**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.

- 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 Advanced 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.

### KEY CAPABILITIES

- Detect and block exploits, phishing, ransomware and other modern malware that other solutions miss
- Protect users and devices regardless of platform or OS, at the DNS layer, including BYOD, IoT, and ICS
- Defend mobile devices from emerging threats like those that abuse photos taken of malicious QR codes
- 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
- 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
- Control the risks of rising DoH use: block DoH (DNS over HTTPS) domain access and gracefully revert DoH requests to existing, trusted DNS
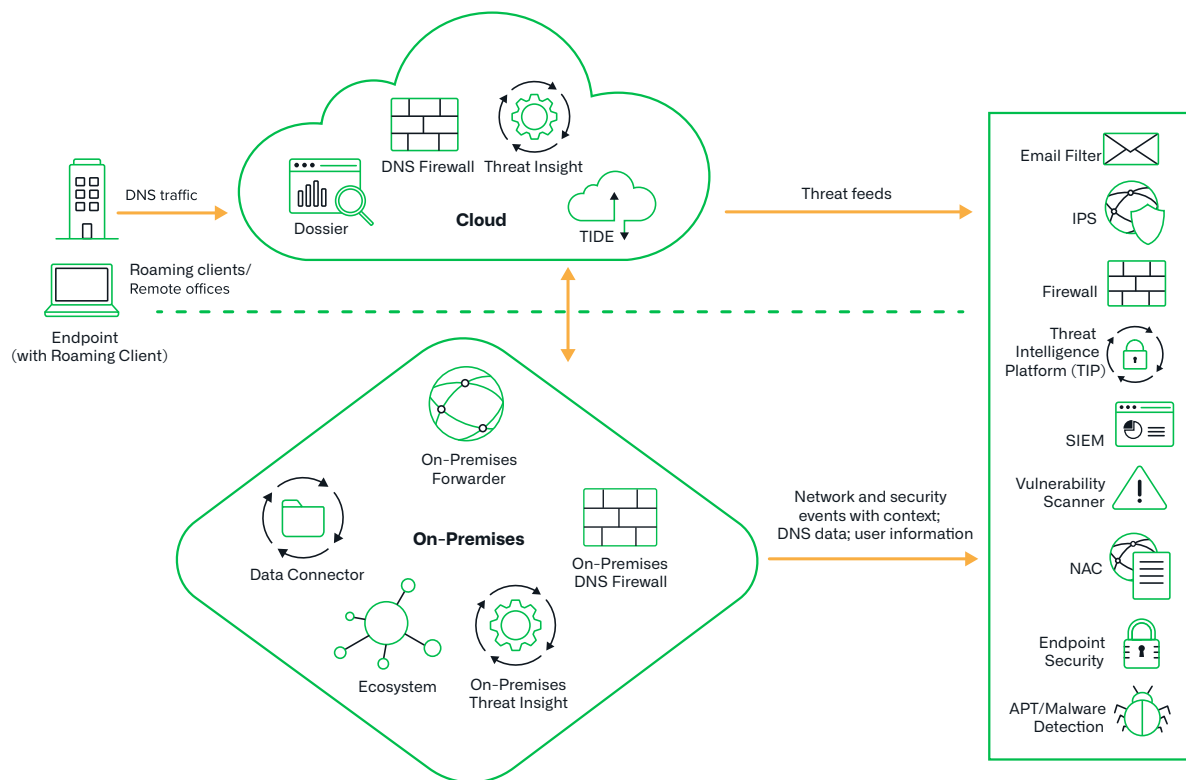
*Figure 1:  Infoblox hybrid architecture enables protection everywhere and deployment anywhere*

## 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.
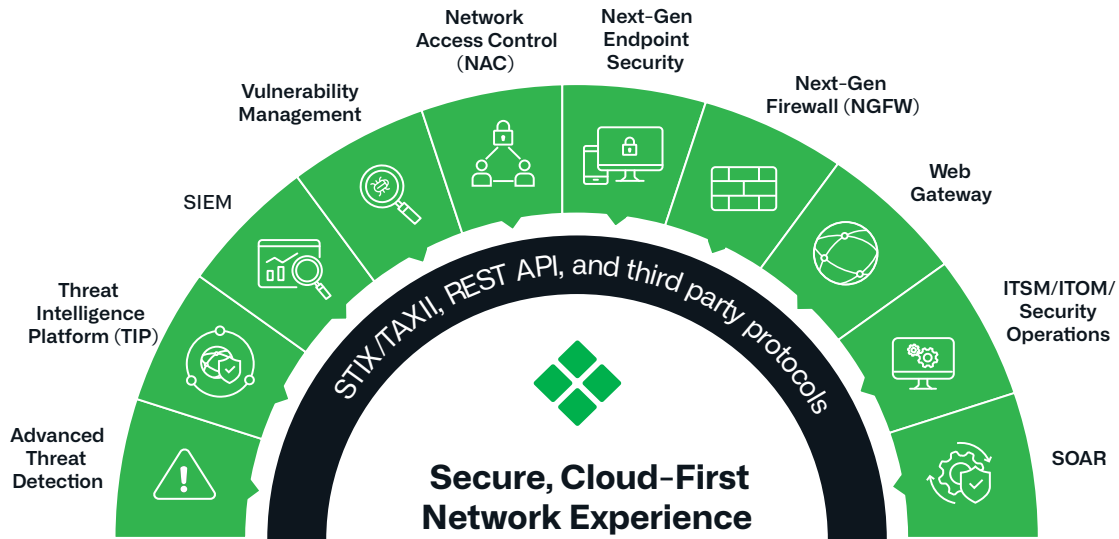
- Reduce human analytical capital needed

infoblox.

Network
Access Control
(NAC)

Next-Gen
Endpoint
Security

Vulnerability
Management

Next-Gen
Firewall (NGFW)

SIEM

Web
Gateway

Threat
Intelligence
Platform (TIP)

STIX/TAXII, REST API, and third party protocols

ITSM/ITOM/
Security
Operations

Advanced
Threat
Detection

Secure, Cloud-First
Network Experience

SOAR

*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**

## HYBRID APPROACH PROTECTS WHEREVER YOU ARE DEPLOYED

| Analytics in the Cloud | Threat Intel Scaling | Full Integration with On-premises Ecosystem | Remote Survivability |
|---|---|---|---|
| •Detect more threats in the cloud and enforce anywhere | •Apply more threat intel in the cloud without limitations of appliance | •Enable faster response<br>•Achieve network wide remediation | •Continue to protect and service clients even if connection to internet is down |

infoblox.

## 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

### 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

**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