

DATASHEET

# BloxOne™ Threat Defense Essentials

*Strengthen and Optimize Your Security Posture from the Foundation*

## BLOXONE THREAT DEFENSE ESSENTIALS 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 using analytics and machine learning
- **Enhance visibility:** Get precise visibility and rich network context including IPAM and asset metadata about your network devices for better correlation of events
- **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; achieve up to 60 times reduction in traffic sent to NGFWs\*

\*Based on real customer data

## 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.
- 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 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.

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 Brand Protection

BloxOne Threat Defense Essentials 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 protects customers from data exfiltration, provides scalable malware mitigation, delivers precise visibility for faster correlation of events and reduces burden on strained perimeter security devices.

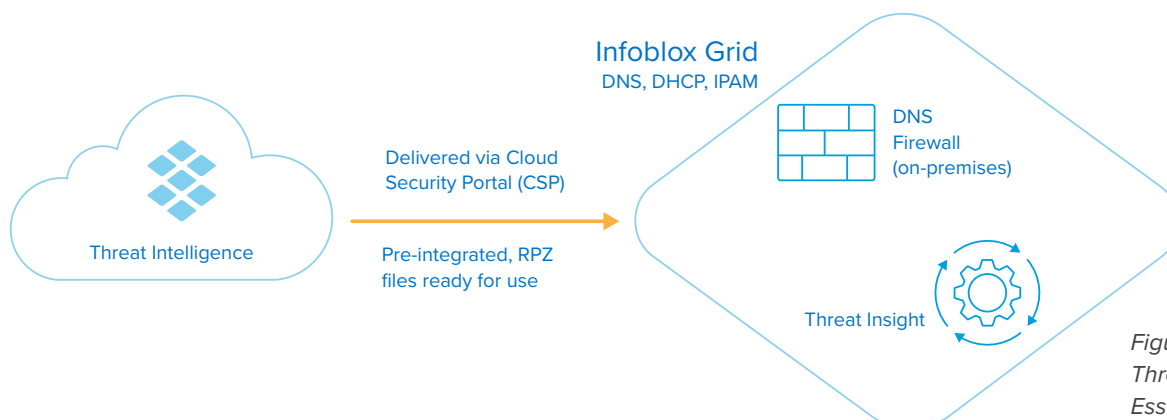


Figure 1: BloxOne Threat Defense Essentials Architecture



*“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

## Threat Intelligence Data Feeds

Here are the threat intelligence data feeds that are available as part of BloxOne Threat Defense Essentials package:

- 1. Base hostnames:** The base hostnames set enables protection against known hostnames that are dangerous as destinations and are sources of threats, such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.
- 2. Anti-malware:** Enables protection against hostnames containing known malicious threats, such as malware command and control (C&C), malware download and active phishing sites
- 3. Ransomware:** Enables protection against hostnames containing malware that restricts access to the computer system it infects and demands a ransom for the removal of the restriction

**4. Bogon:** Bogons are often source addresses of DDoS attacks and is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by an Internet Authority or Registry. Bogons are usually the result of accidental or malicious misconfiguration.

**5/6. DHS AIS\_IP and DHS AIS\_Hostname (2 feeds):** AIS is a part of the Department of Homeland Security’s (DHS’s) effort to create an ecosystem in which, as soon as a company or federal agency observes an attempted compromise, the indicator is shared with AIS program partners, including Infoblox. Indicators from the AIS program are classified and normalized by Infoblox to ease consumption.

**7/8. DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IPs (2 feeds):** Indicators contained in these feeds appear on the watch list from the National Cybersecurity and Communications Integration Center (NCCIC), which are not verified or validated by DHS or Infoblox.

---

### For More Information

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

For more details on threat intelligence data feeds, please visit: <https://www.infoblox.com/wp-content/uploads/infoblox-solution-note-threat-intelligence.pdf>.



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](mailto:info@infoblox.com) | [www.infoblox.com](http://www.infoblox.com)



© 2019 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).