PARTNER SOLUTION BRIEF

Orchestrating Security Response with Infoblox and Rapid7

Overview

The integration of Infoblox and Rapid7 provides organizations with much-needed security orchestration capabilities in today's world of disparate security tools and processes. Our joint solution enables security operations teams to automate asset discovery, gain a single-pane-of-glass view across diverse network infrastructure and improve the efficiency of vulnerability management. When a new device or host joins the network, Infoblox sends a notification to Rapid7's Nexpose to add that device to its list of assets. Infoblox also triggers Rapid7 to scan for vulnerabilities when new devices join the network or when malicious events occur, helping organizations identify potential security issues in near real time. In addition, Infoblox and Rapid7 integration makes it easier for security teams to prioritize their response to security events. It does so by presenting a clear picture of the risks posed by individual incidents through the automatic sharing of valuable contextual data, such as the IP address, Dynamic Host Configuration Protocol (DHCP) fingerprint and lease history of devices and hosts.

Background and Challenges

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

In addition, hackers and cybercriminals are deliberately targeting critical but under-protected network infrastructure such as the Domain Name System (DNS) to infect devices, propagate malware and exfiltrate data. More than 90 percent of malware uses DNS to carry out campaigns. The longer it takes to discover and respond to such attacks (a concept known as "dwell time"), the higher the cost of damage. Organizations have invested in a broad assortment of security tools as part of their security strategy. But assembling data from such siloed sources is cumbersome and time consuming, making rapid responses to high-priority threats harder to achieve when time is of the essence. Disjointed security tools present several challenges, including:

- The lack of integration and data sharing between security and network tools often causes costly delays in discovering new networks, hosts and Internet of Things (IoT) devices that join the network.
- Malicious activity happening in the gap between scans can go undetected and unaddressed.
- With scant contextual information on threats, security ops teams cannot tackle important threats first or prioritize the scanning of high-risk assets. Instead, they spend valuable time sifting through mountains of log file entries and alerts.

Infoblox - Rapid7 Joint Solution

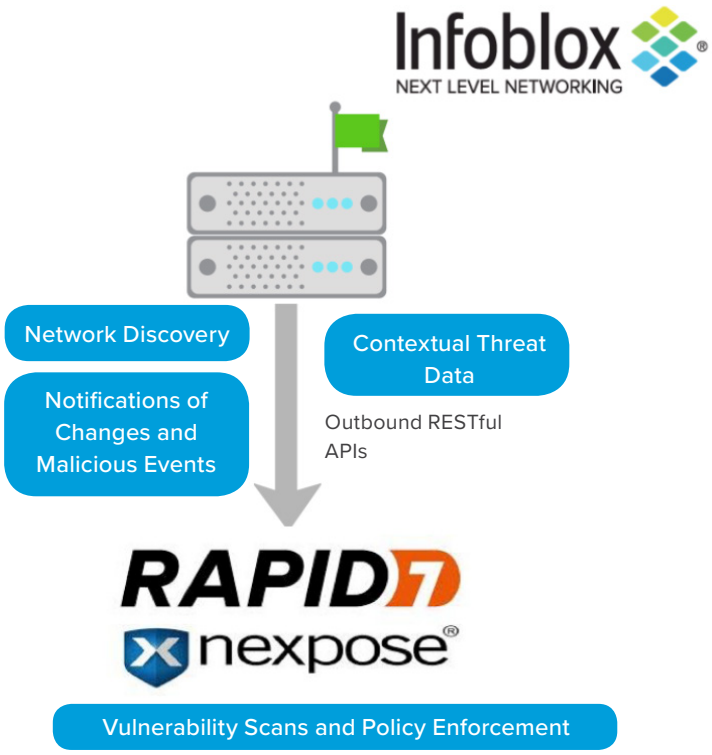

Figure 1: The joint Infoblox and Rapid7 solution orchestrates security response by automating asset discovery, threat prioritization and risk management.

Key Capabilities

In tandem with Rapid7's vulnerability management solution, Infoblox provides security orchestration capabilities that organizations can use to automatically scan new devices and hosts when they join the network or when malicious activity is detected, even between scheduled scans. Such automated scans eliminate the risk of malicious activity going undetected during scanning gaps. Infoblox sends outbound notifications to Rapid7 through RESTful APIs.

Asset Discovery and Management

Infoblox provides automated device discovery and a unified view of devices and networks. It notifies Rapid7's Nexpose when new devices join or when new virtual workloads are spun up. Rapid7 then organizes assets, automates tracking and gives a 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 Infoblox detects such indicators of compromise, it triggers Rapid7 to scan the compromised assets for vulnerabilities, without waiting for the next scan window. This capability helps accelerate remediation and reduces threat dwell time, resulting in greater security operations efficiency.

Compliance and Audit

Infoblox furnishes complete and up-to-date information about network devices, including noncompliant hosts, enabling organizations to boost the efficiency of their vulnerability management and compliance processes.

Benefits

Infoblox is the first and only DNS, DHCP and IP address management (DDI) vendor to integrate with Rapid7 to automate asset management, accelerate remediation and enable centralized network visibility. Through our integrated solution, customers benefit from the following capabilities:

- **Context-based action**: Vulnerability scanners lack visibility into devices and end hosts, including valuable context such as what type of device joined the network and where it resides or the source of malicious communications. By sharing such granular information, Infoblox provides Rapid7 with valuable context about new and infected network assets in near real time, enabling organizations to more accurately prioritize scanning and remediation efforts. Infoblox also provides a consolidated view across diverse infrastructure—on-premises and in private, public, and hybrid cloud environments, including visibility into virtual workloads.
- **Security orchestration**: Infoblox's ecosystem integrations and outbound notifications help eliminate silos between network and security teams, accelerate remediation processes and increase operational efficiency by enabling near real-time automation from initial threat detection through resolution.
- **Improved efficacy of security investments**: Organizations have already invested substantially in security technologies such as vulnerability management. Through a combination of automation and data sharing, Infoblox optimizes and improves the efficacy of solutions such as Rapid7, enabling organizations to gain more value from their existing security investments.

About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,400 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

To learn more, visit www.rapid7.com.

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