DATASHEET

Infoblox Threat Defense™ Business On-Premises

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

PROTECT BEFORE IMPACT WITH FOUNDATIONAL DNS SECURITY

Protecting infrastructure, data and users is more challenging than ever. Traditional, reactive security models can no longer keep up. Today's threats are faster, smarter and designed to bypass conventional defenses.

- AI-enabled attacks like lookalike domains, smishing, multi-factor authentication (MFA) bypass and targeted phishing evolve too quickly for legacy tools to catch.
- The perimeter is gone. Users connect directly to cloud apps from anywhere, leaving traditional tools blind.
- SD-WAN and branch offices often route traffic directly to the internet, bypassing centralized inspection points.
- IoT and unmanaged devices expand the attack surface and evade endpoint security coverage.
- Most legacy systems rely on detecting known malware or content signatures—reactive methods that are too slow.

Security operations teams are also under pressure. They face chronic staffing shortages (an estimated global shortfall of 4.7 million professionals, per the International Information System Security Certification Consortium, or ISC2[1]), fragmented toolsets and overwhelming alert values that drain time and focus.

To stay ahead, organizations need **scalable, preemptive protection at the DNS layer.** Infoblox delivers foundational DNS security that identifies and blocks threats before they impact endpoints, cloud workloads or branch locations. With unmatched visibility, predictive threat intelligence and seamless on-premises integration, Infoblox helps reduce alert fatigue, simplify operations and stop attacks before they can spread.

PROTECTIVE DNS SECURITY AT SCALE

Modern networks span across data centers, SD-WAN, cloud services and IoT-connected environments. As infrastructure grows more distributed, maintaining consistent security coverage becomes more complex—but more critical than ever.

Infoblox Threat Defense™ Business Cloud delivers cloud-delivered DNS security that scales with your business. Whether you are protecting remote users, cloud workloads or globally distributed sites, Infoblox applies consistent DNS-layer enforcement wherever it is needed without relying on endpoint agents or costly infrastructure rollouts.

With built-in integrations for SOAR, SIEM and threat intelligence ecosystems, security teams can detect, prioritize and respond faster, reducing time to resolution and strengthening the value of your existing tools.

Because it is cloud-delivered, Infoblox can scale rapidly to meet shifting demands, support new locations and deliver protection everywhere your users connect, while minimizing IT overhead and operational complexity.

KEY CAPABILITIES

Protect every connection—on-premises, in the cloud and everywhere in between.

Preempt Modern Malware Threats: Stop ransomware, phishing and other malware early by identifying attacker infrastructure and blocking threats before they reach endpoints or move laterally.

Gain Visibility Across Your Network: Correlate DNS activity with asset and IP address management (IPAM) data to detect threats faster, reduce false positives and strengthen your response across hybrid environments.

Block Data Exfiltration: Detect and stop DNS-based exfiltration, domain generation algorithms (DGAs), DNSMessenger and fast-flux activity using behavior analytics and machine learning.

Block Before Impact: Disrupt threats early at the DNS layer. Share enriched event data across your ecosystem to reduce remediation time and accelerate response.

Accelerate Investigations: Look up threat data from internal and external sources instantly. Help analysts investigate faster, reduce dwell time and make confident decisions.

Integrate across Your Ecosystem: Automatically share threat intelligence and logs with next-generation firewall (NGFW), IPS, SIEM, SOAR, endpoint or other security tools.

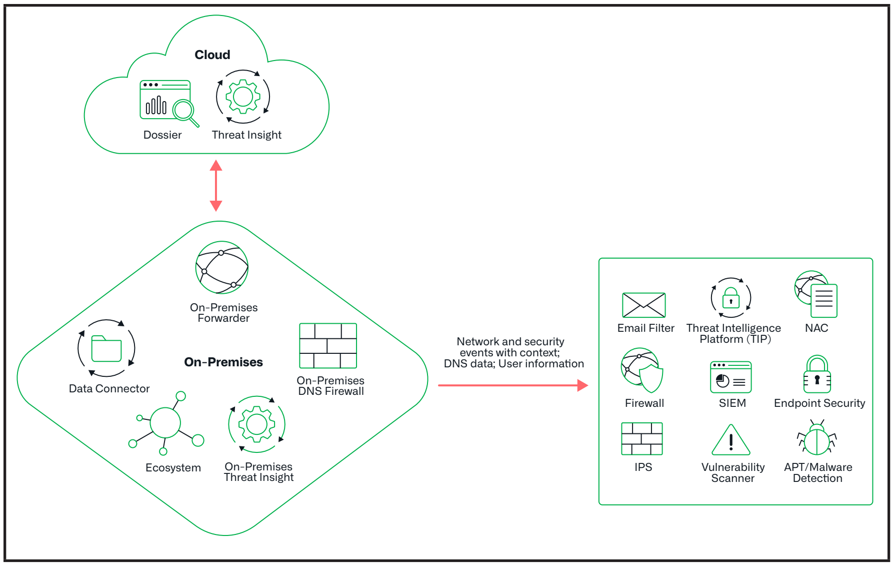

Figure 1. Infoblox Threat Defense Business On-Premises architecture

MAXIMIZE SECURITY OPERATIONS CENTER EFFICIENCY

Start with Preemptive DNS Protection

- Block threats at the DNS layer before they reach firewalls, reducing alert volume and downstream noise.
- Automatically block malicious activity and share indicators with other tools for investigation, quarantine and remediation.
- Improve SOC efficiency and reduce overall threat defense costs by filtering earlier in the kill chain.
- Minimize alert fatigue by preventing known and emerging threats before they generate noisy downstream detections.

Automate and Accelerate Incident Response

- Cut time to remediation by up to two-thirds with earlier detection and automated threat blocking.
- Optimize SOAR outcomes using contextual network and DNS threat intelligence from Infoblox.
- Distribute Infoblox and partner threat intelligence to existing tools to drive consistent enforcement.
- Improve threat feed return on investment (ROI) by reducing duplication and expanding coverage across the stack.
- Enrich SIEM workflows with DNS-layer context for faster triage and correlation.

Empower Analysts to Investigate Faster

- Make threat analysts up to three times more effective with automated threat lookups, related threat insights and research tools.
- Reduce time spent on manual correlation and human-intensive triage workflows.
- Improve confidence in decision-making with rich DNS-based context from internal and external sources.

> “*Sharing information among a user, community and getting collective intelligence on attack vectors and methods keeps victims from having to ask, ‘Is it just us, or is someone else getting hit by this attack?’ ”*
>
> **Elderwood Data Breach**

THE ROI OF INFOBLOX SECURITY

Lower Infrastructure Costs

Reduce the load on security infrastructure by blocking threats earlier.

- Use DNS as a first line of defense to filter threats before they reach firewalls, proxies and IPS.
- Offload perimeter tools—achieve up to 60 times reduction in traffic to NGFWs.
- Lower SIEM costs by forwarding only suspicious DNS activity for analysis.
- Reduce duplicate detections by stopping threats before they trigger alerts downstream.

Maximize the Value of Existing Tools

Make your entire security stack work smarter with shared intelligence.

- Share Infoblox threat intelligence with SIEM, SOAR and endpoint detection and response (EDR) tools to improve detection and response.
- Enhance alert context and prioritization using DNS-based visibility.
- Get more value from existing investments—without increasing headcount or complexity.
- Strengthen Zero Trust and defense-in-depth strategies through DNS-layer integration.

Reduce Operational Burden with Automation

Simplify operations, improve efficiency and free up your security team.

- Deploy and configure in hours, not months—cut onboarding time by 60 percent.
- Reduce manual effort and risk with automated threat response and data sharing.
- Make your analysts up to three times more effective with a unified console and real-time intelligence.
- Alleviate staffing challenges by lowering day-to-day demand on SOC resources.

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

[1] *2024 ISC2 Cybersecurity Workforce Study*, ISC2, October 31, 2024.

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: 20240415v2