FORESCOUT

ForeScout Extended Module for Rapid7 Nexpose

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 Extended Module for Rapid7 communicates with the Rapid7 Security Console 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 Rapid7 Nexpose and act on Rapid7 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, 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 Rapid7 Nexpose

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 Rapid7 Nexpose.

Rapid7 Nexpose is a Vulnerability Assessment product that consists of two main components, the Rapid7 management console called Security Console, and Scan Engines. More than one Scan Engine may be configured on the network, and typically, each Scan Engine is designed to monitor/maintain a particular network segment or location. The Scan Engines report to a single Security Console. This makes the sharing of information between Rapid7 and CounterACT particularly efficient, as CounterACT only needs to talk to a single device to find properties of endpoints that are managed by Rapid7.

1. An endpoint attempts to connect to the network. ForeScout immediately detects it.
2. ForeScout optionally puts the endpoint in limited access and requests Rapid7 to initiate a real-time scan of the device.
3. Rapid7 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.

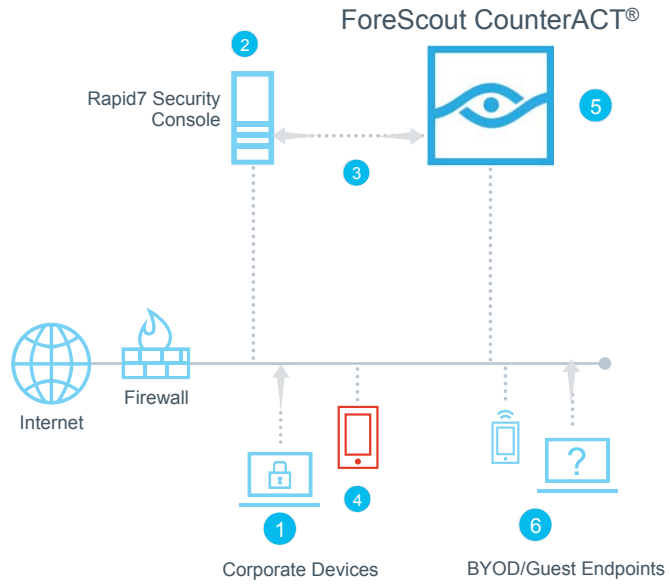

Figure 1: The Extended Module for Rapid7 Nexpose works with the Nexpose Security Console to provide real-time monitoring and automated mitigation of vulnerabilities and risks.

CounterACT communicates bi-directionally with Nexpose through the ForeScout Extended Module for Rapid7 Nexpose. When CounterACT detects endpoints as they connect to the network in a comply to connect scenario, CounterACT will isolate the endpoint on an isolated network segment and trigger a Nexpose scan. Once the endpoint has been scanned and Nexpose has determined the endpoint is compliant, it is allowed on the corporate network. Other capabilities include:

- CounterACT can direct Nexpose to perform a scan on devices that meet certain policy conditions, such as endpoints with specific applications, or when endpoint configuration changes are detected.
- CounterACT can direct Nexpose to perform a scan on devices that have been connected for a specified period of time, in a "comply-to-remain-connected" scenario. This is a typical situation for guest endpoints.
- By applying a risk score to changes identified by a routine Nexpose scan, an operator can request CounterACT to remediate a single endpoint or group of endpoints if their risk score is above an acceptable value.

With the Extended Module for Rapid7 Nexpose, 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 Rapid7 Nexpose is an optional module for ForeScout CounterACT and is sold and licensed separately. It is just 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

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