Organizational Challenges

- Obtain continuous discovery and assessment of devices without disrupting business operations
- Ensure corporate devices are compliant with needed patches, appropriate software versions and management/security agents are installed, running and current
- Apply appropriate policy controls based on cohesive device and threat intelligence
- Achieve continuous monitoring and mitigation capabilities network-wide across device types
- Keep both internal and external auditors satisfied that your devices, data and network are secure
- Obtain real-time endpoint compliance capabilities without the costs and delays associated with security personnel interventions

Technical Challenges

- Detect and contain suspicious or rogue endpoints the instant they access the network
- Maximize corporate endpoint protection, enforce endpoint compliance and prevent the lateral spread of threats
- Control endpoint configurations according to organizational best-practice policies and regulatory mandates
- Eliminate vulnerabilities on common software platforms that leave you exposed to breaches and make it difficult to validate device compliance

ForeScout and Palo Alto Networks® Traps™

Increase enterprise-wide endpoint security to reduce your attack surface and improve compliance

Noncompliant endpoints equal business risk. ForeScout solutions find and secure devices—measuring compliance against endpoint security policies and enforcing the appropriate controls to help you comply with internal mandates and industry regulations. Palo Alto Networks® Traps™ advanced endpoint protection minimizes endpoint infections by blocking malware, exploits and ransomware. The combined ForeScout and Palo Alto Networks solution delivers coordinated threat analysis, shared intelligence and automated containment. The result is vastly improved situational awareness, rapid threat response and improved security policy compliance.

The Challenge

With the explosion of critical system connections and virtual machines dramatically expanding the numbers of managed and unmanaged devices accessing networks every day, IT professionals are dealing with endpoint security challenges like never before. Still worse, point-in-time scans, manual inventory assessments and other traditional methods for maintaining device compliance are largely ineffective.

Fortunately, there is nothing traditional about the ForeScout platform. It offers a unique combination of agentless visibility and continuous monitoring of connected devices, as well as orchestration with popular security and infrastructure tools such as Palo Alto Networks Traps.

The ForeScout and Palo Alto Networks Traps Integrated Solution

ForeScout integrates with Palo Alto Networks® Traps™ to increase endpoint and network protection. The integration combines the ForeScout platform's vast visibility and control capabilities across heterogeneous network tiers and device types, including IoT, OT, BYOD and guest devices, with Palo Alto Networks Traps' Advanced Endpoint Protection for Microsoft Windows®, Apple MacOS® and Linux systems. The integration enables joint Palo Alto Networks Traps and ForeScout customers to:

- Optimize endpoint/device compliance and Traps protection coverage
- Extend threat and incident-response actions to include ForeScout network and system controls and remediation workflows

Benefits

Automate Threat Containment

The ForeScout-Palo Alto Networks Traps integration lets you automate host and network controls to immediately contain threats identified by Traps. ForeScout can also contain noncompliant endpoints that are missing the Traps agent.

Accelerate Remediation

Automate policy-based actions to restrict or quarantine noncompliant or compromised devices, achieving a higher level of security protection. Remediation actions include initiating workflows to install patches or functioning Traps agents. Also, by revealing unmanaged/unsecured devices connecting to your network, ForeScout helps you proactively secure and onboard rogue endpoints with Traps.

Increase Efficiency, Reduce Costs and Improve Audits

Automate previously manual network hygiene tasks and free up IT management and security staff to focus on more strategic projects. By reaching a higher level of device hygiene through automation, your security teams have fewer tasks that require their attention, and auditors can point to far fewer issues.

- Proactively hunt for threats, including zero-day exploits, across all connected devices network-wide

Together, ForeScout and Palo Alto Networks offer exceptional endpoint and overall network protection across today's ever-evolving threat landscape.

Optimize Endpoint Compliance and Traps Protection Coverage

ForeScout continually assesses endpoints upon connection to verify that device profiles adhere to corporate policies, including configuration requirements, segmentation rules and that threats are not present. Due its agentless capabilities, ForeScout discovers new, noncompliant and rogue endpoints that lack the Traps agent. For endpoints with the Traps agent, ForeScout also verifies the Traps agent is up to date, running as it should and communicating with the Traps management server. If an endpoint is found to be noncompliant, ForeScout can initiate the appropriate policy-driven workflows to, for example, move the endpoint to a VLAN until compliant, initiate installation of the Traps agent and onboard the endpoint with the Traps server. The ForeScout-Palo Alto Networks Traps integration helps you ensure that corporate-managed Windows, MacOS and Linux endpoints are equipped with Traps.

Extend Threat Response Beyond the Endpoint to Include ForeScout Controls and Workflows

Traps has a comprehensive mechanism by which it protects endpoints against threats such as malware and application exploit vulnerabilities, whether endpoints are on or off-network. ForeScout extends this protection by enabling automated policy-driven network and system actions that are triggered by endpoint information from both Traps and ForeScout. ForeScout helps prevent risky network access and threat propagation outside the compromised endpoint with actions such as isolating the compromised or noncompliant endpoint, enforcing segmentation rules, generating an email alert and initiating remediation procedures to, for example, install a Traps agent or a needed patch.

Increase Protection with Threat Hunting and Dynamic Segmentation

You can further extend protection capabilities by leveraging a Traps subscription to Palo Alto Networks WildFire® for malware analysis. The ForeScout integration with WildFire continuously updates the ForeScout platform with WildFire threat intelligence, including zero-day exploits. ForeScout uses the indicators of compromise (IOC) information it receives to proactively hunt for threats across managed and unmanaged endpoints on your enterprise network. Endpoints are assessed as soon as they connect and continuously while connected. ForeScout can also immediately respond to threats discovered with policy-driven actions to isolate and remediate as explained earlier.

The ForeScout integration with Palo Alto Networks NGFW enables you to automatically tag devices and enforce NGFW segmentation rules with those tags. Segmentation rules can be as granular as desired based on the device classification and rich context ForeScout gathers, including Traps intelligence on managed endpoints. These additional capabilities do not require upfront device knowledge or a network redesign. Security protection is increased across managed and unmanaged endpoints, including BYOD, guest and IoT. The powerful combination of ForeScout and Palo Alto Networks allows you to dynamically reduce attack surfaces and combat threats across device types and network tiers on your global network.

ForeScout and Palo Alto Networks Traps Integration Capabilities

Verify Traps agent compliance

ForeScout's agentless visibility helps to maximize corporate endpoint compliance with Traps agent protection. To achieve this, ForeScout scans connected endpoints to verify required processes are running on corporate devices. A device is deemed compliant only if Traps is installed, running properly and up to date. If noncompliant, ForeScout can also initiate remediation workflows to, for example, isolate the noncompliant device in a VLAN, install the Traps agent and onboard the endpoint with the Traps server.

Verify Traps heartbeat

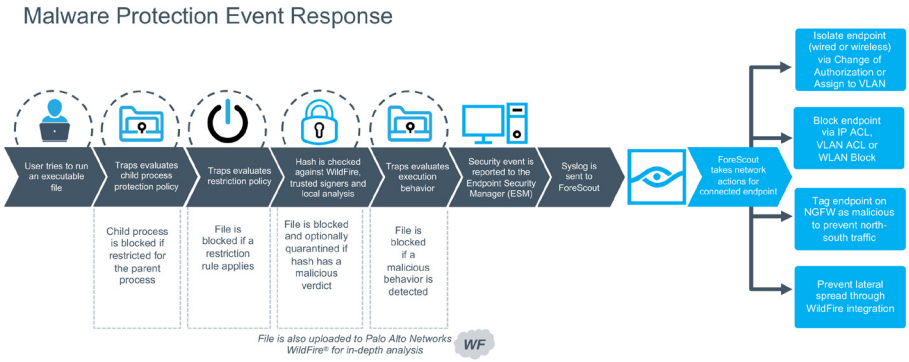
A Traps heartbeat is an essential communication mechanism between an endpoint's Traps agent and the Traps server. While an agent may be installed and running on an endpoint, the process could still be compromised with an attempt to block communication with the Traps server and prevent the endpoint from getting the latest security updates. This creates threat vulnerability. ForeScout can continuously monitor corporate endpoints to verify a heartbeat is occurring. A policy can also be configured to act if no heartbeat is detected, so the issue can be rapidly addressed.

Protect Traps server

While endpoint security is of primary importance, we cannot ignore the security aspects of the server from where all the endpoints are monitored. The ForeScout platform monitors the Traps server to see if the Traps services are running, such as Console Upload Service, Core Upload Service and the Endpoint Security Manager Service. In the event ForeScout detects an issue with the Traps server, specifically from the operating system, ForeScout can take a variety of actions including running a vulnerability scan or patching the system via SCCM, thus protecting the server and the network from vulnerabilities.

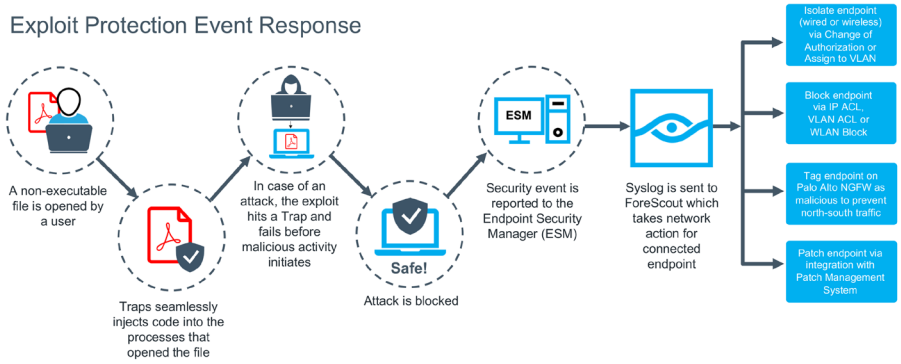
Respond to malware protection events

Traps has a comprehensive mechanism which detects malware on an endpoint. Based upon Traps analysis done of malware from, for example, Microsoft Office, DLL and EXE files, the ForeScout platform receives information from the Traps server about the event details such as Event Type, Protection Type, File Name/ Process Name, File Hash, Endpoint IP and details on what child process was called upon. All of these details are mapped in ForeScout to Host Properties for the specific endpoint. Policies can then be built in ForeScout based on those details to take the most effective action(s) to respond to events. An action can be at the network or endpoint level, or can simply trigger email alerts. Actions can also include, for example, triggering a network scan for IOC information collected from ForeScout integrated threat intelligence sources such as Palo Alto Networks WildFire.



Respond to exploit protection events

Traps collects Exploit Event information such as vulnerabilities in software application processes. ForeScout receives Exploit Event information from the Traps server, including details such as Event Type, Protection Type, File Name/ Process Name, File Hash and Endpoint IP. All of these details are mapped in ForeScout to Host Properties for the specific endpoint. Policies can be built in ForeScout to take appropriate actions based on these details from Traps. Action(s) taken can be at the network level, endpoint level or trigger Microsoft SCCM for patch management. ForeScout provides the flexibility to manage numerous actions for increased endpoint and network protection.



Learn more at
www.ForeScout.com

Summary

The integrated combination of ForeScout and Palo Alto Networks solutions helps close security gaps and increases overall endpoint and network protection. The closed-loop workflows afforded by integration with Palo Alto Networks Traps helps automatically enforce endpoint compliance and dynamically segment endpoint devices based on policies built with combined intelligence from ForeScout and Traps. Intelligence and security controls can be enhanced further via ForeScout integrations with Palo Alto Networks NGFW and WildFire. The end result is increased operational efficiency and effectiveness in reducing risk.

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