NOTAS DE LA SOLUCIÓN

# HABILITAR SEGURIDAD ZERO TRUST MODERNA CON INFOBLOX

## INTRODUCCIÓN

En el panorama digital actual, la adopción de modelos de seguridad Zero Trust es cada vez más esencial. Según una encuesta de Gartner, el 63% de las organizaciones de todo el mundo han implementado estrategias Zero Trust total o parcialmente, impulsadas por la necesidad de mitigar sofisticadas ciberamenazas o de incorporar las mejores prácticas del sector. Sin embargo, en una estrategia típica de confianza cero hay lagunas. Muchas organizaciones confían implícitamente en los dominios a los que acceden los usuarios en internet, lo que deja a la organización expuesta a dominios sospechosos, maliciosos y similares pertenecientes a agentes de amenazas y puede dar lugar a violaciones de la seguridad. No se puede aplicar el modelo Zero Trust sin comprender el flujo de tráfico en una red. Infoblox ofrece un enfoque moderno del modelo Zero Trust, que se centra en el papel fundamental del DNS en la seguridad de los entornos híbridos y multinube.

> *"Para la mayoría de las organizaciones, una estrategia Zero Trust suele abordar la mitad o menos del entorno de una organización y mitigar una cuarta parte o menos del riesgo global de la empresa."*
>
> **Gartner**

## ¿POR QUÉ ZERO TRUST?

Zero Trust es un marco de seguridad que asume que las brechas son inevitables y se centra en minimizar el impacto de dichas brechas. Los impulsores clave para la adopción de Zero Trust incluyen:

- La sofisticación de los actores de amenazas
  - » Ransomware y dominios de spear phishing similares
  - » Sistemas de distribución de tráfico (TDS)
- Hiperconectividad e iniciativas digitales
  - » Entornos híbridos y multinube
  - » IoT/OT y trabajo remoto

Con la hiperconectividad y las transformaciones digitales omnipresentes, como la adopción de redes multinube e híbridas, las violaciones de seguridad son cada vez más comunes. Tras una brecha inicial, las amenazas pueden moverse lateralmente con gran rapidez. Un enfoque Zero Trust puede limitar el alcance, el impacto y el coste de una violación, lo que permite a las organizaciones abordar rápidamente cualquier incidente y minimizar la interrupción de las operaciones.

Los principios Zero Trust incluyen asumir la violación, no confiar nunca y verificar siempre, utilizar el acceso con privilegios mínimos, la supervisión constante y la segmentación para limitar el desplazamiento lateral de las amenazas.

## CONSIDERACIONES SOBRE EL DNS EN ZERO TRUST

El DNS desempeña un papel fundamental en las estrategias Zero Trust. Los modelos tradicionales de confianza cero suelen despreocuparse del DNS y confiar implícitamente en él, lo que puede suponer una brecha importante, ya que permite a usuarios y dispositivos acceder a dominios maliciosos vinculados a amenazas como el ransomware, el phishing, los dominios similares y el DNS de día cero, de modo que la red queda expuesta a violaciones de seguridad. Infoblox hace hincapié en que una estrategia Zero Trust no debe confiar implícitamente en el DNS, sino que debe garantizar:

- **Conexiones DNS cifradas y autenticadas**
- **Supervisión de la exfiltración de datos y las amenazas del DNS de día cero**
- **DNS protector (PDNS) para impedir el acceso a dominios maliciosos**

El enfoque de Infoblox incluye DNS cifrado para garantizar la privacidad, además de datos actualizados sobre los activos para tomar decisiones de acceso y PDNS, con el fin de bloquear dominios de alto riesgo, comunicaciones de mando y control (C2) y exfiltración de datos.

## DNS CIFRADO PARA LA EMPRESA

La norma NIST SP 800-207 establece: «Todas las comunicaciones deben efectuarse de la forma más segura posible, proteger la confidencialidad y la integridad, y proporcionar la autenticación de la fuente». Debería incluir la habilitación de la privacidad (anti-snooping) para la resolución del DNS recursivo. El cifrado incluye DNS sobre TLS (DoT), que utiliza el conocido puerto 853, y DNS sobre HTTP (DoH), que utiliza el puerto 443 intercalado con el tráfico web.

## DNS PROTECTOR PARA LA EMPRESA

La solución de DNS protector (PDNS) de Infoblox para empresas ofrece seguridad proactiva mediante:

- **Prevención de infecciones iniciales, al rechazar la resolución de dominios de alto riesgo**
- **Interrupción de las comunicaciones C2 en curso**
- **Bloqueo de la exfiltración de datos**

PDNS de Infoblox integra inteligencia sobre amenazas, motores de IA/ML y la aplicación de políticas del DNS para ofrecer una protección completa contra las ciberamenazas. Los componentes incluyen:

- **Servidor del DNS recursivo:** halla las direcciones IP correspondientes a los dominios y las transmite al cliente
- **Inteligencia sobre amenazas del DNS:** identifica dominios maliciosos y de alto riesgo pertenecientes a actores de amenazas
- **Motor de aprendizaje de IA/ML:** identifica amenazas avanzadas por medio de inspeccionar el tráfico del DNS de una organización en tiempo real y llevar a cabo análisis de comportamiento
- **Motor de políticas del DNS o RPZ:** permite o deniega la resolución del DNS en función de las políticas establecidas

## APLICACIÓN A NIVEL DE DISPOSITIVO

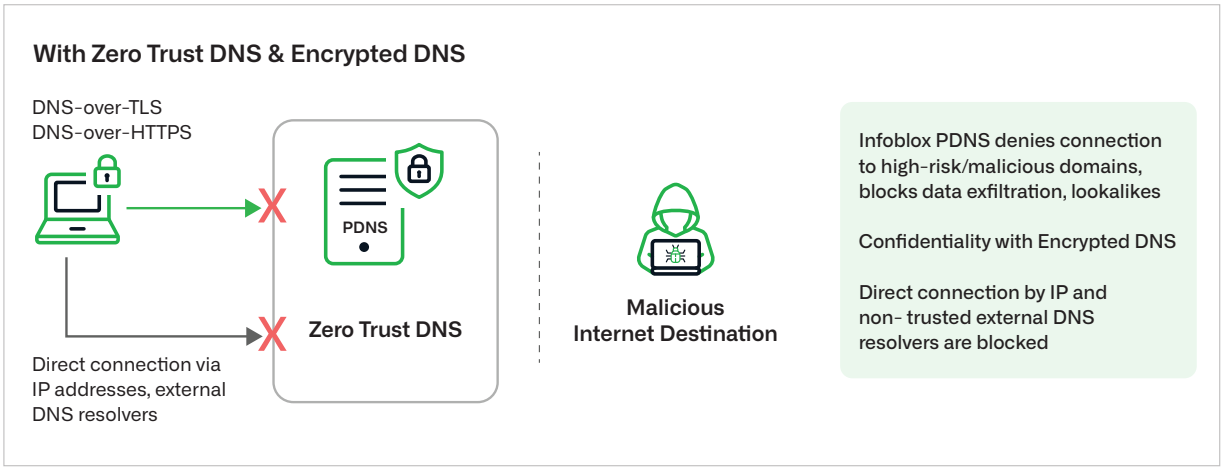
El modelo Zero Trust de Infoblox para el DNS incluye la aplicación a nivel de dispositivo para impedir que se eluda el DNS y restringir el tráfico IP saliente. Así se garantiza que los dispositivos solo se conecten a servidores PDNS aprobados, lo que mejora la seguridad general de la red.

## DETECCIÓN DE ACTIVOS Y DATOS COMO ENTRADA A LOS SISTEMAS ZERO TRUST PARA TOMAR DECISIONES SOBRE EL ACCESO

La visibilidad de todos los activos de la red es fundamental para el modelo Zero Trust. Universal Asset Insights de Infoblox proporciona una vista unificada de los activos en entornos híbridos y multinube, automatizando la detección y el análisis. De este modo, es posible mantener un inventario de activos actualizado, detectar dispositivos no autorizados y relacionar la actividad de los dispositivos con las identidades. Los metadatos de DNS e IPAM son fuentes importantes de telemetría, pues proporcionan información detallada sobre los clientes y el comportamiento de la red como entrada a los sistemas Zero Trust. Se pueden utilizar para tomar mejores decisiones sobre el acceso y asignar políticas, pero el acceso puede concederse o denegarse en función de la geolocalización del usuario/dispositivo, el puerto del conmutador de red, etc. Por ejemplo, Infoblox puede indicarle que un dispositivo es una impresora y que solo puede acceder a determinados dominios. Otro ejemplo es que Infoblox puede identificar dispositivos IoT/TO (por ejemplo, cámaras) y determinar que, en la última semana, solo han realizado determinadas llamadas al DNS. A continuación, el administrador puede decidir crear una política Zero Trust para esas cámaras.

## AUTOMATIZACIÓN Y ORQUESTACIÓN

Zero Trust se basa en gran medida en la automatización y la coordinación para respaldar las funciones de respuesta de seguridad. Infoblox se integra con diversas herramientas y plataformas de seguridad para automatizar la aplicación de políticas, la detección de amenazas y la respuesta a incidentes, y aportar información contextual.




## CONCLUSIÓN

Las soluciones Zero Trust de Infoblox ofrecen un marco sólido para proteger redes modernas. Al integrar la seguridad basada en el DNS, la visibilidad de los activos y la automatización, Infoblox ayuda a las organizaciones a implementar estrategias Zero Trust eficaces, lo que reduce el riesgo de ciberamenazas y mejora la postura de seguridad general.

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

**Sede corporativa**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es



Versión: 20241205v1