Infoblox
CONTROL YOUR NETWORK

Automatically Manage Assets and Contain Threats with Infoblox and Tenable

PARTNER SOLUTION BRIEF

Overview

Infoblox and Tenable have joined hands to ease security operations, eliminate silos between network and security tools and provide automatic response to incidents. The integration enables security operations teams to:

- Discover new assets automatically
- Gain visibility and context around new devices or hosts that join the network
- Initiate action in near real-time when threats are discovered
- Enforce Network Access Control policy based on assessment results

When a new device or host joins the network, Infoblox sends a notification to Tenable SecurityCenter to add the newly-discovered device to its list of assets for continuous visibility and monitoring. In addition, when Infoblox DNS security solution detects malicious events, it can trigger SecurityCenter to assess the infected host to help identify potential vulnerabilities in near real time. Acting as the “single source of truth” for network and devices, Infoblox also provides device context such as IP address, MAC address, DHCP fingerprint information, lease history, etc. Combining this rich data, along with SecurityCenter’s ability to manage and analyze vulnerability data across the enterprise,security operations teams are now equipped to quickly identify threats and prioritize response based on risk profile.

Background and Challenges

Security has always been a layered defense approach, which means most organizations have multiple security tools for detecting various threats and responding to them. More often than not though, security tools lack real-time visibility into today’s complex networks that use diverse deployment architectures including physical, virtual and private/hybrid cloud. Discovering new networks, hosts and IoT devices or knowing when virtual workloads are spun up is critical to proactively managing threats and adhering to compliance. Lack of complete and up-to-date information about network devices, compromised hosts, and DNS threats limits effectiveness of vulnerability and compliance assessments.

Another challenge security professionals are faced with is that cybercriminals misuse under-protected network infrastructure like DNS to infiltrate the network and spread malware. 91% of malware uses DNS to carry out their campaigns and the longer it takes to discover, the higher the cost of damage. Securing DNS and informing tools like vulnerability management solutions in near-real time helps to contain threats before they become a serious incident.

Automatically Manage Assets and Contain Threats with Infoblox and Tenable

PARTNER SOLUTION BRIEF

Infoblox-Tenable Joint Solution

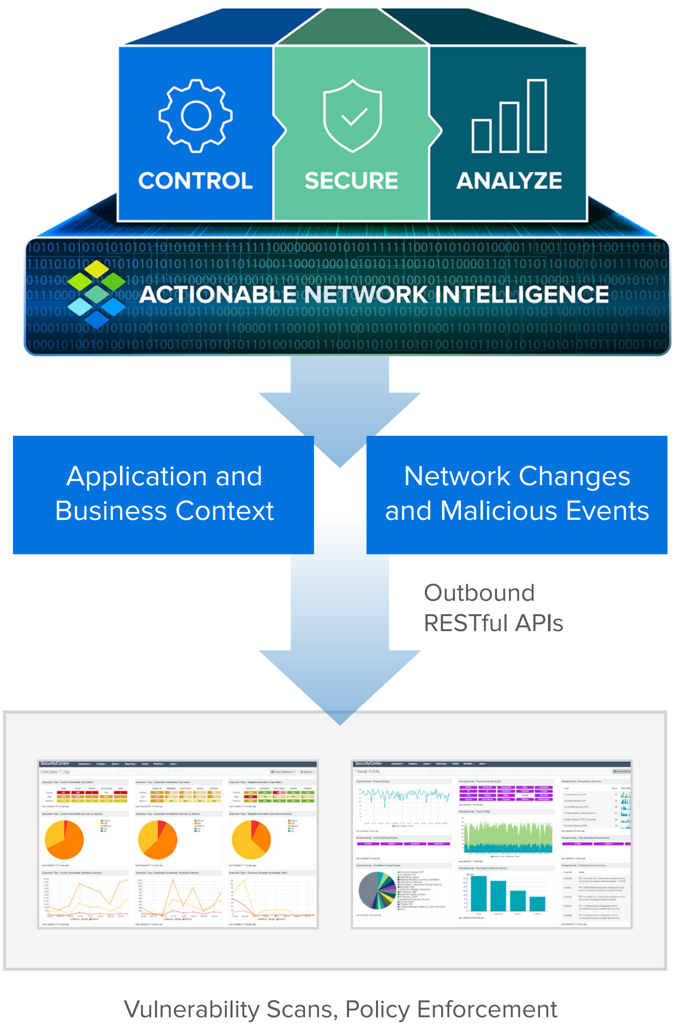

Fig 1: Infoblox and Tenable for Efficient threat containment and compliance

Key Capabilities

Infoblox's integration with Tenable SecurityCenter using outbound APIs enables organizations to eliminate silos between network and security tools by leveraging orchestration to provide continuous visibility, asset discovery and enhanced security.

Network and Device Discovery

Infoblox provides device discovery and acts as the single source of truth for devices and networks using metadata to provide context. Infoblox notifies Tenable SecurityCenter when new devices join the network or when new virtual workloads are spun up. SecurityCenter can leverage this information for organizing assets, automated tracking and a continuous, more detailed view of the network.

On-Demand Scanning Based on Malicious Events

Infoblox detects and blocks data exfiltration and malware communications at the DNS control plane using curated threat intelligence and streaming analytics. When such indicators of compromise (IoCs) are detected, Infoblox triggers SecurityCenter to perform an on-demand vulnerability assessment of the compromised assets. Security teams can also leverage actionable network context for accurate risk assessment and event prioritization to quickly contain threats before they become bigger incidents. In addition, SecurityCenter can help enforce Network Access Control policy based on assessment results.

Security Troubleshooting and Compliance

Infoblox provides historical DNS data for troubleshooting and audit. It helps organizations adhere to compliance mandates by providing up-to-date information about network devices, including non-compliant hosts for more efficient vulnerability management and compliance processes. Once Infoblox notifies SecurityCenter of a non-compliant device, a configuration check can be initiated using one of the numerous audit files available in the SecurityCenter Feed. These configuration checks allow SecurityCenter to provide a unique combination of detection, reporting, and pattern recognization using industry-recognized compliance standards.

Benefits

Infoblox is the first and only DDI vendor to integrate with Tenable to automate asset discovery, provide in-depth and continuous visibility and enhance overall security posture.

Benefits to customers include:

- **Security Orchestration –** By automating response based on new or malicious events in the network, Infoblox and Tenable provide much need security orchestration for today's overburdened security operations personnel. Security teams can now perform vulnerability and compliance assessments based on events in near real time, eliminating any issues that could arise due to blind spots within the network.
- **Context for Prioritization of Threats –** By leveraging DNS, DHCP and IPAM data, security teams can get much needed context around new or unmanaged devices and infected hosts. This rich context can be shared with SecurityCenter to help determine if an asset is vulnerable or out of compliance. These findings can help security teams prioritize action based on actual risk of the asset.
- **Improved ROI of security investments already made –** Many organizations have made investments in leading security tools to address various threats as part of their defense in depth strategy. By combining Infoblox and Tenable SecurityCenter, security teams are able to improve the efficacy of both solutions and thereby improve the ROI of these investments.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 23,000 customers globally in over 150 countries, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

To learn more, visit www.infoblox.com and www.tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

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