DATASHEET

BloxOne™ Threat Defense Business Cloud

Strengthen and Optimize Your Security Posture from the Foundation

BLOXONE THREAT DEFENSE BUSINESS CLOUD KEY CAPABILITIES

- Securing branches locations including SD-WAN branches and remote users
- **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
- **Use web content categorization and web access policy enforcement:** Restrict users from accessing certain categories of web content and review content activity
- **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
- **Get access to data via S3 Bucket:** Export your activity logs to Amazon S3 buckets and easily use your data in common formats (CSV, JSON and CEF)
- **Accelerate threat investigation and hunting:** Automatically lookup threat data from dozens of sources for faster investigation, making threat analysts **3 times more effective**

The Need for Pervasive Security at Scale

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

- The workforce is becoming increasingly mobile and distributed offices are on the rise.
- SD-WAN drives network transformation and branch offices directly connect to Internet with no ability to replicate full HQ security stack.
- **More than 80 percent** of mobile knowledge workers connect to unsecured free public WiFi access points using their work devices.
- Some organizations lack dedicated IT resources (especially in remote and branch offices) to manage and secure infrastructure on premises.
- Roaming users do not always use secure access mechanisms such as VPN.

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 Cloud-based Platform That Maximizes Your Threat Defenses Using Your Existing Investment

BloxOne Threat Defense Cloud protects data and devices everywhere, on the enterprise network, roaming, and in remote and branch offices. Delivered as a service, it is easy to configure and use without the need for dedicated IT resources or added security infrastructure.

Infoblox 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 Cloud for reporting
- Automatically switches to bypass mode when it is on a corporate network protected by on-premises BloxOne Threat Defense

The Endpoint Agent can be installed on Windows (7/8/10) and Mac OSX 10.10–10.12 and can be mass deployed using automated solutions such as SCCM or McAfee ePO.

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.

"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

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
- Immediate access to next-generation features for trial
- Minimized IT overhead

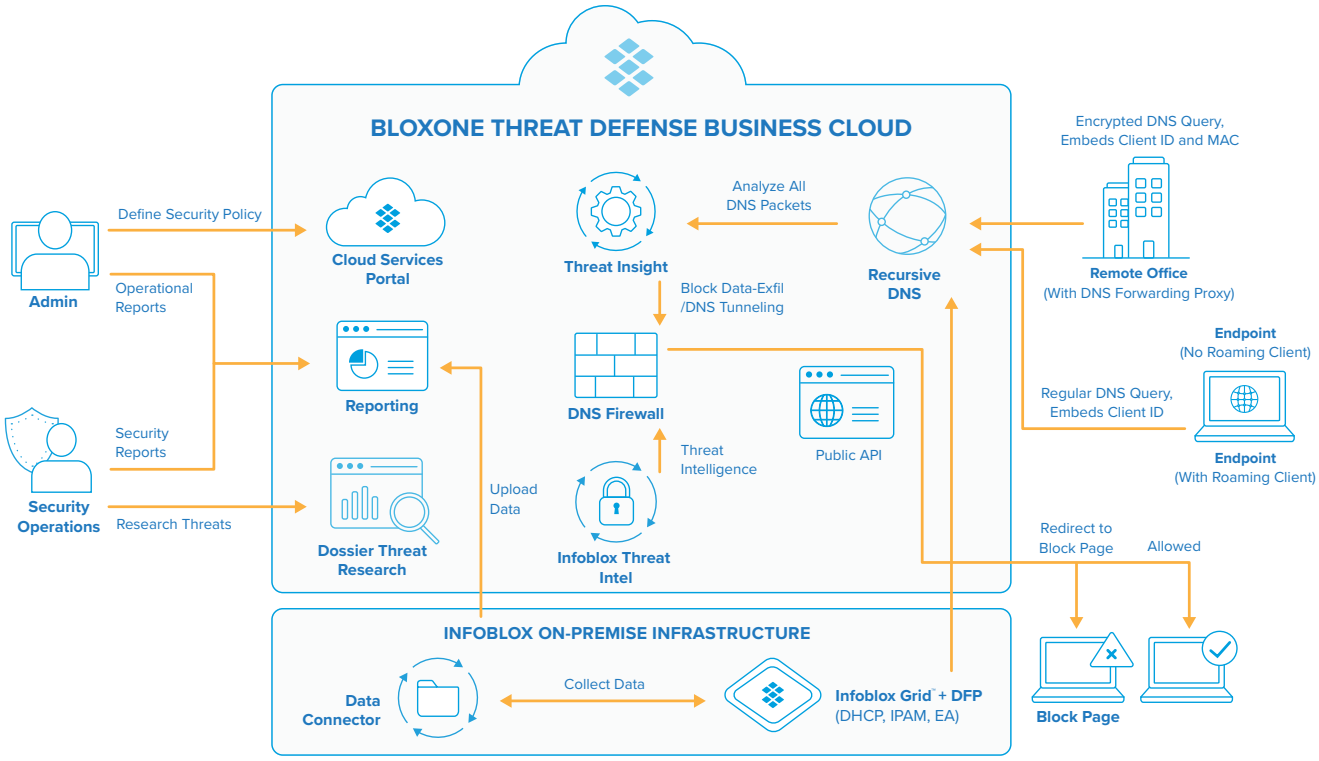

Figure 1: Workflow Scenario for BloxOne Threat Defense Business Cloud

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 and 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.

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
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