Akamai

LIVRE BLANC

Un modèle pour la construction d'une architecture Zero Trust

Table des matières

Introduction

Le concept de Zero Trust existe depuis 2009, année durant laquelle Forrester Research en a fait la promotion pour la première fois, avertissant les organisations qu'il était temps de revoir la méthode traditionnelle consistant à accorder un accès illimité à tout utilisateur ou application qui franchissait le périmètre du réseau. Au contraire, chaque terminal, utilisateur et flux réseau devrait être contrôlé avant de pouvoir accéder à l'ensemble du réseau. Au cours des années suivantes, adopter le concept de Zero Trust est devenu de plus en plus urgent en raison de nombreux facteurs. La pandémie de COVID-19 a engendré une augmentation du nombre d'employés qui travaillent à distance, en dehors du périmètre réseau. Les attaques par ransomware sont de plus en plus fréquentes et sophistiquées, ce qui accroît les risques qu'un pirate parvienne à percer vos défenses et augmente les coûts une fois qu'il y parvient. Selon le rapport IBM Cost of a Data Breach 2022, le coût moyen d'une violation de données a atteint le montant record de 9,44 millions de dollars aux États-Unis. En outre, l'augmentation du nombre de terminaux connectés au réseau, notamment ceux de l'Internet des objets (IoT), et les exigences supplémentaires relatives à l'accès réseau des partenaires et des clients ont considérablement augmenté la surface d'attaque des entreprises. Dans cet écosystème de cybersécurité en constante évolution, les fournisseurs de réseau et de logiciels de sécurité se sont empressés d'apposer la marque Zero Trust sur leurs produits existants ou de lancer de nouveaux produits, tandis que les consultants et les analystes introduisent de nouveaux acronymes et de nouvelles définitions du marché. Les équipes de sécurité ont donc du mal à expliquer ces concepts parfois complexes et à prendre des décisions d'achat qui posent les bases d'une politique Zero Trust.

Ce livre blanc a pour objectif de fournir aux équipes de sécurité un modèle pour investir dans la technologie Zero Trust en identifiant par où commencer et en soulignant les facteurs clés de différenciation.

Le télétravail et les applications cloud bouleversent les principes de sécurité des réseaux

Les horaires, les méthodes et les lieux de travail dépassent aujourd'hui le cadre du bureau traditionnel.

Par conséquent, le périmètre réseau n'existe plus (du moins plus sous une forme reconnaissable). Vos utilisateurs peuvent aussi bien se trouver à l'intérieur qu'à l'extérieur de ce périmètre. Il en va de même pour les applications qu'ils utilisent, car les logiciels en tant que service (SaaS) et les implémentations multicloud se multiplient. De plus, compte tenu des menaces avancées et persistantes, vous pourriez facilement donner par inadvertance à des acteurs malveillants un accès complet à vos ressources les plus précieuses une fois qu'ils sont entrés dans le réseau. Sans programme Zero Trust complet, les acteurs malveillants ont le champ libre dès qu'ils sont dans le réseau.

Et ce n'est pas qu'une théorie. Cela se manifeste clairement dans les nombreuses et coûteuses violations de données de ces dernières années, la plupart d'entre elles ayant résulté d'un abus de confiance dans le périmètre réseau.

En même temps, les applications conçues pour fonctionner à l'intérieur d'un périmètre réseau présentent souvent les profils de sécurité les moins efficaces. En effet, les développeurs d'hier, qui considéraient que seuls les employés autorisés et bien intentionnés pouvaient entrer dans votre système, ne faisaient pas autant preuve de prudence que les codeurs actuels, qui savent qu'une armada de pirates informatiques attend la moindre occasion d'exploiter leur application Internet.

La solution à ces défis sur l'ensemble du marché, c'est le Zero Trust.

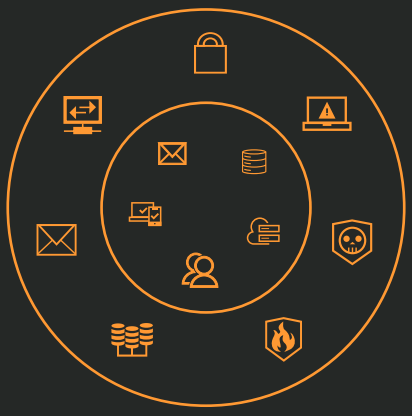
Architecture de sécurité Zero Trust

Aussi simple soit-il, le principe de l'approche Zero Trust est redoutable : la confiance n'est pas une affaire d'emplacement. Vous n'avez aucune raison d'accorder votre confiance à un individu ou système sous prétexte qu'il se trouve derrière votre pare-feu. Toute action, quel que soit l'endroit où elle se produit, ne devrait bénéficier de la confiance que si elle a été explicitement autorisée. En fin de compte, seul ce qui *doit* se produire *peut* se produire. Les entreprises doivent supprimer toute confiance implicite pour les actions qui ne sont pas nécessaires. Par exemple, donner à tous les utilisateurs de votre groupe comptable un accès au système financier alors que seule une poignée en a besoin crée un risque, mais pas de valeur.

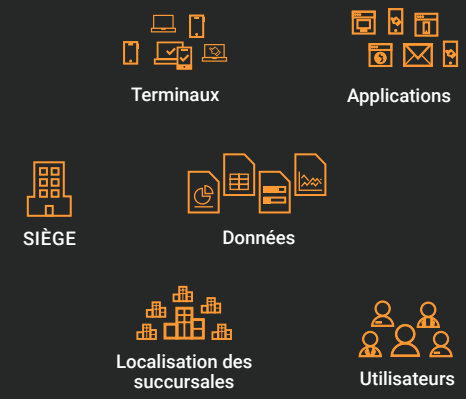
La méthode de preuve de fiabilité consiste en des mesures d'authentification et d'autorisation solides, et les systèmes ne doivent pas transférer de données tant que la confiance n'a pas été établie. En outre, des mesures d'analyse et d'enregistrement doivent être mises en œuvre pour vérifier les comportements et constamment guetter les signes de dangers éventuels.

Ce changement fondamental permet de contrer une grande partie des types d'attaques observés ces dix dernières années. Les pirates informatiques ne peuvent plus se dédier à tirer profit de vos failles pour franchir votre périmètre, puis exploiter vos données ou applications sensibles une fois à l'intérieur de celui-ci. Ce périmètre est devenu obsolète. Tout se résume désormais à des applications et des utilisateurs, qui doivent tous s'authentifier et voir leur accréditation vérifiée avant de bénéficier d'un accès.

Architecture de sécurité traditionnelle



Réalité actuelle



Comment une entreprise crée-t-elle une architecture Zero Trust ?

Tout d'abord, toutes les entreprises doivent élaborer une politique pour leur écosystème existant et déterminer si et quand elles doivent embaucher de nouveaux talents. Cette étape clé du processus pourrait faire l'objet d'une entière publication en soi, mais les produits pouvant véritablement contribuer à la mise en œuvre d'une politique Zero Trust devraient viser trois objectifs.

1. **Ne faites confiance à aucune entité, procédez toujours à une vérification.** À priori, cela semble simple, mais c'est bien plus facile à dire qu'à faire. En effet, si vous coupez simplement tout accès à tous les systèmes et à toutes les données, vous bloquez votre réseau. Le véritable défi consiste à mener des vérifications en permanence sans provoquer d'interruptions massives de l'activité, en particulier lorsque la plupart des systèmes ont été conçus dans un esprit de confiance implicite. Une visibilité et un contrôle étendus de tous les types d'accès ainsi que des moyens simples et pratiques d'appliquer et de maintenir les politiques sont nécessaires.
2. **Une fois la vérification effectuée, assurez-vous que vous fournissez un accès minimal.** Dans un environnement Zero Trust, une fois qu'un utilisateur a été vérifié, il ne peut accéder qu'aux éléments requis par son rôle.
3. **Surveillez les menaces en permanence.** Comme la plupart des experts du secteur vous le diront, l'approche Zero Trust est un processus continu. Les acteurs malveillants utilisent des méthodes de plus en plus sophistiquées pour tenter de percer les défenses d'une entreprise et celle-ci doit continuellement surveiller, vérifier et limiter les accès. L'un des avantages d'un modèle Zero Trust est que l'accent n'est pas mis sur les actions des pirates, mais sur ceux de l'entreprise. Avec une véritable politique Zero Trust en place, les chaînes d'attaques peuvent difficilement corrompre tous les éléments dont votre entreprise a besoin pour fonctionner en même temps. Vous pouvez donc arrêter chaque attaque à un endroit précis de la chaîne. Cela inclut la capacité d'arrêter des attaques qui n'ont pas encore été conçues. Peu importe qu'il s'agisse d'une attaque de type Zero Day ou non, l'approche Zero Trust peut contribuer à l'atténuer.

Le côté sombre de l'approche Zero Trust

Cependant, lorsqu'une entreprise se lance dans la mise en œuvre d'une approche Zero Trust, elle doit également considérer le revers de la médaille lié à toute cette méfiance et aux limites d'accès. Un des aspects fondamentaux de l'approche Zero Trust est la restriction de l'accès, principalement par le biais d'une liste d'autorisations. Cette pratique consiste à dicter ce qui peut être fait, tout le reste étant refusé par défaut. Mais, en diminuant la capacité d'action malveillante d'un attaquant, une entreprise peut accidentellement augmenter le risque d'empêcher un utilisateur légitime de travailler. Par ailleurs, les vérifications répétées des charges de travail et des terminaux peuvent entraîner à la longue des retards et des frustrations. Une politique Zero Trust qui empêche les employés de travailler efficacement n'a pas lieu d'être.

Une politique Zero Trust solide doit donc établir un équilibre entre la sécurité et l'accès. Elle doit aussi concilier ce qui peut effectivement être accompli et les ressources (budgétaires et humaines) de votre équipe de sécurité.

Constituants de l'approche Zero Trust

Forrester a décrit pour la première fois le concept de Zero Trust il y a plus de 10 ans. De nombreuses entreprises qui entament tout juste leur transition vers l'approche Zero Trust sont confrontées à un marché de produits logiciels alambiqué. Certains produits existent depuis des années et incluent des constituants de l'architecture Zero Trust, de nouveaux produits ont émergé et de nombreux fournisseurs de logiciels se sont empressés de renommer leurs offres en incluant le terme Zero Trust. De plus, comme de nombreux analystes et observateurs du secteur vous le diront, « Zero Trust n'est pas un produit, c'est une politique globale » et « Zero Trust n'est pas un point d'arrivée, c'est un parcours ». Ces affirmations maintes fois répétées n'aident pourtant guère ceux qui sont confrontés à des décisions d'achat de solutions technologiques Zero Trust et, en réalité, peuvent créer davantage de confusion.

Parce qu'il n'existe pas de produit unique permettant à une entreprise d'adopter une approche Zero Trust et parce que les entreprises individuelles ont des priorités et des vulnérabilités différentes, le point de départ sera différent pour chacune d'entre elles. Cependant, grâce aux progrès technologiques et à la consolidation de l'industrie, les entreprises sont désormais en mesure d'obtenir les outils nécessaires à la mise en œuvre de politiques Zero Trust auprès d'une source unique. Les cabinets d'analystes commencent eux aussi à le reconnaître. Gartner suit ce qu'il appelle le Secure Service Edge (SSE), une combinaison de passerelles Web sécurisées, de courtiers en sécurité d'accès au cloud et d'accès réseau Zero Trust (ZTNA). Dans son rapport intitulé What Are Practical Projects for Implementing Zero Trust?, Gartner inclut également la microsegmentation, qu'il appelle la segmentation de la charge de travail à la charge de travail, en recommandant que « les entreprises souhaitant passer à la mise en œuvre pratique se concentrent sur deux projets principaux : la segmentation de l'utilisateur à l'application (ZTNA) et la segmentation de la charge de travail à la charge de travail (segmentation basée sur l'identité). »

De la même manière, IDC résume la chose ainsi : accès sécurisé et segmentation, qu'il définit comme une vue d'ensemble des technologies émergentes et anciennes utilisées pour protéger les systèmes informatiques, les ressources et les données par la segmentation logique, le contrôle d'accès et la détection des menaces.

La plupart des experts s'attendent à ce que le marché suive l'exemple en adoptant plusieurs applications d'un seul fournisseur. Dans son rapport intitulé Predicts 2022: Consolidated Security Platforms Are the Future (Prédictions 2022 : les plateformes de sécurité consolidées représentent l'avenir), Gartner prévoit que : « d'ici 2025, 80 % des entreprises auront adopté une politique visant à unifier l'accès au Web, aux services cloud et aux applications privées à partir de la plateforme SSE (Security Service Edge) d'un seul fournisseur ».

Cependant, réunir ces systèmes distincts dans une politique cohésive devient un défi central. Quels sont les éléments clés et que doivent rechercher les directeurs informatiques, les responsables des technologies de sécurité de l'information et les autres professionnels de la sécurité lorsqu'ils construisent une architecture Zero Trust adaptée à leur entreprise ?

Les principes de l'approche Zero Trust

Accès réseau Zero Trust

Souvent confondue avec l'approche Zero Trust globale, la solution ZTNA est un élément fondamental de la pile technologique. L'accès sécurisé est la première étape clé de toute structure Zero Trust. Malheureusement, comme tant d'éléments du processus, il devient rapidement plus complexe qu'il n'y paraît. L'accès sécurisé n'est pas une décision binaire. Fournir le niveau d'accès adéquat à la bonne application, aux bons utilisateurs et au bon moment est devenu beaucoup plus complexe, car les utilisateurs et les applications sont de plus en plus largement distribués. En fait, la définition même d'un utilisateur signifie désormais bien plus qu'un simple employé et peut inclure les clients, les fournisseurs et les partenaires. Les applications peuvent inclure des applications anciennes, SaaS ou pour mobile et nécessitent un accès vers et depuis le centre de données, Internet ou les environnements cloud.

Une solution ZTNA efficace vérifie l'identité de l'utilisateur et de son terminal, et s'assure qu'il peut accéder aux applications dont il a besoin, où qu'il soit, réduisant ainsi la zone d'attaque possible et améliorant la flexibilité et la surveillance. Pendant des décennies, les entreprises se sont appuyées sur des réseaux privés virtuels (VPN) soutenus par des fournisseurs d'identité pour fournir les accès. Ces VPN, conçus pour une autre époque, ne sont plus suffisants pour la taille et la répartition du personnel d'aujourd'hui. Le ZTNA a évolué. Bien plus qu'un simple remplacement des VPN, il gère désormais les accès non seulement en vérifiant l'identité de l'utilisateur et du terminal, mais en se basant également sur des éléments tels que l'heure et la date, la géolocalisation et la posture du terminal, afin d'accorder un niveau de confiance approprié.

Facteurs clés à prendre en compte pour l'achat de solutions Zero Trust d'accès au réseau

Alors que les entreprises commencent à remplacer leurs anciens VPN par des solutions de gestion d'identité plus sophistiquées, de nombreux éléments doivent être pris en compte. Les solutions actuelles les plus avancées doivent combiner la gestion des identités et des accès, la sécurité des applications, l'authentification multifactorielle (MFA) et l'authentification unique, le tout avec une visibilité et un contrôle de gestion au sein d'une seule interface. Les entreprises qui mettent en œuvre des initiatives Zero Trust doivent rechercher des solutions capables de répondre à leurs besoins actuels, mais aussi d'évoluer avec l'entreprise. Cela leur permettra d'intégrer rapidement les employés à la suite d'une fusion ou d'une acquisition d'entreprise, de permettre la fabrication ou la production sur différents marchés ou dans différentes zones géographiques, d'ajouter et de supprimer facilement des sous-traitants pour répondre aux besoins changeants de l'entreprise, et de déplacer les applications vers le cloud de manière rentable sans sacrifier la sécurité.

Les entreprises doivent rechercher des solutions qui peuvent s'intégrer directement aux infrastructures d'identité existantes, même si elles comprennent plusieurs répertoires et fournisseurs de services d'identité. Cela permet de déployer rapidement le service ZTNA sans avoir à modifier l'infrastructure ou l'architecture d'identité existante.

Se tourner vers la bordure de l'Internet

Les équipes en charge des décisions d'achat concernant l'approche Zero Trust ignorent souvent un facteur de différenciation entre les produits du marché important, alors qu'elles auraient tout intérêt à le prendre en compte. Les solutions qui sont combinées avec des plateformes cloud en bordure de l'Internet peuvent offrir des avantages supplémentaires en agissant comme un proxy sensible à l'identité qui soustrait la connectivité à la plateforme en bordure de l'Internet, garantissant que toute l'authentification est effectuée en bordure de l'Internet, loin du centre de données. Bien que certaines entreprises se tournent vers des architectures de proxy d'accès exécutées dans la zone démilitarisée (DMZ), cela ne permet pas de tirer parti de la capacité du cloud à mieux absorber les attaques, à fournir une bande passante pour la mise en cache et à s'adapter automatiquement aux besoins. Un proxy basé sur l'identité construit dans le cloud peut évoluer en fonction de la demande, exploiter des ressources lourdes pour le processeur et absorber les attaques. De plus, il se trouve sur une adresse IP privée qui n'est pas directement accessible depuis Internet. Les activités les plus sensibles en matière de performances et de sécurité ont lieu en bordure de l'Internet, au plus près de l'utilisateur final. En outre, le chemin d'entrée sensible à l'application passe par un tunnel d'application inversé, ce qui masque l'adresse IP du périmètre et réduit les risques d'exposition aux attaques de grand volume.

> **Les solutions associées à des plateformes cloud en bordure de l'Internet peuvent offrir des avantages supplémentaires en agissant comme un proxy basé sur l'identité.**

Facteurs à prendre en compte pour l'authentification multifactorielle dans l'élaboration d'un modèle Zero Trust

Avec l'essor du télétravail et le besoin d'un accès plus large, la plupart des entreprises ont déjà adopté l'authentification multifactorielle et mis en place un type de solution. Il est toutefois important de reconnaître que la combinaison de l'accès à l'échelle de l'entreprise et de l'authentification multifactorielle est plus importante que la somme de ses composantes. L'authentification multifactorielle est au cœur du concept de confiance, car elle exige d'avoir plus qu'un simple mot de passe. Une seconde vérification est nécessaire pour garantir de ne pas être la proie de l'un des abus de confiance les plus courants. Il est également important de se souvenir que toutes les solutions d'authentification multifactorielle ne se valent pas.

Lors de l'évaluation des solutions d'authentification multifactorielle dans le cadre d'une politique Zero Trust, les entreprises doivent rechercher des solutions qui sont :

- intégrées à la gestion d'identité et à l'accès d'entreprise ;
- conformes à la norme FIDO2 pour garantir que les informations d'identification des utilisateurs sont décentralisées, isolées et cryptées sur les terminaux personnels des utilisateurs, ce qui est capital pour contrer les attaques par hameçonnage ;
- capables de procéder à la vérification des utilisateurs via leur smartphone sans s'appuyer sur une clé physique.

Microsegmentation

Le Zero Trust parfait n'existe pas. Elle présente inévitablement des lacunes que les attaquants les plus tenaces pourraient trouver et exploiter. Toute vision globale de l'approche Zero Trust nécessite donc une microsegmentation. Aujourd'hui, la plupart des réseaux ne sont pas segmentés, ou le sont très peu. En effet, les entreprises ont l'habitude de protéger leurs applications critiques avec des pare-feu, mais cela peut s'avérer difficile pour un certain nombre de raisons. Les pare-feu vous obligent essentiellement à appliquer une politique réseau, ce qui crée un point de contrôle. Les connexions réseau doivent passer par un pare-feu, lequel se révèle rapidement coûteux, incapable de détecter la plupart des risques liés au trafic réseau actuel et extrêmement difficile à modifier. Au lieu de cela, les entreprises se tournent vers la microsegmentation logicielle qui simplifie bon nombre de ces processus laborieux.

Facteurs de différenciation dans la microsegmentation

Bien qu'il s'agisse d'une exigence fondamentale de toute initiative Zero Trust, la microsegmentation a souvent été considérée séparément des solutions ZTNA de base. Et, bien que la microsegmentation soit vendue à la fois par les fournisseurs de plateformes de sécurité et comme solution individuelle, il existe quelques différences fondamentales que les acheteurs doivent comprendre.

Où puis-je la déployer ? Les acheteurs potentiels devraient se méfier des solutions de microsegmentation qui ont été conçues comme des outils de réseau plutôt que dans une optique de sécurité, ou de celles qui ont été conçues pour des systèmes sur site. Les outils d'aujourd'hui doivent pouvoir être déployés dans le cloud, dans des environnements sur site, sur des terminaux (y compris ceux sur lesquels vous ne pouvez pas installer d'agents) et au sein des conteneurs dans des environnements hybrides. Cela nécessite généralement des logiciels basés sur le cloud. Si une solution de microsegmentation ne peut couvrir que 80 % de votre environnement, elle n'est pas suffisante.

Quel degré de visibilité offre-t-elle ? Bien que les solutions de microsegmentation restreignent l'accès, une restriction excessive peut nuire aux processus métier et le directeur des opérations s'en plaindrait. La microsegmentation exige une compréhension sophistiquée de votre environnement. Quels serveurs peuvent accéder à quels serveurs ? Pouvez-vous définir des politiques entre un cluster Kubernetes et un serveur Windows 2008 ? Beaucoup d'outils n'ont pas d'agents antérieurs à 2008 ou assez novateurs pour mettre en œuvre la politique sur Kubernetes. Votre logiciel de microsegmentation doit être capable de résoudre ce type de complexités si vous voulez déployer efficacement une approche Zero Trust. En outre, les acheteurs de logiciels de microsegmentation doivent tenir compte de la granularité des politiques que le produit prendra en charge. La plupart des systèmes appliquent des politiques au niveau de la couche applicative sur l'ensemble des ports et des processus. Les produits plus sophistiqués peuvent appliquer des politiques au niveau de la couche des microservices. Par exemple, les pirates peuvent utiliser certains des services du processus svchost, comme le planificateur de tâches, pour se déplacer latéralement sur le réseau. Cependant, les entreprises ne peuvent pas purement et simplement bloquer svchost, car il prend en charge bien trop de fonctions importantes. C'est là qu'une solution de microsegmentation qui applique une politique au niveau de la couche des microservices peut faire la différence.

Quelle est la difficulté de la mise en œuvre ? Il est essentiel lors de la sélection de toute solution de formulation de prendre en compte la facilité de formulation de la politique dont vous avez besoin en ce moment, et dont vous aurez besoin à l'avenir, ce qui est tout aussi important. Qu'il s'agisse d'une politique de temps de paix lorsque vous êtes en phase de planification ou d'une politique de temps de guerre lorsqu'une menace pèse sur votre environnement et que vous devez le verrouiller, vous devez vous assurer que le moteur dans lequel vous investissez prendra facilement les deux en charge. Par exemple, commencer par la liste d'autorisations dans un projet de microsegmentation peut être intimidant pour les équipes de sécurité en raison des risques de refuser par erreur une application ou un service requis. Une solution de microsegmentation sophistiquée devrait être fournie avec des modèles de listes de refus que les équipes peuvent déployer rapidement et facilement afin d'établir de petites réussites rapides pour le projet. Une fois cela accompli, les entreprises peuvent poursuivre leur parcours vers une protection complète par listes d'autorisations qui comprend des capacités précises de cartographie des dépendances et des inventaires contextuels.

> **Les acheteurs potentiels devraient se méfier des solutions de microsegmentation qui ont été conçues comme des outils de réseau plutôt que dans une optique de sécurité, ou de celles qui ont été conçues pour des systèmes sur site.**

Passerelle Web sécurisée

Dans un environnement Zero Trust, ce ne sont pas seulement les personnes qui ne sont pas dignes de confiance, mais Internet lui-même. Les employés ont besoin d'accéder à Internet et, à mesure que les applications SaaS et pour mobile, les services cloud, le télétravail et les terminaux IoT se répandent, la surface d'attaque d'une entreprise se développe également. Protéger les entreprises et les utilisateurs contre les menaces telles que les logiciels malveillants, les ransomwares, l'hameçonnage et le vol de données devient incroyablement plus difficile. Les entreprises disposent de ressources limitées pour gérer les complications et les complexités des points de contrôle de la sécurité, ainsi que les lacunes de sécurité des anciennes solutions sur site.

L'application de l'approche Zero Trust entre une personne et Internet nécessite une passerelle Web sécurisée (SWG), qui devient un élément central de toute initiative Zero Trust.

Exigences fondamentales de l'approche Zero Trust pour tout investissement dans une passerelle Web sécurisée

Même si cela semble simple, les acheteurs de technologie doivent prendre en compte certaines exigences lorsqu'ils investissent dans une passerelle Web sécurisée. De nombreuses entreprises ont déployé des passerelles Web sécurisées sur site, mais ont besoin d'étendre cette protection aux utilisateurs, quel que soit leur emplacement. Comme pour la gestion de l'identité, les fournisseurs qui disposent de solides plateformes en bordure de l'Internet ont généralement une sécurité SWG renforcée grâce à l'intelligence de la plateforme étendue. Les décideurs devraient examiner attentivement ces exigences fondamentales.

Inspection DNS. Les fournisseurs doivent être en mesure de procéder à des inspections en temps réel de tous les domaines grâce à des renseignements sophistiqués sur les menaces et de bloquer automatiquement les domaines malveillants. Les solutions doivent également être efficaces sur tous les ports et protocoles, offrant ainsi une protection contre les logiciels malveillants qui ne visent pas les protocoles et ports Web classiques. La qualité de l'inspection DNS peut varier considérablement d'un fournisseur à l'autre et les acheteurs devraient rechercher ceux qui ont de l'expérience sur le marché et qui ont fait leurs preuves auprès des clients.

Inspection des URL. De même, les requêtes HTTP et HTTPS doivent être vérifiées en temps réel et les URL malveillantes doivent être bloquées automatiquement.

Analyse de la charge utile. Toutes les charges utiles doivent être analysées en vue de détecter les logiciels malveillants à l'aide de plusieurs techniques afin de fournir une protection complète de type Zero Day contre les fichiers malveillants. Idéalement, les signaux de vos produits SWG devraient être partagés avec d'autres produits de sécurité afin de garantir la restriction de l'accès aux ressources compromises ou leur isolement.

Surveillance des menaces

Le dernier élément de la technologie Zero Trust est la surveillance des menaces. Bien que l'approche Zero Trust repose sur l'hypothèse que rien n'est implicitement fiable et que votre passerelle Web sécurisée aidera à bloquer les ransomwares et les programmes malveillants, les entreprises doivent rester vigilantes pour déceler les attaques en cours et émergentes, ainsi que les risques potentiels (comme les erreurs de configuration ou les droits d'accès trop permissifs). Lors de l'évaluation des logiciels sur le marché, les équipes de sécurité doivent examiner les trois éléments suivants pour une surveillance efficace des menaces.

Facteurs indispensables

- **Algorithmes efficaces**
  Les algorithmes sophistiqués présentant un palmarès de réussite basé sur les anomalies de l'activité des utilisateurs et du réseau, l'analyse des exécutables, l'analyse des journaux et plus encore devraient faire partie de tous les services de surveillance des menaces.

- **Détection de signaux forts**
  Même si les logiciels et l'intelligence artificielle sont des outils essentiels de la surveillance des menaces, les décideurs en matière d'approche Zero Trust doivent tout de même évaluer l'expertise interne des fournisseurs avec lesquels ils travaillent. Les services de surveillance des menaces doivent être capables de séparer les bons signaux des mauvais afin d'éviter une saturation d'alertes et de fournir des notifications immédiates de tout incident. Les entreprises doivent également prévoir des rapports réguliers avec des analyses des campagnes de grande envergure.

- **Personnel expérimenté**
  Les équipes doivent réunir des personnes ayant un large éventail d'expériences, notamment dans les domaines militaire, offensif, de la réponse aux incidents et de la science des données, et doivent être disponibles 24 h/24, 7 j/7. Dans ce domaine, les fournisseurs de services de diffusion de contenu peuvent apporter un avantage considérable. Les informations issues de la surveillance de centaines de téraoctets de données par seconde apportent une perspective unique à toute détection de signal.

Par où commencer ?

Une initiative Zero Trust n'est jamais complète. Pour ceux qui envisagent les besoins en logiciels, en matériel et en recrutement, la question principale est donc souvent : « Par quelle technologie commencer ? ».

Comme pour beaucoup de questions, la réponse va dépendre des besoins individuels de l'entreprise, de l'évaluation des risques et des forces et faiblesses relatives. Pour de nombreux observateurs du secteur, la solution consiste à commencer par la mise en œuvre du ZTNA. En effet, protéger l'entreprise contre le trafic malveillant nord-sud peut être un point de départ judicieux. Pourtant, certains estiment qu'une approche est-ouest avec la microsegmentation, plus précisément la microsegmentation définie par logiciel, est un meilleur choix.

Pourquoi commencer par la microsegmentation ?

Si vous considérez, comme la plupart des experts, qu'il n'existe pas de défense parfaite et qu'une attaque malveillante finira par se frayer un chemin, alors vous voulez être en mesure de protéger vos ressources les plus précieuses. C'est ce que permet la microsegmentation.

Cette approche est perçue comme complexe ; c'est pourquoi les entreprises hésitent à se lancer dans la microsegmentation. Premièrement, la microsegmentation n'est pas une approche de type « tout ou rien ». Tout comme l'approche Zero Trust, elle peut être entreprise par étapes. Les entreprises peuvent commencer par identifier les ressources les plus précieuses. Vous devez vous concentrer sur ce qui est primordial. Assurez-vous que même si quelqu'un s'introduit dans votre système, votre entreprise ne s'effondrera pas. L'importance d'une

ressource peut être basée sur les données qu'elle contient ou sur le niveau de protection existant. Dans de nombreux cas, il s'agira de vos anciens systèmes, car les fournisseurs de sécurité ne les prennent pas en charge.

Deuxièmement, la microsegmentation définie par logiciel supprime une grande partie de la complexité perçue. Vous n'aurez pas besoin de vous occuper du matériel et de faire appel à vos architectes de réseau et de sécurité continuellement. Vous n'aurez qu'à déployer le logiciel, ce qui abaisse considérablement les obstacles à surmonter.

Une fois qu'une initiative de microsegmentation a été lancée, les premiers avantages sont clairs et peuvent aider à faire avancer le reste du projet. Par exemple, vous disposerez alors d'une source fiable sur ce qui se passe dans votre environnement. Vous pouvez l'obtenir immédiatement sans même appliquer de politique et, vous bénéficierez d'une excellente compréhension du fonctionnement des flux dès que vous l'aurez.

Par ailleurs, une fois que vous avez commencé à mettre en place un cloisonnement des applications, vous pouvez rapidement et facilement verrouiller les applications stratégiques afin qu'elles ne communiquent que par des ports et des processus spécifiques. Une autre solution pour une réussite rapide peut être de cibler des politiques spécifiques aux menaces. Les plateformes de microsegmentation sophistiquées disposent d'une liste de refus intégrée. Cela signifie que vous pouvez rapidement créer une politique pour arrêter les connexions inutiles entre les services de bureau à distance et Internet. Les entreprises peuvent rapidement bloquer le type de vulnérabilités qui a conduit à l'attaque Colonial Pipeline, par exemple.

Quel que soit le point de départ, la clé de tout processus continu de Zero Trust est l'équilibre. Par exemple, une gestion d'identité de classe mondiale avec une segmentation médiocre ou des protections d'accès au Web médiocres ne constitue pas un bon dispositif de sécurité.

Plateforme ou outils spécialisés

Comme pour de nombreuses décisions technologiques, l'achat d'un logiciel Zero Trust se résume souvent au choix entre des spécialistes individuels et une plateforme qui combine plusieurs composants. L'impact de Zero Trust sur les équipes de sécurité, les intégrateurs, les architectes et les analystes, ainsi que leur besoin de maintenir une politique sur plusieurs consoles, différents agents et plusieurs intégrations constituent des arguments convaincants pour s'engager sur la voie de la plateforme. Ceci est particulièrement pertinent dans un marché du travail tendu avec une pénurie de professionnels qualifiés en cybersécurité. La gestion de solutions provenant de plusieurs fournisseurs peut augmenter considérablement les coûts de personnel, car les solutions qui ne communiquent pas efficacement créent des faux positifs qui pèsent sur les utilisateurs finaux et peuvent nécessiter une assistance et une formation supplémentaires.

En outre, n'avoir affaire qu'à un seul et même interlocuteur pour les négociations sur l'assistance et les contrats constitue un argument de poids en faveur de la mise en œuvre d'une approche Zero Trust avec un fournisseur de plateforme.

> **Cette approche est perçue comme complexe ; c'est pourquoi les entreprises hésitent à se lancer dans la microsegmentation.**

Résumé des constituants de l'approche Zero Trust

Sachez qui sont vos utilisateurs.
Veillez à leur vérification.

Protégez vos ressources.
Authentifiez/autorisez toutes les transactions.

Protégez vos utilisateurs.
Empêchez les programmes malveillants d'infecter les utilisateurs.

Conclusion

En définitive, la plupart des entreprises soucieuses de se protéger contre les cyberattaques sont conscientes qu'elles doivent adopter une architecture Zero Trust le plus vite possible. Nombre d'entre elles ont déjà entamé cette démarche, de manière progressive ou rapide, en réponse à l'essor du télétravail. Néanmoins, à mesure que les pirates deviennent plus sophistiqués, que l'étendue des menaces progresse et que de plus en plus de composants nécessitent un accès à distance, le besoin d'un portefeuille complet d'applications qui fonctionnent ensemble ne fait que croître.

Pour plus de détails sur les éléments spécifiques de l'approche de Zero Trust d'Akamai, contactez l'un de nos experts.