DATASHEET

BloxOne™ Threat Defense Business On-Premises

Strengthen and Optimize Your Security Posture from the Foundation

BLOXONE THREAT DEFENSE BUSINESS ON-PREMISES KEY CAPABILITIES

- Secure existing networks and digital transformations like SD-WAN, IoT and cloud leveraging existing infrastructure
- **Block data exfiltration:** Detect and block DNS-based data exfiltration, DGA, DNSMessenger, and fast-flux attacks using analytics and machine learning
- **Detect and block modern malware:** Block ransomware, phishing, exploits and other modern malware; monitor east-west traffic and prevent malware from propagating
- **Automate incident response: Reduce time to remediation by two-thirds** and respond to threats faster by first blocking them and then sending event data to rest of ecosystem using public APIs or on-premises integrations
- **Accelerate threat investigation and hunting:** Automatically lookup threat data from dozens of sources for faster investigation, making threat analysts **3 times more effective**
- **Enhance visibility:** Get precise visibility and rich network context including IPAM and asset metadata about your network devices for better correlation of events

The Need for Foundational Security at Scale

Protecting your infrastructure and data is more complicated than it once was. That's because the traditional network security model is inadequate.

- The perimeter has shifted, and your users directly access cloud-based applications from everywhere.
- IoT leads to an explosion in the number of devices that can't be protected using traditional endpoint protection technologies.
- 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

BloxOne Threat Defense Business On-Premises strengthens and optimizes your security posture from the foundation. It maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It powers security orchestration, automation and response (SOAR) solutions by providing rich network and threat context, slashing the time to investigate and remediate cyberthreats, optimizing the performance of the entire security ecosystem and reducing your total cost of enterprise threat defense.

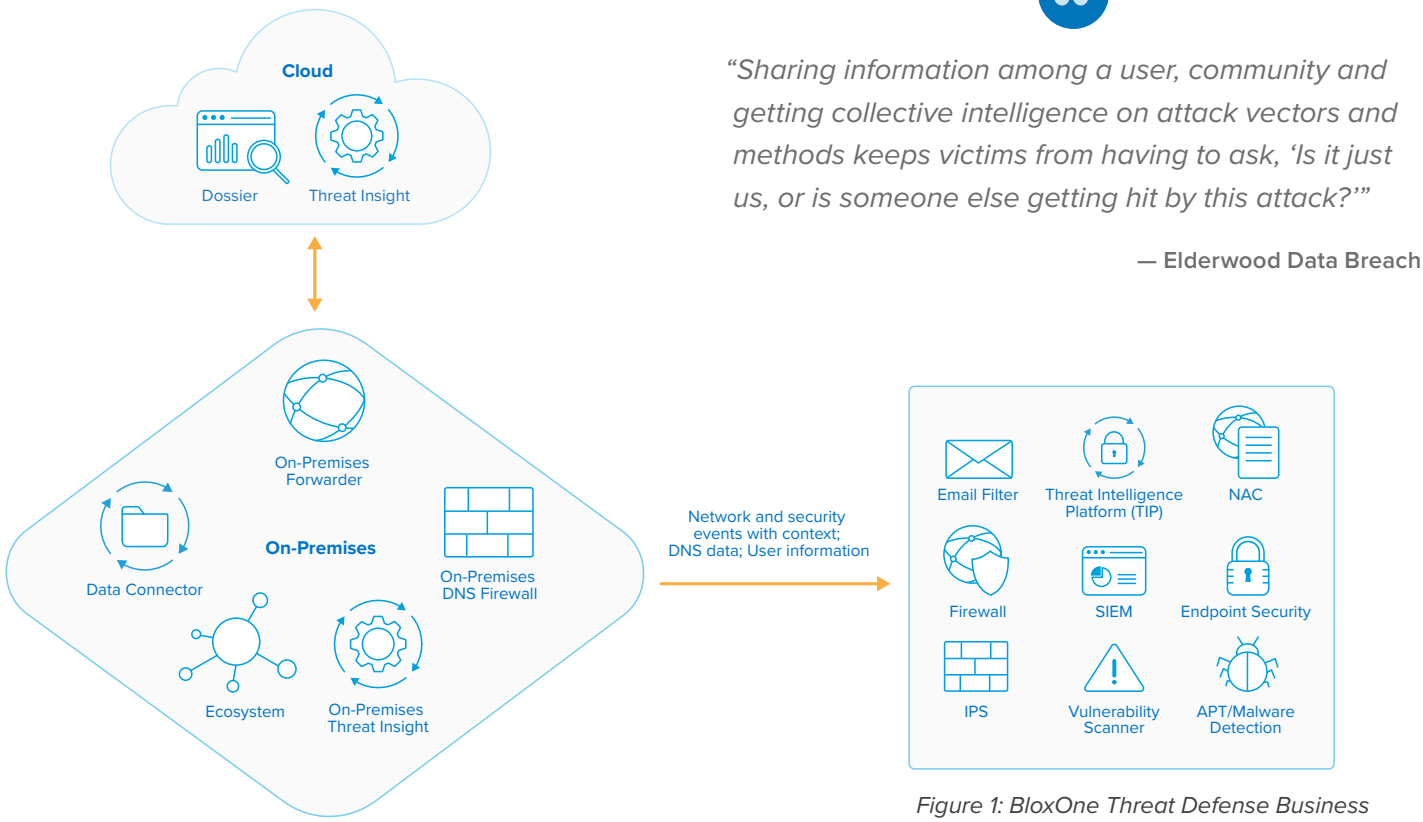

Figure 1: BloxOne Threat Defense Business On-Premises Architecture

> *"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

Maximize Security Operations 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 time to remediation by **two-thirds**
- Use curated threat intelligence and block bad stuff before it even gets to perimeter defenses to reduce the noise from firewalls and the number of alerts teams must review
- Reduce total expense of threat defense by making all components more productive and efficient

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

Accelerate Threat Investigation and Hunting

- Make 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 faster, more accurate decisions on threats.
- Reduce human capital required for threat analytics

To learn more about the ways that BloxOne Threat Defense Business On-Premises 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

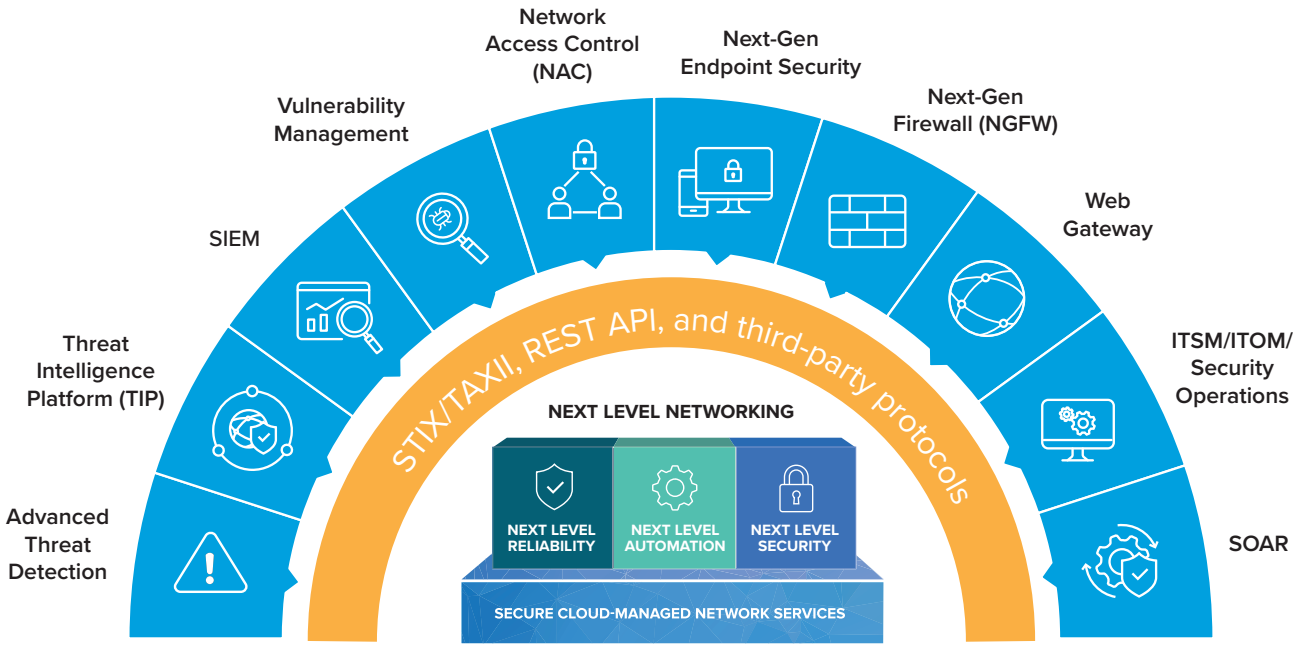

Figure 2: BloxOne Threat Defense Business On-Premises integrates with the entire cybersecurity ecosystem

Infoblox
NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 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