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.

- Threats are growing in speed and complexity, with MFA attacks, smishing, lookalike domains and spear phishing leading the chart when it comes to top attacks targeting enterprises in recent months.
- 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 the 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 use a malware and website content-centric approach, which is reactive.

What organizations need is a scalable, simple and proactive security solution that identifies and disrupts cybercrime pre-incident.

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.

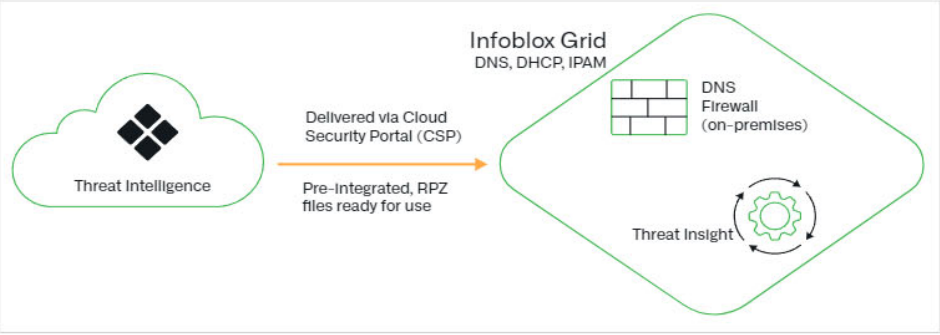

Figure 1: BloxOne Threat Defense Essentials Architecture

KEY CAPABILITIES

Detect and block modern malware:
Block ransomware, phishing, exploits and other modern malware using Infoblox Threat Intel

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 intel data feeds that are available as part of the BloxOne Threat Defense Essentials package:

Infoblox Base: Infoblox Base feed enables protection against known malicious or compromised domains. This includes known Malware, Ransomware, APTs, exploit kits, malicious Name Servers, sinkholes etc. We recommend blocking them for all users.

Bogon: Bogon IPs are often the source addresses of DDoS attacks. "Bogon" 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 the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The areas of unallocated address space are called "bogon space." Many ISPs and end-user firewalls filter and block bogons because they have no legitimate use and are usually the result of accidental or malicious misconfiguration.

DHS AIS IP and DHS AIS Hostname (2 feeds): The Department of Homeland Security (DHS) Automated Indicator Sharing (AIS) program enables the exchange of cyber threat indicators between the federal government and the private sector. AIS is a part of the 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. The IP indicators contained in this feed are not validated by DHS because they emphasize velocity and volume. Infoblox does not modify or verify the indicators. However, indicators from the AIS program are classified and normalized by Infoblox to ease consumption.

Data included in these AIS IP, AIS Hostname feeds include AIS data subject to the U.S. DHS Automated Indicator Sharing Terms of Use available at www.us-cert.gov/ais and must be handled in accordance with the Terms of Use. Prior to further distributing the AIS data, you may be required to sign and submit the Terms of Use available at www.us-cert.gov/ais. Please email ncciccustomerservice@hq.dhs.gov for additional information.

DoH Public Hostnames and DoH Public IPs (2 feeds) This policy-based feed contains domain names and IPs of third-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 third-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

> *"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: 20240415v2