NOTE DE SYNTHÈSE

ACTIVER LE CADRE ZERO TRUST MODERNE AVEC INFOBLOX

INTRODUCTION

Dans l'environnement numérique moderne, l'adoption de modèles de sécurité Zero Trust devient de plus en plus essentielle. Selon une enquête Gartner, 63 % des entreprises dans le monde ont entièrement ou partiellement mis en œuvre des stratégies Zero Trust, motivées par la nécessité d'atténuer les cybermenaces sophistiquées et/ou de se conformer aux meilleures pratiques du secteur. Cependant, une stratégie Zero Trust classique présente des failles. De nombreuses entreprises font implicitement confiance aux domaines auxquels les utilisateurs accèdent sur Internet. Cela expose l'organisation à des domaines suspects, malveillants ou similaires appartenant à des acteurs malveillants, ce qui pourrait entraîner des failles de sécurité. On ne peut pas mettre en œuvre le modèle Zero Trust sans comprendre le flux de trafic au sein d'un réseau. Infoblox propose une approche moderne du cadre Zero Trust, soulignant le rôle essentiel du DNS dans la sécurisation des environnements hybrides et multi-cloud.

> *"Pour la plupart des organisations, une stratégie Zero Trust ne couvre généralement que la moitié, voire moins, de leur environnement, et ne permet d'atténuer qu'un quart, ou moins, du risque global de l'entreprise."*
>
> **Gartner**

POURQUOI ZERO TRUST ?

Le Zero Trust est un cadre de sécurité qui part du principe que les violations sont inévitables et se concentre sur la minimisation de leur impact. Les principaux facteurs d'adoption du Zero Trust incluent :

- L'évolution de la sophistication des acteurs malveillants
  - » Ransomware et domaines de spear phishing similaires
  - » Systèmes distribués de trafic (TDS)
- Hyperconnectivité et initiatives numériques
  - » Environnements hybrides et multi-cloud
  - » IoT/OT et travail à distance

Avec l'hyperconnectivité et les transformations numériques omniprésentes, telles que l'adoption de réseaux multicloud et hybrides, les violations de données sont de plus en plus courantes. Après une violation initiale, les menaces peuvent se déplacer latéralement très rapidement. Une approche Zero Trust peut limiter la portée, l'impact et le coût d'une violation, permettant ainsi aux organisations de traiter rapidement tout incident et de minimiser les perturbations opérationnelles.

Les principes du Zero Trust comprennent l'hypothèse d'une violation, le fait de ne jamais faire confiance et de toujours vérifier, l'utilisation d'un accès avec le moins de privilèges possible, la surveillance constante et la segmentation pour limiter le mouvement latéral des menaces.

CONSIDÉRATIONS DNS DANS LE ZERO TRUST

Le DNS joue un rôle central dans les stratégies Zero Trust. Les modèles Zero Trust traditionnels négligent souvent le DNS, lui faisant implicitement confiance, ce qui peut constituer une faille importante, permettant aux utilisateurs et aux appareils d'accéder à des domaines malveillants liés à des menaces telles que les ransomwares, le phishing, les domaines similaires et le DNS zero-day, exposant ainsi le réseau à des violations. Infoblox souligne qu'une stratégie Zero Trust ne doit pas implicitement faire confiance au DNS mais doit garantir :

- **Connexions DNS chiffrées et authentifiées**
- **Surveillance de l'exfiltration de données et des menaces DNS de type zero-day**
- **La protection DNS (PDNS) pour empêcher l'accès à des domaines malveillants**

L'approche d'Infoblox inclut un DNS chiffré pour la confidentialité, ainsi que des données actualisées sur les actifs pour les décisions d'accès et un PDNS pour bloquer les domaines à haut risque, les communications de commande et de contrôle (C2) et l'exfiltration de données.

DNS CHIFFRÉ POUR L'ENTREPRISE

La norme NIST SP 800-207 stipule que « toutes les communications doivent être effectuées de la manière la plus sécurisée possible, protéger la confidentialité et l'intégrité, et fournir une authentification de la source ». Cela inclut la garantie de la confidentialité (anti-snooping) pour la résolution DNS récursive. Le chiffrement inclut les DNS sur TLS (DoT), qui utilisent le port 853, et DNS sur HTTP (DoH), qui utilisent le port 443 entrecoupé de trafic Web.

DNS DE PROTECTION POUR L'ENTREPRISE

La solution Protective DNS (PDNS) d'Infoblox pour les entreprises offre une sécurité proactive grâce à :

- **Prévenir les infections initiales en refusant de résoudre les domaines à haut risque**
- **Interrompant les communications C2 en cours**
- **Bloquant l'exfiltration de données**

Infoblox PDNS intègre la Threat Intelligence, des moteurs d'IA/ML et l'application de politiques DNS pour offrir une protection complète contre les cybermenaces. Les composants incluent :

- **Serveur DNS récursif :** trouve les adresses IP des domaines et les renvoie au client
- **DNS Threat Intel :** identifie les domaines à haut risque et malveillants appartenant à des acteurs maveillants
- **Moteur d'apprentissage IA/ML :** identifie les menaces avancées en inspectant le trafic DNS d'une organisation en temps réel et en effectuant une analyse comportementale
- **Moteur de politique DNS/RPZ :** autorise ou refuse la résolution DNS en fonction de la politique définie.

APPLICATION AU NIVEAU DES APPAREILS

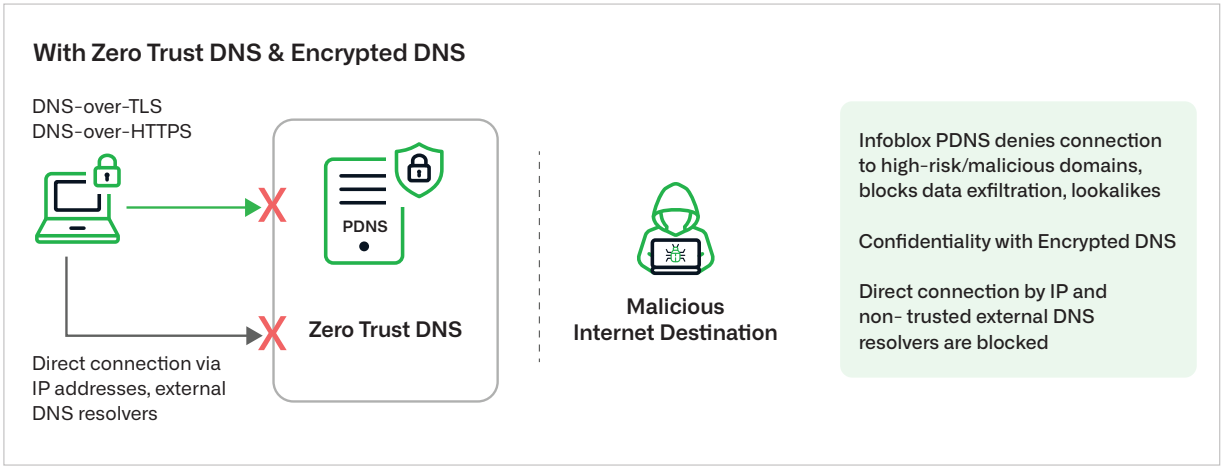
Le modèle DNS Zero Trust d'Infoblox inclut une application au niveau des appareils pour empêcher le contournement du DNS et restreindre le trafic IP sortant. Cela garantit que les appareils se connectent uniquement aux serveurs PDNS approuvés, renforçant ainsi la sécurité globale du réseau.

LA DÉCOUVERTE DES ACTIFS ET LES DONNÉES SONT UTILISÉES PAR LES SYSTÈMES ZERO TRUST POUR PRENDRE DES DÉCISIONS EN MATIÈRE D'ACCÈS.

La visibilité sur tous les ressources réseau est cruciale pour le cadre Zero Trust. Universal Asset Insights d'Infoblox offre une vue unifiée des actifs dans les environnements hybrides et multi-cloud, en automatisant la découverte et l'analyse. Cela permet de maintenir un inventaire des actifs à jour, de détecter les appareils non autorisés et de corréler l'activité des appareils avec les identités. Les métadonnées DNS et IPAM sont d'importantes sources de télémétrie, fournissant des informations détaillées sur les clients et le comportement du réseau comme données d'entrée pour les systèmes Zero Trust. Elles peuvent être utilisés pour prendre de meilleures décisions en matière d'accès et d'attribution de politiques, mais l'accès peut être accordé ou refusé en fonction de la géolocalisation de l'utilisateur/de l'appareil, du port du commutateur réseau, etc. Par exemple, Infoblox peut vous indiquer qu'un appareil est une imprimante et qu'il ne peut accéder qu'à certains domaines. Un autre exemple est qu'Infoblox peut identifier les appareils IoT/OT (par exemple, les caméras) et déterminer que, au cours de la semaine dernière, ils n'ont effectué que certains appels DNS. L'administrateur peut alors décider de créer une politique Zero Trust pour ces caméras.

AUTOMATISATION ET ORCHESTRATION

Zero Trust s'appuie fortement sur l'automatisation et l'orchestration pour soutenir les fonctions de réponse à la sécurité. Infoblox s'intègre à divers outils et plateformes de sécurité pour automatiser l'application des politiques, la détection des menaces et la réponse aux incidents, et fournir des informations contextuelles.



CONCLUSION

Les solutions Zero Trust d'Infoblox offrent un cadre fiable pour sécuriser les réseaux modernes. En intégrant la sécurité DNS, la visibilité des actifs et l'automatisation, Infoblox aide les organisations à mettre en œuvre des stratégies efficaces de Zero Trust, réduisant ainsi le risque de cybermenaces et renforçant la sécurité globale.

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20241205v1