Akamai

4 raisons pour lesquelles votre entreprise doit adopter un modèle de sécurité Zero Trust

Table des matières

Introduction

À mesure que les attaquants deviennent plus pointus, que les groupes de ransomwares prolifèrent et que les progrès technologiques introduisent de nouvelles vulnérabilités, les entreprises se tournent de plus en plus vers le modèle de sécurité Zero Trust. À l'origine, cette approche met fin à la confiance implicite accordée aux utilisateurs, applications et terminaux, qui était un principe clé des précédentes approches de sécurité. En pratique, il existe quatre scénarios clés dans lesquels une entreprise bénéficiera d'un modèle de sécurité « Zero Trust » : une attaque par ransomware contre votre entreprise, un passage au télétravail, la nécessité de sécuriser votre environnement cloud ou un audit à venir.

Ces scénarios sont le résultat des tendances récentes (augmentation des attaques par ransomware, passage à un personnel hybride, migration vers le Cloud Computing et augmentation des demandes des audits de sécurité) qui nécessitent une approche de sécurité qui repose sur la vérification de l'identité des utilisateurs, où qu'ils se trouvent, et qui prend des mesures proactives en cas de violation. Zero Trust est la seule approche qui exige une forte identité de l'utilisateur pour accéder aux données et qui prévoit des mesures d'atténuation proactives une fois qu'une attaque s'est produite.

Mettre en place une stratégie Zero Trust peut sembler complexe pour les équipes de sécurité déjà surchargées, mais ce n'est pas forcément le cas. En adoptant une approche progressive et en vous concentrant sur les résultats rapides que cela pourrait vous apporter, vous pouvez non seulement réduire la complexité et les risques associés aux solutions de sécurité traditionnelles, mais aussi améliorer votre posture de sécurité.

Vous n'avez pas à remplacer toutes vos technologies existantes pour vous lancer. Commencez par aligner vos investissements Zero Trust avec les besoins les plus urgents de votre entreprise. Choisissez un fournisseur de solutions Zero Trust de confiance plutôt qu'un de ces fournisseurs qui s'est contenté de rebaptiser son ancienne solution « Zero Trust » du jour au lendemain. Considérez fortement un fournisseur qui peut combiner plusieurs éléments de sécurité Zero Trust (accès au réseau Zero Trust, pare-feu DNS, microsegmentation, etc.) sous une seule plateforme. Quelle que soit la raison de votre choix, Zero Trust vous permettra de gagner en agilité, d'optimiser les coûts et de consolider les outils, tout en améliorant l'ensemble de vos opérations.

Les 4 principales raisons pour lesquelles les entreprises se tournent vers le Zero Trust

Augmentation des attaques par ransomware

Personnel hybride

Adoption de ressources de Cloud Computing

Exigences de conformité rigoureuses

01

Augmentation des attaques par ransomware

Amélioration de votre protection contre les ransomwares

Au cours des dernières années, des entreprises du monde entier (hôpitaux, banques, pipelines et autres infrastructures essentielles, par exemple) ont été victimes d'attaques par ransomware. En fait, **Cybersecurity Ventures** prévoit que les ransomwares coûteront à leurs victimes environ 265 milliards de dollars par an d'ici à 2031. Il prévoit que les auteurs de ransomwares lanceront une nouvelle attaque (contre un internaute ou une entreprise) toutes les deux secondes, à mesure qu'ils affineront les charges utiles de leurs logiciels malveillants et les activités d'extorsion qui y sont liées.

Sans une stratégie Zero Trust, les groupes de ransomwares peuvent tirer parti des faiblesses suivantes :

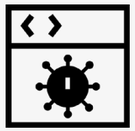
- ☑ Confiance implicite accordée aux utilisateurs, applications et réseaux, qui permet aux attaquants qui ont réussi à accéder au réseau de s'y déplacer latéralement et d'y diffuser des logiciels malveillants
- ☑ Stratégies d'accès trop permissives qui laissent le champ libre aux infections, elles-mêmes susceptibles d'être utilisées pour injecter des ransomwares
- ☑ Systèmes ne demandant qu'un mot de passe, ce qui facilite le vol d'identifiants

Rôle du Zero Trust

Les entreprises qui mettent en place une architecture Zero Trust, ont des stratégies de contrôle d'accès et utilisent une microsegmentation limitent les dommages qu'une telle attaque peut causer. Non seulement il est plus difficile pour les attaquants d'accéder au système, mais leur surface d'attaque s'en trouve également limitée.

Comment Akamai stoppe la chaîne d'attaque des ransomwares

Une attaque par ransomware implique généralement une infection initiale, un mouvement latéral, ainsi que l'exfiltration et le chiffrement des données. Avec le Zero Trust, les entreprises peuvent aborder les étapes au fur et à mesure, voire les anticiper.



Infection initiale

La plateforme Akamai Guardicore permet d'empêcher une attaque de se propager au-delà du point d'entrée initial, tandis que Akamai MFA protège les utilisateurs contre le vol et l'utilisation abusive de leurs identifiants.

Mouvements latéraux

La plateforme Akamai Guardicore réduit les voies de propagation et permet d'empêcher les mouvements latéraux.
Akamai Guardicore Access limite les mouvements de l'attaquant, l'empêchant ainsi d'infecter l'application qu'il espérait exploiter.
Akamai Hunt détecte et atténue les menaces avancées évasives sur votre réseau.

Exfiltration et chiffrement des données

La plateforme Akamai Guardicore limite l'accès aux applications critiques, empêchant ainsi les attaquants d'accéder aux données sensibles au sein d'un réseau compromis.
Secure Internet Access Enterprise d'Akamai bloque les requêtes vers les sites d'hameçonnage et les sites de commande et de contrôle.
Enfin, Akamai Hunt détecte les comportements anormaux, empêchant ainsi les attaquants de chiffrer des données précieuses susceptibles de faire l'objet d'une demande de rançon.

02

Personnel hybride

Sécurisation des nouveaux collaborateurs hybrides

Il est plus difficile de sécuriser les nouveaux collaborateurs hybrides, dont le nombre a augmenté en raison de la pandémie COVID-19, lorsque les entreprises utilisent des outils de sécurité obsolètes (pare-feu et VPN, par exemple). Lors du lancement des VPN d'accès à distance il y a 30 ans, tout était différent : Internet n'était qu'à ses débuts, les applications étaient exécutées dans le centre de données et le nombre d'utilisateurs se connectant depuis des sites distants était bien moins élevé. Continuer à authentifier les utilisateurs à l'aide d'un VPN et leur accorder l'accès à l'ensemble du réseau augmente la surface d'attaque et ouvre la porte à de nombreuses failles Zero Day liées aux anciens VPN. Tout utilisateur disposant des informations d'identification nécessaires peut se connecter à un VPN d'entreprise et, une fois connecté, parcourir latéralement le réseau et accéder aux ressources que le VPN était censé protéger.

Rôle du Zero Trust

Basé sur le principe d'accès de moindre privilège, le Zero Trust suppose qu'aucun utilisateur ou qu'aucune application ne doit être considéré(e) comme fiable. La technologie Zero Trust Network Access (ZTNA) adopte une approche complètement différente de celle des VPN pour sécuriser l'accès des travailleurs à distance. Au lieu de mettre l'ensemble du réseau en péril, les utilisateurs sont connectés directement aux applications et données dont ils ont besoin, empêchant ainsi tout mouvement latéral d'utilisateurs malveillants disposant de droits d'accès trop permissifs aux données et ressources sensibles. En cas de violation, une solution de microsegmentation Zero Trust efficace peut segmenter le réseau interne de manière à ce que la violation ne se propage pas et n'endommage pas d'autres parties du réseau. Selon **Gartner**, d'ici 2025, au moins 70 % des nouveaux déploiements d'accès à distance seront principalement traités par la technologie ZTNA plutôt que par des services VPN, contre moins de 10 % fin 2021.

Comment Akamai facilite le travail hybride et à distance

La plateforme complète Zero Trust d'Akamai répond aux besoins de vos collaborateurs hybrides. Avantages :

Réduction des risques

Akamai connecte directement le bon utilisateur à la bonne application, ce qui réduit la surface d'attaque et limite les mouvements latéraux.

Expérience utilisateur améliorée

Les utilisateurs distants bénéficient d'un accès aux ressources quel que soit leur emplacement, leur terminal ou leur application, leur évitant ainsi de devoir se connecter au VPN et s'en déconnecter.

Plus d'agilité

Étant donné que la solution Akamai est utilisée en tant que service, les entreprises n'ont pas de matériel à déployer et n'ont pas à se soucier de l'évolutivité de leur infrastructure à mesure que les demandes augmentent, ce qui réduit les coûts et la complexité.

03

Adoption de ressources de Cloud Computing

Facilitation de la migration vers le cloud

Les entreprises migrent leurs applications vers le cloud pour améliorer leur flexibilité et leur agilité, mais aussi pour moderniser leur infrastructure. Toutefois, ces environnements cloud élargissent la surface d'attaque et introduisent de nouvelles exigences de sécurité. Les intégrations au sein de différents clouds et environnements sur site peuvent nuire aux applications et mettre la sécurité en danger. Lorsque les entreprises tentent de migrer leurs applications vers le cloud à l'aide d'infrastructures réseau traditionnelles (VPN et pare-feu, par exemple), elles sont souvent confrontées à un risque accru de menaces latérales, de faible évolutivité et de coûts élevés. Même une fois la migration terminée, les ressources doivent toujours être sécurisées et les utilisateurs doivent être authentifiés en fonction des autorisations de rôle. Les utilisateurs de l'infrastructure cloud bénéficient généralement d'un accès plus large aux ressources, aux services et aux droits de gestion qu'ils ne le pourraient avec des environnements sur site, ce qui entraîne des risques supplémentaires et une éventuelle interruption de service.

Rôle du Zero Trust

Les stratégies Zero Trust facilitent la migration vers le cloud. Le Zero Trust supprime la confiance implicite inhérente aux nombreuses applications basées sur le cloud, en particulier les applications tierces, qui peuvent introduire des vulnérabilités. Les solutions Zero Trust permettent aux entreprises de déployer plus facilement leurs applications basées sur le cloud, le tout en bénéficiant de meilleures protections. Déployer des solutions Zero Trust pour le cloud présente les avantages suivants :

- ☑ Meilleure visibilité des ressources et des risques
- ☑ Réduction de la surface d'attaque grâce à la segmentation Zero Trust et à l'accès de moindre privilège aux ressources du cloud
- ☑ Infrastructure réseau modernisée qui offre vitesse et agilité
- ☑ Réduction des coûts opérationnels et de la complexité

Comment Akamai améliore la migration vers le Cloud

Les solutions Zero Trust d'Akamai peuvent vous aider à migrer automatiquement vos ressources et leurs stratégies respectives. L'entreprise ne connaît aucune interruption ni aucun temps d'arrêt. Akamai offre les avantages suivants :

Meilleure visibilité

Grâce à une meilleure compréhension des dépendances des applications, vous pouvez créer des stratégies de segmentation du cloud efficaces pour réduire la surface d'attaque et minimiser les risques.

Zero Trust Network Access

Les utilisateurs ne peuvent se connecter qu'aux applications auxquelles ils sont autorisés à accéder, le tout via une authentification forte.

Recherche des menaces

L'équipe dédiée d'Akamai recherche en permanence des comportements d'attaque anormaux dans les environnements cloud et informe les clients d'Akamai de tout risque pour leur réseau.

04

Exigences de conformité rigoureuses

Simplification de la conformité et réduction des risques

Bien que les responsables de la sécurité sachent que le respect des exigences de conformité n'assure pas véritablement la sécurité d'une entreprise, les audits de sécurité restent leur priorité. En cas d'échec aux audits, ils savent que cela peut entraîner d'importantes perturbations pour l'entreprise et avoir des conséquences sur ses résultats. Procéder à une évaluation de la conformité est l'une des activités les plus chronophages et gourmandes en ressources pour les équipes de sécurité. De plus, la migration vers des environnements digitaux sans périmètre et la prévalence du travail à distance ont rendu la tâche encore plus difficile. Les entreprises doivent généralement isoler leurs environnements et cloisonner leurs ressources réglementées afin de respecter les normes de conformité, telles que la norme de sécurité de l'industrie des cartes de paiement (PCI DSS), la loi HIPAA (Health Insurance Portability and Accountability Act) et la norme SWIFT (Society for Worldwide Interbank Financial Telecommunications).

Les entreprises doivent également s'adapter aux utilisateurs distants, aux utilisateurs sur site de l'entreprise, aux partenaires, aux fournisseurs et bien plus encore, ce qui rend le périmètre de l'environnement d'une entreprise presque impossible à définir. Alors que les équipes de sécurité se préparent à des audits dans lesquels le contrôle d'accès est un facteur déterminant clé de la réussite, elles doivent répondre aux questions suivantes :

- Comment pouvons-nous limiter l'accès aux informations sensibles aux utilisateurs autorisés uniquement ?
- Comment pouvons-nous limiter la portée de l'environnement d'audit ?
- Comment pouvons-nous simplifier le processus d'audit ?

Rôle du Zero Trust

Heureusement, une approche Zero Trust peut aider à répondre à toutes ces questions et plus encore. Les deux piliers clés du Zero Trust (vérification explicite et prise en charge d'un accès de moindre privilège) simplifient considérablement le processus de conformité. Les entreprises peuvent isoler leurs ressources réglementées des autres trafics de leur centre de données ou du cloud, et y autoriser l'accès après vérification de l'identité des utilisateurs, où qu'ils se trouvent. Une visibilité accrue montre ce qui transite par leur environnement réglementé et aide à identifier les éléments concernés. Cela réduit considérablement la complexité et le coût de l'audit, et facilite la vie de l'auditeur.

Comment Akamai facilite la conformité

Le portefeuille complet de solutions Zero Trust d'Akamai vous aide à vous préparer à chaque audit (PCI DSS, HIPAA, Organisation internationale de normalisation [ISO], Sarbanes–Oxley [SOX] ou tout autre cadre). Enterprise Application Access d'Akamai contrôle l'accès des tiers aux informations personnelles sensibles, conformément aux exigences du Règlement général sur la protection des données (RGPD). Akamai Guardicore Segmentation améliore la compréhension des ressources réglementées en vertu de la norme PCI DSS, isole les fonctions de centre d'échange conformément à la loi HIPAA, et limite l'accès à Internet et isole les systèmes critiques pour répondre aux réglementations SWIFT. Akamai MFA protège les informations sur les patients en vertu de la loi HIPAA contre les attaquants disposant de mots de passe pour accéder aux systèmes de santé. Cette solution renforce la conformité SWIFT en empêchant les informations d'identification d'être compromises.

Une banque internationale obtient la conformité SWIFT en deux semaines

Les organismes de réglementation externes ont exigé qu'un des clients d'Akamai, une banque internationale, cloisonne toutes ses applications critiques afin de répondre aux exigences de la norme SWIFT pour un transfert d'argent sécurisé entre institutions financières. En général, une application de ce type nécessite plus de 100 serveurs déployés sur différents sites, y compris des serveurs dédiés physiques et virtuels. En moyenne, la planification et l'exécution de ce processus prendraient entre 8 et 12 mois pour une banque de cette taille, car il faudrait créer un réseau local virtuel (VLAN) pour le segment sur plusieurs sites. Déterminer les dépendances de l'application SWIFT et s'assurer que l'ensemble de règles était correct et conforme n'aurait fait que retarder les délais. En attendant, le projet aurait également exigé l'achat de nouveaux équipements de pare-feu. L'application SWIFT étant essentielle pour le secteur bancaire, la banque ne pourrait tolérer de temps d'arrêt. Dans l'ensemble, le projet de segmentation devait nécessiter l'intervention de nombreuses personnes. Mais grâce à Akamai, il n'a fallu qu'un seul ingénieur de sécurité et environ deux semaines pour exécuter le processus.
La banque n'avait pas à changer de réseau ni d'application, évitant ainsi tout temps d'arrêt.

Mise en conformité simple et rapide

Banque internationale

- Cloisonnement nécessaire de l'application SWIFT
- Environnement complexe avec serveurs dédiés physiques, VMware et OpenStack

Segmentation traditionnelle

- Difficile de définir des segments dans une infrastructure complexe
- Aucune visibilité sur les applications et les dépendances
- Temps d'arrêt requis
  Durée : 8 à 12 mois
  Intervenants : au moins 5

Guardicore Segmentation

- Mappage de l'application SWIFT terminée en quelques heures
- Stratégies de segmentation automatiquement suggérées et affinées
- Inutile d'acheter et de déployer de nouveaux matériels et pare-feux
- Aucun temps d'arrêt
  Durée : 2 semaines
  Personnes : 1 architecte

Découvrez comment répondre aux besoins de votre entreprise grâce au portefeuille de solutions Zero Trust d'Akamai

En savoir plus

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur **akamai.com** et **akamai.com/blog**, ou abonnez-vous à Akamai Technologies sur **X** (anciennement Twitter) et **LinkedIn**. Publication : 09/24.