E-BOOK

Les SD-WAN traditionnels sont vulnérables aux attaques de ransomware. Comment se protéger efficacement ?

Introduction

Alors que les défis de sécurité n'ont cessé de progresser, force est de constater que les architectures réseau n'ont pas évolué au même rythme. Selon le rapport Zscaler ThreatLabz 2024 sur les ransomwares, nous avons observé des paiements de rançon plus importants que jamais, avec un bond de 58 % en un an du nombre d'entreprises. Les ransomwares se propagent rapidement dans les entreprises pour une raison simple : les réseaux traditionnels font implicitement confiance à tout ce qui y est connecté, ce qui permet aux ransomwares de se déplacer librement, à partir des appareils infectés vers les sites distants et les applications critiques.

Par le passé, les entreprises comptaient sur un modèle de sécurité cloisonnée dans lequel tout le trafic au sein du réseau était considéré comme sûr par défaut. Les fonctionnalités de sécurité n'étaient appliquées qu'au niveau du périmètre réseau. À mesure qu'elles se sont décentralisées et qu'elles ont migré vers le cloud, les entreprises ont simplement étendu leurs réseaux privés aux sites distants et aux clouds à l'aide de réseaux étendus programmables (software-defined SD-WAN) et de VPN de site à site. Il en résulte de vastes réseaux plats et de confiance au sein desquels les hackers peuvent se déplacer latéralement, et ce, malgré la multitude de pare-feu déployés un peu partout.

Parallèlement, les réseaux intègrent un nombre toujours plus important de dispositifs IoT. Selon les estimations, 55,7 milliards de ces dispositifs seront connectés aux réseaux d'entreprise d'ici 2025, générant 80 milliards de zettaoctets de données chaque année.[1] Cette expansion de l'edge réseau élargit toujours plus la surface d'attaque, exposant les entreprises à davantage de vulnérabilités. Ces tendances rendent les approches de sécurité basées sur le périmètre de moins en moins pertinentes. Par conséquent, année après année, le nombre et le coût des incidents de données ne cessent de progresser, tandis que l'activité des ransomwares s'intensifie.

Pour protéger leur infrastructure contre ces menaces toujours plus nombreuses, les entreprises s'orientent vers une approche de la cybersécurité fondée sur le principe du Zero Trust.

Hausse de 17,8 % des attaques de ransomware de 2023 à 2024[2]

Versement record de **75 millions de dollars** en 2024 suite à une attaque de ransomware[2]

Bond de 104 % du nombre de victimes de piratage de données entre 2023 et 2024[3]

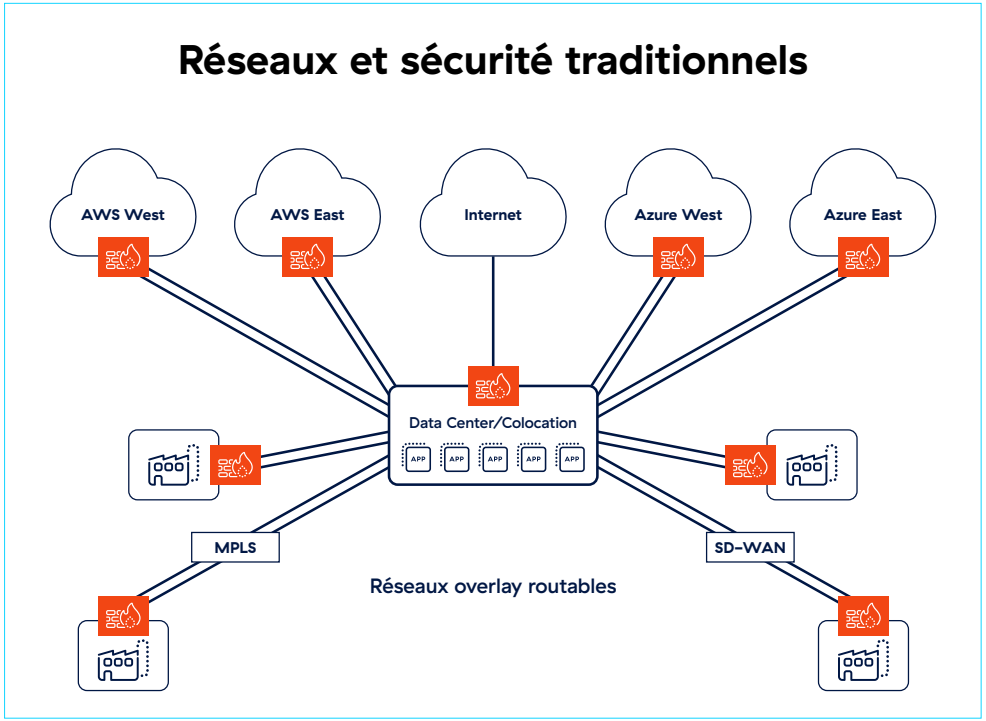
Le coût moyen d'un piratage de données a atteint le niveau record de **4,88 millions de dollars** en 2024[4]

1 : IDC Research, Future of Industry Ecosystems: Shared Data and Insights, 2021.
2 : Rapport Zscaler ThreatLabz 2024 sur les ransomwares.
3 : Identity Theft Resource Center, H1 2024 Data Breach Analysis.
4: IBM, Cost of a Data Breach Report 2024.

SD-WAN traditionnel : principes et limites

Le SD-WAN mise sur l'automatisation pour orienter le trafic réseau vers le chemin le plus performant, via les différents services et infrastructures de transport du réseau. Les protocoles de routage adaptés aux applications améliorent les performances de ces dernières en rendant le trafic entre applications critiques prioritaire.

Les solutions SD-WAN traditionnelles se contentent d'étendre le réseau de l'entreprise aux sites distants et aux data centers. Conçu pour simplifier la connectivité, le SD-WAN permet à tous les appareils, y compris ceux des sites distants, des usines et de sites tiers, de communiquer avec les applications hébergées dans le data center ou dans le cloud public. Composées d'un maillage d'appliances et de VPN de site à site, ces architectures offrent peu ou pas de protection contre le déplacement latéral des menaces et les ransomwares.



Permet le déplacement latéral des menaces et facilite les attaques par ransomware

Étend la surface d'attaque aux sites distants, aux usines et au cloud

Augmente les coûts, la complexité et les délais de déploiement

Le SD-WAN a été conçu pour améliorer la connectivité et permettre aux utilisateurs d'accéder plus rapidement et facilement aux ressources. Mais connectivité n'est pas synonyme de sécurité. L'architecture Zero Trust exige au contraire que l'identité et la posture de sécurité soient vérifiées avant d'autoriser une connexion. La confiance implicite accordée par les réseaux traditionnels complique leur sécurisation et facilite la propagation rapide des ransomwares.

Pour intégrer le Zero Trust dans un SD-WAN traditionnel, l'entreprise doit faire appel à de nouveaux outils et appliances, mais aussi définir des points de contrôle de sécurité supplémentaires. Il en résulte un patchwork de pare-feu, de VPN et d'outils dédiés au contrôle d'accès au réseau (NAC), à la sécurité des DNS, etc. Cette architecture est complexe et sa gestion pèse tant que les budgets que sur les ressources.

> « En réalité, lorsque la connectivité est établie dans un contexte de confiance accordée par défaut, elle va à l'encontre du modèle de Zero Trust. »

Qu'est-ce que le Zero Trust ?

Zero Trust est une stratégie de sécurité qui stipule qu'aucune entité (utilisateur, application, service ou appareil) ne doit être considérée comme fiable et de confiance par défaut. Selon le principe de l'accès sur la base du moindre privilège, le niveau de confiance est établi avant toute connexion compte tenu d'éléments de contexte et de la posture de sécurité de l'entité, puis réévalué en permanence à chaque nouvelle connexion, même si l'entité a déjà été authentifiée auparavant.

Démarrer avec le Zero Trust

Il est complexe et coûteux de vouloir initier un projet Zero Trust en instaurant des points d'application de la politique et des fonctionnalités de sécurité sur un réseau ouvert et plat. D'autre part, les projets de segmentation du réseau courent souvent sur des mois, voire des années, tandis que leur cahier des charges évolue souvent en cours de projet. Et si vous pouviez démarrer ce projet ailleurs que sur votre réseau ? Imaginons que vos sites distants soient indépendants, sans réseau routable qui les relie aux applications d'entreprise dans le cloud ?

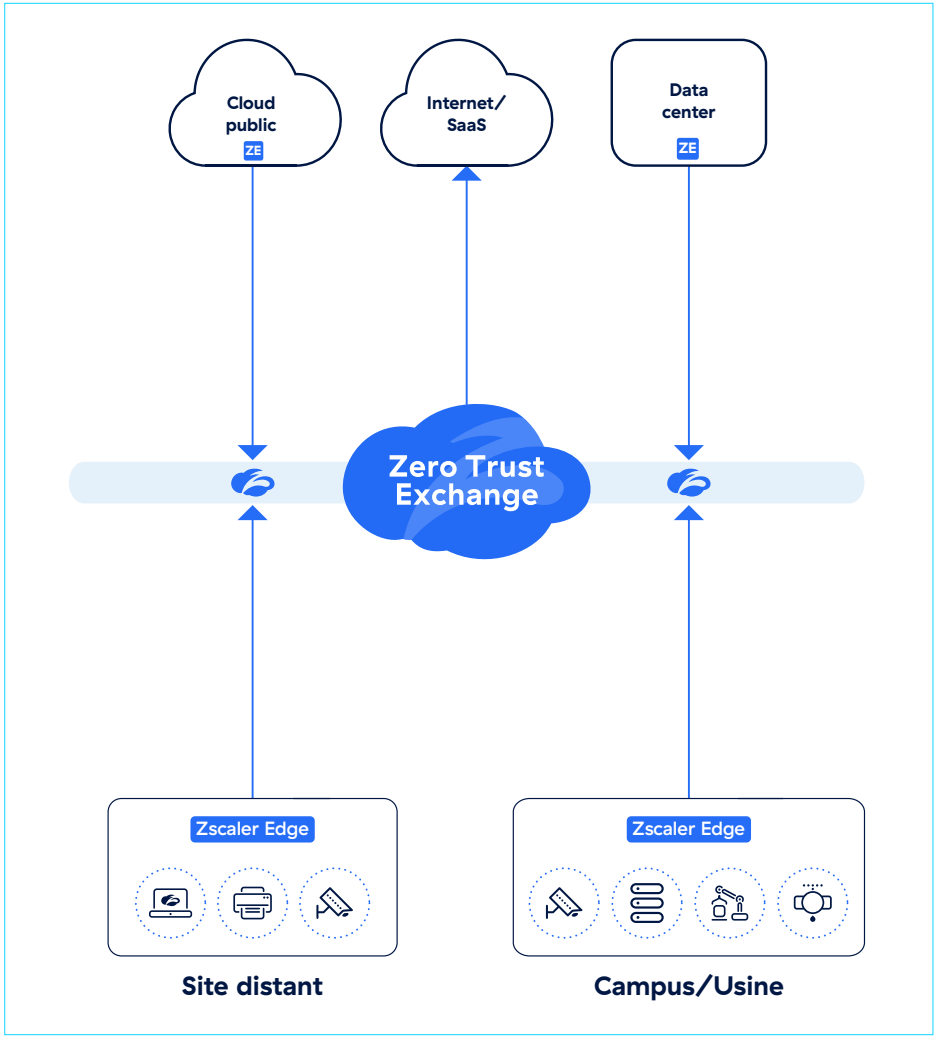
Dans ce contexte, les utilisateurs et les dispositifs sont connectés aux applications selon les principes d'une politique, et non en fonction de leur présence sur le réseau, ce qui garantit à la fois une sécurité robuste et une simplicité opérationnelle.

Il s'agit d'une approche Zero Trust native qui prévient tout déplacement latéral, puisque les utilisateurs et les appareils, y compris les dispositifs de l'Internet des objets (IoT) et OT (operational technology) ne sont jamais connectés directement aux applications. Au lieu de cela, ils communiquent via la plateforme Zero Trust Exchange™ de Zscaler, qui favorise une protection totale des données et contre les cybermenaces grâce à des contrôles d'accès robustes basés sur l'identité et le contexte.

« Le SD-WAN Zero Trust est une nouvelle façon de fournir aux sites distants et aux data centers un accès rapide et fiable à Internet, aux applications privées et aux services cloud, sans étendre le réseau de l'entreprise dans plusieurs directions. »

Cette approche Zero Trust présente de réels atouts. Elle :

- **Améliore les performances des applications.**
  Les entreprises peuvent remplacer les VPN site à site complexes par une architecture simple, directe vers le cloud, qui offre des performances élevées et encourage la productivité.
- **Réduit la surface d'attaque sur Internet.**
  Les solutions WAN traditionnelles exposent les ports VPN à l'Internet public, ce qui rend le réseau vulnérable aux attaques. Avec le SD-WAN Zero Trust, les applications privées se situent en aval de Zero Trust Exchange : elles ne peuvent donc pas être identifiées ou ciblées depuis Internet.
- **Prévient le déplacement latéral des menaces.**
  Les VPN de site à site créent un vaste réseau routable où toute infection par un malware peut se propager d'un seul dispositif à l'ensemble du réseau. Avec le SD-WAN Zero Trust, les connexions sont établies directement avec les applications, et non avec le réseau. Les déplacements latéraux (en interne) sont par conséquent impossibles.
- **Réduit les coûts et la complexité.**
  Cette approche élimine le besoin de multiples pare-feu, VPN, outils NAC et autres technologies. L'architecture qui en résulte est plus simple, moins coûteuse et beaucoup plus facile à configurer et à gérer.



Zscaler pallie les carences du SD-WAN traditionnel

En s'appuyant sur Zero Trust Exchange pour connecter en toute sécurité les sites distants, les usines et les data centers, Zscaler garantit un accès Zero Trust uniforme et cohérent pour tous les utilisateurs, dispositifs IoT/OT et applications.

	SD-WAN Zero Trust	SD-WAN traditionnel
Réduit la surface d'attaque et prévient le déplacement latéral des menaces	Oui	Non
Simplifie les règles de pare-feu et ACL	Oui	Non
Évite d'avoir à arbitrer entre sécurité et performances	Oui	Non
Élimine le besoin d'un pare-feu sur les sites distants	Oui	Non

Le SD-WAN Zero Trust de Zscaler est suffisamment flexible pour s'adapter à différentes options de déploiement qui n'exigent pas de totalement remplacer l'existant. Il peut être opérationnel aux côtés de votre infrastructure SD-WAN actuelle pour vos sites distants et créer des réseaux overlays Zero Trust vers Zero Trust Exchange. Ainsi, les dispositifs présents sur votre site distant bénéficieront d'un accès sécurisé et performant vers des applications privées sur d'autres sites et dans le cloud, sans autoriser le déplacement latéral des menaces.

Si vous envisagez une nouvelle approche pour répondre aux besoins de connectivité de votre entreprise, commencez par une architecture Zero Trust native qui élimine la nécessité de déployer des pare-feu supplémentaires. Le SD-WAN Zero Trust de Zscaler gère les connexions de vos FAI et oriente intelligemment le trafic des applications, ce qui protège vos utilisateurs sur vos sites distants et met votre entreprise à l'abri des attaques de ransomware.

Zero Trust : une arme redoutable contre les attaques de ransomware

Le Zero Trust est un levier essentiel pour répondre aux besoins de sécurité actuels et maîtriser les risques d'attaques par ransomware. Avec le SD-WAN Zero Trust de Zscaler, votre entreprise sécurise toutes les communications et élimine le déplacement latéral des menaces, sans les coûts ni la complexité opérationnelle propres aux approches traditionnelles. De plus, une expérience digitale optimale contribue à la productivité et à la satisfaction des clients, des collaborateurs et des autres utilisateurs finaux.

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 Zero Trust Exchange™ de Zscaler 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. Adossé à un écosystème de plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr**.

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