DATASHEET

# BloxOne® Threat Defense Advanced

## Strengthen and optimize your security posture from the foundation

### THE NEED FOR FOUNDATIONAL SECURITY AT SCALE

The traditional security model is inadequate in today's world of digital transformations.

- Threats are growing in speed and complexity, with MFA attacks, smishing, lookalike domains and spear phishing leading the chart when it comes to top attacks targeting enterprises in recent months.
- The perimeter has shifted, and your users directly access cloud-based applications from everywhere.
- IoT leads to an explosion of devices that do not accept traditional endpoint technologies for protection.
- Most security systems use a malware and website content-centric approach, which is reactive.

What organizations need is a scalable, simple and proactive security solution that identifies and disrupts cybercrime pre-incident.

### INFOBLOX PROVIDES A SCALABLE PLATFORM THAT MAXIMIZES YOUR EXISTING THREAT DEFENSE INVESTMENT

Infoblox BloxOne Threat Defense Advanced, a comprehensive DNS Detection and Response (DNSDR) solution, detects threat activity that other solutions miss and stops attacks before they occur with hunted, pre-campaign DNS threat intel to disrupt attacker supply chains. Intelligent ecosystem integrations and automation reduce manual effort, while Infoblox's unique AI-driven analytics focus analysts on what matters most and provide insights that reduce MTTR, raise the ROI of existing security tools, and elevate overall SecOps efficiency.

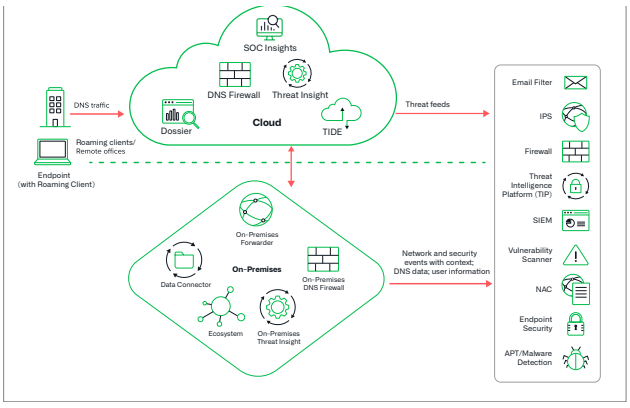



*Figure 1: Infoblox hybrid architecture enables protection everywhere and deployment anywhere*

### KEY CAPABILITIES

- Detect and block emerging and targeted attacks, including phishing, ransomware, suspicious domains, spear phishing and other modern threats using Infoblox Threat Intel
- Protect users and devices, regardless of platform or OS, at the DNS layer, including BYOD, IoT, and ICS
- Discover high-risk applications and manage your Shadow IT, Insider, Compliance and other risks
- Prevent data exfiltration techniques with machine learning/AI analytics, including DNS-based data exfiltration, DGA, and DNSMessenger
- Detect and block Zero Day DNS™ attacks within minutes of a malicious domain getting registered and used
- Restrict user access to inappropriate or unwanted web content and track activity
- Protect your brand with Lookalike Domain Monitoring for your most valuable internet properties
- Accelerate investigations 3X and streamline threat response and threat-hunting activities
- Enhance visibility: Get precise visibility "and rich network context" by integrating with IPAM asset metadata for optimum event understanding and correlation
- SOC Insights lets you jump-start investigation and response on the threats that matter most and reduce MTTR with AI-driven insights

## MAXIMIZE SECURITY OPERATION CENTER EFFICIENCY

### Reduce Incident Response Time

- Automatically block malicious activity and provide the threat data to the rest of your security ecosystem for investigation, quarantine and remediation
- Optimize your SOAR solution using contextual network and DNS threat intel data and Infoblox ecosystem integrations (a critical enabler of SOAR)-reduce threat response time and OPEX
- Use Infoblox SOC Insights capabilities to know which events matter most with the AI-driven analytics that go beyond simple malware risk-ranked dashboards

### Unify Security Policy with Threat Intel Portability

- Distribute Infoblox Threat Intel and partner feeds to existing security systems
- Reduce cost of threat feeds while improving effectiveness of threat intel across entire security stack

### Faster Threat Investigation and Hunting

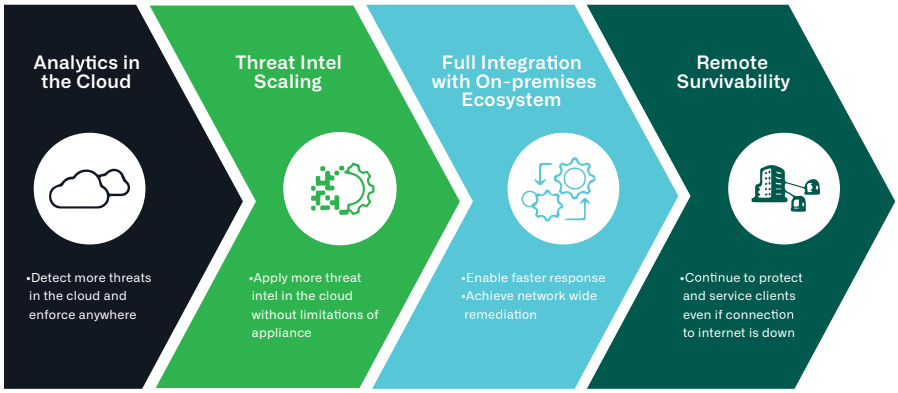
- Jump-start investigation and response on the threats that matter most and reduce MTTR with AI-driven insights that go beyond simple malware risk-ranked dashboards
- Makes your threat analysts team **3x more productive** by empowering security analysts with automated threat investigation, insights into related threats and additional research perspectives from expert cyber sources to make quick, accurate decisions on threats


*Figure 2: BloxOne Threat Defense integrates with the entire cybersecurity ecosystem*

> *"ZK Research believes that DNS security is the simplest and most effective starting point for any security strategy. As the leader in that area, Infoblox should be at the top of your list to unify networking and security and stop most malware before it becomes a problem."*
>
> **ZK Research**

> *"Planning a review of DNS threats and how to respond to them within a broader XDR framework should be a matter of 'when' rather than 'if'."*
>
> **HardenStance**

## HYBRID APPROACH PROTECTS WHEREVER YOU ARE DEPLOYED




### Analytics in the Cloud

- Leverage greater processing capabilities of the cloud to detect a wider range of threats, including data exfiltration, domain generation algorithm (DGA), fast flux, fileless malware, Dictionary DGA and more, using machine learning-based analytics
- Detect threats in the cloud and enforce anywhere to protect HQ, data center, remote offices or roaming devices

### Threat Intelligence Scaling

- Apply comprehensive intelligence from Infoblox Threat Intel and partner feeds to enforce policies on-premises or in the cloud and automatically distribute it to the rest of the security infrastructure
- Apply more threat intel in the cloud without huge investments into more security appliances for every site

### Powerful integrations with your security ecosystem

- Enables full integration with on-premises Infoblox and third-party security technologies, enabling network-wide remediation and improving the ROI of those technologies

### Remote survivability/resiliency

- If there is ever a disruption in your Internet connectivity, the on-premises Infoblox can continue to secure the network

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

## THE ROI OF INFOBLOX SECURITY

### Offload strained security devices

- Decrease the burden on strained perimeter security devices such as firewalls, IPS, and web proxies by using your already available DNS servers as the first line of defense
- **Up to 60 times reduction in traffic** sent to NGFWs*

### Improve ROI on existing investments

- Get more value out of adjacent/complementary products by bi-directionally sharing threat and attacker information
- If sending DNS data to SIEM, reduce the cost of SIEM solutions by sending only suspicious DNS data to these platforms

### Automation

- Reduce cost of human touch/error using automation
- Overcome lack of skilled resources - 60% less demand on your team to implement (configure in hours instead of months) and operate for both skills and cost
- Make your threat analysts 3x more productive with an easy-to-use, single console

*Based on real customer data*

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

© 2024 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20240809v3