ForeScout Extended Modules for Vulnerability Assessment

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

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, IoT devices and operational technologies

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

ForeScout Extended Modules for Vulnerability Assessment Systems

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 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, BYOD endpoints, guest or IoT devices. Also, they may have disabled or broken agents, or are transient devices that aren't detected by periodic scans. As such, you are unaware 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 are focused 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 device and OS diversity, network complexity, mobility and BYOD, are creating 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.

How ForeScout Extended Modules for Vulnerability Assessment Work

The ForeScout platform is a visibility and control solution that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. It provides policy-based control of these devices and orchestrates information sharing to automate operation among disparate security and IT management tools, including VA systems.

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

Supported Vulnerability Assessment Systems

Products supported by Extended Modules for Vulnerability Assessment:

- Rapid7 Nexpose
- Qualys Vulnerability Management
- Tenable Vulnerability Management

For details on our licensing policy, see www.forescout.com/licensing.

Learn more at
www.ForeScout.com

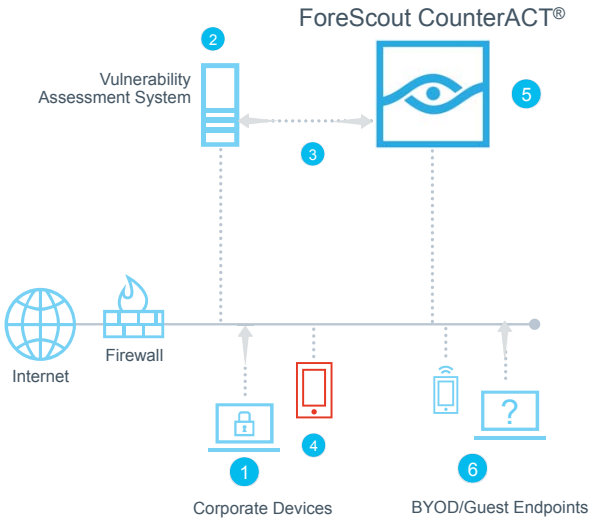

Figure 1: The ForeScout platform and VA systems work together to provide real-time monitoring and mitigation of vulnerabilities and risks.

The ForeScout platform communicates bi-directionally with VA systems through ForeScout Extended Modules for Vulnerability Assessment. It detects devices the moment they connect to the network and informs the VA system. This enables several unique capabilities:

- The ForeScout platform can trigger the VA system to perform a real-time scan of the connecting device when it joins the network. This significantly increases the chance of detecting transient endpoints while they are on the network and helps produce more up-to-date and complete vulnerability reports.
- The ForeScout platform can isolate a connecting device in an inspection VLAN in order to confirm its risk posture while the VA system performs a scan. If the VA system determines that the endpoint's risk rating is acceptable, ForeScout can admit the endpoint to the production network.
- The ForeScout platform can trigger VA scans on devices that meet certain policy conditions, such as endpoints with specific applications, or when endpoint configuration changes are detected.

After the VA system scans a device, the ForeScout platform obtains the scan results and initiates risk mitigation actions if vulnerabilities are detected. Based on policy, the ForeScout platform can enforce controls with a level of response appropriate to the issue at hand. For example, it can quarantine endpoints with critical vulnerabilities, initiate built-in remediation actions, or trigger external remediation via patch management and other IT systems.

Through this integration, you gain:

- More up-to-date information about the vulnerabilities on your network
- More comprehensive information about the vulnerable endpoints on your network
- Automated remediation and faster mitigation of risks on your network

Extended Modules for VA are optional modules and are sold separately. When used in conjunction with your existing VA systems, the ForeScout platform and these Extended Modules provide automated response to Indicators of Compromise (IOCs) while providing a dynamic threat detection approach to security, thereby reducing the attack surface of your network.

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