Solution Brief

The ForeScout-Qualys® Joint Integration

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

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, 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
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

Vulnerability Assessment (VA) is considered a security best practice and is an important part of modern security programs. 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 Challenges

1. VA systems typically do periodic scanning and provide a snapshot of an organization's risk posture at a given point in time. Thus, the information gathered may not be valid between scheduled scans. This leaves organizations blind to risks that have emerged since the last scan.
2. With an increasing number of transient devices, many endpoints may not be assessed for vulnerabilities and risks because they are offline or off-premises during scheduled scans. As a result, the vulnerability assessment report can be incomplete.
3. By themselves, VA systems are not meant to take action or mitigate security risks. Thus they only provide vulnerability information, leaving remediation and risk mitigation to other systems or human intervention. This can leave organizations with large windows of exposure to malware, targeted attacks and data breaches.

How it Works

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 ForeScout ControlFabric™ Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

CounterACT communicates bi-directionally with Qualys through a connection known as the Vulnerability Assessment Integration Module. This allows CounterACT to inform Qualys about devices that are on the network, thereby addressing the challenges listed above.

- CounterACT can inform Qualys the moment that a device has joined the network or changed its configuration. This can trigger Qualys to scan the device immediately. This significantly increases the chance of actually "catching" the endpoint while it is on the network and producing a vulnerability report.
- CounterACT can provide a list of IP addresses to Qualys, allowing Qualys to produce a report which details which endpoints were not reached by the scan.

- Some organizations are especially meticulous about security and they want to confirm the endpoint's health before it gets access to the network. CounterACT can be configured to put a new endpoint into a "lobby" network (essentially, a quarantine) when it first attaches to the network, then trigger Qualys to scan the endpoint for critical vulnerabilities. If the endpoint is seen by Qualys to be sufficiently clean, CounterACT can admit the endpoint to the production network.

After Qualys scans a device, it tells CounterACT about the vulnerabilities it has discovered. CounterACT is able to use this information within its policy engine. For example, if Qualys determines that an endpoint has a critical vulnerability, CounterACT can automatically quarantine the endpoint and/or initiate remediation. Because CounterACT includes fine-grained remediation capabilities, the remediation can be defined based on the vulnerability that Qualys identifies. For example:

- If Qualys determines that a server has a vulnerable HTTP service, CounterACT can block the server from accessing the Internet while still allowing it to access internal network services
- If Qualys determines that an endpoint has a certain vulnerability, CounterACT can block access to specific high-security zones within the network

Through this integration, IT security managers can obtain more current and more complete information about the vulnerabilities on their network, more efficient operations and less wasted network bandwidth from your scanner, and faster remediation of risks.

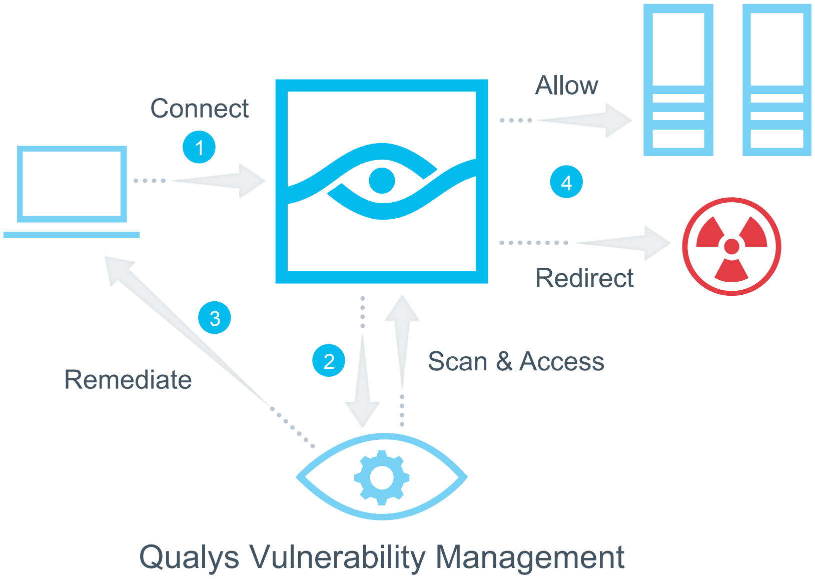

Figure 1: ForeScout CounterACT and Qualys Vulnerability Management work in concert to assess and remediate devices as they access the network.

1. Device connects to the network
2. CounterACT informs Qualys of device status
3. If non-compliant, CounterACT remediates the device
4. CounterACT allows or denies access based on Qualys assessment

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 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 1_16