SOLUTION NOTE

AUTOMATE ASSET MANAGEMENT AND CONTAIN THREATS USING INFOBLOX AND TENABLE

OVERVIEW

With the partnership between Infoblox and Tenable, organizations can ease security operations, eliminate silos between network and security teams and automate incident response.

Our integration enables organizations to:

- Discover new assets automatically
- Gain a centralized view of new devices and hosts that join the network, along with valuable context
- Initiate action in near real time when threats are discovered
- Enforce Network Access Control (NAC) policy based on assessment results

When a new device or host joins the network, Infoblox notifies Tenable SecurityCenter to add it to its list of assets for continuous visibility and monitoring. In addition, when the Infoblox DNS security solution detects malicious events, it triggers SecurityCenter to assess the infected host to help identify potential vulnerabilities in near real time. Acting as the single source of truth for networks and devices, Infoblox also provides device context, such as IP address, MAC address, DHCP fingerprint information and lease history. Infoblox combines this rich device-related data with SecurityCenter's ability to manage and analyze vulnerability-related data across the enterprise. The powerful combination enables security teams to quickly identify threats and prioritize responses based on risk profile.

BACKGROUND AND CHALLENGES

Many organizations rely on a layered defense approach. Most employ multiple security tools for detecting and responding to various threats. But typically, these tools operate in isolated silos and don't readily exchange information with each other. Security tools also often lack real-time visibility into today's complex networks that use diverse deployment architectures, including physical, virtual and private, public and hybrid clouds. Without clear visibility, it is becoming increasingly challenging to discover new networks, hosts and Internet of Things (IoT) devices or to detect when virtual workloads are spun up. As a consequence, it is becoming more difficult for operations teams to proactively manage network threats and adhere to compliance mandates. In addition, the lack of complete, current information about network devices, compromised hosts and DNS threats limits the effectiveness of vulnerability and compliance assessments.

Adding to the challenges organizations face is that cybercriminals are increasingly targeting under-protected network infrastructure like DNS to infiltrate the network and spread malware. More than 90 percent of malware uses DNS to carry out attacks. The longer it takes to discover and remediate such attacks (known as "dwell time"), the higher the cost of damage. To contain threats before they become serious incidents requires securing DNS infrastructure and enabling incident response tools, such as vulnerability management solutions, to share information on pending and unfolding attacks in near real time.

INFOBLOX-TENABLE JOINT SOLUTION

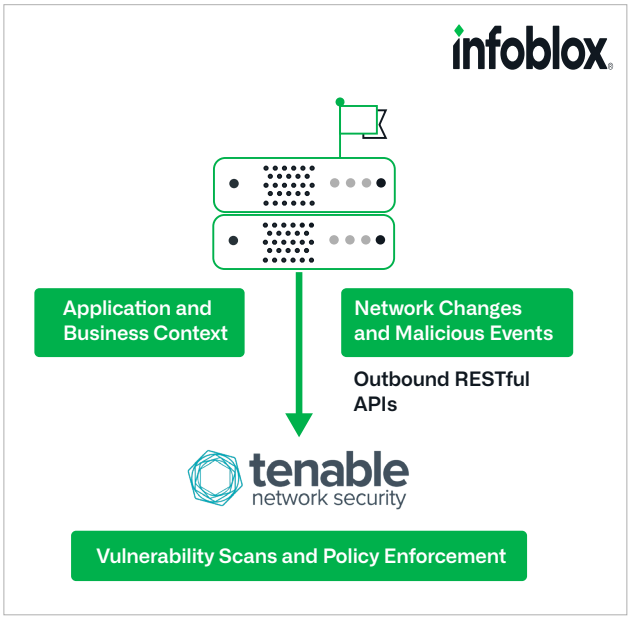

Figure 1: The joint Infoblox and Tenable solution enables efficient threat containment and compliance.

KEY CAPABILITIES

Using outbound APIs, the integration between Infoblox and Tenable SecurityCenter eliminates silos between network and security tools. It enables organizations to better orchestrate security responses by providing continuous visibility, automated 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 and uses metadata to provide valuable network context about network changes and security incidents. In addition, Infoblox notifies Tenable SecurityCenter when new devices join the network or when new virtual workloads are spun up. SecurityCenter uses this information to organize and automatically track assets and provide security teams with a continuous, more detailed view of the network.

On-demand Scanning Based on Malicious Events

Using curated threat intelligence, Infoblox detects and blocks data exfiltration and malware communications at the DNS control plane. When indicators of compromise (IoCs) are detected, Infoblox triggers SecurityCenter to assess the vulnerability of the compromised assets. By providing network context, the joint solution enables security organizations to more accurately assess risks and prioritize events so they can quickly contain threats before they become bigger incidents. In addition, SecurityCenter helps enforce NAC policy based on assessment results.

Security Troubleshooting and Compliance

Infoblox supplies historical DNS data for troubleshooting and auditing. It helps organizations automate and streamline compliance by providing up-to-date information about network devices, including noncompliant hosts. When Infoblox notifies SecurityCenter of a noncompliant device, a configuration check can be initiated using one of the numerous audit files available in the SecurityCenter feed. The configuration checks employ a unique combination of detection, reporting and pattern recognition using industry-approved compliance standards.

BENEFITS

Infoblox is the first and only DNS, DHCP and IPAM (DDI) vendor that integrates with Tenable to automate asset discovery, provide in-depth and continuous visibility and enhance overall security. Through this integration, customers gain:

- **Security orchestration**: By automating responses based on new or malicious events in the network, Infoblox and Tenable furnish essential 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 blind spots within the network and making security operations more efficient.
- **Context for prioritization of threats**: By leveraging DNS, DHCP and IPAM data, security teams gain much-needed context about new or unmanaged devices and infected hosts. They can share this rich context with SecurityCenter to help determine whether an asset is vulnerable or noncompliant. As a result, security teams can better prioritize action based on the actual risk to the asset.
- **Improved ROI from security investments**: As part of their defense strategy, many organizations have invested in leading security tools to address various threats. By combining Infoblox and Tenable SecurityCenter, security teams can enhance the efficacy of both solutions and thereby improve the ROI from security 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.tenable.com.

Contact us: Please email us at sales@tenable.com or visit tenable.com/contact.

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

Version: 20230918v1