DATASHEET

Infoblox Threat Defense Advanced

Stop threats other solutions miss and often before threat actors launch their attack

DNS IS A CRITICAL ASSET FOR SECOPS AND NETOPS

In today's intricate network landscapes, DNS has transcended its traditional role as a directory service to become a pivotal asset for NetOps and SecOps professionals. Serving as the backbone of modern communication, especially with the surge of hybrid multi-cloud, IoT and ICS/OT, DNS provides an unparalleled central point of visibility and control of all connected assets across on-premises, remote, mobile, and multi-cloud environments.

As the first step of any communication, detecting and blocking threat activity at the DNS-layer reduces malicious traffic that reaches downstream security tools and alerts generated from those tools. And by correlating DNS data with device and asset information, NetOps and SecOps teams gain greater insights into network activities, enhancing both their operational efficiency and security posture.

And today, adoption of AI by cybercriminals has significantly enhanced their ability to generate new malware variants at a very rapid pace and counter traditional defenses such as Next-Generation Firewalls (NGFW), Email Security Gateways (ESG), and Endpoint Detection and Response (EDR) systems. AI-driven attacks, composed of AI developed tools, can adapt in real-time, learning from the defenses they encounter and evolving to bypass them. As a result, leveraging DNS as a visibility and control point becomes even more crucial to an organization's security stack.

Infoblox Threat Defense Advanced is a comprehensive DNS Detection and Response (DNSDR) solution designed to detect and stop threats that other solutions miss. It enhances overall SecOps efficiency through intelligent automation and AI-driven analytics that help eliminate wasted effort, reduce alert fatigue, lower false positives so that analysts can quickly identify and focus on what matters most. This means higher detection and lower mean time to respond (MTTR) for maximum return on investment.

Infoblox's threat intelligence, derived from DNS data, gives Infoblox Threat Defense industry leading proactive security capabilities. It helps identify and disrupt attacker supply chains before they can cause harm. And Infoblox Threat Defense Advanced can share this threat intelligence across other security tools, enhancing the security ecosystem's efficiency and effectiveness.

INFOBLOX THREAT DEFENSE FACTS & FIGURES

- Ultra-low false positive rate of 0.0002% out of over 20 million indicators
- Blocked 75.4% of threats before the first query
- Delivered protection 63 days before an attack on average
- Saved an average of 500 SOC analyst hours per month*
- Realized $400k in productivity savings per year*
- Reduced 10s of thousands of alerts down to a handful*
- The SANS 2023 SOC Survey revealed that 8 of the top 10 barriers preventing full SOC utilization involve alerts, tool integration, and skill shortages

*Based on real world customer data

FIND THREATS OTHER TOOLS MISS

Infoblox Threat Defense Advanced applies unique DNS Threat Intel with machine language and AI-driven analytics on real-time DNS traffic to uncover threat activity that other tools fail to detect. Most security tools lack the visibility and expertise to detect Indicators of Compromise (IoCs) within DNS when threat actors attempt to evade detection in more commonly secured channels like HTTP(S).

> *"Using secure DNS would reduce the ability for 92% of malware attacks both from command and control perspective, deploying 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 & 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.

This comprehensive approach to DNS gives Threat Defense customers unique threat protection that compliments existing tools, enabling defenders to detect and respond to threat activity across their entire protocol attack surface.

LEVERAGE PROACTIVE THREAT INTELLIGENCE

Infoblox is the leading creator of original DNS threat intelligence. We're proactive, not just defensive, using our insights to track threat actor infrastructure and disrupt cybercrime where threat actors begin, often before they have launched their planned attack.

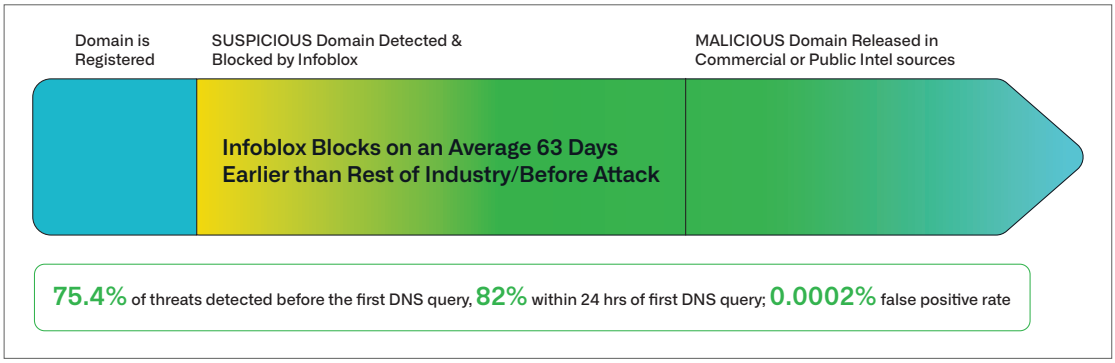

Figure 2. Infoblox Threat Intel can protect against threats before the rest of the security industry.

How Infoblox creates original DNS threat intelligence:

DNS Experts - We discover threat actors hiding in DNS because we know where to look. Starting with high-risk/suspicious domains, we connect the dots and identify actor infrastructure, then begin tracking it as it evolves. Identifying new domains as they emerge so customers are continually protected.

Threat Expertise - We know how malicious actors operate and how malware, ransomware, phishing, and other threats manifest in DNS. We've used this knowledge to develop specialized systems to detect lookalike domains, DNS C2 malware, registered domain generation algorithms (RDGAs) and suspicious behavior.

Data Science - We use machine learning and data science to analyze very large volumes of DNS queries every day to provide near-real time protection against data exfiltration, domain generation algorithms (DGAs), and a wide range of other threats.

PROTECT YOUR BRAND

Infoblox offers two essential services to help organizations protect their brand reputation: Lookalike Domain Monitoring and Domain Mitigation Services. Together, these services provide a robust defense against a wide variety of advanced, evasive cyber threats, helping organizations protect their brand reputation and maintain business continuity.

Lookalike Domain Monitoring proactively stops socially engineered threats using lookalike domains in advanced targeted attacks. These fake domains can be used to attack your customers by imitating your brand or pose a risk to employees by impersonating your supply chain or other trusted partners, both of which can lead to devastating results.

Figure 3: Infoblox Threat Intelligence shared surprising research data on the escalating risk of Lookalike domains.

Lookalike domains are used in many different attack vectors, including SMS messages, phone calls, social media, emails, and QR codes. Infoblox's Lookalike Domain Monitoring capability helps organizations stay ahead of these threats by identifying lookalike domains before they can cause harm.

Included with Infoblox Threat Defense Advanced, or sold separately, this service is crucial in protecting against phishing, ransomware, Business Email Compromise (BEC), and other enterprise threats, ensuring that organizations can maintain their brand integrity and customer trust.

Domain Mitigation Services are designed to swiftly take down domains that pose a risk to organizations or their customers. Infoblox leverages a proprietary blend of investigative skills, automated techniques, and industry relationships to resolve issues such lookalike domains used in phishing, site spoofing and other cyber threats with industry-leading SLAs measured in hours. This service is a comprehensive solution for organizations victimized by malicious cybercriminals, helping them respond quickly to mitigate financial and brand reputation risks.

The service includes validation to confirm incidents and collect necessary evidence to takedown efforts, mitigation through coordination with ISPs and regulators, and 30-days of ongoing monitoring to reduce the risk of subsequent attacks. Infoblox's deep ties with the ISP community and global regulatory agencies ensure swift and effective resolution of cyber incidents.

RAISE SECOPS EFFICIENCY

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

- Reduce wasted time and frustration with ultra-low false positive rates (0.0002%).
- Help analysts to know what matters most with AI-driven analytics that distill hundreds of thousands of alerts down to a handful of 'insights'.
- Automate log, threat intel, and other data collection and correlation so analysts can jumpstart investigation and response.
- Reduce alerts and workloads on downstream devices by blocking threat activity at DNS. Customers report as much as a 50% reduction of alerts on NGFW and EDR tools alone.
- Speed threat research with a dedicated portal where analysts can pivot around WhoIs, IoCs, Threat Actor profiles, and other data.
- Enabling bi-directional data exchange across your security ecosystem with through custom or pre-built, certified Integrations.

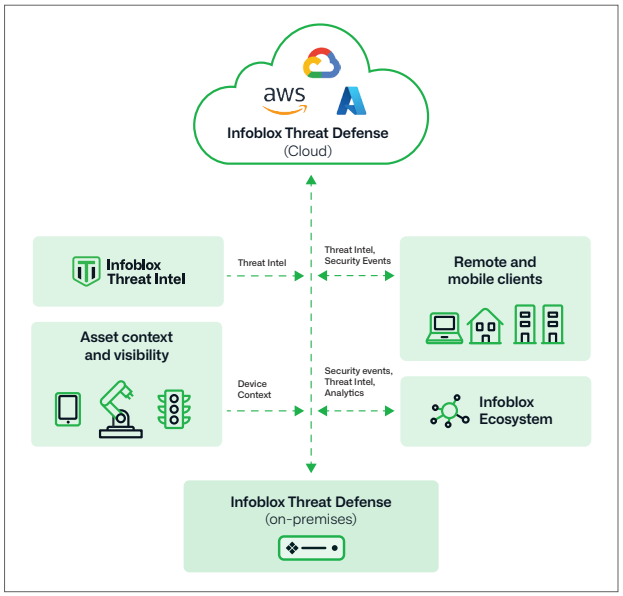

Figure 4: The Infoblox hybrid architecture enables protection everywhere and deployment anywhere to counter today's AI enabled threat landscape.

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

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