Automate Remediation and Ease Compliance with Infoblox and Qualys

PARTNER SOLUTION BRIEF

Overview

Infoblox and Qualys together enable security and incident response teams to leverage the integration of vulnerability scanners and DNS security to enhance visibility, automate remediation, and improve the efficacy of security investments customers have already made. Infoblox provides visibility into malicious domains and infected devices, including contextual information such as where on the network the infected device is, what department, who the device is assigned to, etc. for prioritizing response. The integration with Qualys enables Infoblox customers to automatically trigger scanning when new devices join the network or when malicious events are detected, helping with asset management and remediation through near real time visibility and automation.

Background

Today's networks are increasingly complex and use diverse deployment architectures including physical, virtual, and private/hybrid cloud. Getting visibility into devices and end hosts in a diverse and complex network is challenging.

Meanwhile intruders and cybercriminals rely on critical network infrastructure such as DNS to infect devices, propagate malware, and exfiltrate data. 91% of malware uses DNS to carry out campaigns and the longer it takes to discover, the higher the cost of damage. Organizations have invested in advanced security technologies as part of a defense-in-depth security strategy. While they try to connect the various systems, it is a cumbersome process to assemble data from dissimilar sources and respond to high priority threats quickly.

Challenges

- Discovering when new networks, hosts, and IoTs join the network takes time and is not automated.
- Once a host is compromised by malware or other security threats, the ability to quickly identify and remedy the breach is paramount, but not easy.
- There is little to no information on priority of threats, which means security ops teams cannot tackle the important threats first or prioritize scanning of high-risk assets. They spend time sorting through mountains of log file entries and alerts.

Infoblox-Qualys Joint Solution

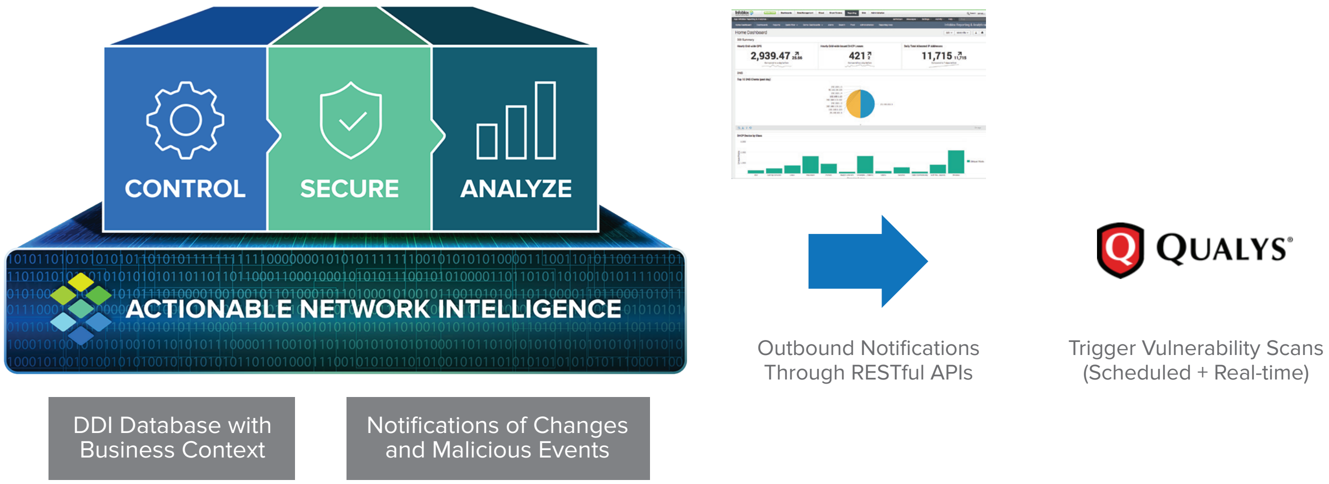
CONTROL
SECURE
ANALYZE
ACTIONABLE NETWORK INTELLIGENCE
DDI Database with Business Context
Notifications of Changes and Malicious Events
Outbound Notifications Through RESTful APIs
QUALYS
Trigger Vulnerability Scans (Scheduled + Real-time)

Figure 1: Infoblox and Qualys together provide automated asset management, remediation, and risk management.

Automate Remediation and Ease Compliance with Infoblox and Qualys

PARTNER SOLUTION BRIEF

Key Capabilities

By combining the leading Infoblox DNS solution with the leading vulnerability management solution, 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 for organizing assets, automated tracking, and a detailed view of the network. Joint Qualys and Infoblox customers can create/delete asset groups, enable and disable IP's for scanning, create the host assets and authentication records, and enable scanning all from the InfoBlox console, utilizing Qualys' comprehensive scanning technology to verify IT assets before being allowed on a network.

Malware and Data Exfiltration Threat Identification

Infoblox uses advanced threat intelligence to detect and control malware communications at the DNS level by disrupting C&C communications. It can proactively control the spread of malware such as ransomware and others that use DNS.

Infoblox Threat Insight is a unique and advanced technology that uses streaming analytics to detect and block data exfiltration via DNS and scales the protection to various parts of the network. These indicators of compromise related to malicious communications and data exfiltration can be easily shared with Qualys for further analysis and remediation.

Compliance and Audit

Infoblox triggers Qualys when new devices join the network–physical, virtual, cloud–to check for security and compliance posture before these devices are allowed on the network. In case of any new threats detected in the network, automatic scanning of an appliance can be scheduled so a customer can be sure that the asset is compliant with security policy. Qualys compliance reports can assist auditors with documentation for multiple regulatory and compliance initiatives including PCI, HIPAA, and others.

Benefits

Infoblox is the first and only DDI vendor to integrate with Qualys to improve visibility, automate asset management and remediation, reduce risk, and ease compliance. By integrating Infoblox and Qualys, customers gain the following:

- **Visibility**: Vulnerability scanners lack visibility into devices and end hosts including identifying information such as IP address, MAC address, device type, DHCP lease history, etc. and are unaware of DNS security threats in the network. Infoblox provides outbound notifications to Qualys using RESTful APIs to provide visibility into new networks, hosts, and IoTs that join the network, and automatically scan all new devices connected to a network and provides visibility into malicious activities for further scan, analysis, and remediation. Infoblox provides visibility across a diverse infrastructure–on premises, private/hybrid, or public cloud environments.
- **Automated remediation and risk management**: Infoblox's ecosystem integrations and outbound notifications help bridge silos across network and security teams to accelerate remediation through near real time automation between detection and remediation to ease security operations.
- **Improved efficacy of security investments already made**: Customers have already made big investments in security technologies such as vulnerability management. Infoblox can optimize and improve 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 provides valuable business context for scanning prioritization by providing information on where and what type of device joined the network or is initiating malicious communications, what department it is in, who it is assigned to, etc. via extensible attributes.

To learn more, visit www.infoblox.com and www.qualys.com.

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.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com