SOLUTION NOTE

ACCURATE ASSET DISCOVERY AND THREAT CONTAINMENT USING INFOBLOX AND QUALYS

Automate remediation and simplify compliance

The Infoblox and Qualys joint solution merges advanced vulnerability scanning capabilities and industry-leading Domain Name System (DNS) visibility and security, enabling incident response teams to automate remediation and streamline compliance activities.

The solution's integrated capabilities provide organizations with a centralized view of network assets while enabling them to boost the efficiency of their existing security investments. The integration with Infoblox proactively alerts security analysts on critical threats and provides visibility into malicious domains and infected devices, including contextual information, such as where infected devices appear on the network and to whom devices are assigned. The integration with Qualys also enables customers to automatically trigger scanning when new devices join the network or as malicious events are detected. These capabilities combine near–real-time visibility and automation, making it easier for organizations to manage assets and remediate threats. The outcome is greater efficiency for SecOps.

CHALLENGES

Today's progressively complex networks use diverse deployment architectures, including physical, virtual and private/hybrid cloud infrastructure. In such heterogeneous network environments, it is becoming more difficult for organizations to gain visibility into devices and end hosts.

Meanwhile, intruders and cyber criminals increasingly rely on critical network infrastructure such as DNS to infect devices, propagate malware and exfiltrate data; over 90 percent of malware uses DNS to carry out campaigns. The longer it takes to discover and remediate such attacks (a concept known as "dwell time"), the higher the cost of damage. Organizations have invested in advanced security technologies as part of an in-depth security strategy. Still, ultimately, their ability to respond quickly to high-priority threats is put in jeopardy because their security tools and systems are siloed, poorly integrated and cumbersome, resulting in the following challenges:

- Inability to quickly discover when new networks, hosts and Internet of Things (IoT) devices join the network because discovery is not automated.
- Incident response teams can't quickly identify and remedy breaches when malware or other security threats compromise a host because of the lack of automation or security system integration.
- With little to no information on threats' priorities, SecOps teams cannot tackle important threats first or prioritize scanning of high-risk assets. Instead, they must sort through mountains of log file entries and alerts.

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.

INFOBLOX-QUALYS JOINT SOLUTION

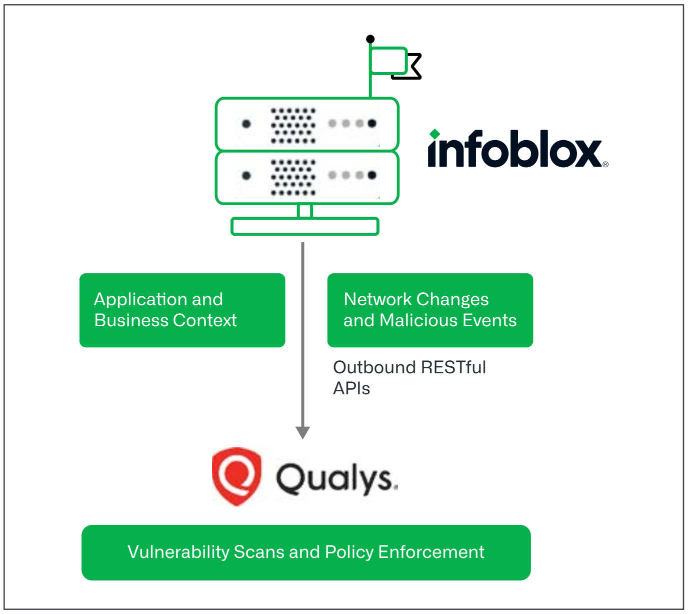
infoblox
Application and Business Context
Network Changes and Malicious Events
Outbound RESTful APIs
Qualys
Vulnerability Scans and Policy Enforcement

Figure 1: The joint Infoblox and Qualys solution automates asset tracking, risk management, incident detection and remedation

KEY CAPABILITIES

By combining the leading Infoblox DNS solutions with the leading vulnerability management solution from Qualys, organizations can automate scanning when new devices join the network or when malicious activity is detected. The outbound notifications from Infoblox to Qualys happen through RESTful application programming interfaces (APIs).

Asset Management

Infoblox provides device discovery and the authoritative source of truth for devices and networks, which Qualys can leverage to organize assets, automate tracking and gain a detailed network view. Qualys and Infoblox customers can create and delete asset groups, enable and disable IPs for scanning, create host assets and authentication records, and enable scanning—all from the Infoblox console. They can also utilize Qualys's comprehensive scanning technology to verify IT assets before being allowed on a network.

Malware, Suspicious Domains and Data Exfiltration Threat Identification

Infoblox strengthens defenses against ransomware, suspicious domains and other advanced attacks by illuminating hidden threat signals in DNS traffic. It monitors attacker infrastructure using original DNS-hunted threat intelligence and disrupts command-and-control (C&C) communications between devices and malicious and suspicious destinations. As a result, organizations can proactively limit the spread of malware, such as ransomware, that uses DNS pathways.

Infoblox's DNS Detection and Response (DNSDR) solution, BloxOne Threat Defense, enhanced with SOC Insights, automatically mines massive amounts of DNS threat intelligence and asset data to correlate and prioritize actionable responses to threats. The solution turns vast amounts of event, network, ecosystem and DNS intelligence data into actionable insights to elevate SecOps efficiency. The rich security data generated by BloxOne Threat Defense with SOC Insights removes blind spots and increases the ability to fully understand DNS-based attacks.

Further, Infoblox Threat Insight detects and blocks data exfiltration via DNS using streaming analytics and automation, and can scale protection to various parts of the network. Infoblox readily shares indicators of compromise (IoCs) related to malicious communications and data exfiltration with Qualys for further analysis and remediation. Through this data-sharing arrangement, organizations can accelerate remediation and reduce the dwell time of the threats, thereby enhancing the efficiency of SecOps.

Compliance and Audit

When new devices join the network—whether in physical, virtual or cloud environments—Infoblox automatically triggers Qualys to perform security and compliance scans before they are allowed on the network. When any new threats in the network occur, automatic scanning of an appliance ensures customers that the asset complies with security policy. Qualys compliance reports can assist auditors with documentation for multiple regulatory and compliance initiatives, such as the Payment Card Industry Data Security Standard (PCI DSS), Healthcare Information Portability and Accountability Act (HIPAA), and others.

BENEFITS

Infoblox is a global DNS, DHCP and IP address management (DDI) vendor to integrate with Qualys to improve network visibility, automate asset management and remediation, reduce risk and increase compliance. Through the Infoblox and Qualys integration, customers gain the following benefits:

- **Enhanced Visibility:** Vulnerability scanners lack visibility into devices and end hosts, including identifying information, such as an IP or MAC address and DHCP lease history, and are unaware of DNS security threats in the network. Infoblox enables visibility into new networks, hosts and IoT devices that join the network through outbound notifications to Qualys using RESTful APIs. Infoblox also automatically scans all new devices connected to a network and reveals malicious activities for further scanning, analysis and remediation. With Infoblox, organizations gain a holistic, consolidated view across their diverse infrastructure—including on-premises and private, public and hybrid cloud environments.
- **Automated Remediation and Risk Management:** Infoblox's ecosystem integrations and outbound notifications help 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:** Organizations have already invested substantially in security technologies such as vulnerability management. Infoblox optimizes and enhances the effectiveness of solutions such as Qualys, by triggering on-demand scanning when new devices join the network or when malicious events are detected. It also furnishes valuable context for scanning prioritization by providing information such as where devices join the network, who those devices are assigned to and the source of malicious communications.

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 Qualys 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 return on investments for the IT tech stack.

ABOUT QUALYS

Qualys, Inc. (NASDAQ: QLYS) is a leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes and substantial cost savings. For more information, please visit www.qualys.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: 20240724v4