Forescout eyeExtend for Rapid7® Nexpose

Uncover device vulnerabilities in real time and mitigate your risk exposure

Vulnerability assessment (VA) is widely considered a security best practice and an important part of any modern security program. However, vulnerability management programs are challenged by the speed of today's targeted attacks and a proliferation of unmanaged and transient devices. Vulnerability scanners such as Rapid7 Nexpose can scan the network for known devices and vulnerabilities, but they cannot possibly scan devices they're not aware of. Periodic scans also miss transiently connected devices with dangerous vulnerabilities that expose an organization to data breaches.

Forescout eyeExtend for Rapid7 Nexpose lets you harness complete device visibility agentlessly across your entire attack surface and automates response workflows for device compliance, remediation and risk mitigation.

Challenges

- Understanding the risk exposure across the extended enterprise
- Scanning, detecting and remediating endpoint vulnerabilities immediately when new devices attempt to connect
- Reducing IT and security staffs' manual workload of managing and securing an ever-increasing number of connected devices, and their vulnerabilities
- Preventing devices from accessing sensitive network systems until vulnerabilities have been remediated

The Solution

Forescout works together with Rapid7® Nexpose through Forescout eyeExtend for Rapid7 Nexpose to help eliminate cyberattacks that target unmanaged and transient devices, prevent damaging data breaches and slash IT and security workloads by managing vulnerabilities across your extended enterprise.

Forescout eyeExtend for Rapid7 Nexpose leverages the complete device visibility and context provided by Forescout eyeSight to make Nexpose aware of every single network-attached device—whether managed, unmanaged or transient—the instant it connects, enabling Nexpose to detect vulnerabilities across the entire enterprise attack surface.

eyeExtend for Rapid7 Nexpose extends vulnerability management by initiating Nexpose scans automatically every time a new device or a device with an outdated scan, posture change or higher vulnerability risk connects. If Nexpose scans find vulnerabilities, Rapid7 can trigger Forescout to limit the device's network access until it has been remediated—either through Nexpose built-in policies or by activation of external patch management tools in real time. Forescout can also leverage Nexpose's risk scoring system or the Common Vulnerability Scoring System (CVSS) ranking to

eyeExtend

Benefits

- Enahance the power of Rapid7 Nexpose with complete visibility across managed, unmanaged and transient devices
- Increase operational efficiency through real-time discovery, assessment and response to device vulnerabilities
- Streamline network and security operations by continuously enforcing device compliance at all times
- Automate remediation and response for noncompliant devices

Highlights

- Assess device configuration and compliance when and after a device connects to the network
- Scan all new devices the instant they connect
- Initiate scans based on time of last scan, severity of vulnerability, change in device posture and Nexpose-specific metrics
- Automate remediation actions by vulnerability criticality based on Nexpose risk scores and CVSS
- Control network access by dynamically quarantining or blocking vulnerable devices from accessing sensitive parts of the network

organize devices into vulnerability groups and prioritize and accelerate isolation and remediation of the riskiest devices first.

In summary, with Forescout eyeExtend for Rapid7 Nexpose, you can extend and automate vulnerability management on every single device when and after it connects to the enterprise network, eliminating considerable time and resources spent tracking and protecting a myriad of managed and unmanaged network devices and their vulnerabilities.

Use Cases

Assess device vulnerabilities on-connect

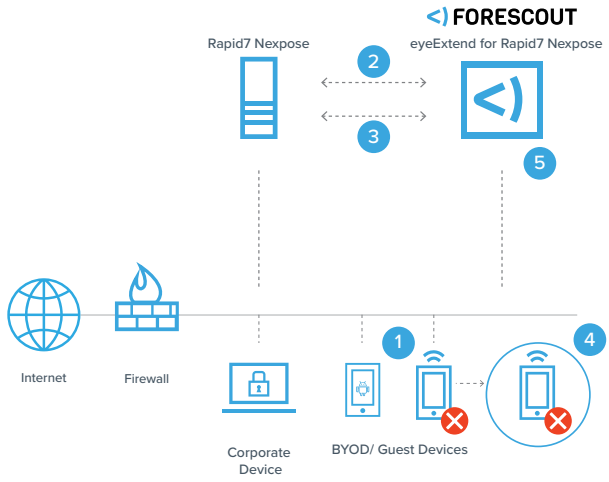
Gain real-time insight into risks and vulnerabilities on your network. eyeExtend for Rapid7 Nexpose prevents exploitation of unmanaged or transient endpoints by detecting devices immediately on connect. After determining if the device is new, unmanaged or has an outdated scan, eyeExtend initiates real-time scans from the Nexpose Security Console, eliminating the problem of missing or out-of-date device scans.

Apply policy-based conditional scans

Manage device vulnerabilities after devices connect. Operators can create a Forescout policy that initiates a Nexpose scan automatically in the event of a device configuration change or noncompliance. For example, Forescout policies can be used to trigger a scan on devices that have not been scanned in X number of days or if a device's vulnerability severity is greater than X, or if any monitored item has changed since the last scan. Forescout can also use this information to initiate remediation in these instances.

Prioritize vulnerabilities and automate response

In cases where there are large numbers of devices with vulnerabilities, Forescout eyeExtend leverages Nexpose's granular risk scoring system or standard CVSS rankings to organize devices with vulnerabilities into priority groups for accelerated isolation and remediation of the riskiest devices to your business. When Nexpose identifies a device as noncompliant, it shares the information with Forescout eyeExtend. Forescout quarantines or blocks the device from accessing the network dynamically and initiates remediation workflows until the device is deemed compliant and healthy. Forescout can also target remediation actions such as installing required security software, updating agents or applying security patches proactively. Once all vulnerabilities are addressed, the device is allowed back onto the network.



1. A device attempts to connect to the network. Forescout immediately detects it
2. Forescout optionally puts the device in limited access and requests Rapid7 to initiate a real-time scan of the device
3. Rapid7 Nexpose scans the connecting device and shares scan results and vulnerability risk scores with Forescout
4. Forescout quarantines or blocks the high-risk device so that it does not become a launching point for infection
5. Forescout initiates remediation via Nexpose or triggers external remediation via patch management. When all vulnerabilities have been remediated, Forescout allows device to access the network

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com