Enabling Security Orchestration with Infoblox and Rapid 7

PARTNER SOLUTION BRIEF

Overview

Infoblox and Rapid 7 integration provides much-needed security orchestration capabilities in today's world of disparate security tools and processes. The integration enables security operations teams to automate asset discovery, gain visibility into today's diverse networks, and improve the efficiency of vulnerability management. When a new device or host joins the network, Infoblox sends a notification to Rapid 7 Nexpose to add to its list of assets. In addition, Infoblox can trigger scanning when new devices join the network or when malicious events are detected, helping identify potential vulnerabilities in near real time. To aid in prioritizing response to issues based on risk, Infoblox shares with Rapid 7 network context and actionable intelligence such as IP address, DHCP fingerprint, lease history, etc. of the devices and hosts.

Background

Today's networks use diverse deployment architectures including physical, virtual, and private/hybrid cloud. Knowing what's on the network at all times can be challenging in diverse networks, and you can't protect what you can't see.

Cybercriminals rely on critical but under-protected network infrastructure such as DNS to infect devices, propagate malware, and exfiltrate data. 91 percent of malware uses DNS to carry out their campaigns and the longer it takes to discover, the higher the cost of damage. Organizations have invested in several security tools as part of a defense-in-depth security strategy. But it is a cumbersome process to assemble data from dissimilar sources and respond to high priority threats fast, making security operations less efficient.

Challenges

- It takes time for security tools to discover when new networks, hosts, and IoTs join the network.
- Malicious activity happening during the scan gap (between consecutive scans) could go undetected and unaddressed.
- There is little to no contextual information on threats, which means security ops teams cannot tackle the important threats first or prioritize scanning of high-risk assets. Instead they spend time perusing mountains of log file entries and alerts.

Infoblox-Rapid 7 Joint Solution

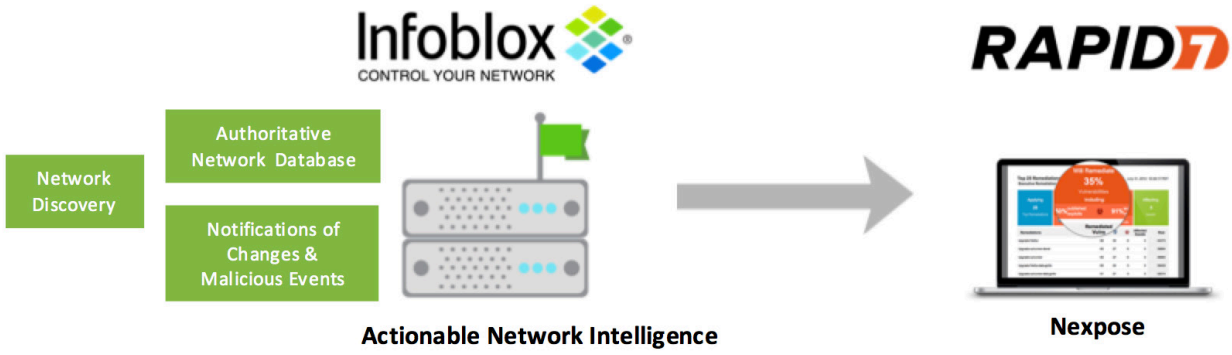

Figure: Infoblox and Rapid 7 together provide automated asset discovery and risk management.

Infoblox
CONTROL YOUR NETWORK

Enabling Security Orchestration with Infoblox and Rapid 7

PARTNER SOLUTION BRIEF

Key Capabilities

Infoblox together with Rapid 7's vulnerability management solution provides security orchestration capabilities with which organizations can automate scanning when new devices/hosts join the network or when malicious activity is detected, even if it is in between scheduled scans. This eliminates the chances of malicious activity going undetected during scan gaps. The outbound notifications from Infoblox to Rapid 7 happen through RESTful APIs.

Asset Discovery and Management

Infoblox provides device discovery and single source of truth for devices and networks. It notifies Rapid 7 Nexpose when new devices join or when new virtual workloads are spun up. Rapid 7 can leverage this for organizing assets, automated tracking, and detailed view of the network.

Malicious Event-based Scanning

Infoblox uses curated threat intelligence and streaming analytics to detect and block data exfiltration and malware communications at the DNS level. It can proactively control the spread of malware such as ransomware and disrupt the cyber kill chain. When such indicators of compromise have been detected, Infoblox can trigger Rapid 7 to scan the compromised assets for vulnerabilities, without having to wait for the next scan window. This helps accelerate remediation and reduces dwell time of the threats.

Compliance and Audit

Infoblox provides complete and up-to-date information about network devices, including non-compliant hosts, for more efficient vulnerability management and compliance processes.

Benefits

Infoblox is the first and only DDI vendor to integrate with Rapid 7 to automate asset management, accelerate remediation, and provide deep visibility. By integrating Infoblox and Rapid 7, customers gain the following:

- **Context-based action**: Vulnerability scanners lack visibility into devices and end hosts including valuable business context such as where and what type of device joined the network or is initiating malicious communications, what department it is in, who it is assigned to, etc. By sharing such actionable network intelligence, Infoblox provides Rapid 7 context around new and/or infected network assets in near real time to help prioritize scanning and remediation. Infoblox provides visibility across a diverse infrastructure—on the premises, private/hybrid or public cloud environments, including visibility into virtual workloads.
- **Security orchestration**: Infoblox's ecosystem integrations and outbound notifications help bridge silos between network and security teams through near real time automation between detection and remediation to ease security operations and minimize issues during scan gaps.
- **Improved efficacy of security investments already made**: Customers have already made big investments in security technologies such as vulnerability management. Infoblox can optimize and improve the efficacy of solutions like Rapid 7.

To learn more, visit www.infoblox.com and http://www.rapid7.com.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com