Un livre blanc SANS

Zero Trust : Ce que vous devez savoir pour sécuriser vos données et vos réseaux

Rédigé par **Dave Shackleford**

Mars 2020

Commandité par :

Gigamon

Introduction

Les professionnels de la sécurité repensent la façon dont nous abordons la sécurité des réseaux et des données. Nous avons réalisé que nous devons :

- Considérer l'ensemble de notre environnement comme non fiable ou compromis, en plus de penser en fonction des vecteurs d'attaque « extérieure ». De plus en plus, les scénarios d'attaque les plus dommageables proviennent de logiciels malveillants avancés et d'hameçonnage se traduisant par un accès malveillant d'un adversaire aux données provenant d'hôtes internes compromis et d'utilisateurs de « confiance ».
- Mieux comprendre le comportement des applications sur le réseau et au point d'extrémité et examiner les types d'applications approuvées par la communication réseau, qui devraient être réellement transmises.
- Réduire ou supprimer les relations de confiance implicites et les relations système-système en général dans toutes les parties de notre environnement. La plupart des communications que nous constatons dans les réseaux d'entreprise aujourd'hui sont entièrement inutiles ou non applicables aux systèmes ou applications nécessaires à l'entreprise.
- Mettre l'accent sur les approches axées sur les données liées à la protection qui s'alignent sur les types de classification et les environnements de traitement.

Ces objectifs sont tous utiles, mais beaucoup de nos contrôles traditionnels nécessitent des technologies ou des processus supplémentaires pour les accomplir. Ce défi constitue l'avènement des charges de travail hautement virtualisées et convergentes, ainsi que des charges de travail de cloud public qui sont dynamiques par nature. Les charges de travail cloud peuvent migrer entre les environnements de service cloud sur site et externe ou entre différents segments au sein d'un environnement de fournisseur de services cloud.

La nature des volumes de charges change également. Par exemple, il est rare qu'une charge de travail soit téléchargée dans AWS ou Azure et qu'elle reste intacte ou ne soit pas déplacée. Le mouvement continu vers des environnements logiciels de plus en plus hybrides a contraint les entreprises qui conçoivent des modèles d'architecture de sécurité dynamique à commencer à adopter un modèle global : un parmi « Zero Trust ». Comme pour toute architecture ou concept de design en évolution, il est toujours possible de définir les éléments fondamentaux d'un modèle Zero Trust complet. En plus des éléments bien connus d'un plan de données et d'un plan de contrôle dans les architectures Zero Trust proposées, l'élément manquant essentiel pour sécuriser vos données et votre réseau reste l'intégration d'un plan de surveillance complet, que nous examinons dans ce document.

Zero Trust : définition

Qu'est-ce que le Zero Trust, exactement ? Le Zero Trust désigne un modèle où les données, plutôt que les périphériques et les utilisateurs, constituent l'axe central de toutes les stratégies d'isolement et de protection, et tous les actifs dans un environnement d'exploitation informatique manipulant des données sensibles ; considérés comme non fiables par défaut ; jusqu'à ce que le trafic et le comportement réseau soient validés et approuvés. Au départ, le concept signifiait la segmentation et la sécurisation du réseau sur les sites et les modèles d'hébergement. Cependant, il existe plus d'intégration dans les serveurs et charges de travail individuels pour inspecter les composants d'application, les binaires et le comportement des systèmes communiquant dans une architecture d'application.

L'approche Zero Trust n'implique pas l'élimination du périmètre ; elle tire plutôt parti de la micro-segmentation réseau pour déplacer le périmètre le plus près possible des applications privilégiées et des zones de surface protégées. Elle comprend également l'évaluation continue des relations d'identité et des privilèges utilisés. À ce jour, il y a eu une grande variété d'approches adoptées pour atteindre ce concept global de « Zero Trust », mais le concept continue à évoluer et se développer.

Le Zero Trust est un modèle où les données constituent l'axe central de toutes les tactiques d'isolation et de protection et tous les actifs dans un environnement d'exploitation informatique qui traitent des données importantes sont considérés comme non fiables par défaut jusqu'à ce que le trafic et le comportement réseau soient validés et approuvés.

Éléments de Zero Trust

La version préliminaire du NIST publiée récemment SP800-207,[1] axée sur un modèle d'architecture Zero Trust comprend les éléments suivants dans une stratégie complète de sécurité de données/réseau qui respecte les principes de Zero Trust :

- **Identité—**Définitions des rôles et des privilèges pour l'accès utilisateur/compte
- **Informations d'identification—**Contrôles d'authentification tels que les mots de passe et les codes
- **Gestion des accès—**Contrôles et politiques qui régissent les actifs et services accessibles et le point d'accès

[1] « Zero Trust Architecture », National Institute of Standards and Technology, https ://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

- **Opérations—**Les outils et processus généraux nécessaires pour définir, mettre en œuvre, maintenir et surveiller les architectures Zero Trust
- **Critères d'évaluation—**Systèmes et charges de travail distincts faisant partie d'un environnement Zero Trust
- **Environnements d'hébergement—**Environnement où une architecture Zero Trust est mise en œuvre (par exemple, un centre de données ou une infrastructure de fournisseur de cloud)
- **Infrastructure interconnectée—**Outils et plates-formes facilitant la connectivité vers et depuis des actifs à la fois dans une architecture Zero Trust et en externe

Avec ces composants et ces principes comme base, les architectures Zero Trust se sont concentrées sur des contrôles fondamentaux qui peuvent faciliter l'accès limité aux systèmes et aux données (voir Figure 1). Le Zero Trust en tant que concept est en perpétuelle évolution, mais il existe un certain nombre de contrôles suggérés comme éléments d'architecture principaux.

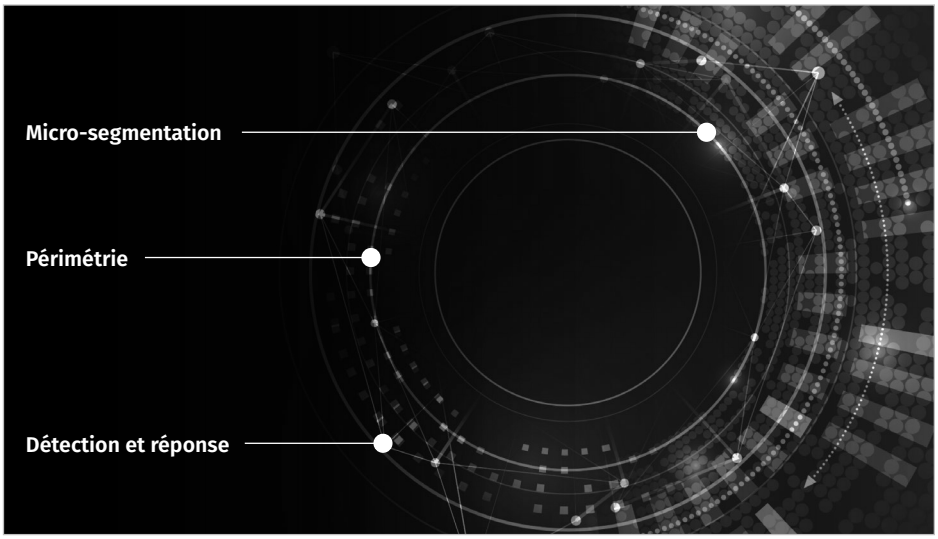

Figure 1. Éléments fondamentaux du Zero Trust

Contrôle d'accès réseau : Micro-segmentation

Le premier principal composant d'un modèle de conception Zero Trust traditionnel est la segmentation réseau étroitement alignée sur un type spécifique de système ou de charge de travail (souvent appelé micro segmentation). Le concept traditionnel de micro segmentation réseau Zero Trust s'efforce d'empêcher les attaquants d'utiliser des connexions réseau non approuvées pour attaquer les systèmes, de se déplacer latéralement à partir d'une application ou d'un système compromis ou d'effectuer toute activité de réseau illicite quel que soit l'environnement.

En réduisant le mouvement latéral, un modèle de micro segmentation Zero Trust réduit également le risque de compromis ultérieur, lorsqu'un attaquant a accédé à un actif au sein d'un centre de données ou d'un environnement cloud. Les équipes d'architecture et d'exploitation de sécurité (et souvent les équipes DevOps et d'ingénierie du cloud) se réfèrent à cela pour limiter le « rayon de projection » d'une attaque, car tout dommage est contenu dans la zone de surface la plus petite possible, tout en empêchant les attaquants d'exploiter un actif compromis pour accéder à un autre. Cette réduction du mouvement est rendue possible en comprenant correctement les flux de trafic des applications vers les ressources hébergeant des données importantes, en comprenant les comportements des applications et en appliquant les restrictions appropriées. Par exemple, si une charge de travail d'application (services Web tels que NGINX ou Apache) est légitimement autorisée à communiquer avec un serveur de base de données, un attaquant essayant de s'introduire, devrait compromettre le système, puis émuler parfaitement les services Web lors de la tentative de déplacement latéral vers le serveur de base de données (même en émettant un trafic directement depuis les binaires et services locaux installés). Bien que la micro segmentation réduise les risques, le vol et la réutilisation d'informations d'identification, restent la menace la plus importante pour toute architecture Zero Trust.

Identité « Périmétrique » : Utilisateurs et droits d'accès

La gestion de l'identité et de l'accès (IAM) constituent un autre élément fondamental d'un modèle Zero Trust, spécifiquement axé sur les utilisateurs et la gestion des accès et de l'intégration basée sur les rôles avec des applications et des services. La plupart des interactions avec les applications et les services ont un lien entre les rôles et les privilèges (utilisateurs, groupes et comptes de service), en veillant à ce que toute technologie Zero Trust puisse interagir avec les magasins d'identité et les politiques en temps réel et appliquer les décisions de politique sur les actions autorisées et interdites. IAM est une zone étendue à couvrir, englobant tout, des répertoires utilisateur aux contrôles d'accès, à l'authentification et à l'autorisation. Pour faciliter un modèle sécurisé et restreint, qui est au cœur d'une conception Zero Trust, l'IAM doit être considéré comme un domaine prioritaire et d'engagement des ressources.

Selon le projet NIST, il existe certains principes d'architecture Zero Trust qui doivent être en place pendant la conception et le déploiement :[2]

1. **Toutes les sources de données et les services informatiques sont considérés comme des ressources.** Bien qu'il soit assez explicite, ce principe constitue la base de la politique, la définition des ressources et des sources de données qui comprendront des modèles de contrôle d'accès autour d'eux.
2. **Toutes les communications sont sécurisées indépendamment de l'emplacement du réseau.** Ce principe se concentre principalement sur la protection du trafic réseau via l'utilisation de chiffrement et d'autres contrôles technologiques.
3. **L'accès aux ressources individuelles de l'entreprise est accordé par session.** Conformément au modèle Zero Trust, chaque tentative de connexion est vérifiée et évaluée par rapport à la politique définie avant que l'accès ne soit accordé.
4. **L'accès aux ressources est déterminé par une politique dynamique, incluant l'état observable de l'identité du client, de l'application, de l'actif demandeur et peut inclure d'autres attributs comportementaux.** Comme souligné précédemment dans le document, l'identité est un aspect fondamental du Zero Trust en toutes circonstances et forme la base de nombreuses politiques et décisions d'accès (ainsi que d'autres aspects comportementaux des connexions telles que l'emplacement, les étiquettes du système, les types et les types de données).
5. **L'entreprise veille à ce que tous les dispositifs en sa possession et associés soient dans l'état le plus sûr possible et surveille les actifs afin de garantir qu'ils restent dans cet état le plus sûr possible.** Ce composant du Zero Trust est axé sur la configuration et le verrouillage du système et du service, ainsi qu'un certain degré de surveillance pour garantir que l'état de configuration souhaité est maintenu au fil du temps.
6. **L'authentification et l'autorisation des ressources sont dynamiques et strictement appliquées avant que l'accès ne soit autorisé.** Conformément à l'élément précédent axé sur l'IAM, l'accès utilisateur nécessitera des contrôles d'authentification dynamiques mis en place et intégrés aux décisions des politiques.
7. **L'entreprise recueille autant d'informations que possible sur l'état actuel de l'infrastructure réseau et des communications et les utilise pour améliorer sa sécurité.** Une entreprise collecterait des données sur le trafic réseau et les demandes d'accès, qui seraient ensuite utilisées pour améliorer la création et l'application des politiques. Ces données peuvent également être utilisées pour fournir un contexte pour les demandes d'accès.

---

[2] « Zero Trust Architecture », National Institute of Standards and Technology, https ://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

Essentiellement, le Zero Trust facilite la création de « politiques d'affinité », où les systèmes disposent de relations, d'applications autorisées et un trafic, toute tentative de communication est évaluée et comparée à ces politiques afin de déterminer si les actions doivent être autorisées. Ce processus se produit en continu et une technologie de contrôle Zero Trust efficace doit également inclure un certain nombre de capacités de machine learning pour effectuer le traitement analytique des tentatives de comportement, en s'adaptant dynamiquement dans le temps, aux modifications apportées aux charges de travail et aux environnements d'application.

Nouveauté : Détection et réponse

Les éléments originaux de Zero Trust sont concentrés sur la réduction ou le retrait de la confiance implicite en matière d'accès aux données. Cependant, pour un modèle complet Zero Trust, un autre domaine majeur doit être intégré au cadre : la détection et la réponse. L'accent mis sur le contrôle d'accès n'est pas suffisant dans les environnements hautement dynamiques d'aujourd'hui : une architecture Zero Trust doit intégrer la détection automatisée et l'alerte des menaces avec une haute fidélité, fournissant des alertes et des alarmes à une équipe de surveillance, comme le Centre d'opérations de sécurité (SOC). Le tri peut alors être effectué.

Cette boucle de rétroaction, ainsi que le modèle automatisé d'activités potentielles de réponse pouvant provenir de conceptions d'architecture Zero Trust, peuvent aider les entreprises à détecter et à réagir à diverses menaces plus efficacement.

Le lien manquant : Le plan de surveillance

Il existe trois éléments fondamentaux d'un cadre/d'une architecture Zero Trust. Avant tout, pour réussir à concevoir un modèle Zero Trust, une surveillance continue du réseau doit être réalisée. Malheureusement, aucun plan de surveillance réseau dédié n'est décrit dans les cadres communs d'architecture Zero Trust. C'est un élément fondamental qui permet la découverte, le déploiement, la détection et la réponse. Le deuxième élément est le plan de données, l'endroit où sont stockées les données critiques des entreprises, accessible par les ressources (systèmes), les applications et les utilisateurs. Le troisième élément et le plus souvent abordé du cadre Zero Trust est le plan de contrôle. Le plan de contrôle facilite la réduction (ou le retrait) de la confiance implicite lors de l'accès aux données. Chaque élément est détaillé dans le Tableau 1.

Tableau 1. Éléments d'une structure Zero Trust progressive

Élément	Objet
Plan de surveillance	Un plan de surveillance fournit la base pour : • Identification et classification de vos données • Cartographie des flux de vos données sensibles • Comprendre votre réseau, vos équipements et vos applications • Surveillance continue des activités malveillantes, détection des menaces et facilitation des mesures d'atténuation Exemples clés de composants : • Collecteur de paquets réseau • Analyse du trafic réseau • Intelligence et filtrage des applications • Systèmes de détection des menaces • Collecteurs de métadonnées pour l'analyse juridico-informatique de réseau • SIEMs

Élément	Objet
Plan de données	Le plan de données correspond à l'emplacement de vos données importantes. Il inclura des ressources (systèmes), des applications et des utilisateurs qui interagissent avec les données. Ici, vous devez construire vos micro-périmètres autour de vos données importantes et mettre en œuvre des passerelles qui contestent chaque interaction avec les données pour une authentification et une autorisation continues par politique. Exemples clés de composants : • Systèmes de gestion d'accès aux identités • Facteurs d'authentification forts • Passerelles pare-feu/Contrôles d'accès réseau
Plan de contrôle	Le plan de contrôle est l'endroit où vos règles commerciales sont créées et conservées pour réduire (supprimer) la confiance implicite. Le plan de contrôle administrera les politiques en interagissant avec les passerelles qui protègent vos données importantes. Le plan de contrôle doit également fonctionner pour faciliter les politiques de réponse basées sur la détection de menaces potentielles. Exemples clés de composants : • Moteurs de politique et autorisations • Gestion des magasins d'authentification et des identifiants

Étapes des mises en œuvre de Zero Trust

Malgré d'autres cadres Zero Trust qui impliquent la nécessité d'un plan de surveillance, il s'agit souvent d'une omission malheureuse qui a conduit à la conclusion erronée que les déploiements de Zero Trust avec micro segmentation et validation d'identité forte sont suffisants. À cette fin, un plan de surveillance distinct constitue un élément essentiel d'une architecture Zero Trust exigible, pouvant faciliter la *découverte continue* et la surveillance, ainsi que la *détection et la réponse*. Une répartition des étapes clés (voir Figure 2) dans toute mise en œuvre de Zero Trust doit inclure les éléments suivants :

Figure 2. Étapes clés de la mise en œuvre Zero Trust

- **Découverte : Découvrir, cataloguer et classer les données et les actifs—**La phase de découverte est l'une des phases les plus importantes dans un modèle d'architecture Zero Trust, car les différents types d'actifs, flux de trafic et données dans tout environnement devront être continuellement identifiés et évalués par rapport aux politiques définies. Dans la plupart des centres de données traditionnels, la découverte s'est avérée difficile à l'échelle en raison d'un manque de visibilité cohérente dans tous les segments de réseau. Dans un environnement Zero Trust, la découverte doit être axée sur la surveillance du réseau qui détecte, catalogue et classifie les données dans tous les déploiements de stockage et d'applications. Le mappage des flux de données pour les scénarios de données sensibles constitue un autre outil important de découverte de fonctions.

> *Un plan de surveillance distinct est un élément essentiel d'une architecture Zero Trust mature.*

- **Déploiement : Micro-périmètres et architecture—**Dans un déploiement de Zero Trust, un type de moteur de micro segmentation doit être mis en place pour promulguer des politiques de contrôle d'accès, définies par un moteur de politique centrale. Ce moteur peut inclure des outils de micro segmentation basés sur le cloud, comme les groupes de sécurité Amazon EC2, ainsi que des moteurs de politiques internes sensibles à l'identité qui peuvent restreindre et limiter l'accès entre les actifs en cours d'exécution sur des centres de données sur site et les environnements de fournisseurs de cloud. Une fois que les identités sont remises en question, confirmées et validées (par l'intégration au répertoire et d'autres magasins d'identité), un modèle d'accès d'autorisation moins privilégié doit être appliqué par la politique.

- **Détection : Surveillance du trafic du réseau et des applications—**Un plan de surveillance est nécessaire pour détecter et suivre continuellement le trafic réseau dans l'environnement, pour mapper l'utilisation des applications, les services exposés, les modèles d'interaction utilisateur et les modèles de comportement du réseau dans les scénarios d'utilisation des applications attendus et inattendus. Dans un modèle Zero Trust, il n'est pas suffisant de supprimer la confiance implicite dans les relations utilisateur et système. Vous devez également supposer que votre approche Zero Trust n'est pas impénétrable et que vous concentrez les efforts pour détecter les adversaires dans votre environnement.
- **Réponse : Politiques et actions d'automatisation—**Dans les environnements dynamiques d'aujourd'hui, les actions de réponse automatisées deviennent plus courantes pour des cas d'utilisation et des manuels spécifiques. Les actions de réponse peuvent être « déclenchées » par le biais d'une surveillance continue et de la détection d'événements et de comportements susceptibles d'indiquer un compromis ou une tentative de compromission et peuvent inclure la quarantaine d'actifs, la suspension ou la suppression de systèmes et de charges de travail, la nouvelle segmentation des réseaux et des flux de trafic, la suspension ou la suppression des privilèges ou des comptes d'utilisateurs et des identités, etc. Pour que cela se produise à grande échelle, une analyse puissante et une intégration de l'environnement sont probablement nécessaires pour la plupart des entreprises.

Technologie et évolution de Zero Trust

Comment les entreprises devraient-elles mettre en œuvre une architecture robuste Zero Trust, incluant un moteur de politique, des outils de contrôle et de suivi du trafic, des outils de surveillance et de détection, et des capacités de détection et de réponse ? Les stratégies, technologies et outils suivants sont importants dans la mise en œuvre d'un environnement Zero Trust intégrant un plan de surveillance distinct (voir Figure 3).

- **Collecteurs de paquets—**Les collecteurs de paquets sont des outils agissant comme moteurs d'interception et de surveillance du réseau, facilitant la capture de trafic et/ou la redirection pour analyse par un nombre quelconque d'outils de surveillance et d'analyse prédictive de réseau différents. Les collecteurs en paquets réseau modernes peuvent diriger le trafic vers un seul emplacement ou plusieurs outils simultanément et doivent pouvoir gérer de nombreux flux entrants dans des environnements réseau à grande vitesse. Les collecteurs en paquets modernes peuvent également supprimer les données redondantes, si cela est souhaité et peut également inclure l'inspection et l'analyse comportementales des couches d'application et du protocole. Pour mettre en œuvre une

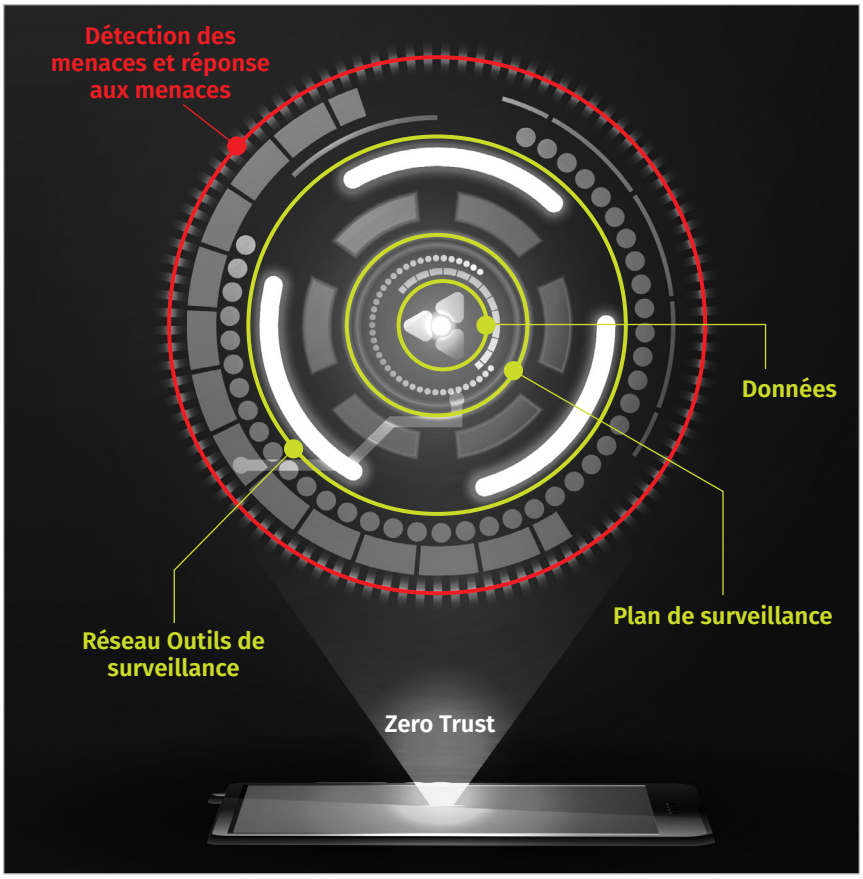

Figure 3. Outils, technologies et tactiques importants pour la mise en œuvre réussie de Zero Trust

architecture Zero Trust, utiliser des outils de collecteur de paquets doit vraiment être une exigence pour décrypter le trafic SSL/TLS à des vitesses élevées pour effectuer une analyse. Sans ce type de visibilité du réseau, la promulgation et l'application des politiques définies par un moteur de politique peuvent s'avérer extrêmement difficiles. Pour des raisons de confidentialité, les outils de courtage de trafic modernes doivent être capables de masquer ou de filtrer le trafic.

- **Outils de surveillance du réseau—**Bien que les collecteurs de paquets modernes comprennent souvent l'analyse de surveillance, la plupart des équipes de sécurité d'entreprise emploieront probablement une variété d'outils de surveillance pour l'analyse approfondie des collecteurs de paquets, les analyses scientifiques du réseau, l'enregistrement de trafic et la capture de métadonnées de trafic de collecteurs complets ou de réseau, ainsi que la détection d'intrusion réseau. La plupart des meilleures pratiques Zero Trust ont mis fortement l'accent sur les contrôles basés sur l'identité, évoqués précédemment, mais pour présenter une image complète du Zero Trust qui s'adapte à une défaillance potentielle dans ces zones de contrôle, la surveillance du réseau en temps réel doit être incluse.
- **Détection/Réponse des menaces—**Pour compléter l'ensemble de contrôles dans une architecture Zero Trust progressive, les capacités de détection et de réponse automatisées ou semi-automatisées doivent également être intégrées à l'infrastructure. Idéalement, ces contrôles exploitent tous les éléments majeurs d'une architecture Zero Trust (terminal, identité et réseau) et aident les entreprises à détecter des scénarios d'attaque spécifiques tels que :
  - **Mouvement latéral—**Le mouvement latéral entre les systèmes est un scénario courant dans les campagnes d'attaques actuelles, où la pénétration initiale dans un environnement réseau est généralement suivie par des sondes et tente de compromettre des systèmes supplémentaires à proximité. La détection et la prévention des mouvements latéraux malveillants nécessitent une compréhension de votre micro-segmentation, des identités autorisées et des flux de trafic normaux dans l'environnement, ainsi que des capacités de surveillance et de réponse en temps réel.
  - **Menaces internes—**les menaces d'initiés sont notoirement difficiles à détecter, car les initiés ont généralement une autorisation, limitant ainsi l'efficacité des contrôles spécifiques à l'identité ou aux critères d'évaluation dans une conception Zero Trust. Seule une maîtrise approfondie des comportements attendus et non déterminés dans une interaction, spécifique avec les utilisateurs, avec des données et des applications peut permettre de détecter les menaces internes.
  - **Vol d'informations d'identification—**Le vol d'informations d'identification est une stratégie d'attaque courante qui entraîne souvent des scénarios de mouvements latéraux et d'usurpation d'utilisateur/de compte. Le vol d'informations d'identification peut être difficile à détecter sans contrôle de surveillance comportementale.
  - **Fuite des données—**La fuite des données se produit généralement sur des canaux cryptés tels que TLS, ce qui rend l'interception et l'analyse du trafic critiques dans la détection et la réponse.
  - **Commande et contrôle (C2)—**Il peut être difficile de détecter et d'éviter les fuites données, de commande et de contrôle des données sans visibilité en temps réel du comportement du réseau.

À mesure que le déploiement de Zero Trust se développe et devient plus stable, les entreprises voudront déterminer l'efficacité de l'approche dans leurs environnements. Les indicateurs de Zero Trust à l'échelle du secteur sont peu nombreux, et à l'heure actuelle, étant donné que la plupart des entreprises sont toujours en phase de déploiement et n'ont pas encore développé de stratégies à long terme pour ce type d'architecture.

Conclusion : Une image complète de Zero Trust

La référence d'architecture d'ébauche NIST SP800-207 reconnaît l'importance de la visibilité du réseau à un design d'architecture Zero Trust, mais ne fait pas mention explicite d'une exigence de plan de surveillance. Même sans déchiffrement SSL/TLS complet, les métadonnées réseau peuvent être collectées et analysées afin de détecter les tendances et les attaques anormales, mais une architecture de Zero Trust complète doit inclure un plan de contrôle avec définition de la politique, des contrôles d'application et des outils, un plan de données où les systèmes et données résident (ainsi que les magasins d'identité possibles) et un plan de surveillance intégrant la collection et la surveillance du réseau :

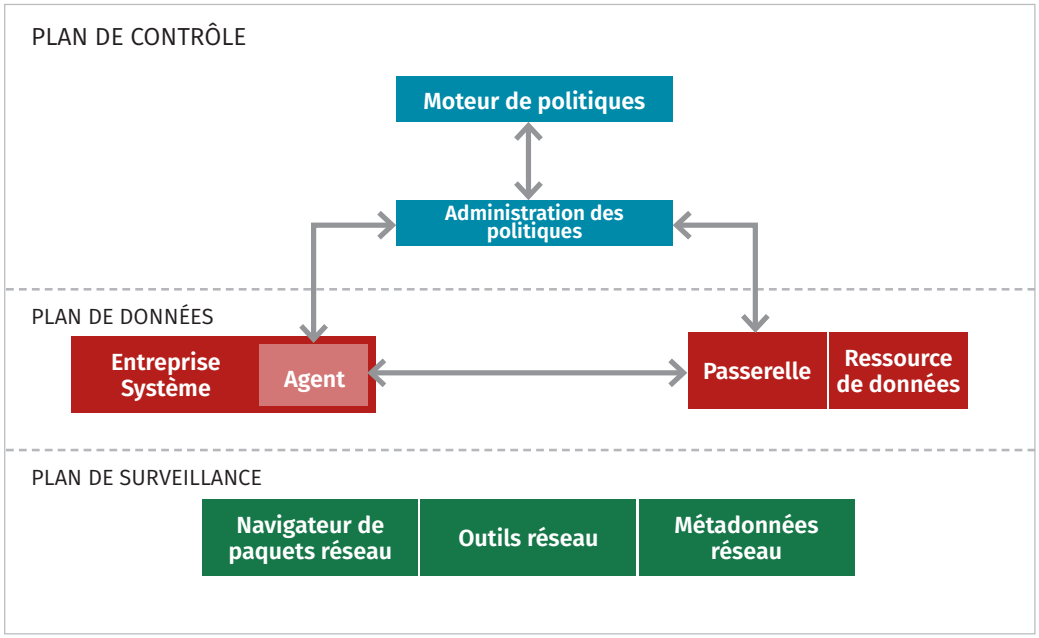

Figure 4. Architecture Zero Trust avec les plans de contrôle, de données et de surveillance

De nombreuses entreprises ont déjà un ou plusieurs éléments d'un modèle Zero Trust déployés, mais ces contrôles ne fonctionnent souvent pas en tandem. Globalement, il existe un certain nombre de bonnes pratiques générales que les organisations doivent garder à l'esprit pour mettre en œuvre des outils et des contrôles Zero Trust. Ces pratiques comprennent les éléments suivants :

- Commencer par la détection passive des applications, généralement implémentée avec la surveillance du trafic réseau. Attendre plusieurs semaines d'identification pour trouver les relations en place et coordonner avec les parties prenantes qui connaissent les tendances de trafic « normales » et les communications inter-systèmes. Les politiques de renforcement doivent être adoptées ultérieurement, après avoir confirmé les relations appropriées qui doivent être mises en place, ainsi que le comportement de l'application.
- Concevez une architecture Zero Trust en fonction de la façon dont les données se déplacent sur le réseau et la façon dont les utilisateurs et applications accèdent aux informations sensibles. Cette conception permettra de déterminer comment le réseau doit être segmenté et où la protection et les contrôles d'accès doivent être positionnés à l'aide de mécanismes virtuels et/ou de dispositifs physiques entre les frontières de différents segments de réseau.

Exemples de mesures que nous avons vues et utilisées

- Découverte : Nombre d'applications identifiées et mappées (souvent suivies par plage réseau, unité commerciale ou région géographique)
- Découverte : Nombre d'identités suivies et étiquetées, segments réseau, inventaire des actifs, inventaire des applications et flux de données sensibles
- Réduction de pourcentage des alertes de contrôle d'accès au réseau (après la mise en œuvre des politiques d'application)
- Pourcentage de réduction des systèmes compromis et des charges de travail applicatives après une mise en œuvre Zero Trust
- Pourcentage de réduction des incidents et/ou temps moyen de détection ou temps moyen de réponse

Une architecture Zero Trust complète doit inclure un plan de contrôle avec des contrôles et des outils de définition de la politique et de mise en application, un plan de données où les systèmes et données résident et un plan de surveillance intégrant le courtage et la surveillance du réseau. Un exemple de ce type d'architecture est illustré à la figure 4.

- Les outils Zero Trust plus avancés intègrent les « identités » (qui peuvent faire partie d'une architecture d'application, alignés à une unité commerciale ou un groupe ou un représentant d'un type de système spécifique). Prenez le temps de catégoriser les systèmes et les applications, ce qui permettra de créer des lignes de base et des comportements de trafic applicatifs.
- Assurez-vous que vous disposez de solutions de détection et de réponse qui traitent le trafic du réseau, identifiez les signaux malveillants, autorisez l'investigation de l'activité et facilitez les actions de réponse automatisées.
- Recherchez des produits qui fonctionnent dans des environnements cloud internes et publics lorsque cela est possible, ce qui nécessitera presque toujours une solution basée sur un agent.

Une architecture Zero Trust doit inclure des contrôles d'authentification et d'autorisation, des contrôles d'accès et d'inspection du réseau, ainsi que des contrôles de surveillance/d'application tant pour le réseau que pour les terminaux. Aucune technologie unique n'offrira actuellement une conception et une mise en œuvre complètes « Zero Trust », une combinaison d'outils et de services est nécessaire pour fournir le degré complet de couverture nécessaire. Pour la plupart, une approche hybride de Zero Trust et de l'infrastructure existante devra coexister pendant une certaine période et l'accent doit être mis sur les composants communs et les catégories de contrôle qui pourraient permettre à tous deux de gérer les identités et l'accès via l'intégration des services d'annuaire, la sécurité des points de terminaison et l'application des politiques, ainsi que la surveillance du réseau et l'inspection du trafic. Les projets Zero Trust sont également des projets à long terme. Dans de nombreux cas, la mise en œuvre d'un ensemble cohésif de contrôles fonctionnant ensemble peut prendre plusieurs années (peut-être aussi longtemps que 4-5 ans dans certains environnements). À l'heure où les structures Zero Trust se développent et évoluent, les normes et l'interopérabilité de la plate-forme vont probablement permettre d'obtenir des approches plus rationalisées et efficaces.

À propos de l'auteur

Dave Shackleford, analyste, instructeur senior, auteur de cours, directeur technique GIAC et membre du conseil d'administration pour l'Institut technologique SANS, est le fondateur et le consultant principal de Voodoo Security. Il a consulté des centaines d'entreprises dans les domaines de la sécurité, de la conformité réglementaire et de l'architecture et de l'ingénierie du réseau. Vmware vExpert, Dave a une vaste expérience dans la conception et la configuration d'infrastructures virtualisées sécurisées. Auparavant, il travaillait comme directeur de la sécurité pour Configuresoft et CTO pour le Centre de sécurité Internet. Dave participe actuellement au chapitre Atlanta de l'Alliance de sécurité du cloud.

Sponsor

SANS souhaite remercier le sponsor de ce livre blanc :

Gigamon®