Forescout eyeExtend for Trellix® Email Security

Benefits

- Reduce security risk by extending Trellix Email Security's threat detection to all network devices—known or unknown
- 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 IOC's discovered by Trellix Email Security
- Identify threats delivered through emails, attachments and embedded URLs that may not have been delivered through Trellix Email Security-monitored corporate emails
- Contain threats by limiting or blocking access of infected devices to the network in real time
- Eliminate threats from infected emails and devices by killing suspicious processes
- Notify stakeholders such as security teams via emails detailing specific threats and their affected devices

Protect against advanced email attacks and accelerate threat response

Cybercriminals often use spear phishing as well as malicious file attachments and URLs in emails to launch advanced cyberattacks. Hackers combine these tactics with email to routinely bypass conventional signature-based defenses such as antivirus and spam filters. Email threat detection solutions such as Trellix® Email Security (EX series) help protect organizations against advanced attacks on their corporate email accounts. However, evaluating potential advanced threats takes time and manual efforts to address them can overwhelm security teams, rendering defenses ineffective.

Forescout eyeExtend for Trellix Email Security enhances the power of Trellix's Email Security solution by helping organizations detect, share and hunt for Indicators of Compromise (IOCs) across all network-connected devices, including unmanaged devices, and contain compromised devices dynamically to limit malware propagation and minimize data breaches.

Challenges

- Reducing the time to detect and evaluate potential email-borne threats across the entire attack surface including managed and unmanaged devices
- Responding quickly and effectively to advanced email-related threats coming from any email account on any device connecting to the corporate network

The Solution

This integration combines the email threat detection mechanisms of Trellix Email Security with the device visibility and compliance enforcement capabilities of the Forescout Platform to multiply the benefits of working with an Advanced Threat Detection (ATD) product.

Trellix Email Security product fortifies network security by examining corporate email accounts, attachments and embedded URLs, detecting and stopping unknown malware, viruses and other threats they deliver. However, preventing personal email accounts, unmanaged devices and devices infected on outside networks or via non-network pathways—such as USB devices—from connecting to and infecting the corporate network remains a challenge. Organizations must also find ways to determine the full extent of network infection from email-related threats and contain threats to prevent further internal propagation. It is often up to security teams 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 Email Security steps in. The Forescout platform uses the threat information from Trellix Email Security to scan all corporate devices that may contain identified threats. It also extends visibility to other threat vectors outside of the corporate network, such as personal email, cloud storage accounts, smartphone text messages and other sources of malicious files that can be introduced into your network. Based on your policy, the Forescout

platform quickly applies its rich device knowledge and response automation to take actions such as notifying security teams, blocking infected endpoints from accessing the network, and activating remediation processes to stop threats from spreading.

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

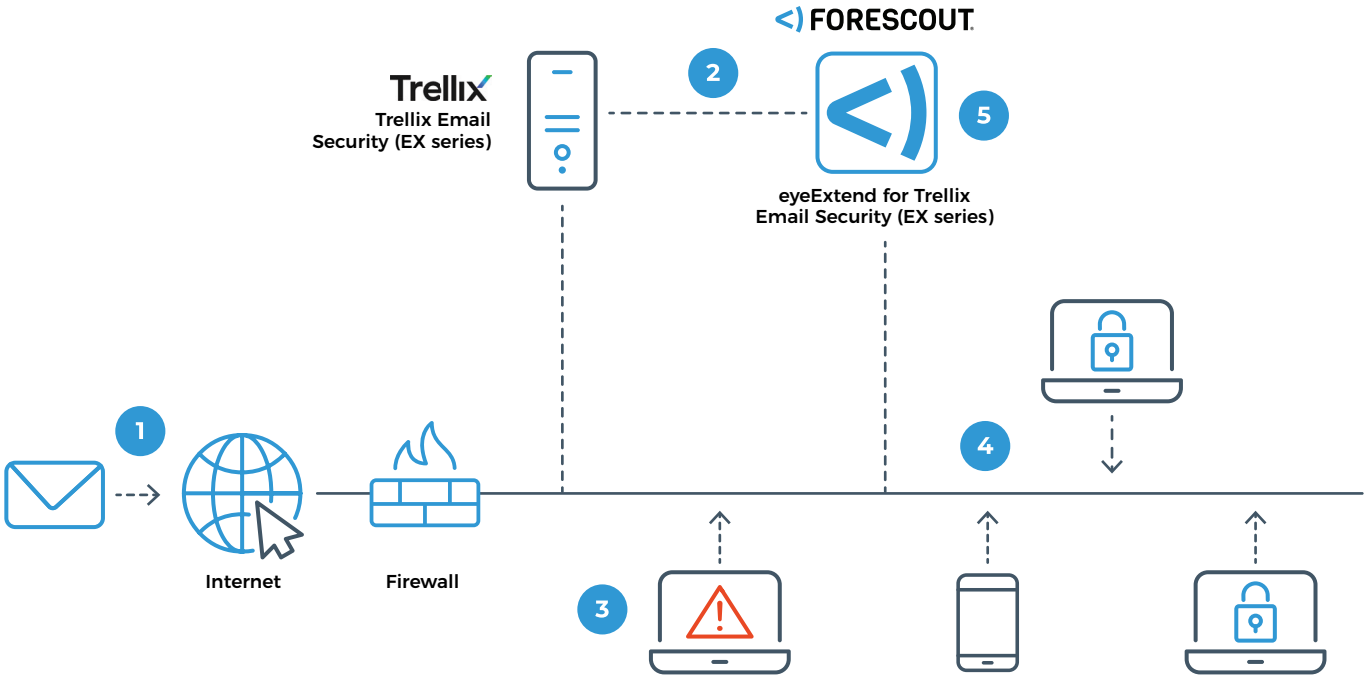
Use Cases

Leverage shared threat intelligence to maximize joint threat hunting and detection

When Trellix Email Security identifies malicious emails, attachments or embedded URLs and their IOCs, it immediately notifies Forescout eyeExtend for Trellix Email 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 this threat information to scan newer or transiently connected devices for threat IOCs the moment they connect.

Accelerate and automate policy-driven threat response

When Trellix Email Security detects an infected email, it quarantines the email and provides contextual information to Forescout eyeExtend for Trellix Email Security. Based on policy and threat severity, the Forescout platform automatically takes appropriate actions such as quarantining or blocking infected devices, scanning other devices for IOCs on the network, initiating direct remediation, sharing real-time context with other incident response systems or notifying the user via email or text message. These custom-defined actions can be performed manually or automatically.



1. Trellix Email Security detects email-related malware and other advanced threats.
2. Trellix Email Security notifies Forescout eyeExtend about infected emails, devices and IOCs.
3. Forescout isolates the infected device based on security policy in real time.
4. Forescout scans other devices on the network for the new IOCs and initiates isolation and mitigation actions on infected devices.
5. The Forescout platform scans new devices attempting to connect to the network for known IOCs.

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