FORESCOUT

ForeScout Extended Module for Tenable® VM

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, creates new challenges for vulnerability management programs.

The ForeScout Extended Module for Tenable® VM communicates with the Tenable® SecurityCenter, which is the centralized console for management and for viewing scan data. For organizations with large and complex networks, SecurityCenter combines Nessus scanning with an enterprise-class vulnerability management platform.

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 Tenable VM
- 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, 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 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 Tenable VM

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, including Tenable VM.

Tenable VM is a Vulnerability Assessment product that consists of two main components, the Nessus scanners and SecurityCenter, which is used in large, complex network environments.

CounterACT communicates bi-directionally with Tenable SecurityCenter through the ForeScout Extended Module for Tenable VM. CounterACT detects devices the moment they connect to the network and informs SecurityCenter, which allows the operator to trigger scan requests based on network activity, as well as using CounterACT policies to monitor, manage, remediate and restrict endpoints based on Nessus scan results.

1. An endpoint attempts to connect to the network. CounterACT is immediately aware of it.
2. CounterACT requests Nessus provide a real-time scan of the connecting endpoint
3. Nessus scans the connecting endpoint and shares the scan results with CounterACT
4. CounterACT quarantines or blocks a high-risk endpoint so it doesn't become a network launching point for advanced threats.
5. CounterACT initiates automated remediation actions, or triggers external remediation via patch management.

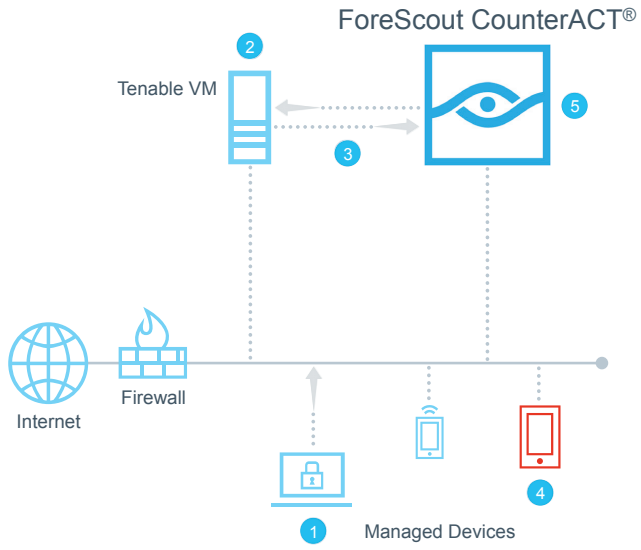

Figure 1: ForeScout CounterACT and Tenable VM work together to provide real-time monitoring and automated mitigation of vulnerabilities and risks.

For organizations that are particularly meticulous about security and want to confirm an endpoint's health before it connects to the network, CounterACT can be configured to automatically "scan on connect." This allows the endpoint to be put into an isolated network segment and have Nessus scan the device. If the endpoint is considered safe, it is allowed onto the network. This function is particularly helpful when transient endpoints connect to the network, as they may have not been scanned in the routine scan performed by Nessus.

In organizations large or small, even when there are hundreds of Nessus scanners, CounterACT can trigger a selected Nessus policy through Tenable SecurityCenter to provide a system scan, daily scan, or scan on connect. Once the scan is complete, CounterACT can review the results and take action, including automated remediation, in cases where vulnerabilities are found. Other capabilities include:

- SecurityCenter can trigger a policy in CounterACT to isolate vulnerable endpoints and remediate the vulnerabilities before being allowed back onto the network.
- CounterACT policies can be used to trigger a SecurityCenter policy to launch a scan on endpoints that have not been scanned in X number of days.
- If an endpoint is determined to have a particular vulnerability, or, a server has a vulnerable HTTP service, CounterACT policies can be created to only allow the endpoint access to low security network segments, or, in the case of the HTTP service, block access from the public network while allowing access from the private network.
- CounterACT can leverage SecurityCenter information to trigger a scan if the endpoint's vulnerability severity is greater than X, or if any monitored item has changed since the last scan. CounterACT can also use this information in policies that would trigger remediation for both of these instances.
- CounterACT can also retrieve information from SecurityCenter that indicates vulnerabilities found. This information can be used to create an inventory view that allows the admin to see devices with vulnerabilities and create reports that show endpoints with particular vulnerabilities or with specific vulnerability severities.

With the Extended Module for Tenable VM, 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 Tenable VM 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