Trellix eyeExtend

Forescout eyeExtend for Trellix® ePO™

Benefits

- Gain complete visibility across all IP-connected devices, including BYOD, guest and transient devices across IT and OT networks
- Increase operational efficiency through real-time assessment of unmanaged devices to ePO
- Minimize mean time to detect and respond to threats by automating remediation and response for noncompliant devices

Highlights

- Report new devices to ePO and bring all devices under Trellix ePO unified security management
- Share device contextual insight with ePO about unmanaged and rogue devices
- Automate installation and repair of Trellix ePO agents
- Ensure ePO agents are healthy and up-to-date at all times
- Isolate, restrict or prevent noncompliant devices from accessing the network dynamically and initiate remediation actions

Close the Gap Between Detection and Enforcement

Automatically Restrict, Isolate, or Remediate Devices Based on Endpoint Health

Organizations deploy security tools such as Trellix ePolicy Orchestrator, formerly known as McAfee ePO, to identify, manage and respond to endpoint security posture and threats. However, unmanaged devices, such as IoT and OT assets can evade visibility. This lack of visibility combined with a gap between detection and automated policy enforcement pose a security risk to the business. Compromised devices can be used as launch pads to target higher-value assets, gaining access to sensitive information that can cause significant impact, including failed audits in highly regulated environments.

Forescout eyeExtend for Trellix ePO provides enterprises with a comprehensive approach that spans complete endpoint detection and real-time response to security risks.

Challenges

Organizations use endpoint security products to manage endpoint protection of their managed devices. However those products don't provide visibility into unmanaged devices and lack the native ability to enforce access compliance in real-time. Endpoint alerts alone do not guarantee remediation or prevent lateral movement if a device or unmanaged asset is non-compliant, infected, or unprotected. Challenges include:

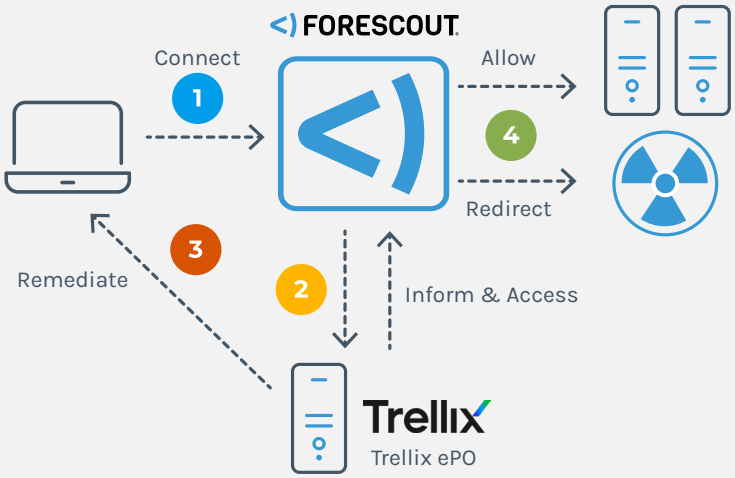
- Gap between detection and access control
- Lack of real-time policy enforcement based on endpoint posture
- Inability to maintain continuous endpoint compliance
- Lack of visibility into security posture for unmanaged devices

The Solution

Forescout eyeExtend for Trellix ePO lets network engineers and security operations teams visualize and automatically restrict, isolate, or remediate devices based on end-point compliance to access policies. eyeExtend orchestrates information sharing and security workflows between Forescout and Trellix ePO to improve device compliance and automate threat detection and response.

The Forescout solution leverages the comprehensive device visibility, and context provided by Forescout eyeSight. With in-depth device information, Forescout eyeExtend makes Trellix ePO aware of every single network attached device – including BYOD, transient and other non-traditional devices that are not managed by Trellix – enabling Trellix ePO to be aware of the entire enterprise attack surface.

Forescout eyeExtend also helps ensure that devices maintain the correct security posture and are compliant with enterprise security policies from the time they connect to the network and for the entire duration they remain connected. Forescout continuously validates the integrity of Trellix ePO agents on all devices. Forescout provides automated response options to isolate or restrict network access for noncompliant devices, facilitating remediation actions that enforce device compliance at all times.



1. Device connects to the network.
2. eyeExtend for Trellix ePO tells Trellix ePO whether a device is compliant.
3. Based on compliance posture and security, Forescout allows or denies network access to the device.
4. If device is noncompliant, it can be remediated either through ePO or via Forescout.

Use Cases

Expand Device Security Coverage

With its agentless complete device discovery, Forescout makes Trellix ePO aware of every single IP-connected device – whether managed, unmanaged or transient across IT and OT infrastructures – the instant it connects. This enables Trellix ePO to bring more devices under its centralized security management platform.

Improve Device Compliance

eyeExtend for Trellix ePO improves security hygiene by verifying that the Trellix ePO agent is installed and running on all devices and that it is communicating properly with Trellix ePO. If eyeExtend finds devices with missing, disabled or broken agents, it alerts Trellix ePO to install or repair the agent. Forescout can also trigger automated workflows for self-remediation to enforce managed device compliance.

Accelerate and Automate Policy-driven Threat Response

eyeExtend for Trellix ePO continuously monitors device status both at the time the device connects to the network and after. When Trellix ePO determines that a device is noncompliant with security policy, it informs Forescout in real time. Forescout can automatically take appropriate actions such as restricting, isolating or blocking compromised devices and initiating remediation workflows. Forescout eyeExtend for Trellix ePO addresses these use cases by bridging the gap enforcement gap between endpoint and network controls, enabling automated, policy-driven responses and supporting scalable infrastructure.

FORESCOUT®

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