SOLUTION NOTE

ACCURATE ASSET DISCOVERY AND THREAT CONTAINMENT USING INFOBLOX AND TENABLE

Automate remediation and simplify compliance

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 Security Center 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 Security Center to assess the infected host to help identify potential vulnerabilities in near-real time. Acting as the authoritative source of truth for networks and devices, Infoblox provides device context, such as IP address, MAC address, Dynamic Host Configuration Protocol (DHCP) fingerprint information and lease history. Infoblox combines this rich device-related data with Security Center's ability to manage and analyze vulnerability-related data across the enterprise. This powerful combination enables security teams to quickly identify threats and prioritize responses based on risk profile.

KEY BENEFITS

- **Enhanced Visibility:** Gain full visibility into new networks, hosts and all devices joining the network to gain a holistic, consolidated view across diverse network infrastructures.
- **Automated Remediation and Risk Management:** Bridge silos between network and security teams to accelerate remediation using near-real time automation from incident detection through resolution.
- **Improved Efficacy of Security Investments:** Proactively trigger on-demand vulnerability scanning when new devices join the network or when malicious events are detected.

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. Consequently, it is becoming more difficult for operations teams to manage network threats and adhere to compliance mandates proactively. In addition, the lack of complete, current information about network devices, compromised hosts and Domain Name System (DNS) threats, limits the effectiveness of vulnerability and compliance assessments.

Adding to organizations' challenges, cyber criminals increasingly target 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. Controlling threats before they become serious incidents requires securing DNS infrastructure and enabling incident response tools, such as vulnerability management solutions, to share real-time information on pending and unfolding attacks.

INFOBLOX-TENABLE JOINT SOLUTION

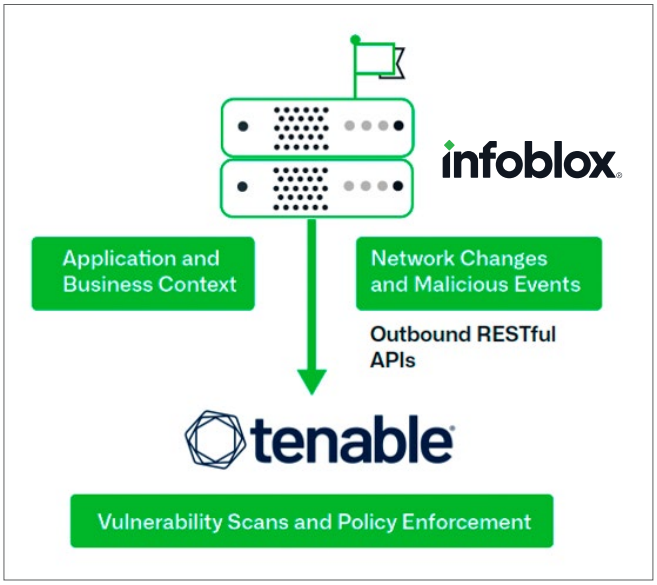

Figure 1: The joint Infoblox and Tenable solution automates asset tracking, risk management, incident detection and remediation.

KEY CAPABILITIES

Using outbound application programming interfaces (APIs), the integration between Infoblox and Tenable Security Center 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, 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 Security Center when new devices join the network or new virtual workloads are spun up. Security Center uses this information to organize and automatically track assets, providing 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 Security Center 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 more significant incidents. In addition, Security Center helps enforce Network Access Control (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 non-compliant hosts. When Infoblox notifies Security Center of a non-compliant device, a configuration check can be initiated using one of the numerous audit files in the Security Center feed. The configuration checks employ a unique combination of detection, reporting and pattern recognition using industry-approved compliance standards.

BENEFITS

Infoblox is a global 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 the following benefits:

Security Orchestration: By automating responses based on new or malicious network events, Infoblox and Tenable furnish essential security orchestration for today's overburdened SecOps 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 SecOps more efficient.

Context and Prioritization of Threats: By leveraging DDI data, security teams gain much-needed context about new or unmanaged devices and infected hosts. They can share this rich context with Security Center to help determine whether an asset is vulnerable or non-compliant. Infoblox can turn vast amounts of event, network, ecosystem and DNS intelligence data into critical, actionable insights to remove blind spots and increase the ability to understand DNS-based attacks fully. As a result, security teams can better prioritize action based on the actual risk to the asset and gain greater efficiency.

Improved Return on Investment (ROI) From Security investments: Many organizations have invested in leading security tools to address various threats as part of their defense strategy. By combining Infoblox and Tenable Security Center, security teams can enhance the efficacy of both solutions and thereby improve the ROI from security investments.

CONCLUSION

Due to siloed security tools and a need for more automation, organizations need help gaining visibility into devices and quickly responding to threats. The Infoblox and Tenable joint solution combines DNS visibility and security, and advanced vulnerability scanning to automate remediation and streamline compliance by automating asset tracking, risk management, incident detection and remediation. The integrated solution enhances SecOps' efficiency and unlocks significant benefits, including faster response, reduced complexity and a quicker ROI for the IT tech stack.

ABOUT TENABLE

Tenable® is the Exposure Management company. Approximately 44,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 65 percent of the Fortune 500, approximately 50 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

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: 20240719v1