DATASHEET

Infoblox Professional Services: BloxOne Threat Defense Services Overview

Realize the full value of your Infoblox BloxOne Threat Defense investment with configuration and integration services

Infoblox designed a service offering to configure and integrate the Infoblox BloxOne® Threat Defense suite of security services into the Infoblox Grid and existing legacy platforms.

BLOXONE THREAT DEFENSE SERVICE

Infoblox BloxOne Threat Defense bundles Infoblox DNS Firewall, Infoblox Threat Insight in the Cloud, Infoblox Threat Intelligence Data Exchange (TIDE) and Infoblox Dossier. BloxOne Threat Defense helps prevent data exfiltration and malware C&C communications via DNS. It centrally aggregates and distributes curated internal and external threat intelligence to the existing security infrastructure and enables rapid investigation to identify context and prioritize threats. Professional services for BloxOne Threat Defense begin with the configuration of the Infoblox Cloud Services Portal. As part of that task, Infoblox engineers perform a whitelisting review of initial DNS logs to eliminate potential false positives. Once tuned, the BloxOne Threat Defense service is set to automatically block or redirect malicious DNS queries.

FEATURES AND BENEFITS

- **Experienced engineers**
  Infoblox experts who are familiar with all aspects of your solution bring focused engineering expertise and experience to the table. Assistance from our team optimizes efforts by allowing your staff to focus on service design and service operation instead of spending time researching technologies and products. This approach also helps you cut costs by lowering operational expenditures.

- **Proven methodology**
  Infoblox has performed hundreds of projects just like yours using tried-and-true methodologies. Your project will follow a proven game plan from start to finish and get your Infoblox investment working and returning value for you as quickly as possible. In addition, we provide valuable experience to mitigate project risk at each phase and facilitate successful execution.

- **Customer focus**
  Infoblox strives to help you understand every aspect of your Infoblox solution. Knowledge transfer and communication are our foundation, helping your staff refine, operate and scale your environment as you move forward.

UNLEASH THE FULL VALUE OF INFOBLOX BLOXONE THREAT DEFENSE

Service	Description	Benefit

Design Deployment Model	• Deployment Model Overview (Forwarding, DFP, ATE, On-Premises DNSFW)
	• BloxOne Threat Defense On-Premises Configuration (if applicable)
	• BloxOne Threat Defense Cloud Configuration
	   • Security Policies
	   • Custom Lists (Block/Allow lists)
	• Category Filters
	• Configure custom redirects
	   • Internal sandbox
	   • Customized landing page
		Save time on mapping out deployment strategy and integration with your existing security stack. These steps ensure that you'll get into a strengthened security posture as quickly as possible.

Administration Setup	• Define Administrator User Accounts • Define DFP (NIOS or Standalone) • Define Network/Ranges for Standalone DFP where applicable • Define Bypass domains for Standalone DFP where applicable	Quickly establish secured access privileges for your admin staff. Gain secure operation of the solution from the ground up.

Configuration	• Configuration of policies and content filtering per customer requirements
	   • Network Scope
	   • DNS Forwarding Proxies (NIOS and/or Standalone)
	   • Endpoint Groups
	   • Policy Rules or Feeds as per Precedence
	   • Bypass Codes
	• Assist with Cloud Services Portal (CSP) configuration
	   • Configuring on-premises DNS Firewall information
	   • Defining security policies
	   • Configuring on-premises DNS Forwarders and by-pass domains
	   • Analyze security logs and tune BloxOne Threat Defense Allow lists
	   • Provide assistance with initial integration of Grid configuration
	   • Supply assistance with initial DNS Firewall and Threat Feed configuration
	• Set up Threat Feeds, allow and block lists
		Optimize the effective deployment of BloxOne Threat Defense and further automate security responses by having Infoblox experts configure and integrate your Infoblox solution with your existing SOAR and SIEM systems. With accurate analysis of security data and logs, you get optimal results from the solution.

infoblox.

Service	Description	Benefit
Production Changes	• On-Premises BloxOne Threat Defense configuration where applicable • DFP configuration within NIOS where applicable • Standalone DFP configuration where applicable (virtual infrastructure to support ESX or Docker is a prerequisite) • Reconfigure clients to point to DFP if using standalone DFP • Install BloxOne Threat Defense Endpoint on subset of clients not to exceed (5) five • Configure DFP on NIOS where applicable	Ensure success regardless of deployment challenges by relying on Infoblox expertise in implementing production changes when needed to your unique on-premises and hybrid network environments.
Knowledge Transfer	Infoblox Professional Services will provide knowledge transfer on general DNS security functions, including: • Threat Feeds • Block/Allow lists • Security policies, custom lists and/or category filters • BloxOne Threat Defense Cloud reports and dashboards • Threat lookup, Dossier, and TIDE where applicable	Optimize your security operations well into the future with guidance from Infoblox experts on how to most effectively incorporate BloxOne Threat Defense into your complex network architectures.

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