SOLUTION NOTE

INFOBLOX FOR PROTECTIVE DNS

OVERVIEW

Cybercrime is rising fast, with global costs expected to hit $23 trillion by 2027.[1] Breaches like ransomware continue to succeed—highlighting critical gaps in current approaches. In response, government agencies such as the UK's National Cyber Security Centre (NCSC) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) are strongly advocating for the adoption of Protective DNS (PDNS). In some cases, they are mandating it.

DNS uses the DNS protocol as a control point to analyze queries and block threats such as malware command-and-control, ransomware, phishing and domain generation algorithms (DGAs). Since over 90 percent of malware relies on DNS at some stage, PDNS is uniquely positioned to be the earliest point of prevention for all cyberattacks.

PDNS is also a foundational element of a preemptive security strategy. This is one that identifies and blocks threats before they reach the network or trigger downstream alerts. This approach reduces reliance and burden on reactive tools and helps security teams stay ahead of increasingly AI-driven threats.

KEY BENEFITS OF PROTECTIVE DNS

Blocks Malicious Domains at the Earliest Point of Connection. PDNS prevents users and devices from connecting to high-risk and malicious sites owned by threat actors which are already hosting, or may host in the future, malware, ransomware and other threats. It also blocks command-and-control callbacks to contain active infections. Advanced PDNS solutions can also identify and block threat actor supply chain such as traffic distribution systems and malicious URL shortening services.

Scales with Threat Intelligence. PDNS can process and act on millions of threat indicators in real time, delivering broad and efficient protection.

Delivers Visibility and Context. PDNS logs, combined with data from DHCP and IP address management, provide rich context that helps security teams link threats to specific users, devices or workloads, and respond faster.

Protects Everywhere. PDNS protects every inch of your infrastructure, including on-premises, remote workers, branch offices, IoT and cloud workloads, even when traditional security stacks are not present.

PDNS VALIDATION IS STRONG

Governments Are Taking Action

The NCSC offers PDNS services to public sector organizations in the United Kingdom and recommends commercial PDNS for private industry. CISA has evaluated commercial PDNS providers and outlined the benefits of adoption. Other countries, including Saudi Arabia, are also prioritizing DNS-based defenses as part of national cybersecurity strategies.

NIST SP 800-81 Provides Strong Validation for PDNS

"DNS servers can provide significant insight into the connections and dataflows of endpoints and can often prevent security incidents earlier than other systems."—NIST

The NSA Reinforces the Value of Secure DNS
"Our analysis highlighted that using Secure DNS would reduce the ability for 92 percent of malware attacks both from command-and-control perspective, deploying malware on a given network."—Anne Neuberger, Head of the Cybersecurity Directorate, National Security Agency (NSA).

THREAT DEFENSE BENEFITS ARE TANGIBLE

Infoblox Threat Defense™ is a purpose-built **Protective DNS** solution that stops threats earlier in the attack lifecycle. It uses predictive threat intelligence, AI, machine learning (ML) and DNS telemetry to identify malicious infrastructure before it is weaponized.

Preemptive detection with Infoblox Threat Defense helps reduce risk before threats cause damage:

- DNS can detect and block over **270 types** of threat indicators giving security teams broad, early-stage coverage across the kill chain.
- DNS-layer security can reduce time to detect and remediate threats by up to **92 percent**, helping teams act faster and more decisively.
- DNS-layer security can protect against **82 percent** of threats before impact.
- DNS can detect threats on average **68.4 days** before other tools.
- DNS-layer security has a false positive rate of just **0.0002 percent.**

Infoblox is the only vendor offering Protective DNS and DDI (DNS, DHCP and IP address management) on an integrated platform that is under a single team responsible and accountable for all DNS-related operational issues. This simplifies troubleshooting, improves visibility and ensures consistent protection across all environments, including cloud, on-premises and hybrid networks.

THREAT DEFENSE AS A PDNS SOLUTION

Infoblox Threat Defense provides a unique **preemptive approach** to threat prevention. It uses a combination of **predictive threat intelligence** that blocks threat actor infrastructure before they are weaponized, and algorithmic/ML-based analysis of DNS queries in customer networks—to provide protection before impact. Organizations can now proactively stop connections to malicious and high-risk domains before they begin, keeping harmful and unwanted traffic off the network.

Through pervasive automation and ecosystem integrations, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts, and lowers the total cost for cybersecurity.

	Key Benefits
1	**Protection Before Impact.** Threat Defense detects and blocks most cyberattacks at the earliest point in customer networks, even before endpoint security, Cloud Access Security Broker (CASB), next-generation firewall (NGFW) and network detection and response (NDR), because it sees the threat first as soon as a device requests a connection to an internet location that could be high-risk/malicious. This preemptive approach reduces security incident-related endpoint downtime by 47 percent and sends fewer alerts to the SIEM due to early blocking. Threat Defense detects/blocks sophisticated and AI-enabled attacks, data exfiltration, DGAs, phishing, ransomware and botnets using an unparalleled mix of unique predictive threat intelligence with patented algorithmic/ML models. The "protection before impact" feature in the product enables CISOs and security teams to confidently report to the board with clear, quantifiable metrics on threats neutralized before impact.

2	**Automating Threat Response.** Threat Defense integrates with most security ecosystem tools, including ServiceNow, SIEM, SOAR, network access control (NAC) and vulnerability management, via RESTful APIs for automated and faster response to detected events, while making those tools more effective. Organizations get better ROI out of their existing investments.
3	**Reduction in SecOps Effort through Better Context.** Threat Defense can reduce security operations effort by 34 percent by providing critical telemetry on threats. Threat Defense can pull contextual information from Infoblox on-premises or cloud DDI for assessing threat exposure and severity, and tracking a threat back to the originating source on their network. The contextual details for each threat are presented with deep insight, which saves manual time and effort for SecOps as they investigate a threat. In addition, DNS-based threat intelligence can be added to the ecosystem to enrich the data they already have.
4	**Protecting Cloud Workloads, OT/IoT.** Cloud workloads often lack security systems that traditionally protect on-premises infrastructure and are left exposed. OT systems are often unpatched and run legacy applications. IoT devices are non-standard devices where endpoint security cannot always be deployed. EDR/XDR solutions have limited or no visibility on OT/IoT. Threat Defense protects OT/IoT systems using PDNS to offer protection against malware and data theft.
5	**Asset Insights and Application Discovery.** Threat Defense provides deep asset context for instant visibility into impacted assets, what was protected as part of the preemptive strategy and enabling faster investigation. Threat Defense also provides application discovery and allows admins to proactively manage applications as approved/unapproved, helping to control shadow IT and shadow AI.

[1] *Key Cyber Security Statistics for 2025*, SentinelOne, July 14, 2025.

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: 20250801v3