SOLUTION NOTE

INFOBLOX AND FORESCOUT: ENABLING AUTOMATIC VISIBILITY INTO NETWORK AND SECURITY EVENTS FOR CONSISTENT POLICY ENFORCEMENT

OVERVIEW

Network landscapes are rapidly changing, driven by trends such as digital transformation, data center evolution, cloud adoption and the Internet of Things (IoT). As a result of these trends, networks have grown more complex and their attack surfaces have expanded. Against this backdrop, it is becoming increasingly challenging for organizations to gain up-to-date visibility into what is on their networks— whether physical, virtual or cloud—and to apply appropriate policies.

Integration between Infoblox and ForeScout helps address these challenges and makes the job of security operations much easier. Our joint solution leverages the power of ForeScout's continuous, agentless visibility and control of network-connected devices with Infoblox's critical information from its DNS, DHCP and IPAM services, together known as DDI. With this integration, security operations teams can:

- Enrich ForeScout with information from Infoblox about IPAM and DNS security events
- Consistently set and enforce security and network access control policies
- Streamline compliance reporting
- Use ForeScout to automatically respond to threats, including malicious communications and DNS-based data exfiltration, detected by BloxOne™ Threat Defense suite

Infoblox publishes DDI information using outbound APIs and the ForeScout® Open Integration Module (OIM). ForeScout OIM allows technology partners, such as Infoblox, to provide information to ForeScout CounterACT® that can enhance CounterACT device insight and security policies; those policies can drive automated policy-based network and device controls. By enriching ForeScout CounterACT with Infoblox IPAM data, security teams can set control policies that are consistent across both systems. In addition, when BloxOne Threat Defense detects malicious events, it sends triggers to ForeScout CounterACT to take corrective action such as blocking the offending device from network access until it is remediated. Infoblox provides additional context such as DHCP fingerprint information and lease history of the devices and hosts to help security operations teams prioritize responses based on risk profile.

INFOBLOX-FORESCOUT JOINT SOLUTION

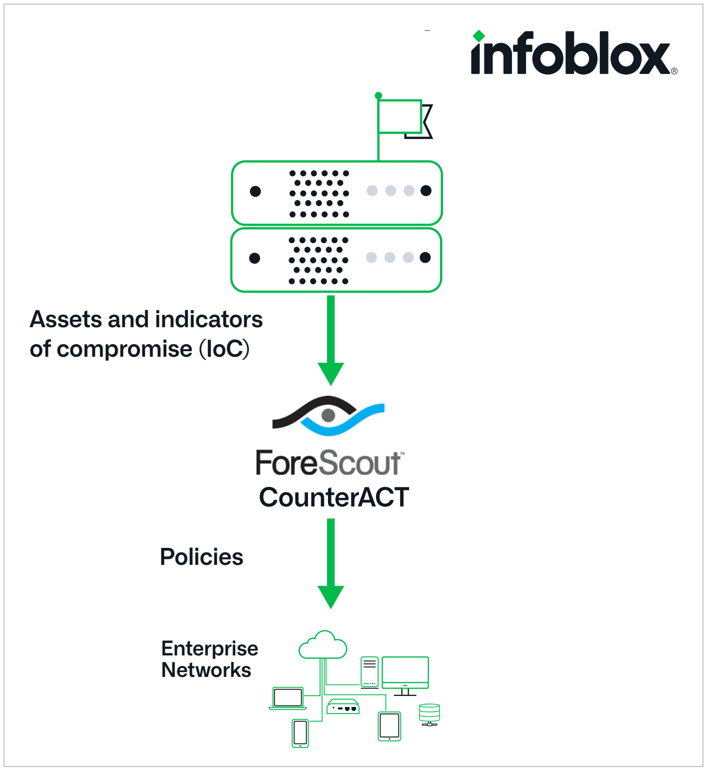

Figure 1: Infoblox and ForeScout enable organizations to automate visibility and achieve consistent policy enforcement.

KEY CAPABILITIES

The Infoblox integration with ForeScout CounterACT uses outbound APIs and ForeScout OIM, which enables organizations to eliminate silos between network and security tools. It offers a single, centralized view of devices and infected hosts present in the network.

Enrichment of Real-time Network Intelligence

Infoblox enriches ForeScout CounterACT with DDI data, which serves as the single source of truth for inventory of real-time connected devices across heterogeneous networks, including metadata. This data furnishes ForeScout CounterACT with additional contextual network intelligence, such as DHCP lease data, including time of issue and length of lease. The additional intelligence allows security administrators to fine-tune ForeScout CounterACT network access policies based on lease terms and optimize responses to security events.

Notification to ForeScout of Infoblox Secure DNS Events

Infoblox detects and blocks data exfiltration and malware communications at the DNS control plane using curated threat intelligence and streaming analytics. When Infoblox Secure DNS detects indicators of compromise (IoCs), it sends triggers to ForeScout CounterACT, which then takes automated policy-driven corrective action, such as quarantining the infected device until it is remediated. The integration enables ForeScout CounterACT to automatically respond to threats detected by Infoblox Secure DNS solutions, reducing time and need for human intervention to respond to threats. By providing rich network context, Infoblox and ForeScout enable security teams to accurately assess risk and better prioritize events. As a result, they can rapidly contain threats and drastically reduce risk.

BENEFITS

The combination of Infoblox's DDI insight and ForeScout's extensive networked-device visibility and policy-driven controls helps joint customers with the following benefits:

- **Reduced time to containment**: To rapidly contain threats, ForeScout automates policy-driven responses to malicious events detected by BloxOne Threat Defense suite, including malware activity and DNS-based data exfiltration. Such orchestration reduces the burden on security teams while ensuring timely response to security and network events and improves the efficiency of security operations.
- **Consistent policy enforcement**: Sharing Infoblox DDI information with ForeScout allows security teams to ensure consistent policy enforcement across the two platforms to optimize network access controls and automate policydriven incident responses.
- **Context for prioritization of threats**: By leveraging DNS, DHCP and IPAM data, security teams obtain much-needed context about infected hosts. This context helps security teams prioritize incidents and initiate appropriate actions based on actual risk.
- **Improved ROI from security efforts**: Many organizations have invested in leading security tools. The ForeScout and Infoblox integration enhances the efficacy of such tools and boosts the ROI from security investments.

ABOUT FORESCOUT

ForeScout Technologies is transforming security through visibility, providing agentless visibility and control of traditional and IoT devices the instant they connect to the network. ForeScout technology works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. See devices. Control them. Orchestrate system wide threat response.

To learn more, visit www.forescout.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: 20230915v1