SOLUTION NOTE

BOOST CYBER RESILIENCE WITH INFOBLOX AND RAPID7 INTEGRATION

OVERVIEW

The integration of Infoblox Threat Defense™ and Rapid7 Nexpose and InsightVM delivers a comprehensive, automated security orchestration solution that enhances both threat prevention and vulnerability management.

By combining Infoblox's predictive threat intelligence, DNS-based analytics and rich IP address management (IPAM), DNS and DHCP context with Rapid7's deep vulnerability insights and automated response capabilities, security teams gain unified visibility across assets and threats. This enables smarter scan targeting, faster threat detection and accelerated remediation workflows, allowing security and network operations teams to identify, prioritize and neutralize vulnerabilities with unprecedented speed and precision.

CHALLENGES

Modern enterprise networks span physical, virtual and hybrid cloud environments creating a sprawling, dynamic attack surface. Maintaining continuous visibility across this landscape is increasingly difficult, yet essential. After all, organizations cannot protect what they cannot see.

At the same time, cyber adversaries are evolving. AI-driven attackers are exploiting underprotected infrastructure like the DNS to deliver malware, exfiltrate data and evade detection. With over 90 percent of malware leveraging DNS in some way, it has become a critical control point for early threat prevention.

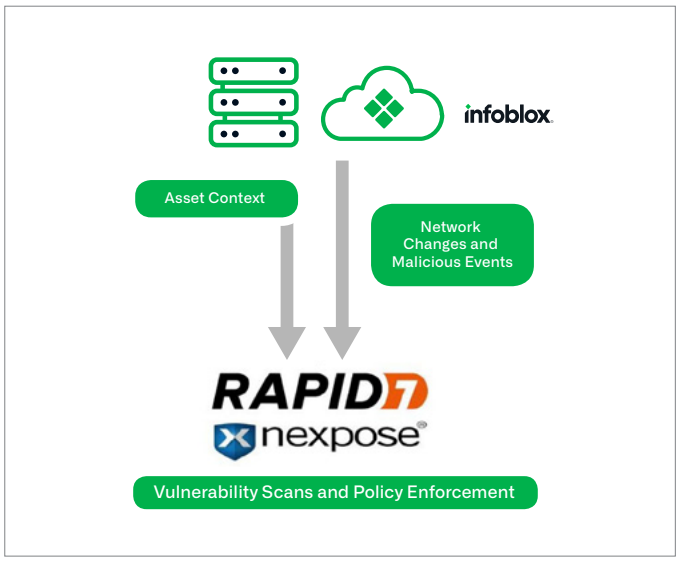
Traditional "detect and respond" tools often miss threats that occur between scans or outside their visibility range. The longer a vulnerability remains undetected, known as dwell time, the greater the risk and cost of damage. Meanwhile, security teams are overwhelmed by fragmented tools and alert fatigue, making it harder to respond quickly and effectively.

Key challenges include:

- **Lack of integration** between network and security tools, delaying the discovery of new assets, including IoT and cloud workloads.
- **Blind spots between scans** increases the threat investigation time for the SOC team when they do not have accurate asset info
- **Insufficient context** around threats, forcing SOC teams to manually correlate data and slowing down prioritization and response
- **Inability to perform the correct depth of scan** for a given circumstance leads to too much overhead

To meet these challenges, organizations benefit from a unified automated approach. This approach leverages DNS as a first line of defense and integrates seamlessly with vulnerability management platforms like Rapid7.

INFOBLOX AND RAPID7 JOINT SOLUTION



KEY CAPABILITIES AND BENEFITS

Infoblox's integration with **Rapid7 Nexpose** and **InsightVM** scanning delivers a unified, preemptive security solution that helps organizations detect, assess and respond to threats before they cause harm. By leveraging DNS as a strategic control point and combining IPAM, DNS and DHCP data with real-time scanning capabilities, this integration automates asset management and accelerates threat response. It also ensures continuous protection across dynamic hybrid environments, including against emerging threats like AI-driven attacks.

Key capabilities and benefits include:

Real-Time Asset Synchronization with Intelligent Grouping

Automatically sync live IPAM data from Infoblox to Rapid7, ensuring only actively used IPs—such as those with MAC addresses—are included. Smart tag-based grouping enables precise scan policies for dynamic and scalable vulnerability management.

Threat-Triggered Scanning for Faster Incident Response

Instantly launch targeted vulnerability scans the moment a threat is detected by Infoblox DNS threat intelligence. Whether it is a malicious domain or suspicious behavior, Rapid7 assesses the exposed asset in real time—accelerating your threat-to-remediation workflow.

Zero-Day Readiness via DHCP-Powered Discovery

Automatically detect and scan any new device as soon as it receives a DHCP lease from Infoblox. No manual effort needed—your network stays continuously protected, even as new endpoints come online.

SOC Insight-Driven Automation to Prioritize Risk

Transform SOC alerts into action. When Infoblox identifies critical behaviors like DNS tunneling or data exfiltration, Rapid7 instantly scans the associated asset, empowering your team to act faster and smarter in high-risk situations.

Fine-Grained Control with Smart Exclusions and Enrichment.

Easily exclude trusted IP ranges from scans while enriching asset records with vulnerability data. Highlight critical risks, enhance reporting and ensure your security teams focus only on what truly matters—without the noise.

CONCLUSION

The integration of Infoblox Threat Defense with Rapid7 InsightVM represents a transformative advancement in cybersecurity operations, offering a unified, automated approach to threat detection, vulnerability management and incident response. By leveraging DNS as a strategic control point and combining it with real-time asset discovery, predictive threat intelligence and event-driven scanning, organizations can significantly reduce dwell time and eliminate blind spots that traditional tools often miss.

This integration empowers security and network operations teams to respond with speed and precision, turning fragmented manual response into automated, streamlined and intelligence-driven processes. With enriched context from IPAM, DHCP and DNS telemetry, teams can prioritize risks more effectively, automate remediation and maintain continuous protection across hybrid and cloud environments.

Ultimately, this joint solution strengthens cyber resilience, improves operational efficiency and delivers measurable outcomes that align with both security and compliance objectives. This helps to ensure organizations are better equipped to defend against today's evolving threat landscape.

To learn more, visit rapid7.com.

PREREQUISITES

Infoblox CSP Requirements

The user must have read and write access to Infoblox SOC Insights and IPAM services.

Rapid7 Requirements

The user must have read and write access to Rapid7 InsightVM and must be authorized to use Rapid7 version 3 APIs.

License Entitlements

IPAM, DHCP, Threat Defense, SOC Insights and Ecosystem.

ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is on a mission to create a safer digital world by making cybersecurity simpler and more accessible. We empower security professionals to manage a modern attack surface through our best-in-class technology, leading-edge research and broad, strategic expertise. Rapid7's comprehensive security solutions help more than 11,000 global customers unite cloud risk management and threat detection to reduce attack surfaces and eliminate threats with speed and precision.[1]

1. Press Release, 2025, *Rapid7 Announces First Quarter 2025 Financial Results*, Rapid7. https://www.rapid7.com/about/press-releases/press-release-rapid7-announces-first-quarter-2025-financial-results/

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250827v1