DATASHEET

# BloxOne® Threat Defense Essentials

## Strengthen and optimize your security posture from the foundation

### 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.

### 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.

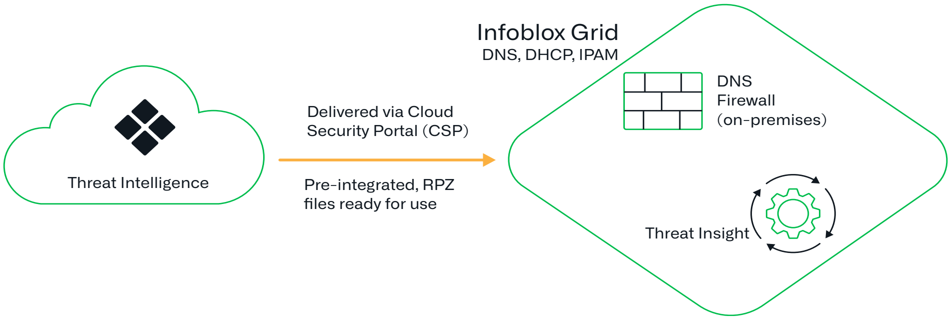
Threat Intelligence
Delivered via Cloud Security Portal (CSP)
Pre-integrated, RPZ files ready for use
Infoblox Grid
DNS, DHCP, IPAM
DNS Firewall (on-premises)
Threat Insight

*Figure 1: BloxOne Threat Defense Essentials Architecture*

### KEY CAPABILITIES

**Detect and block modern malware:**
Block ransomware, phishing, exploits and other modern malware that other solutions miss

**Secure networks through digital transformations**
Like SD-WAN, IoT and cloud leveraging existing infrastructure

**Enhance visibility:**
Get precise visibility and rich network context including IPAM asset metadata for optimum event understanding and correlation

**Simplify Investigations:**
Research security hits with an easy to use threat lookup tool

**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

## 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 companyor 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.

9. **DoH Public IPs and Hostnames:** This policy-based feed contains Domain names and IPs of 3rd party DoH (DNS over HTTPS) services Organizations wishing to provide security policy enforcement through DNS may wish to prevent the bypass of DNS security policies by using 3rd-party DoH servers.

### 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

> *“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**

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

Version: 20230920v1