SOLUTION NOTE

ENABLING MODERN ZERO TRUST WITH INFOBLOX

INTRODUCTION

In today's digital landscape, the adoption of Zero Trust security models is becoming increasingly essential. According to a Gartner survey, 63% of organizations worldwide have fully or partially implemented Zero Trust strategies, driven by the need to mitigate sophisticated cyber threats and/or comply with industry best practices. However, there are gaps in a typical zero trust strategy. Many organizations implicitly trust domains that users are reaching out to on the Internet. This leaves the organization open to suspicious, malicious and lookalike domains owned by threat actors, which could lead to breaches. You can't do zero trust without understanding the flow of traffic in a network. Infoblox offers a modern approach to Zero Trust, emphasizing the critical role of DNS in securing hybrid and multi-cloud environments.

> *"For most organizations a zero-trust strategy typically addresses half or less of an organization's environment and mitigates one-quarter or less of overall enterprise risk."*
>
> **Gartner**

WHY ZERO TRUST?

Zero Trust is a security framework that assumes breaches are inevitable and focuses on minimizing the impact of such breaches. Key drivers for Zero Trust adoption include:

- Threat Actors Getting Sophisticated
  - » Ransomware and lookalike spear phishing domains
  - » Traffic distributed systems (TDS)
- Hyperconnectivity and digital initiatives
  - » Hybrid, multi-cloud environments
  - » IoT/OT and remote work

With hyperconnectivity and ubiquitous digital transformations, such as adopting multi-cloud and hybrid networks, breaches are becoming increasingly common. After an initial breach, threats can move laterally very quickly. A Zero Trust approach can limit a breach's scope, impact and cost, enabling organizations to quickly address any incidents and minimize disruption of operations.

Zero Trust principles include assuming breach, never trusting and always verifying, using least-privilege access, constant monitoring, and segmentation to limit lateral movement of threats.

DNS CONSIDERATIONS IN ZERO TRUST

DNS plays a pivotal role in Zero Trust strategies. Traditional Zero Trust models often overlook DNS, implicitly trusting it, which can be a significant gap, allowing users and devices to go to malicious domains linked to threats such as ransomware, phishing, lookalike domains and zero-day DNS, exposing the network to breaches. Infoblox emphasizes that a Zero Trust strategy should not implicitly trust DNS but should ensure:

- **Encrypted and authenticated DNS connections**
- **Monitoring for data exfiltration and zero-day DNS threats**
- **Protective DNS (PDNS) to prevent access to malicious domains**

Infoblox's approach includes encrypted DNS for privacy, plus up-to-date asset data for access decisions and PDNS to block high-risk domains, command and control (C2) communications and data exfiltration.

ENCRYPTED DNS FOR THE ENTERPRISE

NIST SP 800-207 states: "All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication." This should include enabling privacy (anti-snooping) for recursive DNS resolution. Encryption includes DNS over TLS (DoT), which uses well-known designated Port 853, and DNS over HTTP (DoH), which uses port 443 interspersed with web traffic.

PROTECTIVE DNS FOR THE ENTERPRISE

Infoblox's Protective DNS (PDNS) solution for enterprises offers proactive security by:

- **Preventing initial infections by refusing to resolve high-risk domains**
- **Stopping ongoing C2 communications**
- **Blocking data exfiltration**

Infoblox PDNS integrates threat intelligence, AI/ML engines, and DNS policy enforcement to provide comprehensive protection against cyber threats. Components include:

- **Recursive DNS server:** Finds IP addresses for domains and returns them to the client
- **DNS Threat Intel:** Identifies high-risk and malicious domains owned by threat actors
- **AI/ML learning engine:** Identifies advanced threats by inspecting an organization's DNS traffic in real-time and performing behavioral analysis
- **DNS policy Engine/RPZ:** Allows or denies DNS resolution based on policy set

DEVICE LEVEL ENFORCEMENT

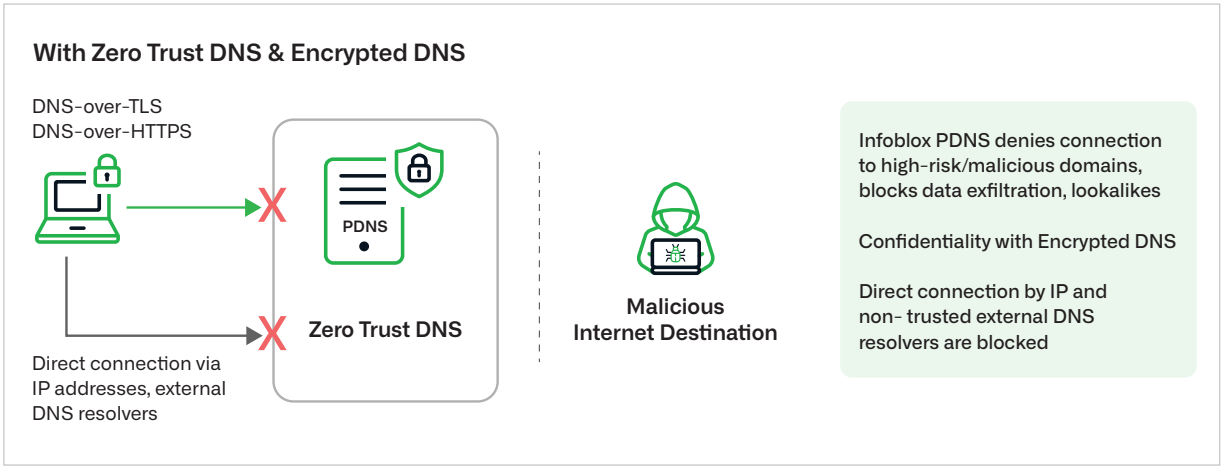
Infoblox's Zero Trust DNS model includes device-level enforcement to prevent DNS bypass and restrict outbound IP traffic. This ensures that devices only connect to approved PDNS servers, enhancing overall network security.

ASSET DISCOVERY AND DATA AS INPUT TO ZERO TRUST SYSTEMS TO MAKE DECISIONS ABOUT ACCESS

Visibility into all network assets is crucial for Zero Trust. Infoblox's Universal Asset Insights provides a unified view of assets across hybrid, multi-cloud environments, automating discovery and analysis. This helps maintain an up-to-date asset inventory, detect unauthorized devices and correlate device activity with identities. DNS and IPAM metadata are important sourcees of telemetry, providing detailed client information and network behavior as input to Zero Trust systems. They can be used to make better decisions about access and assign policy, but access may or may not be granted based on the geolocation of user/device, network switch port etc. For example, Infoblox can tell you that a device is a printer and that it can only go to certain domains. Another example is that Infoblox can identify IoT/OT devices (e.g., cameras) and can determine that, in the last week, they only made certain DNS calls. The admin can then decide to create a Zero Trust policy for those cameras.

AUTOMATION AND ORCHESTRATION

Zero Trust relies heavily on automation and orchestration to support security response functions. Infoblox integrates with various security tools and platforms to automate policy enforcement, threat detection and incident response and provide contextual information.



CONCLUSION

Infoblox's Zero Trust solutions offer a robust framework for securing modern networks. By integrating DNS-based security, asset visibility, and automation, Infoblox helps organizations implement effective Zero Trust strategies, reducing the risk of cyber threats and enhancing overall security posture.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20241205v1