PARTNER SOLUTION NOTE

AUTOMATING REMEDIATION AND SIMPLIFYING COMPLIANCE WITH INFOBLOX AND QUALYS

OVERVIEW

The Infoblox and Qualys joint solution merges advanced vulnerability scanning capabilities and industry-leading DNS security, enabling security and 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 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. With this information, security teams can better prioritize responses. The integration with Qualys enables Infoblox 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 that makes it easier for organizations to manage assets and remediate threats. The outcome is greater efficiency for security operations.

BACKGROUND AND CHALLENGES

Today's increasingly 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 cybercriminals increasingly rely on critical network infrastructure such as DNS to infect devices, propagate malware and exfiltrate data; more than 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. But 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 aren't able to 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 the priority of threats, security ops 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.

INFOBLOX-QUALYS JOINT SOLUTION

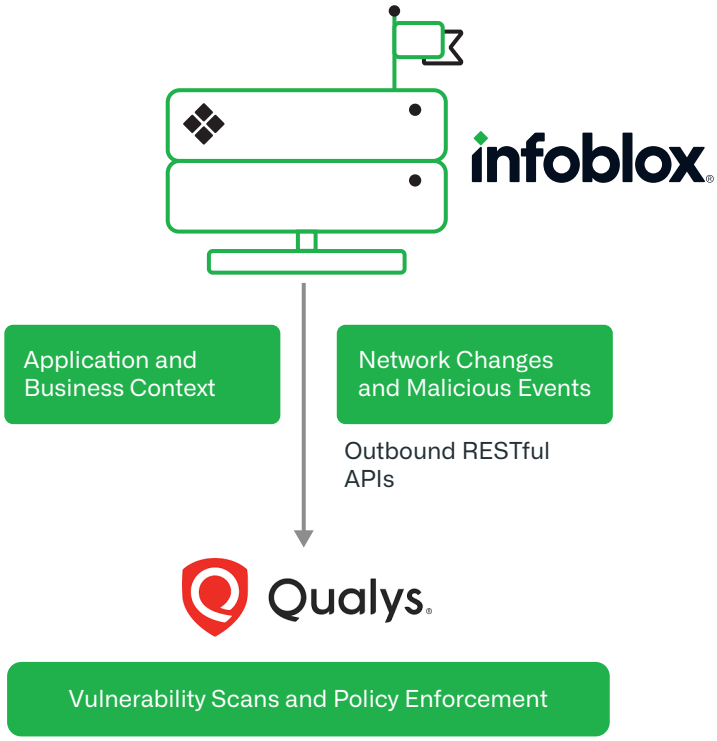

Figure 1: The joint Infoblox and Qualys solution automates asset tracking, risk management, incident detection and remediation.

KEY CAPABILITIES

By combining the leading Infoblox DNS solution 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 APIs.

Asset Management

Infoblox provides device discovery and a single source of truth for devices and networks, which can be leveraged by Qualys to organize assets, automate tracking, and gain a detailed view of the network. Qualys and Infoblox customers can create/delete asset groups, enable and disable IPs for scanning, create host assets and authentication records and enable scanning — all from the Infoblox console, utilizing 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 your defenses against ransomware, suspicious domains and other advanced attacks by illuminating hidden threat signals in your DNS traffic. It does so by monitoring attacker infrastructure using original DNS-hunted threat intelligence and disrupting command-and-control (C&C) communications between devices and malicious/suspicious destinations. As a result, organizations are able to proactively limit the spread of malware, such as ransomware that uses DNS pathways.

Infoblox Threat Insight detects and blocks data exfiltration via DNS using a combination of 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 are able to accelerate remediation and reduce the dwell time of the threats, thereby enhancing the efficiency of security operations.

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 PCI, HIPAA and others.

BENEFITS

Infoblox is the first and only 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 IP or MAC address and DHCP lease history, and are unaware of DNS security threats in the network. Through outbound notifications to Qualys using RESTful APIs, Infoblox enables visibility into new networks, hosts and IoT devices that join the network. 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 improves the efficacy 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.

ABOUT QUALYS

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, SecureWorks, Fujitsu, HCL Comnet, Infosys, NTT, Optiv, Tata Communications, Verizon, and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

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

+1.408.986.4000
www.infoblox.com

Version: 20240315v1