Forescout eyeExtend for Qualys® VM

Uncover device vulnerabilities in real time and mitigate your risk exposure

Many of today's sophisticated cyberattacks exploit well-known device vulnerabilities to break into the enterprise network. Stopping these attacks requires detecting every single endpoint as it connects and remediating its vulnerabilities immediately, before it can become a target for infection. Unfortunately, the proliferation of unmanaged Bring Your Own Devices (BYOD), Internet of Things (IoT), transient and guest devices make it almost impossible to detect and remediate vulnerabilities across an organization's entire attack surface. Vulnerability scanners such as Qualys Vulnerability Management (VM), part of the Qualys Cloud Platform, can scan the network for known devices and vulnerabilities, but they cannot scan devices they're not aware of. Periodic scans also miss transiently connected devices with dangerous vulnerabilities that can become launching pads for data breaches.

Forescout eyeExtend for Qualys VM lets you harness complete device visibility to expose device vulnerabilities and automate response workflows for device compliance, remediation and risk mitigation across managed and unmanaged devices.

Challenges

- Achieving continuous device visibility across every single managed and unmanaged network-attached device
- 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, vulnerabilities and threats
- Preventing devices from accessing sensitive network systems until vulnerabilities have been remediated

The Solution

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

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

eyeExtend for Qualys VM extends vulnerability management by allowing operators to create a policy that initiates a Qualys scan automatically every time a device

eyeExtend

Benefits

- Enhance the power of Qualys VM 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

- Get complete visibility into corporate, personal, guest and transient devices across IT, Cloud and operational technology (OT) networks
- Assess device configuration and compliance when and after it 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 Qualys VM specific metrics
- Control access to network through quarantining or blocking vulnerable devices from accessing sensitive parts of the network

connects, whether it's a new device or one with an outdated scan, posture changes or higher-vulnerability risks. If Qualys VM scans find vulnerabilities, Qualys can trigger Forescout to isolate the device completely or allow access to low-security segments only and initiate remediation workflows, either through built-in policies or via activation of external patch management tools in real time.

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

Use Cases

Assess device compliance on-connect

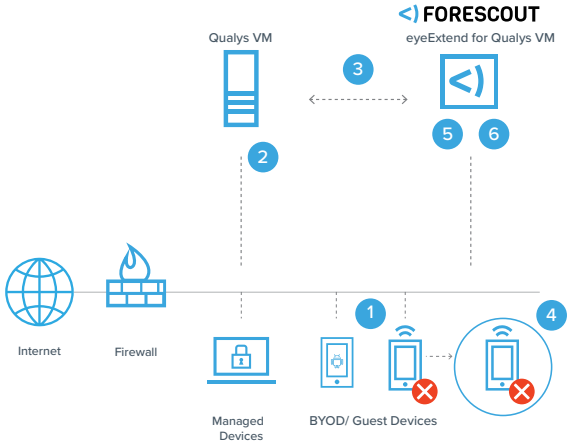
Gain real-time insight into risks and vulnerabilities on your network. eyeExtend for Qualys VM prevents exploitation of unmanaged and transient endpoints by detecting devices immediately on connect. After determining if the device is new, unmanaged or has an outdated scan, eyeExtend initiates real-time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

Apply policy-based conditional scans

Manage device vulnerabilities after devices connect. Operators can create a Forescout policy that initiates a Qualys VM 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.

Automate response and risk mitigation

Limit network access or quarantine high-risk devices identified by Qualys VM and initiate remediation actions automatically to fix vulnerabilities. When Qualys VM 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. Based on policy, Forescout puts the device in limited access and requests Qualys VM to initiate a real-time scan of the device
3. Qualys VM scans the connecting device and shares scan results with Forescout
4. Forescout quarantines or blocks the high-risk device so it doesn't become a launching point for infection
5. Forescout initiates built-in remediation actions or triggers external remediation via patch management
6. Forescout initiates new Qualys VM scans when it detects changes, such as specific applications or configuration changes on the device

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