Forescout eyeExtend

for IBM® QRadar®

Improve situational awareness, prioritize incidents and accelerate response

Organizations use IBM QRadar to gather, analyze and correlate data from a wide variety of data sources for security monitoring, incident investigation and compliance reporting. But in the absence of complete device visibility across managed and unmanaged devices—including bring your own device (BYOD), transient and Internet of Things (IoT) devices—the data analysis is unable to produce an accurate security snapshot of your network. By combining the Forescout platform's complete device visibility with IBM QRadar's data analytics, Forescout eyeExtend for IBM QRadar allows security managers to achieve a broader understanding of their security posture, prioritize incidents and respond more quickly to mitigate a range of security issues. Organizations benefit by optimizing time to insight, achieving quicker incident response and realizing strengthened network security.

Challenges

- Gaining real-time device visibility across managed and unmanaged devices across IT and OT infrastructures for better situational awareness
- Improving the accuracy and reliability of QRadar's correlation for anomaly detection, incident prioritization and investigation
- Accelerating response time to prevent lateral spread of threats into the network

The Solution

Forescout eyeExtend for IBM QRadar combines complete device visibility, in-depth device context, a broad array of controls and automated response capabilities from Forescout platform with QRadar's data correlation, analytics and incident management technology.

Any attempt to manage security risks must start with knowing who and what is on your network, including visibility into networked device compliance with your security standards. Through its agentless architecture and real-time continuous monitoring, the Forescout platform provides QRadar with up-to-date insight into all IP-connected devices—managed and unmanaged—that touch the extended network across information technology (IT) and operational technology (OT) networks. The comprehensive and rich contextual device data provides a complete picture of your entire enterprise attack surface, helps reduce time to insight, and facilitates investigations. The in-depth device insight contributes to more precise correlation and prioritization of alerts and events, enabling your security team to focus their time and attention on the most critical security incidents. The Forescout platform also helps streamline security operations by automating policy-based actions—limiting access of the device to the network based on incident severity feed from QRadar in real time.

Benefits

- <) Expand the scope of IBM QRadar's security analytics with complete device and network insight on all IP-connected devices
- <) Increase operational efficiency by helping to prioritize incidents accurately with Forescout's rich contextual device data in real time
- <) Minimize security risk by automating incident response to reduce mean time to respond (MTTR) and rapidly remediate threats

Highlights

- <) Broad security posture awareness, including complete device visibility across managed and unmanaged devices, device compliance status, registered/guest status and network access patterns
- <) Continuous IBM QRadar WinCollect agent health assessment
- <) Dynamic isolation, quarantining or blocking of compromised devices for threat containment

Forescout eyeExtend for IBM QRadar helps improve situational awareness, prioritizes incidents and automates remediation to enhance overall IT and security operations efficiency, and minimizes security and business risk to an organization.

Use Cases

Enhance incident correlation and prioritization

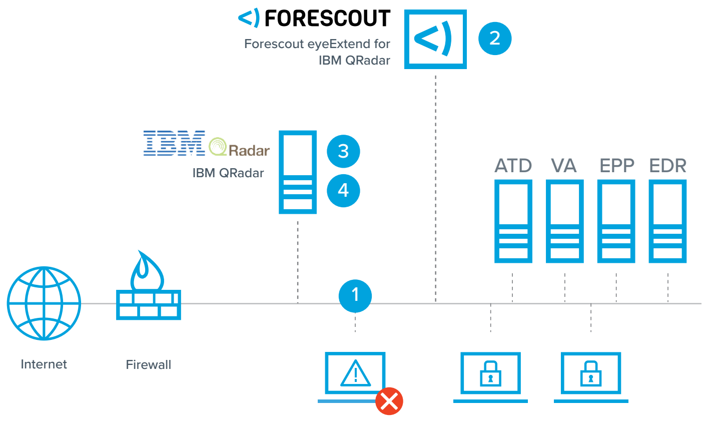
The Forescout platform provides high-value user, network and device context to IBM QRadar. The additional device information from the Forescout platform includes user information, device type, device configuration, network access patterns over time, device compliance status and significant changes in device processes and applications. IBM QRadar correlates rich device context from the Forescout platform with other data sources to better identify and prioritize incidents. IBM QRadar leverages this additional insight to determine if an incident is actually malicious or violates policy and escalates or reduces the severity of the event based on the device and user context.

Continuously assess IBM QRadar WinCollect agent health and compliance

eyeExtend for IBM QRadar verifies that IBM QRadar WinCollect agents, which collect event logs on Windows devices, are installed, configured and properly running on all Windows devices at all times. If a connecting Windows device does not comply with security policy, Forescout platform can facilitate remediation.

Automate incident response

IBM QRadar can trigger Forescout platform to take policy-based response actions such as isolating, quarantining or blocking potentially compromised or noncompliant devices, depending on the severity of the violation. For example, when IBM QRadar detects, via firewall log correlation, a targeted denial of service (DoS) attack, it can direct Forescout platform to have the the firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.



1. Forescout platform discovers, classifies and assesses devices as they connect to the network and shares this information with IBM QRadar
2. Forescout eyeExtend for IBM QRadar sends up-to-date device context to QRadar
3. QRadar correlates device context from Forescout platform with other data sources to identify and prioritize incidents
4. QRadar prompts Forescout platform to take response actions on noncompliant, vulnerable or suspicious devices based on threat severity

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com