Forescout eyeExtend

for Palo Alto Networks® WildFire®

Strengthen advanced threat detection and accelerate threat response

Organizations deploy advanced threat detection (ATD) solutions such as Palo Alto Networks WildFire to detect and prevent zero-day threats and malware. However, the speed and evasiveness of today's targeted attacks and increasing network complexity from a proliferation of unmanaged network attached-devices— bring your own device (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 Palo Alto Networks WildFire® enhances the power of the Palo Alto Networks solution by helping organizations detect, share and hunt for 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 the entire attack surface, including 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 Palo Alto Networks Wildfire enables the Forescout platform and Palo Alto Networks Wildfire to work together to quickly find indicators of compromise (IOCs), detect advanced threats, contain infected endpoints, and disrupt the cyber kill chain, thus preventing further lateral threat propagation and data exfiltration. This helps the security team prevent, detect, analyze, and respond to advanced attacks.

Palo Alto Networks WildFire fortifies network security by analyzing suspicious files, URL links and file transfers forwarded by Palo Alto Networks Next Generation Firewall (NGFW). Using sandboxing, threat intelligence, machine learning and other advanced techniques, it can detect and stop command and control communications and unknown malware, viruses and file transfers. However, preventing 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 and contain threats to prevent further internal propagation. Security teams must analyze threat information and determine the best way to stop

eyeExtend

Benefits

- Reduce security risk by extending WildFire's threat detection to all network endpoints, including known and unknown devices
- Increase operational efficiency by automating indicators of compromise detection and threat containment

Highlights

- Scan all network devices for IOCs discovered by Palo Alto Networks WildFire
- Contain threats by limiting or blocking access of infected devices to the network in real time
- Remediate infected devices by killing suspicious processes running on them
- Notify stakeholders such as security teams via emails detailing specific threats and their affected devices

attacks from spreading and avoid unnecessary delays and errors that enable damaging data breaches.

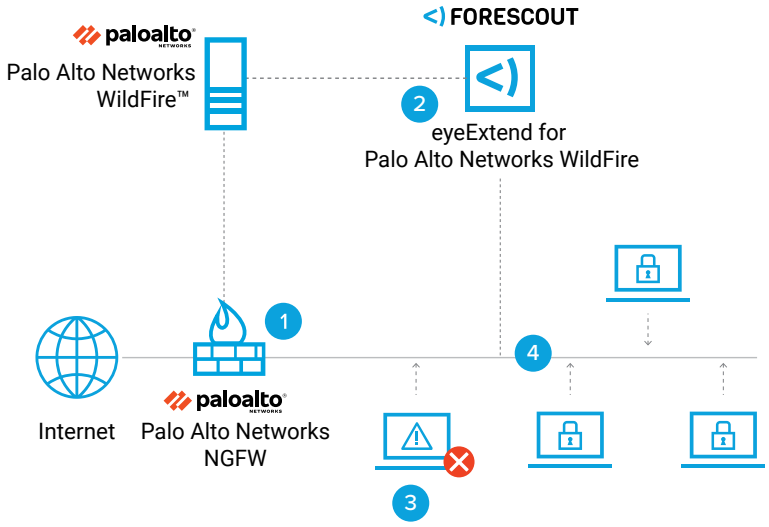
This is where the Forescout eyeExtend for Palo Alto Networks WildFire steps in. Forescout's integration with Palo Alto Networks WildFire powered by eyeSight enables organizations to discover, classify and assess all network connected devices, including campus, data center, IoT, BYOD devices and cloud instances. It then orchestrates device context sharing and automates security workflows for policy-based control of these devices. Forescout eyeExtend receives alerts from Palo Alto Networks NGFW on new threats and queries WildFire for detailed information on alert severity and indicators of compromise. It then quickly applies its rich device knowledge and response automation to take actions such as notifying security teams, blocking infected endpoints from accessing the network, initiating scans of all network-attached devices for new IOCs and activating remediation processes to contain threats.

In summary, Forescout eyeExtend for Palo Alto Networks WildFire 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 FireEye Network Security identifies malicious activity and IOCs, it immediately notifies Forescout eyeExtend for FireEye 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 FireEye 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. When a threat is detected, the Palo Alto Networks NGFW sends an alert to WildFire and eyeExtend
2. eyeExtend then queries WildFire directly to get more granular IOC information.
3. Forescout isolates the infected endpoint, and using details from WildFire such as file size, registry changes and processes spawned, Forescout initiates appropriate remediation actions based on policy.
4. Forescout scans other devices on the network, including those attempting to connect, for the new IOCs and initiates threat-mitigation actions on infected endpoints.

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