infoblox®

DATASHEET

BloxOne® Threat Defense Business Cloud

Strengthen and optimize your security posture from the foundation

THE NEED FOR DNS-LEVEL SECURITY AT SCALE

The traditional security model is inadequate in today's world of digital transformations.

- 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 users directly access cloud-based applications anytime, anywhere.
- IoT leads to an explosion of devices that do not accept traditional endpoint technologies for protection.
- 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.

INFOBLOX PROVIDES A SCALABLE PLATFORM THAT MAXIMIZES YOUR THREAT DEFENSES

Infoblox's DNS Detection and Response (DNSDR) solution, BloxOne Threat Defense Business Cloud, stops attacks earlier with unique DNS threat intelligence, detecting threat activity other solutions miss. It can further elevate SecOps efficiency with AI-driven analytics that turn vast amounts of event, network, ecosystem, and DNS intelligence data into a manageable set of actionable insights.

THE INFOBLOX SAAS ADVANTAGE

BloxOne Threat Defense Business Cloud is a software-as-a-service (SaaS) solution that brings next-generation security capabilities to your existing on-premises infrastructure. Cloud-based and elastically scalable, the solution enables:

- Immediate improvement of a company's security posture
- Easy security coverage for all devices, everywhere
- Minimized IT overhead

KEY CAPABILITIES

- Detect and block exploits, phishing, ransomware and other modern malware using Infoblox Threat Intel
- Protect devices, regardless of platform or OS, at the DNS layer, including BYOD and IoT/OT
- Prevent data exfiltration techniques with analytics and machine learning, including DNS-based data exfiltration, DGA, DNSMessenger, and fast-flux attacks
- Restrict user access to certain web content categories and track activity
- Protect your brand with Lookalike Domain Monitoring for your most valuable Internet properties
- Accelerate investigations by 3X and streamline threat response and hunting activities
- Enhance visibility: Get precise visibility "and rich network context" by integrating with IPAM asset metadata for optimum event understanding and correlation
- SOC Insights lets you jump-start investigation and response on the threats that matter most and reduce MTTR with AI-driven insights

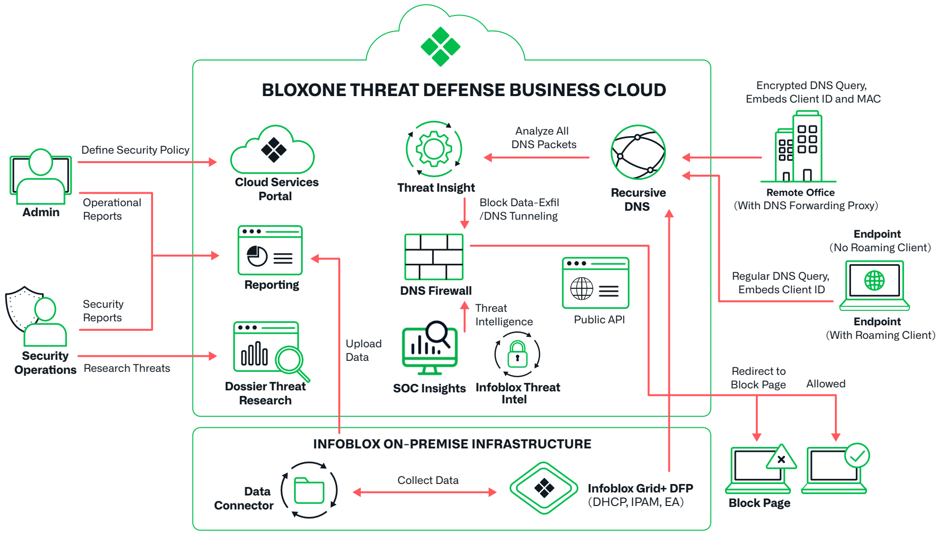

Figure 1: Workflow Scenario for BloxOne Threat Defense Business Cloud

> *“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**

Availability—Anytime, Anywhere Access

The Infoblox service is designed for always-on, anywhere access with reliable service delivery, backed by Infoblox service-level terms that include 99.999 percent uptime for DNS infrastructure, not including scheduled maintenance. Infoblox provides disaster recovery (anycast) and leverages worldwide datacenters. The Infoblox Network Operations Center continuously monitors the service, and configurations policy and user data are backed up daily.

Security and Privacy

Infoblox protects your data and access to the service by encrypting DNS queries during transmission, and by encrypting all databases and stored data. Additional protections include restricting access based on location, IP addresses and role, and having controls in place for movement of data.

Infoblox also adheres to best practices for security, such as making sure all software is patched and by performing penetration testing and static and dynamic code analysis.

Data Privacy: Infoblox SaaS solutions protect the privacy of customer data with logical separation of customer data and through the use of a unique API key for authentication. Infoblox does not share customer data with third-party vendors.

DNS FORWARDING PROXY

In cases where installing an endpoint agent is not always desirable or possible (certain IoT devices), administrators can use a DNS Forwarding Proxy. It is a virtual appliance that embeds client IP into DNS queries before forwarding to the Infoblox cloud. As with the endpoint agent, the communications are encrypted, and client visibility is maintained. The DNS Forwarding Proxy is also integrated with NIOS 8.3 and above, eliminating the need for Infoblox customers to install additional software on-premises.

BLOXONE ENDPOINT

In order to use the cloud-based service, administrators can install the Endpoint Agent on the devices or workstations. This small, lightweight client agent:

- Redirects the endpoint's DNS to Infoblox in the Cloud
- Encrypts and embeds the client identity in DNS packets
- Sends information on the logged-in user to the Cloud for reporting
- Automatically switches to bypass mode when it is on a corporate network protected by on-premises BloxOne Threat Defense

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

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