec les pare-feux, les VPN et les architectures basées sur le périmètre qui faisaient appel à ces outils. En effet, il est impossible de construire un périmètre de sécurité autour d'un réseau qui s'étend sans cesse à de nouveaux utilisateurs, dispositifs, applications hors site et environnements cloud.

Les entreprises qui continuent à utiliser leur architecture traditionnelle dans le cadre de leur transformation digitale subissent de vrais défis en matière de complexité, de rigidité, de coûts et de productivité. De plus, et surtout, cette infrastructure héritée renchérit les cyber-risques et expose les entreprises à des incidents, pour quatre raisons que nous développerons dans les pages suivantes.

Architecture orientée pare-feu et VPN



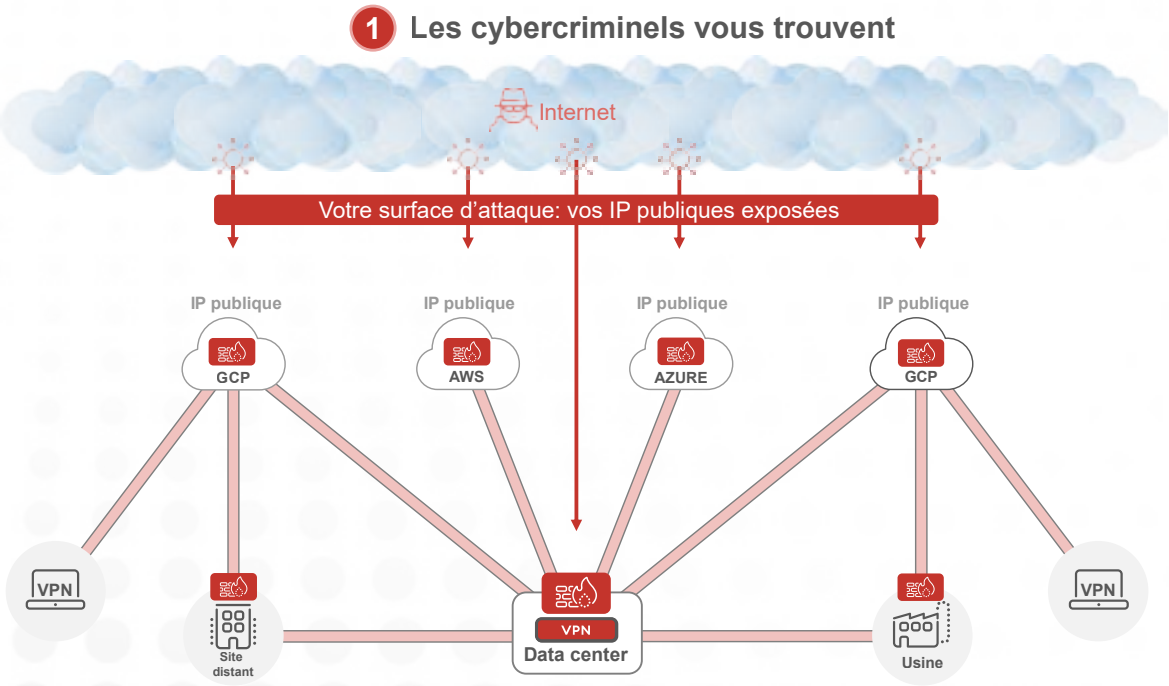
Un réseau de confiance interconnecte les utilisateurs, les sites et les applications. La protection contre les menaces et des données impliquent de sécuriser le réseau.

#1 Les pare-feux et les VPN contribuent à élargir la surface d'attaque

Les cybercriminels sont constamment à la recherche de cibles afin de percer la ligne de défense de ces entreprises et mener leurs exactions. Malheureusement, avec les méthodes de travail actuelles, les architectures basées sur le périmètre élargissent la surface d'attaque et aident involontairement les assaillants à identifier des cibles de valeur.

Comme mentionné précédemment, une topologie réseau en étoile dans le monde moderne signifie étendre continuellement ce réseau à de plus en plus d'utilisateurs distants, d'appareils, de ressources cloud, de sites distants, etc. Ainsi, un vaste réseau plat constitue un véritable concentré de ressources interconnectées et il existe de nombreuses passerelles d'entrée vers ce réseau (applications cloud, utilisateurs distants, etc.) que les cybercriminels peuvent exploiter. En termes simples, un réseau en constante expansion correspond à une surface d'attaque en constante expansion.

Une architecture basée sur les pare-feux et VPN accentue les risques



Malheureusement, les problématiques de surface d'attaque des architectures basées sur le périmètre vont bien au-delà de ce qui précède, et ce à cause des pare-feu et des VPN. Ces outils sont les moyens par lesquels les modèles de sécurité cloisonnée sont censés défendre les réseaux en étoile, mais leur utilisation entraîne des conséquences inattendues.

Les pare-feux et les VPN disposent d'adresses IP publiques qui peuvent être repérées sur l'Internet public. Ces adresses sont conçues pour permettre aux utilisateurs légitimes d'accéder au réseau via le Web, d'interagir avec les ressources connectées et d'accomplir leur travail. Cependant, ces adresses IP publiques peuvent également être trouvées par des acteurs malveillants qui recherchent des cibles qu'ils peuvent pirater afin d'accéder à leur réseau.

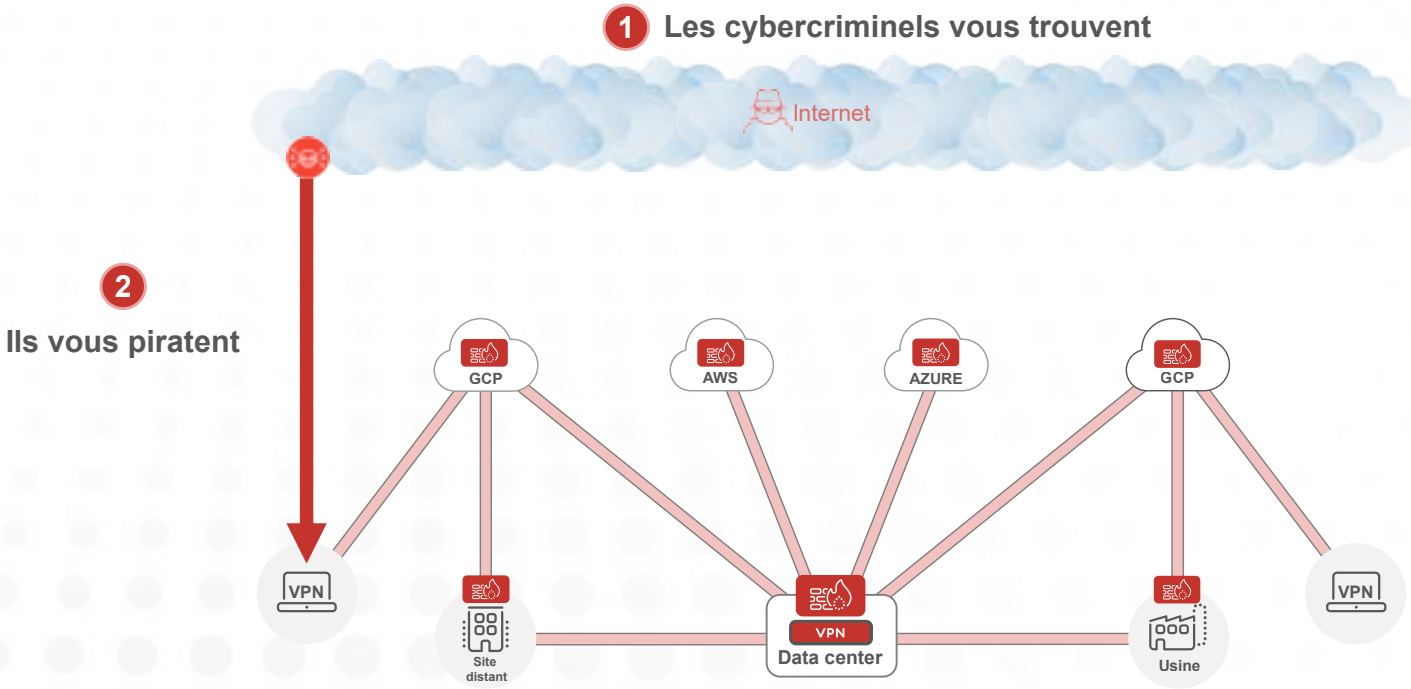
En d'autres termes, les pare-feux et les VPN offrent aux cybercriminels davantage de vecteurs d'attaque en élargissant la surface d'attaque d'entreprise. Ironiquement, cela signifie que la stratégie standard consistant à déployer des pare-feu et des VPN supplémentaires pour faire évoluer et améliorer la sécurité réseau finit par aggraver la problématique de la surface d'attaque.

#2 Les pare-feux et les VPN peinent à déjouer les intrusions

Lorsque les cybercriminels identifient une cible intéressante, ils lancent leurs cyberattaques pour tenter de contourner les défenses en place. Malheureusement, une fois de plus, les outils traditionnels tels que les pare-feux et les VPN ne sont pas conçus pour sécuriser cette étape de l'attaque.

La prévention des intrusions impose de mettre en œuvre, en mode inline, des politiques de sécurité qui neutralisent les menaces en temps réel, avant qu'elles ne puissent pénétrer l'environnement d'une entreprise et engendrer des dommages. Il en résulte que les entreprises doivent être en mesure d'inspecter tout leur trafic pour identifier toute menace potentielle. Pour ce faire, la capacité à inspecter le trafic chiffré est extrêmement importante, puisque la majorité du trafic Web (jusqu'à 95 %) est désormais chiffrée. Et c'est ainsi qu'est révélée une autre faiblesse majeure d'une l'architecture basée sur des pare-feu et VPN.

Une architecture basée sur les pare-feux et VPN accentue les risques



L’inspection du trafic chiffré est un processus gourmand en ressources, ce qui signifie qu’il faut d'importantes ressources informatiques pour déchiffrer le trafic, l'inspecter puis le chiffrer à nouveau. Malheureusement, les appliances de sécurité telles que les pare-feux peinent à fournir les ressources nécessaires, qu’elles soient déployées en tant qu’appliance matérielles sur site ou en mode virtuel sur une instance cloud.

En effet, les appliances ont des capacités fixes, adaptées à un certain niveau de service. Elles ne peuvent pas évoluer indéfiniment pour répondre aux exigences toujours plus importantes d'une inspection de trafic en temps réel, en particulier si le trafic est chiffré. En conséquence, les entreprises qui font appel à des architectures et des outils traditionnels se retrouvent, au mieux, avec une inspection partielle du trafic chiffré et, au pire, sans inspection du trafic chiffré.

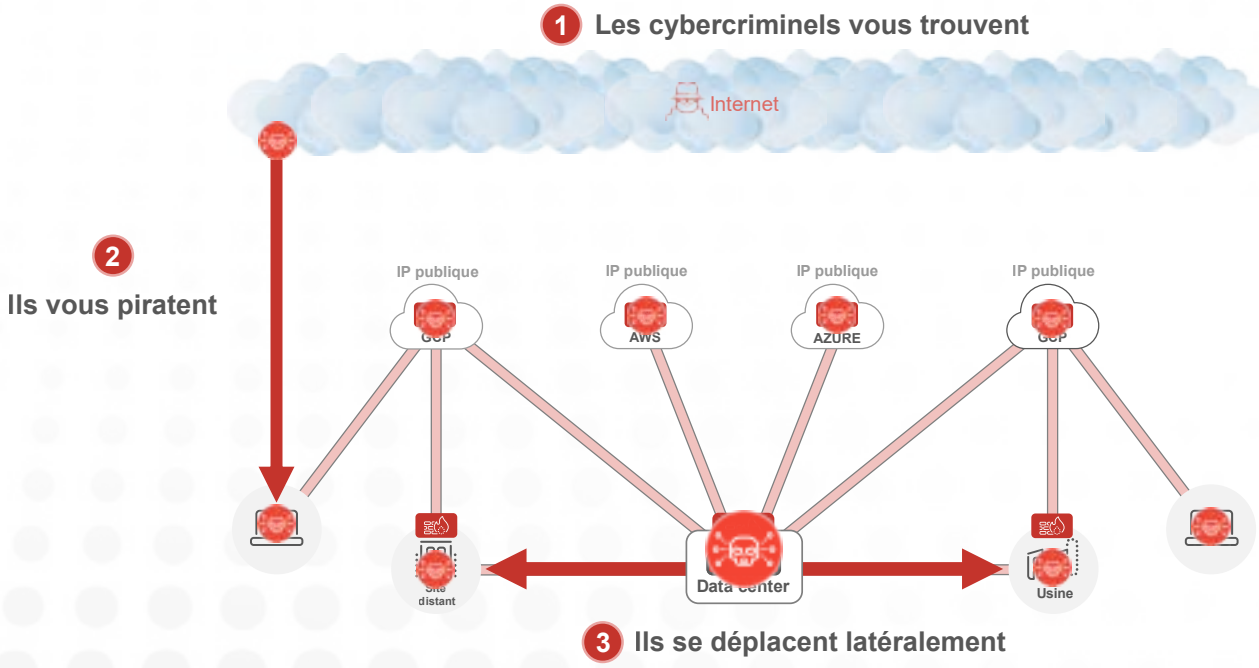
Ne pas inspecter l'ensemble du trafic chiffré signifie que les menaces peuvent transiter via les défenses en place sans être détectées, permettant ainsi aux hackers de mener leurs exactions. Les cybercriminels en sont conscients et ils utilisent le trafic chiffré comme véhicule de leurs attaques. Aujourd’hui, environ **86 %** des cyberattaques passent par un trafic chiffré. Par conséquent, si une entreprise ne parvient pas à inspecter son trafic chiffré, elle ne saura déjouer la majorité des menaces qui tentent de percer ses défenses. En d’autres termes, les architectures de pare-feu et de VPN ne préviennent pas toutes les intrusions.

#3 Les pare-feux et les VPN permettent le déplacement latéral des menaces

Les carences des pare-feux et des VPN sont pleinement mises en évidence lorsqu'une intrusion est effective et qu'une cybermenace a franchi les défenses d'une entreprise. Le déplacement latéral des menaces, également appelé mouvement latéral ou déplacement en interne, fait référence à des menaces sur le réseau qui accèdent aux différentes ressources de l'entreprise, qu'il s'agisse d'applications sur site, d'instances dans des clouds privés ou d'applications SaaS. Il est rare qu'une seule application soit piratée lorsqu'une menace franchit le périmètre d'une entreprise. Pour comprendre le principe du déplacement latéral d'une menace, il suffit de considérer l'analogie contenue dans l'expression anglaise « castle-and-moat security » (ou sécurité cloisonnée en français), qui compare la sécurité périmétrique à une « sécurité d'un château et de ses douves ».

Les douves servent à défendre un château, plus précisément, en empêchant les assaillants d'y accéder, ceci afin de protéger les joyaux de la couronne et les habitants de la forteresse.

Une architecture basée sur les pare-feux et VPN accentue les risques



Cependant, si les assaillants parviennent à franchir les douves, le principal mécanisme de défense du château devient caduc. Dans ce cas, la protection défaillante ne peut empêcher les ennemis de mettre l'intégralité du château à feu et à sang.

La carence des châteaux et des douves mentionnée ci-dessus reste d'actualité avec l'utilisation de pare-feu et de VPN. Ceci est dû à la nature hautement interconnectée des réseaux en étoile encore utilisés par certaines entreprises, ainsi qu'à la manière dont les modèles de sécurité cloisonnée (château et douves) se concentrent sur la protection de l'accès au réseau dans son ensemble.

Imaginez les pare-feux comme des « douves », les VPN comme le « pont-levis » et le réseau lui-même comme le « château ». Une fois qu'une cybermenace a franchi les « douves » et pénètre dans le « château », l'acteur malveillant peut facilement passer d'une ressource connectée à une autre, accédant aux différentes « pièces » du « château ».

En d'autres termes, les pare-feux et les VPN permettent aux menaces de se mouvoir en interne et aux cybercriminels d'étendre leurs exactions à l'ensemble du réseau, entraînant ainsi des dommages, des perturbations et des coûts considérables. Une seule intrusion sur un segment du réseau a valeur d'intrusion générale. Si la segmentation du réseau est souvent présentée comme la solution à ce problème, cette tactique encourage inévitablement à investir dans davantage de pare-feu. Pour autant, cette approche ne résout en rien les carences d'architecture associées aux outils de sécurité périmétriques.

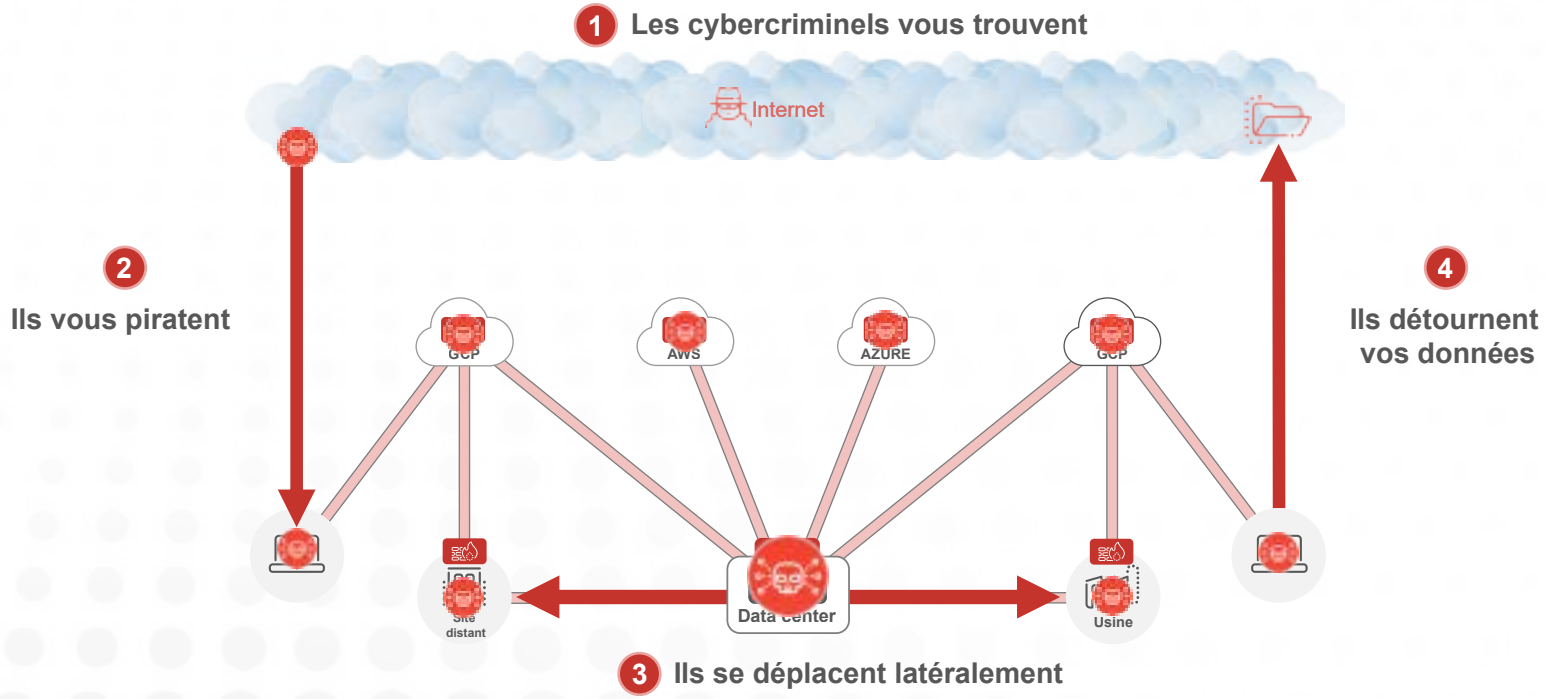
#4 Les pare-feux et VPN n'empêchent pas les pertes de données

Dans la majorité des cyberattaques, les acteurs malveillants ne s'introduisent pas dans les entreprises simplement pour le plaisir. Ils ont un objectif spécifique en tête, qui est souvent de détourner des informations sensibles. En effet, les données volées peuvent être revendues sur le Dark Web pour un bénéfice important, ou utilisées par un ransomware à double extorsion, en tant que moyen de pression sur une entreprise pour qu'elle règle une rançon. Dans les deux cas, les répercussions peuvent être catastrophiques pour toute entreprise.

Ainsi, une fois que les cybercriminels ont identifié une surface d'attaque, percé les défenses et entamé leurs déplacements latéraux (tous trois facilités par des pare-feu et des VPN), ils recherchent autant de données que possible, en privilégiant les informations particulièrement sensibles ou réglementées. Les données de valeur, une fois identifiées, sont exfiltrées.

L'utilisation d'outils traditionnels pour neutraliser ce dernier maillon de la chaîne d'attaque donne une fois de plus des résultats aléatoires et contribue à la perte de données.

Une architecture basée sur les pare-feux et VPN accentue les risques



Comme mentionné précédemment, plus de 95 % du trafic Web est désormais chiffré. L'inspection du trafic chiffré requiert une impressionnante puissance de calcul et les appliances statiques ne sont pas en mesure d'offrir l'évolutivité nécessaire pour traiter les énormes volumes de trafic chiffré générés par les entreprises. Ce défi (tant pour les appliances matérielles que virtuelles) concerne les intrusions, mais également les pertes de données. Les cybercriminels savent que les entreprises ont potentiellement une visibilité moindre sur le trafic chiffré et utilisent ce trafic comme canal d'exfiltration de données.

Mais ce n'est pas seulement ce problème d'évolutivité qui empêche des outils tels que les pare-feux de prévenir l'exfiltration de données. Les technologies d'hier ont été conçues pour le monde d'hier, à une époque antérieure à la généralisation des applications cloud et du télétravail. Elles ne peuvent, par conséquent, sécuriser les canaux modernes des fuites de données, à l'instar de la fonctionnalité de partage intégrée aux applications SaaS telles que Google Drive, Box, Microsoft OneDrive et autres. De même, les ressources cloud mal configurées, comme les buckets AWS S3 définis par erreur sur « public », exposent les données. Cette erreur de configuration ne peut cependant pas être corrigée avec des pare-feu, des VPN ou même des outils conventionnels de prévention des pertes de données.

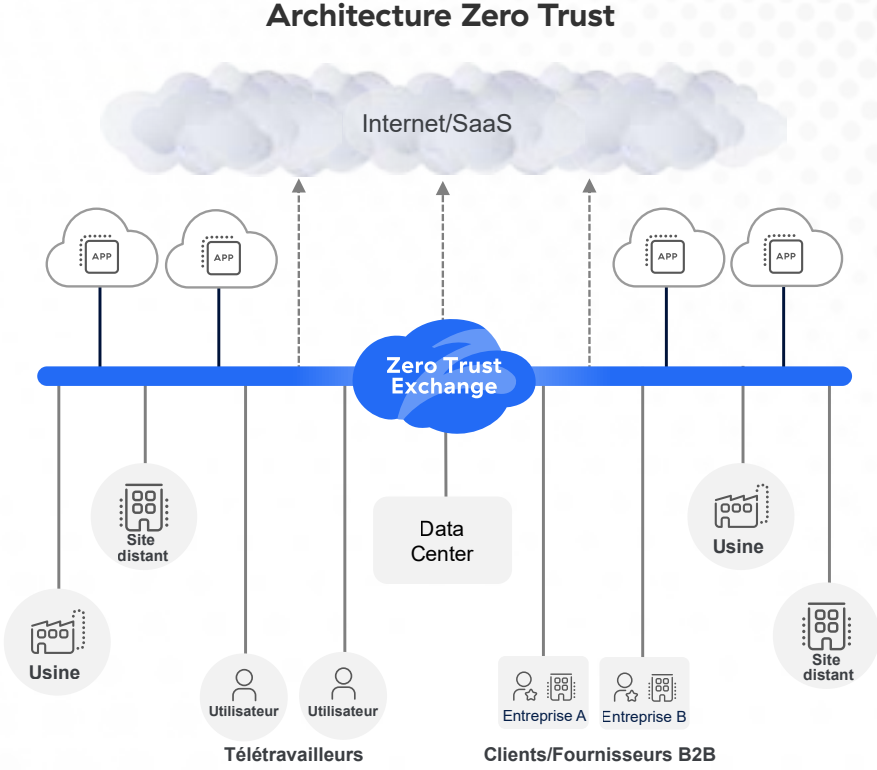
Les hackers externes ne demandent qu'à utiliser ces moyens modernes pour détourner des informations sensibles. Pour autant, ils ne constituent pas la seule menace qui pèse sur les données. Les entreprises doivent se rendre compte que des personnes internes malveillantes ou négligentes peuvent également divulguer des informations sensibles. Quel que soit l'auteur ou l'origine de la fuite, la sécurité doit évoluer pour assurer la protection des données.

Les solutions proposées par l'architecture Zero Trust

Le Zero Trust n'est pas qu'un outil de plus à ajouter au panel des outils de sécurité existants et centrés sur le réseau. Cette approche ne se contente pas de régler les problèmes des architectures basées sur le périmètre sans en résoudre les causes sous-jacentes. Le Zero Trust constitue plutôt une architecture distincte, basée sur le principe d'un accès à moindre privilège. Elle est intrinsèquement différente d'une architecture standard basée sur les pare-feux et VPN.

L'architecture Zero Trust permet aux entreprises qui l'ont déployée de bénéficier d'un cloud de sécurité global qui agit comme un hub intelligent, interconnectant en toute sécurité les utilisateurs, les instances, les dispositifs IoT/OT et les partenaires B2B, sans devoir étendre le réseau vers des utilisateurs ou des dispositifs nouveaux. Parallèlement, le cloud Zero Trust doit proposer des solutions complètes (protection contre les cybermenaces, protection des données, etc.) qui sont fournies en tant que service au niveau de l'edge, au plus proche de l'utilisateur final.

L'architecture Zero Trust dissocie la sécurité de la connectivité du réseau, une vraie innovation par rapport aux architectures traditionnelles, basées sur le périmètre.



Les politiques d'entreprise déterminent qui accède à quoi sur le réseau, le réseau étant un moyen de transport.

Cette architecture moderne permet aux entreprises de mettre fin aux quatre raisons pour lesquelles les pare-feux et les VPN les exposent aux incidents :

- **Minimiser la surface d'attaque :** Tirez parti du modèle Zero Trust pour freiner l'expansion de votre réseau, éliminer les pare-feux & VPN et leurs adresses IP publiques, empêcher les connexions entrantes et dissimuler les applications derrière un cloud Zero Trust.
- **Prévenir les intrusions :** inspectez l'ensemble du trafic, y compris le trafic chiffré, via un cloud Zero Trust hautes performances qui identifie les menaces et applique les politiques de sécurité en temps réel.
- **Empêcher le déplacement latéral des menaces :** connectez les utilisateurs, les instances et les dispositifs directement aux applications, sans passer par le réseau, en respectant le principe d'un accès à moindre privilège.
- **Prévenir toute perte de données :** neutralisez les pertes de données via le trafic chiffré et autres canaux utilisés par les fuites de données, y compris les données au repos dans le cloud et les données utilisées sur les terminaux des collaborateurs.

Au-delà de maîtriser les risques de piratage, une architecture Zero Trust est un vecteur de simplification, dope la productivité des utilisateurs, concrétise des économies et améliore le dynamisme opérationnel, résolvant ainsi une diversité de problématiques qui pèsent sur les architectures traditionnelles, celles basées sur des pare-feu et des VPN.

Synthèse

Pour ceux qui recherchent une architecture Zero Trust, la solution optimisée par IA Zscaler Zero Trust Exchange, constitue un choix pertinent. Cloud de sécurité inline le plus vaste et le plus largement déployé au monde, son envergure et son succès parlent d'eux-mêmes :

150
data centers mondiaux

360 Mrds
de transactions sécurisées chaque jour

500T+
de signaux quotidiens

70
Net Promoter Score

40 %
du Fortune 500 sont des clients

Leader
dans le MQ de Gartner pour le SSE

Pour en savoir plus, inscrivez-vous à notre webinaire mensuel, « Premier pas : une introduction au Zero Trust ». Nous échangerons sur les principes de base d'une architecture Zero Trust et livrerons plus d'informations sur Zscaler afin que chacun puisse initier son adoption du Zero Trust en toute sérénité.

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 le SASE, constitue la plus grande 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