DATASHEET

Infoblox Threat Defense™

Protective DNS powered by predictive threat intelligence protects everything, everywhere—before impact

DNS IS THE EARLIEST POINT OF PREVENTION FOR ALL CYBERATTACKS

Whether triggered by a phishing email, smishing text or an exploited vulnerability, nearly every attack generates a DNS query to a malicious domain. As a result, DNS provides a powerful, centralized point of visibility and control across the enterprise—spanning users, devices, IoT/OT and workloads—whether on-premises, in the cloud or at the edge.

DNS is involved in nearly every digital interaction, making it an ideal control point for early threat prevention. By inspecting DNS traffic in real time, Infoblox can detect and block malicious activity before it reaches downstream tools or triggers alerts. When correlated with asset and identity context, DNS data gives NetOps and SecOps teams deeper visibility across their environments—enhancing both operational efficiency and security posture.

Threat actors increasingly use AI to launch more prolific, sophisticated and stealthy campaigns. They generate uniquely crafted, single-use malware that renders traditional “detect and respond” tools—those waiting for a “patient zero” infection—ineffective. Every attack becomes a “patient zero” scenario, where no signature or known behavior exists. These tools often act too late in the kill chain to prevent damage.

A preemptive approach is needed—one that stops threats before they enter the environment or move laterally. DNS gives security teams a proactive opportunity to detect and block threats earlier, before they reach users, workloads or endpoints.

PREEMPTIVE SECURITY WITH DNS

Infoblox Threat Defense™ provides a unique **preemptive approach** to threat detection—one that doesn’t rely on “patient zero.” 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. Through rapid identification of assets involved in security incidents, ecosystem integrations and intuitive workspaces, it enables faster detection, faster response and greater ROI from your existing security investments.

Powered by DNS-based predictive threat intelligence, Threat Defense enables security teams to identify attacker infrastructure before it is weaponized and preempt the kill chain. It also shares threat and asset context across your broader security ecosystem—improving the accuracy and efficiency of your entire stack.

FACTS & FIGURES

- Monitors **204K** real-time threat actor clusters and growing
- Reduces false positives rate to **0.0002%**
- Blocks **82%** of threats before the first query
- Delivers protection **68.4 days** before an attack on average
- Blocks **5X more** high-risk/ medium-risk domains vs. tools that just look for known malicious behavior
- Saves an average of **500 SOC analyst hours** per month*
- Helps realize **$400K** in productivity savings per year*
- Reduces tens of thousands of alerts down to a handful*

The SANS 2025 SOC Survey revealed that seven of the top 10 barriers preventing full SOC utilization involve alerts, tool integration and skill shortages.

*Based on real-world customer data.

BLOCK THREATS BEFORE IMPACT

Threat Defense applies predictive DNS threat intelligence with algorithmic/machine learning analytics on real-time DNS traffic to block threat activity before they impact your network, often detecting threats that other tools fail to detect. By stopping threats at the DNS layer, Infoblox also helps reduce alert volume and workload on downstream security tools, with customers reporting up to a 50 percent reduction in alerts on next-generation firewall (NGFW) and endpoint detection and response (EDR) systems.

> “*Secure DNS, could reduce the ability of 92% of malware attacks to successfully deploy malware on a given network”*
>
> **Anne Neuberger,**
> **Director of the Cybersecurity Directorate,**
> **National Security Agency (NSA)**

Key Capability	Description	Infoblox Threat Defense	NGFW	SASE	EDR
Enterprise-Wide Secure Resolver and DNS Query Logging	Uses DNS query data to find and convict domains	●	◑	◑	◑
Full DNS Behavior Monitoring	Monitors all DNS record types for malicious activity	●	●	◔	○
Lookalike/ Doppleganger Domain Detection and Takedown	Mitigate lookalike/doppleganger attack surface	●	○	◑	○
Zero Day DNS Protection	Identifies new or emerging domains for your organization that could pose a threat	●	◑	◑	○
Behavior-Based DNS Tunneling Detection	Detects DNS tunnels being used for data exfiltration/infiltration, C2 communications, etc.	●	◑	◑	○
Proactive Suspicious/ High-Risk Domain protection	Identifies and blocks suspicious domains premptively that are likely to be used in future malicious campaigns	●	◑	◑	◑
Automatic, Native Context Enrichment	Correlates network context without the need for clients or sinkholing (user, device, source IP, location, MAC address, VLAN)	●	◑	◑	◑
Proactive Threat Distribution Systems (TDS) Detection and Disruption	Identifies threat actor TDS infrastructure, not just individual domains, to counter threat actors rotating across numerous domains to evade detection	●	◔	○	○

Figure 1. Capabilities unique to Threat Defense that other tools cannot fully address

KEY FEATURES OF THREAT DEFENSE

- **“Protection Before Impact” Monitor**—Enabling CISOs and security teams to execute their preemptive security strategy and confidently report to the board with clear, quantifiable metrics on threats neutralized before impact.
- **Asset Discovery and Inventory Integration**—Rapid identification of assets involved in security incidents for faster incident assessment and response.
- **Security Workspace**—Simplified and intuitive UI that lets security teams understand what is happening within their environment and suggest ways to decrease security risks.
- **Detection Mode**—For easy deployment and proof of concept, without changing existing IT or network infrastructure.

POWER PREEMPTIVE SECURITY WITH PREDICTIVE INTELLIGENCE

Infoblox is the leading creator of original DNS threat intelligence. The company takes a preemptive, not just defensive, approach by using its insights to track threat actor infrastructure as it is being built and disrupt cybercrime at the source, often before an attack is even launched.

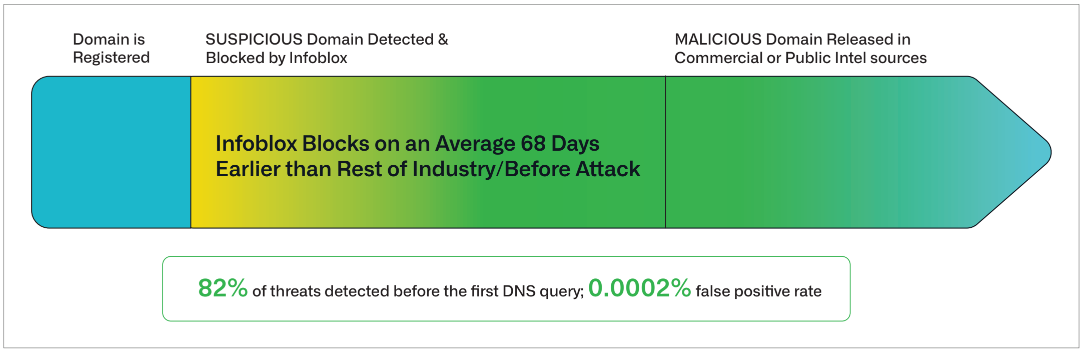
Domain is Registered
SUSPICIOUS Domain Detected & Blocked by Infoblox
MALICIOUS Domain Released in Commercial or Public Intel sources
Infoblox Blocks on an Average 68 Days Earlier than Rest of Industry/Before Attack
82% of threats detected before the first DNS query; 0.0002% false positive rate

Figure 2. Infoblox threat intelligence can protect against threats against threats before the rest of the security industry

How Infoblox Creates Original DNS Threat Intelligence

DNS Experts: Infoblox discovers threat actors hiding in DNS by knowing where to look. Starting with high-risk or suspicious domains, the team connects the dots to identify attacker infrastructure and track it as it evolves and surfaces new threats, before they are recognized elsewhere.

Threat Expertise: Infoblox understands how malicious actors operate and how threats such as malware, ransomware, phishing and DNS-based exploits manifest. That expertise powers predictive systems that detect lookalike domains, DNS command-and-control activity, registered domain generation algorithms (RDGAs) and other suspicious behaviors.

Data Science: Infoblox applies machine learning and advanced data science to massive volumes of DNS query data. This enables near–real-time protection against data exfiltration, domain generation algorithms (DGAs) and a wide range of evasive threats.

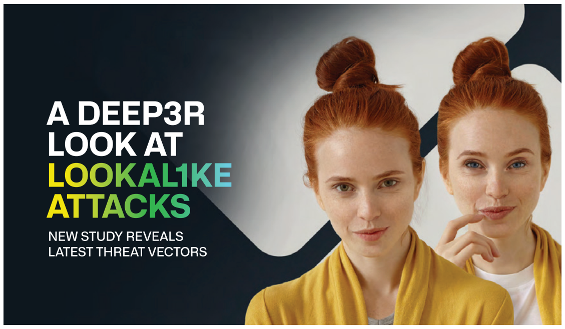
A DEEP3R LOOK AT LOOKAL1KE ATTACKS
NEW STUDY REVEALS LATEST THREAT VECTORS

Figure 3. Infoblox Threat Intel shared surprising research data on the escalating risk of lookalike domains

SECURITY AND REPORTING PACKAGES

Infoblox uses a token-based model that adapts to how and where you defend your infrastructure. Security Tokens enable access to Threat Defense, SOC Insights, Dossier and Lookalike Domain Monitoring. Reporting Tokens are used to export DNS logs to SIEMs, SOARs or data lakes for deeper visibility and correlation.

This flexible system eliminates rigid product tiers and aligns licensing with your actual deployment, whether in the cloud, on-premises or across hybrid environments. Tokens scale as your organization grows and they can be reallocated across capabilities as your priorities change. With centralized visibility through the Licensing Portal and a clear usage-aligned model, it is easier to forecast, budget and demonstrate ROI across your security operations.

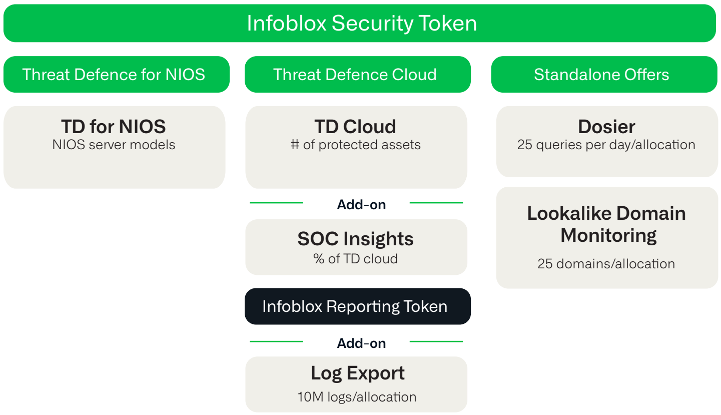

Figure 4. Offer structure: Security and reporting

WORK SMARTER WITH SOC INSIGHTS

From alert fatigue and analyst burnout to lengthy investigation and response efforts, Infoblox Threat Defense offers significant relief to the SOC, with an additional SOC Insights package.

- Help analysts know what matters most with AI-driven analytics that distill hundreds of thousands of alerts down to a handful of insights.
- Automate log, threat intelligence and other data collection and correlation so analysts can jumpstart investigation and response.
- Accelerate incident response with asset discovery and inventory integration, helping analysts identify impacted devices faster.

EXPORT HIGH-VALUE DNS LOGS AT SCALE

Infoblox makes it easy to send high-fidelity DNS query and event data to your SIEM, SOAR or data lake for centralized visibility and faster threat correlation.

- Filter and forward only high-value DNS events to reduce SIEM ingestion costs and alert noise.
- Stream enriched DNS logs in real time using the Infoblox Cloud Data Connector.
- Improve detection and response across your ecosystem by giving every tool the context it needs.
- Share data seamlessly with other tools through certified, bidirectional integrations—improving end-to-end detection, triage and response.

INVESTIGATE FASTER WITH DOSSIER

Dossier equips analysts with a powerful, unified research tool to validate threats, pivot on indicators of compromise (IOCs) and speed up investigations—without the need to switch between different platforms.

- Consolidate internal, Infoblox and third-party threat intelligence into one intuitive interface.
- Quickly investigate IOCs and uncover related threats with built-in enrichment and link analysis.
- Reduce investigation time by up to 67 percent by eliminating manual data gathering and context switching.

SAFEGUARD YOUR BRAND FROM TARGETED DECEPTION

Infoblox offers two integrated capabilities—Lookalike Domain Monitoring and Domain Mitigation Services—that help protect your brand, customers and employees from deception-based cyberattacks. Together, they give you visibility into emerging threats and the ability to take fast, effective action against malicious domains before they impact your business.

Lookalike Domain Monitoring

Stay ahead of impersonation attacks that exploit your brand or trusted third parties.

- Detect domains registered to impersonate your company, supply chain or customer-facing properties.
- Identify domains used in phishing and fraud campaigns that target your employees or customers.
- Monitor high-priority domains for changes in risk posture and receive real-time alerts.

Domain Mitigation Services

Quickly validate and take down malicious domains that are active in the wild.

- Confirm and document malicious activity through human-led incident validation and summary reporting.
- Coordinate with global ISPs, hosting providers and regulatory agencies for swift takedown—often within 24 hours.
- Monitor mitigated threats for 30 days post-removal to detect and remove reactivation attempts at no extra cost.
- Address a range of threat types, including phishing, malware hosting, command-and-control infrastructure and stolen data.

To learn more about the ways that Infoblox Threat Defense secures your data and infrastructure, please visit https://www.infoblox.com/products/threat-defense/.

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: 20250121v1