Forescout eyeExtend for Trellix® Endpoint Security

Benefits

- Increase operational efficiency by real-time device assessment and expanding Trellix Endpoint Security's managed device coverage and security hygiene
- Reduce security risk by extending Trellix Endpoint Security's threat intelligence to automatically hunt for threats across managed and unmanaged devices
- Automate threat remediation and response for noncompliant or compromised devices

Highlights

- Verify that all devices have installed, operational and updated Trellix Endpoint Security agents
- Initiate remediation for noncompliant devices
- Detect, share and hunt for IOCs across campus, IoT, datacenter and cloud in real time
- Automate system-wide response using out-of-the-box or customized policies to quickly mitigate threats and data breaches
- Allow, deny or limit network access of devices based on device posture and security policies

Enterprise-wide threat hunting and protection

Enterprise information technology (IT) and security teams are managing increasingly complex environments with exponential growth in the volume and diversity of devices connecting to the network. The rise in network-connected devices increases the attack surface and allows threat actors to capitalize on the weakest link to gain a foothold on your network. To combat cyberthreats organizations use Trellix® Endpoint Security, an advanced endpoint detection and response solution. However, unmanaged devices that connect to the network unnoticed pose a risk that must still be addressed. If compromised devices are left undetected, they can be used as launch pads to target higher-value assets, gain access to sensitive information and cause significant business impact.

Forescout eyeExtend for Trellix Endpoint Security (HX Series) provides a comprehensive approach to security that spans complete device visibility across your extended enterprise, helps enforce device compliance, extends threat hunting to unmanaged devices and automates network access control for threat mitigation in real time.

Challenges

- Addressing gaps in agent coverage across the enterprise including missing, broken or disabled agents
- Applying threat data to assess all known and unknown devices to increase potential usefulness of Trellix Endpoint Security solution
- Reducing lengthy response time and manual processes for limiting network access of the compromised devices to contain threats in order to avoid lateral threat propagation

The Solution

Forescout eyeExtend for Trellix Endpoint Security orchestrates information sharing and security workflows between the Forescout platform and Trellix Endpoint Security to improve device compliance, proactively detect threats across the entire network and automate threat response.

Although organizations have deployed advanced endpoint detection and response technology such as Trellix Endpoint Security, they are still challenged with addressing agent coverage gaps across the enterprise. Gaps include missing, broken or disabled agents, limited host-based incident response capabilities and partial threat data derived from devices with functional agents only. These coverage gaps limit the total potential usefulness of the solution.

Forescout eyeExtend for Trellix Endpoint Security combines the threat detection mechanisms of Trellix Endpoint Security with complete device visibility and compliance enforcement capabilities of the Forescout platform. With in-depth device discovery and assessment, the Forescout platform continuously verifies and validates the integrity of Trellix Endpoint Security agents on all IP-connected devices. Forescout helps ensure device compliance at all times by initiating

remediation of the nonconforming devices and bringing more devices under Trellix's security coverage.

This integration leverages Trellix Endpoint Security's threat information to hunt for and respond to threats across all devices in the extended enterprise. Trellix Endpoint Security's shared threat intelligence with the Forescout platform helps improve both the mean time to detection (MTTD) and mean time to response (MTTR), preventing threats from propagating in your network. Devices suspected of infection can be isolated, and remediation actions can be initiated automatically instead of requiring human intervention, allowing corporate security teams to deal with other high-profile issues.

Use Cases

Verify and enforce managed device hygiene

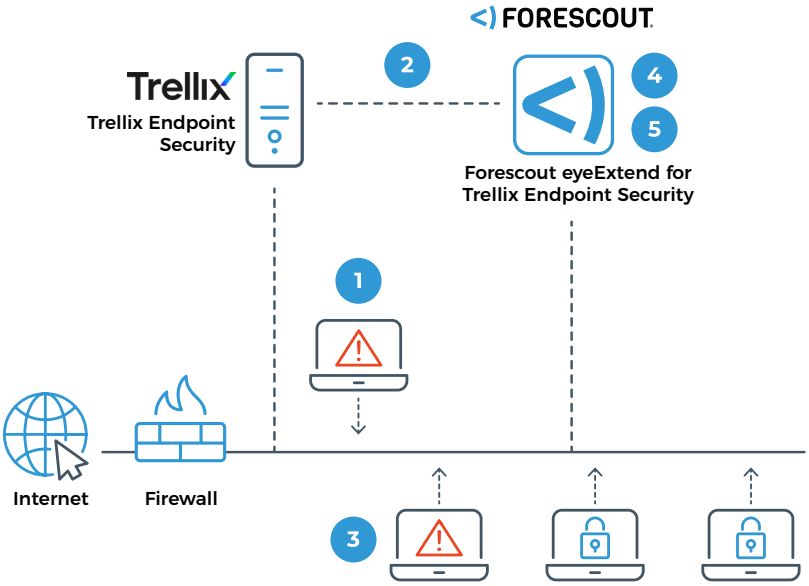
eyeExtend for Trellix Endpoint Security determines if devices have Trellix Endpoint Security agents installed, updated and working correctly both at the time of connection and continuously after connection. If needed, Forescout platform restarts or reinstalls the Endpoint Security agent. It can also redirect the noncompliant devices to a self-help web page to install the Trellix Endpoint Security agent. Devices that leave the network are verified when they reconnect to enforce compliance.

Share threat intelligence to maximize joint threat hunting and detection

Upon detecting threats on devices, Trellix Endpoint Security immediately notifies Forescout eyeExtend. Forescout eyeExtend for Trellix Endpoint Security triggers Forescout IOC Scanner to parse the threat to yield IOCs—measurable events or state properties that can be used as a fingerprint to identify the threat. Forescout platform uses these IOCs to mount further scans, analysis and remediation of threats across all managed and unmanaged IP-connected devices.

Accelerate and automate policy-driven threat response

When Forescout platform discovers infected devices via its own IOC scanner or through Trellix Endpoint Security, it can automatically take policy-based mitigation actions to contain and respond to the threat. Various actions can be performed, depending on the severity or priority of the threat, such as quarantining or isolating infected devices, initiating direct remediation, sharing real-time context with other incident response systems, initiating a scan by another third-party product, and notifying the user via email or text message. These custom-defined actions can be performed manually or automatically to block and prevent lateral propagation of threats across your network.



1. Forescout validates the Trellix Endpoint Security agent is installed, fully functional and up to date on managed devices and initiates remediation in case of noncompliance
2. Trellix Endpoint Security identifies and classifies an IOC on a device and shares the information with Forescout eyeExtend
3. Forescout isolates the infected device and initiates a scan of other devices for the same IOC
4. Forescout then limits access to the network for any devices that are infected and not protected by Trellix Endpoint Security
5. As devices are verified remediated and clean, Forescout allows those devices back onto the network as per policy

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com