Infoblox and ForeScout: Automatic Visibility Into Network and Security Events for Consistent Policy Enforcement

PARTNER SOLUTION BRIEF

Overview

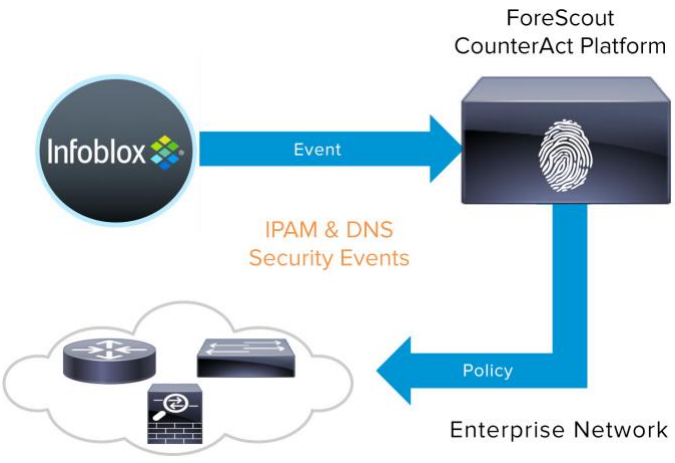
Network landscapes are rapidly evolving, driven by trends like digital transformation, data center evolution, cloud, and the Internet of Things (IoT). What these trends have done is make the network more complex and the attack surface more vast. It gets challenging to get up-to-date visibility on what is on the network – physical, virtual or cloud – so that appropriate policies can be applied.

Infoblox and ForeScout help address these challenges and make the job of security operations much easier. The integration leverages the power of ForeScout's continuous, agentless visibility and control of network connected devices with InfoBlox's critical information from its DNS, Dynamic Host Configuration Protocol (DHCP) and IPAM services, together knowns as DDI. Combining Infoblox and ForeScout information enables security teams to set and enforce consistent policies and streamline compliance reporting. The integration enables security operations teams to:

- Enrich ForeScout with IPAM and DNS security events received from Infoblox
- Consistently set and enforce security and network access control policies
- Have ForeScout automatically respond to threats detected by InfoBlox ActiveTrust suite including malicious communications and DNS based data exfiltration

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 then be used to enhance CounterACT device insight and security policies, which 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 Infoblox ActiveTrust detects malicious events, it can send triggers to ForeScout CounterACT to take corrective action such as blocking the offending device from network access until it is remediated. Infoblox also provides additional context such as DHCP fingerprint information and lease history of the devices and hosts to help security operations teams prioritize response based on risk profile.

Infoblox-ForeScout Joint Solution



Infoblox and ForeScout for Automated Visibility and 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 by leveraging orchestration.

Enrichment of Real-time Network Intelligence Infoblox enriches ForeScout CounterACT with DDI (DNS, DHCP and IPAM) data, which is a single source of truth for inventory of real-time connected devices across heterogeneous networks , including metadata. This provides ForeScout CounterACT with additional contextual network intelligence such as DHCP lease data, including time of issue and length of lease. This additional intelligence allows security administrators to fine tune ForeScout CounterACT network access policies based on lease terms and optimize security event response processes.

Infoblox and ForeScout: Automatic Visibility Into Network and Security Events for Consistent Policy Enforcement

PARTNER SOLUTION BRIEF

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 can send triggers to ForeScout CounterACT. CounterACT can then take automated policy-driven corrective action like quarantine 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. The rich actionable network context from both Infoblox and ForeScout enables security teams to accurately assess risk and prioritize events. As a result, threats are rapidly contained and risk is drastically reduced.

Benefits

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

- **Reduced Time to Containment** – Threats are rapidly contained by having ForeScout automate policy-driven responses to malicious events detected by Infoblox ActiveTrust 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.
- **Consistent Policy Enforcement** – The sharing of Infoblox DDI information with ForeScout allows security teams to ensure consistent policy enforcement across Infoblox and ForeScout to optimize network access controls and automate policy-driven incident responses.
- **Context for Prioritization of Threats** – By leveraging DNS, DHCP and IPAM data, security teams can get much needed context around infected hosts. This context helps security teams to prioritize incidents and initiate the right actions based on actual risk.
- **Improved ROI of Security Investments Already Made** – Many organizations have made investments in leading security tools. Both ForeScout and Infoblox integrations improve the efficacy of such tools and thereby improve the ROI of security investments.

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

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 systemwide threat response.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

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