ForeScout Extended Module for Qualys® Vulnerability Management

Improve real-time visibility over managed and unmanaged devices while automating network access control and threat response

Vulnerability Assessment (VA) is considered a security best practice and is an important part of any modern security program. However, an increasingly mobile enterprise with a proliferation of transient devices, coupled with the speed of today's targeted attacks, has created new challenges for vulnerability management programs.

The ForeScout Extended Module for Qualys® Vulnerability Management communicates with the Qualys Cloud Platform vulnerability management solution to provide workflow automation such as comply-to-connect, automated remediation of security threats as well as other security functions.

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, including corporate, BYOD and IoT endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Orchestrate

- Share contextual insight with Qualys Vulnerability Management and act on Qualys scan results
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

The Challenges

Visibility. According to industry experts, the vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. However, most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed, Bring Your Own Device (BYOD), guest or Internet of Things (IoT) devices. Also, they may have disabled or broken agents, or are transient devices that aren't detected by periodic scans. As such, organizations are not aware of the attack surface on these devices.

Threat Detection. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multivectored, stealthy and targeted, these attacks focus on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need next-generation security controls that do not rely on signatures.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, create the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

Extended Module for Qualys Vulnerability Management

ForeScout CounterACT® is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with the ForeScout ControlFabric® Architecture to orchestrate information sharing and automate operations among disparate security and IT management tools, including Qualys Vulnerability Management.

Qualys Vulnerability Management is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

1. An endpoint attempts to connect to the network. CounterACT immediately detects it.
2. CounterACT optionally puts the endpoint in limited access and requests Qualys to initiate a real-time scan of the device.
3. Qualys scans connecting device and shares scan results with CounterACT.
4. CounterACT quarantines or blocks high-risk endpoint so it doesn't become a launching point for advanced threats.
5. CounterACT initiates built-in remediation actions or triggers external remediation via patch management.
6. CounterACT provides similar conditions/actions for BYOD/Guest endpoints upon connection, or again periodically, as endpoint remains connected.

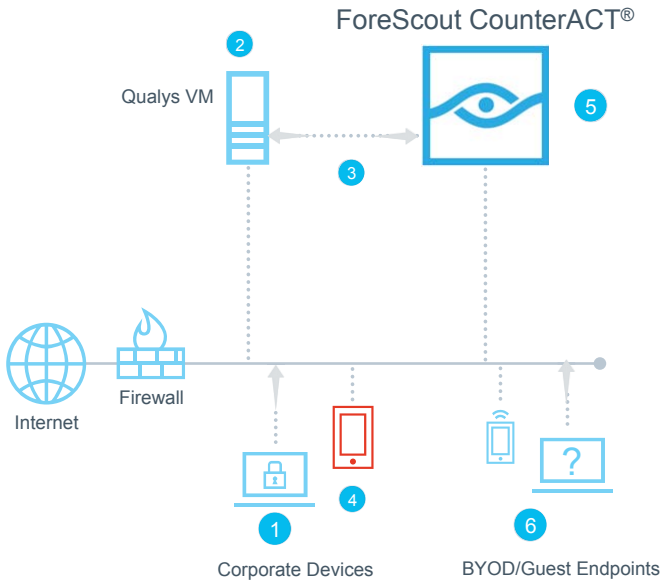

Figure 1: CounterACT works interactively with Qualys Vulnerability Management to provide real-time monitoring and automated mitigation of vulnerabilities and risks using the Extended Module for Qualys Vulnerability Management

CounterACT communicates bi-directionally with Qualys through the Extended Module for Qualys Vulnerability Management. When CounterACT detects endpoints as they connect to the network in a comply-to-connect scenario, CounterACT will isolate the endpoint on a lobby network and trigger a Qualys Vulnerability Management scan. Once the endpoint has been scanned and Qualys has determined the endpoint is compliant, it is allowed on the corporate network. Other capabilities include:

- CounterACT can provide a list of endpoints not presently known to Qualys that can be added to the next Qualys Vulnerability Management scan.
- If a server is identified as having a vulnerable HTTP service, CounterACT can isolate the server so that only internal access is allowed, blocking access from the public network. If an endpoint is identified as having a significant vulnerability, CounterACT can limit access from that endpoint to more secure segments of the network until the vulnerability has been remediated.
- CounterACT can request Qualys to perform a VM scan on devices that meet certain policy conditions, such as endpoints with specific applications, or when endpoint configuration changes are detected.
- CounterACT can evaluate Qualys Vulnerability Management scan results and trigger automated responses to particular situations. For instance, if a critical vulnerability is detected on an endpoint, CounterACT can automatically initiate another scan, or, restrict the endpoint from access the corporate network.

With the Extended Module for Qualys Vulnerability Management, you gain more comprehensive and up-to-date information about the vulnerable endpoints on your network, as well as the ability to automate remediation to more rapidly mitigate risks, increasing the overall security posture of the network.

ForeScout Extended Module

The Extended Module for Qualys Vulnerability Management is an optional module for ForeScout CounterACT and is sold and licensed separately. It is just one of many ForeScout Extended Modules that enable 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

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
Fax 1-408-371-2284

Version 8_16