FORESCOUT

ForeScout Extended Module for Palo Alto Networks WildFire™

Improve defenses against advanced threats and automate threat response

Many of the attacks seen today rely on stealth, persistence and the skilled avoidance of traditional security systems. By continuously monitoring endpoints on the network and scanning for a broad set of indicators of compromise (IOCs), you can quickly identify potential threats and limit data breaches.

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor connected devices, including corporate, BYOD, guest and IoT

Control

- Allow, deny or limit network access based on device posture and security policies
- Reduce attack surface by ensuring endpoints have up-to-date security defenses
- Initiate remediation and risk mitigation actions on non-compliant or infected endpoints

Orchestrate

- Isolate infected endpoints identified by WildFire to prevent lateral malware propagation
- Scan endpoints connecting to your network for IOCs identified by WildFire
- Automate system-wide response to quickly mitigate threats and data breaches

The Challenges

Visibility. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. Most organizations are unaware of a significant percentage of the endpoints on their network because they are not managed, Bring Your Own Device (BYOD), guest or Internet of Things (IoT) endpoints. They may have disabled or broken agents, or aren't detected by periodic scans (transient devices). As such, you are unaware of the attack surface on these devices.

Threat Detection. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multivectored, stealthy and targeted, these attacks focus on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need new security controls that do not rely on signatures.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

ForeScout Extended Module for Palo Alto Networks WildFire

ForeScout CounterACT® and Palo Alto Networks WildFire™ work together to leverage the best-of-breed capabilities of each solution and provide a holistic approach to risk mitigation and threat management. The ForeScout Extended Module for Palo Alto Networks WildFire provides real-time visibility and compliance management of endpoints on your network, effective response to Advanced Persistent Threats (APTs) and zero-day threats, and automation to efficiently and accurately mitigate endpoint risks and advanced threats.

CounterACT is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric® Architecture to orchestrate information sharing and automate workflows among disparate security and IT management tools, including Palo Alto Networks WildFire.

1. A new malicious file is detected by Palo Alto Networks WildFire.
2. WildFire notifies the firewall about the malicious file.
3. CounterACT receives notification from the firewall about the endpoint and queries WildFire for additional information on the IOC detected.
4. CounterACT isolates the infected endpoint, and using details from WildFire such as file size, registry changes and processes spawned, CounterACT initiates appropriate remediation actions.
5. CounterACT scans other endpoints on the network, including those attempting to connect, for the new IOC and initiates threat-mitigation actions on infected endpoints.

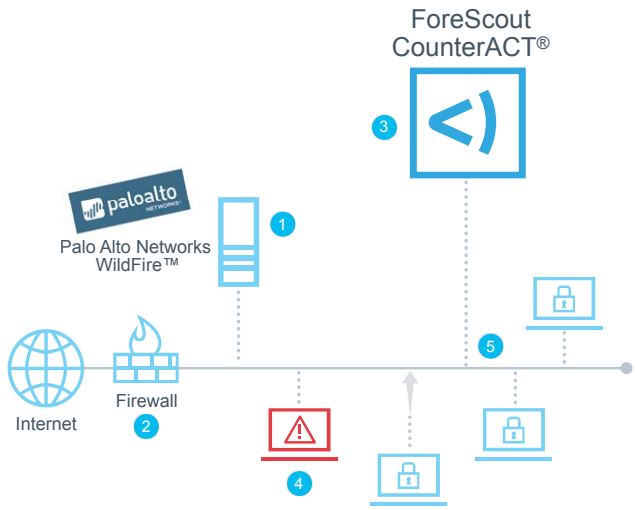

Figure 1: ForeScout CounterACT receives information from Palo Alto Networks WildFire and takes actions against compromised endpoints

ForeScout Extended Modules

The Extended Module for Palo Alto Networks WildFire is an optional module for ForeScout CounterACT and is sold and licensed separately. It is just one of many ForeScout Extended Modules that enables ForeScout CounterACT to exchange information, automate threat response and remediation and more efficiently mitigate a wide variety of security issues.

Learn more at
www.ForeScout.com

Palo Alto Networks WildFire offers a cloud-based, community-driven approach for detecting unknown threats that frequently bypass traditional security defenses. WildFire leverages a malware analysis environment in which new and unknown malware and exploits can run and be identified automatically and conclusively. WildFire then generates automatic protections and distributes them for enforcement within as little as five minutes.

Using IOC details identified by WildFire, such as file size, files created or modified, Windows® registry changes or processes spawned, CounterACT can scan devices connecting to the network for these specific IOCs.

When WildFire detects malware and determines that an endpoint within your network has been compromised, it informs the Palo Alto Networks Next-Generation Firewall. The firewall sends basic information about the IOC and the compromised endpoint to CounterACT. CounterACT can then query WildFire to get more in-depth information about the identified IOC. This allows CounterACT to scan other endpoints that are attempting to connect or are already connected to your network for the presence of infection. Infections on other endpoints may have occurred on public networks, on unmonitored corporate networks or via non-network pathways such as USB devices, and can be detected by CounterACT. CounterACT is able to prevent these infections from spreading at the time the infected endpoints connect to the network. CounterACT is able to take the appropriate action based on the severity of the threat, such as isolating the endpoint, initiating external remediation or sharing real-time context with other incident response systems.

With the Extended Module for Palo Alto Networks WildFire, organizations can realize improved visibility and real-time intelligence, detect advanced threats and zero-day malware, provide a rapid response to compromised endpoints and have policy-based control to automate responses to identified threats. With this capability, customers can limit malware propagation, minimize data breaches, avoid costly investigations and protect their reputation.

FORESCOUT

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591