FORESCOUT

Highlights

See

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor connected devices, including corporate, BYOD, guest and IoT

Control

- Allow, deny, limit or change network access based on user, device profile and security posture
- Initiate remediation actions on non-compliant, vulnerable or compromised endpoints
- Enforce compliance with industry and government mandates and regulations

Orchestrate

- Share high-value endpoint context with IBM QRadar to enhance correlation and incident prioritization
- Verify IBM QRadar WinCollect agent is installed and functioning properly on Windows servers
- Accelerate incident response to quickly mitigate threats and data breaches

ForeScout Extended Module for IBM® QRadar®

Gain in-depth endpoint insight, improve situational awareness and accelerate incident response

The ForeScout Extended Module for IBM® QRadar® enables bi-directional communication and orchestration of workflows between ForeScout CounterACT® and IBM QRadar SIEM. The joint solution combines CounterACT's endpoint visibility, access control and automated response capabilities with QRadar's powerful correlation, analysis and prioritization features. This helps security teams better understand their overall security risk posture, prioritize QRadar offenses and respond more quickly to mitigate a range of security issues.

The Challenges

Visibility. Serious attempts to manage security risks must start with knowing who and what is on your network, including visibility into whether networked devices are compliant with your security standards. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

- Unmanaged guest or Bring Your Own Devices (BYODs)
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

As a result, organizations are often unaware of the additional attack surface and elevated risk from these devices.

Threat Landscape. A vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network. These threats can easily evade traditional security defenses and move laterally across networks to gain access to sensitive applications and information. To reduce your attack surface and limit threat propagation, you need the ability to assess security posture, identify compliance gaps and scan for indicators of compromise (IOCs) on devices as they connect to the network.

Response Automation. Traditional response techniques rely on manual measures and IT staff to correlate information from various sources, identify high-priority incidents and act on the potential threats. The velocity and evasiveness of today's targeted threats, coupled with increasing network complexity, mobility and BYOD, can easily overwhelm this response chain and render it ineffective. For combating cyberthreats, it is essential for IT teams to devise a cohesive, automated incident prioritization and response strategy to limit threat propagation, security breaches and data exfiltration.

How it Works

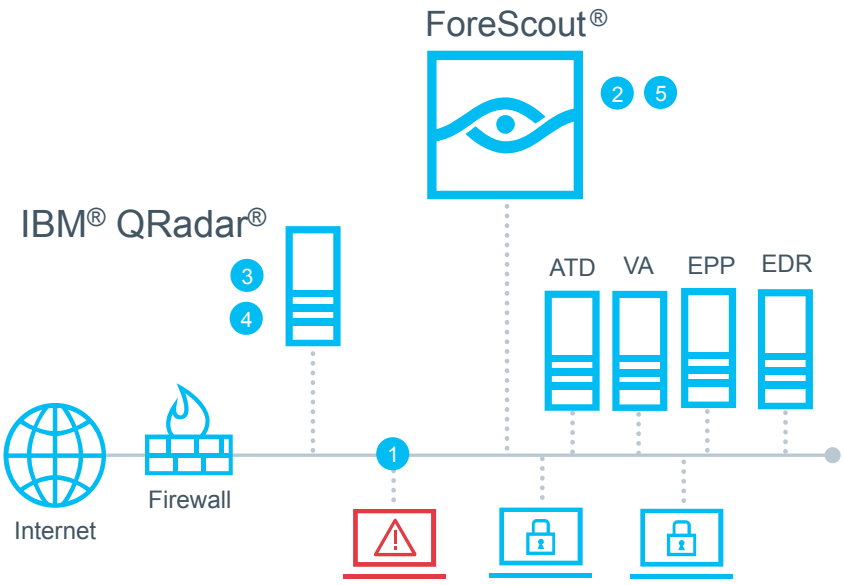
ForeScout CounterACT is a network security solution that gives you the unique ability to see devices, including non-traditional devices, as they connect to the network. CounterACT provides policy-based assessment, monitoring and control of these devices.

1. CounterACT discovers, classifies and assesses devices as they connect to the network
2. The Extended Module sends up-to-date device context to IBM QRadar; verifies WinCollect agent is installed and functioning properly on Windows servers
3. ForeScout App for IBM QRadar visualizes CounterACT data for trend analysis, monitoring and reporting
4. QRadar correlates device context from CounterACT with other data sources to identify and prioritize offenses
5. QRadar initiates CounterACT to take response actions on non-compliant, vulnerable or suspicious endpoints

ForeScout Extended Modules

The ForeScout Extended Module for IBM QRadar is an add-on module for ForeScout CounterACT that is sold and licensed separately. It's one of many ForeScout Extended Modules that enables ForeScout CounterACT to exchange information, automate threat response and remediation, and more efficiently mitigate a wide variety of security issues.

Learn more at
www.ForeScout.com



The Extended Module for IBM QRadar allows you to leverage device context from CounterACT to improve correlation and prioritize offenses within QRadar. The ForeScout App for IBM QRadar enables you to visualize CounterACT data within QRadar and initiate precise, automated endpoint actions from QRadar for incident response.

Based on policy, the Extended Module can share the following CounterACT data with QRadar:

- Real-time inventory of connected devices on the network—from traditional corporate PCs, servers and mobile devices to BYOD and IoT
- Device information, including device type, classification, network connection, operating system, applications, users, peripherals and more
- Device security posture and compliance gaps
- Authentication, access and network location information

The joint solution enables you to:

- Send CounterACT data to QRadar for long-term trend analysis, visualization and incident investigation; comply with log retention mandates
- Verify QRadar WinCollect agent is installed and functioning properly on Windows servers
- Identify anomalous behavior and offenses in QRadar based on CounterACT data
- Correlate high-value endpoint context from CounterACT with other data sources in QRadar to identify and prioritize offenses
- Initiate CounterACT actions from QRadar to automate incident response, remediation and threat mitigation

FORESCOUT

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

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