SOLUTION NOTE

ZERO TRUST BEGINS WITH PREEMPTIVE DNS SECURITY

INTRODUCTION

Zero Trust has become the defining security strategy for modern enterprises. As organizations embrace hybrid work, cloud-first architectures and increasingly distributed environments, the need to continuously verify trust and enforce least-privilege access has never been more urgent. Zero Trust assumes that no user, device or system, internal or external, can be inherently trusted. Every access request must be authenticated, authorized and continuously validated.

But to be effective, Zero Trust must be built on a foundation of visibility, control and preemptive defense. DNS provides exactly that. As the first protocol touched in nearly every digital interaction, DNS offers a unique opportunity to enforce policy, detect threats and inform access decisions before a connection is ever established. Without DNS, Zero Trust strategies are incomplete. Zero Trust is not really Zero Trust if DNS is implicitly trusted.

Infoblox preemptive security enables organizations to operationalize Zero Trust by transforming DNS into the first point of visibility, enforcement and early threat prevention. At the core of this capability is Infoblox Threat Defense™, a Protective DNS security solution that turns DNS into a strategic asset for Zero Trust.

> *63% percent of organizations worldwide have fully or partially implemented a zero-trust strategy [and] 56% of organizations are primarily pursuing a zero-trust strategy because it's cited as an industry best practice."*
>
> **Gartner Group**[1]

WHY DNS IS CRITICAL TO ZERO TRUST

DNS is universally used, protocol-agnostic and difficult for attackers to bypass. It provides a consistent enforcement point across users, devices and workloads, whether on-premises, in the cloud or remote. Every time a user accesses a SaaS application, a cloud workload accesses resources on the internet or malware attempts to reach a command-and-control (C2) server, DNS is involved.

When integrated into a Zero Trust architecture, DNS becomes more than a resolution service. It becomes a strategic control point that supports continuous verification, limits lateral movement, and provides rich telemetry for dynamic access control.

When enriched with IP address management (IPAM) and DHCP metadata, DNS logs can reveal the identity, behavior and risk posture of every device on the network. This context is essential for enforcing Zero Trust policies that adapt to changing conditions and user behavior.

The main areas of relevance of DNS for Zero Trust include:

Security teams face increasing pressure to manage complex environments, rising threat volumes and siloed tools. Common challenges include:

- **Protective DNS** for the enterprise
- **Encrypted DNS** for privacy and anti-snooping
- **Up-to-date asset data** across hybrid, multi-cloud environments using **DHCP and IPAM** to make decisions about access

PREEMPTIVE SECURITY WITH PROTECTIVE DNS—STOPPING THREATS BEFORE THEY START

Gartner envisions preemptive security as a proactive strategy that stops threats before they can cause harm, moving beyond traditional reactive methods. It emphasizes the use of predictive threat intelligence, cybersecurity deception and automated moving target defense to anticipate and block attacks early. Infoblox Threat Defense aligns directly with this vision by using DNS as a first-line control point to enforce policy and block malicious activity at the earliest possible stage. This approach supports Zero Trust principles by enforcing policy before connections are established and continuously validating every DNS request.

Powered by real-time predictive threat intelligence and algorithmic/machine learning protections, Infoblox Threat Defense identifies and blocks domains associated with phishing, malware, ransomware, C2 infrastructure and data exfiltration.

ENCRYPTED DNS

Encrypted DNS enables privacy (anti-snooping) for recursive DNS resolution. The two popular forms of encryption include:

- **DNS over TLS (DoT):** Has well-known designated Port 853
- **DNS over HTTPs (DoH):** Port 443 interspersed with web traffic

Both protocols encrypt DNS queries and responses between the user's device and the DNS resolver to prevent:

- **Eavesdropping:** Prevents ISPs or attackers from seeing which websites the user is trying to visit.
- **Manipulation:** Protects against tampering with DNS data (e.g., DNS spoofing or man-in-the-middle attacks).

UP-TO-DATE ASSET DATA TO MAKE DECISIONS ABOUT POLICY

Always up-to-date asset data across entire hybrid, multi-cloud is needed as input to Zero Trust systems to make accurate decisions about access. DNS and IPAM metadata are an important source of telemetry providing detailed client information and network behavior as input to Zero Trust systems which can be used to make better decisions about access; access may or may not be granted based on geolocation of user/device, network switch port, etc.

> *"All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication."*
>
> **The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207.**[2]

UNIFIED DISCOVERED DNS AND DHCP DATA WITH IPAM METADATA PROVIDE:

- Detailed client information and insights, including for IoT/OT devices
- Granular device history and network activity

The Threat Defense solution combines predictive threat intelligence with algorithmic/machine learning protections to detect emerging threats, monitoring over 200,000 threat actor clusters and blocking threats an average of 68.4 days earlier than traditional tools—with a remarkably low false positive rate of just 0.0002%.

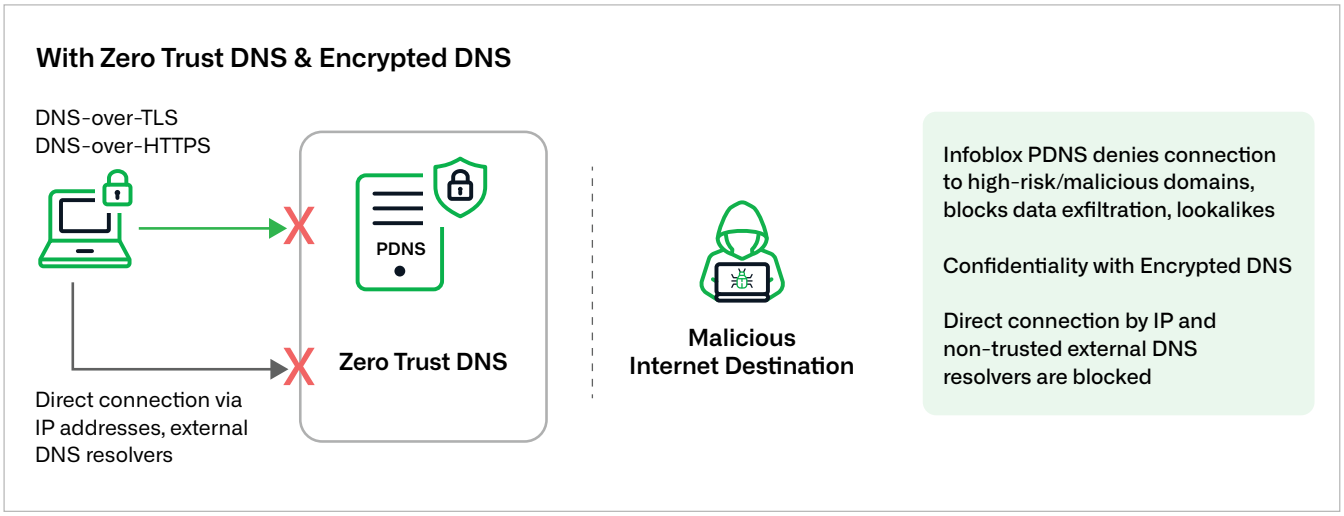

Figure 1. Zero Trust DNS blocks direct IP connections and non-trusted external DNS resolvers

Real-World Use Cases and Measurable Outcomes Availability

Organizations across industries are using Infoblox Threat Defense to strengthen their Zero Trust posture:

- A **transportation company** used a combination of DNS-powered remote access and threat detection along with endpoint solutions, like endpoint detection and response (EDR) and mobile device management (MDM), to form a Zero Trust user and device strategy to protect everyone, everywhere, all at once.
- A **healthcare provider** leveraged Threat Defense to detect and block DNS tunneling activity that bypasses next-generation firewall (NGFW) and secure access service edge (SASE) controls.
- Following ransomware incidents, a **retail chain** deployed Threat Defense to bolster protection against ransomware, gain full visibility into DNS traffic and significantly reduce incident response time.
- In addition to these examples, **financial institutions** have used Threat Defense to comply with regulatory requirements, such as those of the Federal Financial Institutions Examination Council (FFIEC) and Payment Card Industry Data Security Standard (PCI DSS), by demonstrating control over DNS traffic.
- **Educational institutions** have deployed the solution to protect students and faculty from phishing attacks while maintaining open internet access.
- **Government agencies** have leveraged DNS telemetry to detect insider threats and unauthorized data transfers.

These diverse use cases underscore the flexibility and effectiveness of DNS-based security in enabling Zero Trust across industries and operational models.

SEAMLESS INTEGRATION AND OPERATIONAL EFFICIENCY

Infoblox Threat Defense can be deployed as a standalone solution or integrated with the Infoblox DDI platform. When integrated, it consolidates DNS security with core network services, streamlining visibility, policy enforcement and incident response under a unified administrative domain.

Security and networking teams can collaborate more effectively using shared data and workflows. Infoblox's Security Ecosystem integrates with leading SIEM, SOAR, EDR and identity platforms, enabling automated response workflows and contextual threat enrichment. For example, a suspicious DNS query can trigger an automated workflow that isolates the device, updates firewall rules and alerts the SOC. All of this can happen within seconds.

Infoblox SOC Insights also provides intuitive dashboards and reporting tools that help teams prioritize threats, tune policies and demonstrate the impact of their Zero Trust strategy to stakeholders. These capabilities reduce operational overhead and accelerate time to value.

CONCLUSION: DNS AS A PILLAR OF ZERO TRUST

As organizations continue to adopt Zero Trust, the role of DNS will only grow in importance. DNS provides a scalable, cost-effective way to enforce security policies and gain visibility into network activity. Infoblox Threat Defense empowers security teams to act on DNS insights in real time, reducing dwell time and improving overall security posture.

By embedding DNS into the fabric of Zero Trust, organizations can achieve a more resilient and adaptive security architecture that is capable of withstanding modern threats. Infoblox enables this transformation by delivering preemptive protection, contextual visibility and seamless integration across the security stack.

Zero Trust is not a checkbox. It is a continuous journey that requires visibility, control and automation across every layer of the network. DNS plays a critical role in that journey by providing early insight into intent, enforcing policy before connections are made and stopping threats before they impact the business.

Infoblox Threat Defense empowers organizations to operationalize Zero Trust by transforming DNS into a proactive security layer. With unmatched visibility, automation and threat prevention, Infoblox helps organizations reduce risk, accelerate response and support secure digital transformation.

1. *Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy*, Gartner, April 22, 2024.
2. *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207: Zero Trust Architecture*, Rose, Scott, Borchert, Oliver, Mitchell, Stu, Connelly, Sean, NIST, August 2020.

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

+1.408.986.4000
www.infoblox.com

Version: 20250805v1