DATASHEET

BloxOne™ Threat Defense Advanced

Strengthen and Optimize Your Security Posture from the Foundation

KEY CAPABILITIES

- **Secure existing networks and digital transformations** like SD-WAN, IoT and cloud leveraging existing infrastructure
- **Prevent data exfiltration techniques with analytics and machine learning** including DNS-based data exfiltration, DGA, DNSMessenger, and fast-flux attacks
- **Detect and block exploits, phishing, ransomware and other modern malware**
- **Identify malware propagation and lateral movement** through east-west traffic monitoring
- **Restrict user access to certain web content categories and track activity**
- **Protect your brand with Lookalike Domain Monitoring** for your most valuable internet properties
- **Reduce response times through automated blocking and sharing of incident details** to 3rd party ecosystem solutions through public APIs or on-premises integrations
- **Accelerate investigations 3X and streamline threat hunting**
- **Enhance visibility:** Get precise visibility "and rich network context including IPAM and asset metadata about your network devices for better correlation of events
- **Control the risks of rising DoH use:** block DoH (DNS over HTTPS) domain access and gracefully revert DoH requests to existing, trusted DNS

The Need for Foundational Security at Scale

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

- The perimeter has shifted, and your users directly access cloud-based applications from everywhere.
- SD-WAN drives network transformation and branch offices directly connect to Internet with no ability to replicate full HQ security stack.
- IoT leads to an explosion of devices that do not accept traditional endpoint technologies for protection.
- Most security systems are complex, and do not easily scale to the level needed to protect these dynamic environments.

Moreover, security operations teams are chronically short staffed (there is a **shortage of 2.93 million security operations personnel** worldwide according to a recent ISC2 report), use siloed tools and manual processes to gather information, and must deal with hundreds to thousands of alerts everyday.

What organizations need is a scalable, simple and automated security solution that protects the entire network without the need to deploy or manage additional infrastructure.

Infoblox Provides a Scalable Platform That Maximizes Your Existing Threat Defense Investment

Infoblox BloxOne Threat Defense strengthens and optimizes your security posture from the foundation up. It maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It uses a hybrid architecture for pervasive, inside-out protection, powers security orchestration, automation and response (SOAR) solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense.

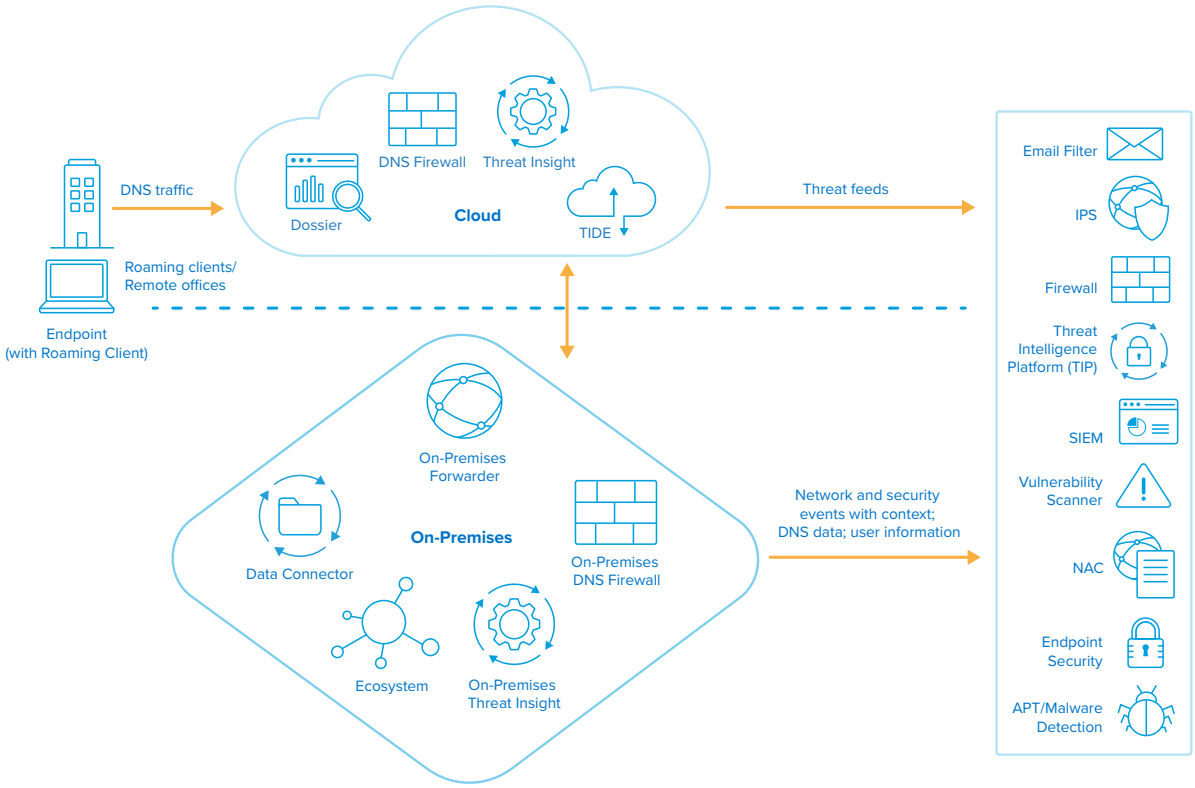


Figure 1: Infoblox hybrid architecture enables protection everywhere and deployment anywhere

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 threat intelligence data, and Infoblox ecosystem integrations (a critical enabler of SOAR)-reduce threat response time and OPEX
- Reduce number of alerts to review and the noise from your firewalls

Unify Security Policy with Threat Intel Portability

- Collect and manage curated threat intelligence data from internal and external sources and distribute it to existing security systems
- Reduce cost of threat feeds while improving effectiveness of threat intel across entire security portfolio

Faster Threat Investigation and Hunting

- 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.
- Reduce human analytical capital needed

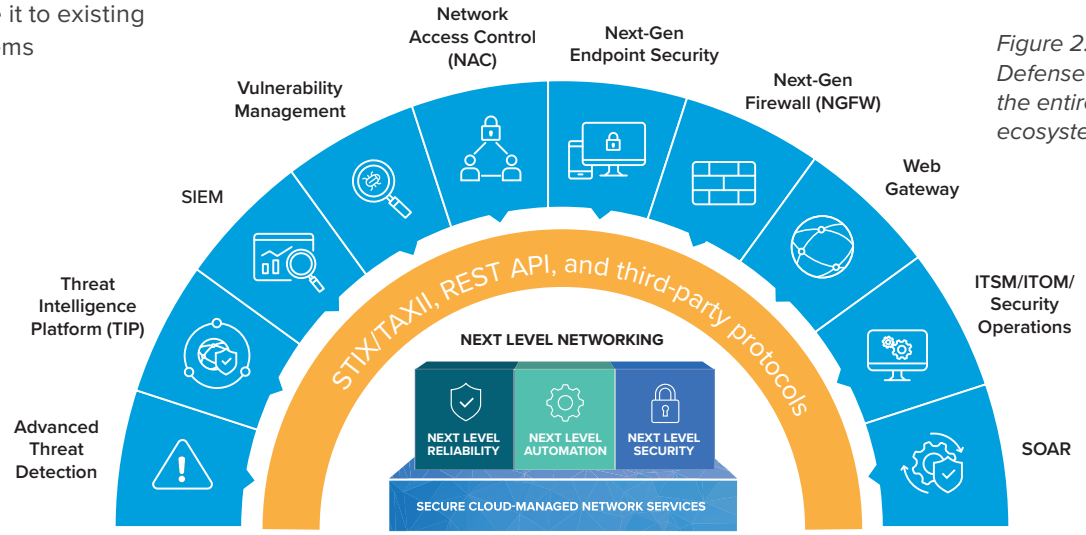


Figure 2: BloxOne Threat Defense integrates with the entire cybersecurity ecosystem

"In this day and age there is way too much ransomware, spyware, and adware coming in over links opened by Internet users. The Infoblox cloud security solution helps block users from redirects that take them to bad sites, keeps machines from becoming infected, and keeps users safer."

Senior System Administrator and Network Engineer,
City University of Seattle

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

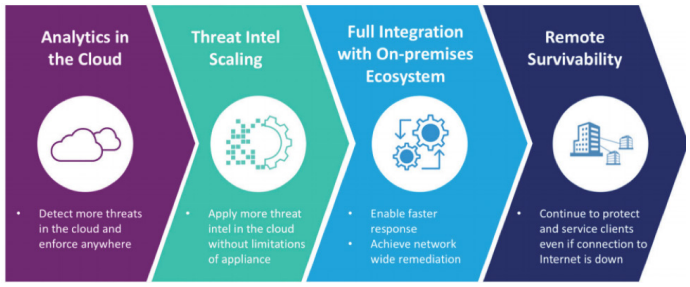
- Get more value out of adjacent/complementary products by bi-directionally sharing threat and attacker information
- If sending DNS data to SIEM, reduce the cost of SIEM solutions by sending only suspicious DNS data sent to these platforms

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 for deep threat intelligence

* Based on real customer data

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, datacenter, remote offices or roaming devices

Threat Intelligence Scaling

- Apply comprehensive intelligence from Infoblox research and third-party providers to enforce policies on-premises or in the cloud, and automatically distribute it to the rest of the security infrastructure
- Apply more threat intelligence 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 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

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com