Forescout eyeExtend for Tenable®

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. Unfortunately, the proliferation of transient and unmanaged bring your own devices (BYOD) and guest devices makes it almost impossible to detect and remediate vulnerabilities across an organization's entire attack surface. Vulnerability scanner and management tools such as Tenable 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 Tenable lets you harness complete device visibility and automate 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, vulnerabilities and threats
- Preventing devices from accessing sensitive network systems until vulnerabilities have been discovered and remediated

The Solution

Forescout eyeExtend for Tenable integration with Tenable.sc ® (formerly Tenable SecurityCenter®) and Tenable.io® helps eliminate cyberattacks that target unmanaged and transient endpoints, prevent damaging data breaches and slash IT and security workload managing vulnerabilities across your extended enterprise (including IT, Operational Technology (OT) and cloud infrastructures).

Forescout eyeExtend for Tenable leverages the comprehensive device visibility and context provided by Forescout eyeSight. With complete device discovery and in-depth device information, Forescout eyeExtend makes Tenable aware of every single network attached device—whether managed, unmanaged or transient—the instant it connects, enabling Tenable to detect vulnerabilities across the entire enterprise attack surface.

eyeExtend for Tenable infinitely extends vulnerability management by allowing operators to trigger Tenable vulnerability scans manually or create a policy that

eyeExtend

Benefits

- Enhance the power of Tenable products by extending it to every single network endpoint, whether managed, unmanaged or transient
- Increase operational efficiency through real-time discovery, assessment and response to 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 OT networks
- Assess device configuration and compliance when and after it connects to the network
- Initiate scans based on time of last scan, severity of vulnerability, change in device posture and Tenable-specific metrics
- Isolate vulnerable devices and remediate vulnerabilities before being allowed back onto the network.
- Control network access through quarantining or blocking vulnerable devices dynamically

initiates a scan automatically every time a device connects, whether it's a new device or one with an outdated scan history, posture changes or higher-vulnerability risks. If Tenable scans find vulnerabilities, Tenable can trigger Forescout platform in real time 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 summary, with Forescout eyeExtend for Tenable 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 vulnerabilities on-connect

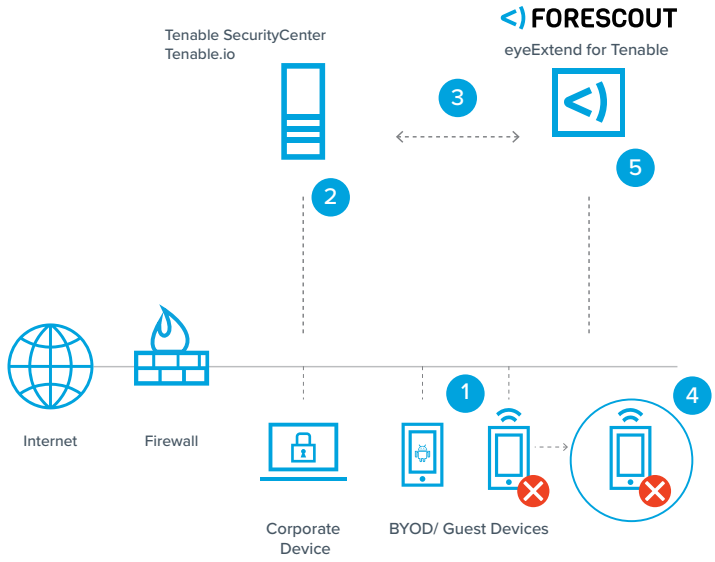
Gain real-time insight into risks and vulnerabilities on your network. eyeExtend for Tenable prevents exploitation of unmanaged or transient endpoints by detecting devices immediately on connect. After determining if the device is new, unmanaged or has an outdated scan, eyeExtend initiates real-time scans from Tenable, 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 platform policy that initiates a Tenable scan automatically in the event of a device configuration change or noncompliance. For example, Forescout platform 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 platform 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 Tenable and initiate remediation actions automatically to fix vulnerabilities. When Tenable identifies a device as noncompliant, it shares the information with Forescout eyeExtend. Forescout platform quarantines or blocks the device from accessing the network dynamically and initiates remediation workflows until the device is deemed compliant and healthy. Forescout platform 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 platform immediately detects it
2. Forescout platform optionally puts the device in a limited access zone and requests Tenable to initiate a real-time scan of the device
3. Tenable scans the connecting device and shares scan results with Forescout platform
4. Forescout platform quarantines or blocks the high-risk device so it doesn't become a launching point for infection
5. Forescout platform initiates built-in remediation actions or triggers external remediation via patch management

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