Trellix

Forescout eyeExtend for Trellix® Network Security

Benefits

- Reduce security risk by extending Trellix Network Security's advanced threat detection to all connected network endpoints– including known and unknown devices
- Increase operational efficiency by automating threat response and remediation of all infected devices the moment they connect or when a new threat is detected

Highlights

- Scan all network devices for IOCs discovered by Trellix Network Security
- Contain threats by limiting or blocking infected devices from accessing the network in real time
- Eliminate threats from infected devices by killing suspicious processes
- Notify stakeholders such as security teams via emails detailing specific threats and their affected devices

Strengthen advanced threat detection and accelerate threat response

Organizations deploy advanced threat detection and prevention solutions such as Trellix Network Security to detect and eliminate known and advanced cyberthreats via multiple methods of security analysis. However, the speed and evasiveness of today's targeted attacks and increasing network complexity from a proliferation of unmanaged network devices—bring your own devices (BYOD), Internet of Things (IoT) and transient—can overwhelm security defenses and render them ineffective. IT and security teams must have a complete picture of the entire enterprise attack surface and a comprehensive, automated response strategy to combat today's cyberthreats, limit threat propagation and prevent security breaches and data exfiltration.

Forescout eyeExtend for Trellix Network Security enhances the power of Trellix's solution by helping organizations detect, share and hunt for advanced threats and indicators of compromise (IOCs) across all network-connected devices, and contain compromised devices to prevent lateral malware propagation.

Challenges

- Reducing the time to detect and evaluate potential threats across managed and unmanaged devices
- Responding quickly and effectively to the most advanced threats before they can propagate across the network and inflict damage

The Solution

Forescout eyeExtend for Trellix Network Security orchestrates workflows between the Forescout platform and Trellix Network Security to share device context, quickly detect threats across all network-connected devices and accelerate threat response by isolating compromised devices in real time to prevent lateral threat propagation.

Trellix Network Security fortifies network security by detecting and immediately stopping advanced, targeted and other evasive attacks hiding in internet traffic. However, preventing unmanaged devices and those infected on outside networks or via non-network pathways—such as USB devices—from connecting to the corporate network remains a challenge. Organizations must also find ways to determine the full extent of network infection and contain threats to prevent further internal propagation. It is often up to IT staff to analyze threat information and determine the best way to stop attacks from spreading, resulting in unnecessary delays and errors that enable damaging data breaches.

This is where Forescout eyeExtend for Trellix Network Security steps in. eyeExtend powered by eyeSight enables organizations to discover, classify and assess all network connected devices—including unmanaged IoT and BYOD systems—across campus, data center and cloud environments. It also orchestrates information sharing and automates workflows for policy-based control of these devices. eyeExtend receives alerts from Trellix Network Security on new threats

detected, their severity and indicators of compromise. Next, the Forescout solution quickly applies its rich device knowledge and response automation to take actions such as notifying security teams, initiating scans of all network-attached devices for new IOCs, blocking infected endpoints from accessing the network and activating remediation processes to stop threats from spreading.

In summary, Forescout eyeExtend for Trellix Network Security helps organizations reduce their attack surface and prevent threats from spreading and breaching sensitive data.

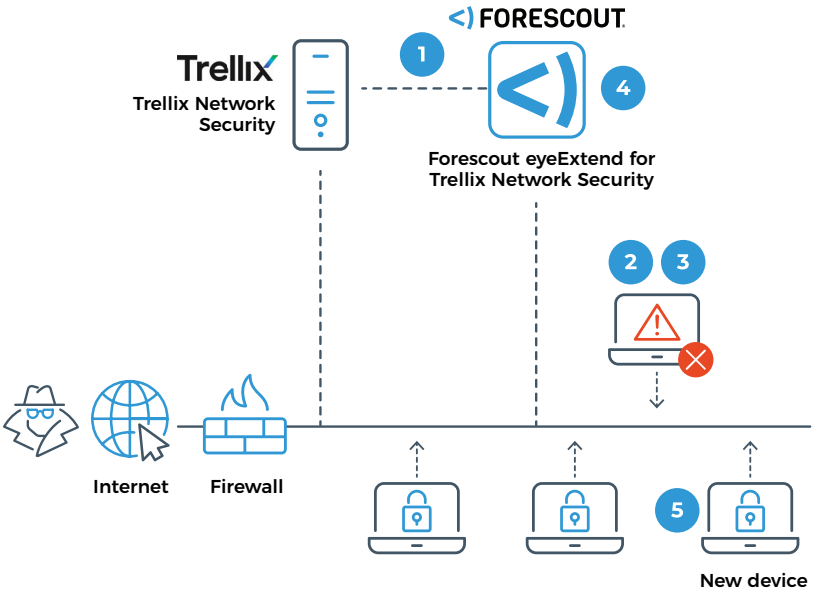
Use Cases

Leverage shared threat intelligence to maximize joint threat hunting and detection

When Trellix Network Security identifies malicious activity and IOCs, it immediately notifies Forescout eyeExtend for Trellix Network Security. The Forescout platform then extends this threat intelligence to the entire network, monitoring all devices—including unmanaged BYOD, guest and IoT devices—for IOCs. The Forescout platform also uses the threat information provided by Trellix Network Security to scan newer or transiently connected devices for threat IOCs the moment they connect. It then initiates device isolation and remediation, preventing the spread of threats from any device across the network.

Accelerate and automate policy-driven threat response

When an infected endpoint is detected, the Forescout platform limits or blocks its network access. This prevents lateral movement of the infection to other devices. The Forescout platform also remediates infected devices by killing suspicious processes and notifies stakeholders with details about which threats were detected on which devices. This helps organizations react in real time to threats based on predefined security policies.



1. Trellix Network Security detects malware and other advanced threats. Trellix Network Security notifies Forescout about infected devices and their threat severity and IOCs
2. Forescout isolates the infected device based on security policy
3. Using details from Trellix Network Security, such as file identification, registry changes and processes spawned, eyeExtend initiates remediation actions on infected devices
4. Forescout scans other devices on the network for the new IOCs and initiates isolation and mitigation actions
5. Forescout scans new devices attempting to connect to the network based on 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