FORESCOUT

Solution Brief

Forescout Extended Modules for Endpoint Protection Platforms

Improve real-time visibility over managed and unmanaged devices while automating network access control and threat response

Highlights

See

- Detect devices the instant they try to access your network
- Profile and classify BYOD and corporate devices without relying on agents
- Scan unmanaged devices to identify malicious files or processes

Control

- Identify and fix corporate devices with missing, disabled or misconfigured EPP agents
- Allow, deny or limit network access based on device posture and security policies
- Restrict and/or remediate malicious or high-risk endpoints to reduce attack surface

Orchestrate

- Leverage the combined intelligence of Forescout CounterACT and your EPP system to improve overall security posture
- Receive contextual threat information from your EPP, allowing security components to operate as one cohesive system
- Automate response workflows using Forescout CounterACT based on information from your EPP system to reduce risks from non-compliant or infected endpoints

Forescout Extended Modules for Endpoint Protection Platform enable contextual sharing of endpoint and threat intelligence between Forescout CounterACT® and your existing Endpoint Protection Platform (EPP) system. This integration allows for automation of response workflows for risk mitigation and threat defense. As a result, customers with Forescout Extended Modules can gain superior visibility and control of both managed and unmanaged endpoints, and protect their networks from non-compliant, infected or malicious endpoints.

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 either unmanaged, Bring Your Own Device (BYOD), guest or Internet of Things (IoT) endpoints. They may have disabled or broken agents, or are transient devices that aren't detected by periodic scans. As such, they remain invisible to most security tools.

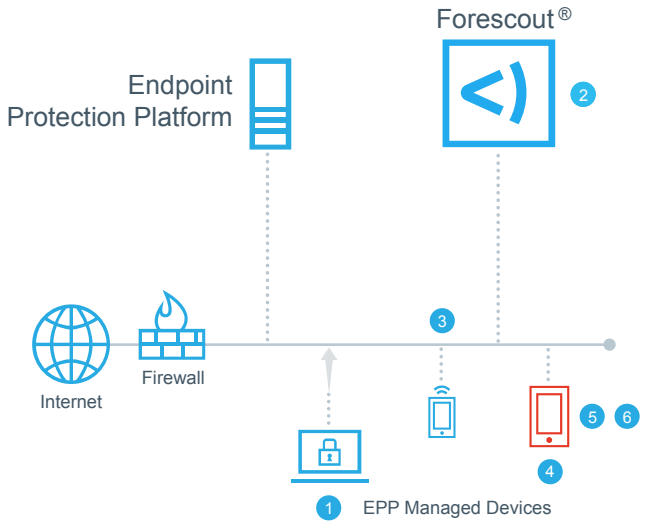
Threat Detection. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multivectored, stealthy and targeted, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need next-generation 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.

How Forescout Extended Modules for EPP Work

Forescout 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 and Forescout Extended Modules to orchestrate information sharing and automate operation among disparate security and IT management tools.

1. An endpoint attempts to connect to the network.
2. Forescout CounterACT scans and classifies the endpoint and if required, looks for the EPP client.
3. If the EPP client is installed and functional, and the endpoint is compliant, it is allowed on the network.
4. If the EPP client is missing, or the device is non-compliant, it is isolated until remediation actions can be performed.
5. If the EPP client is missing or non-functional, the endpoint is isolated and the client is installed per company policy.
6. Once compliant, the endpoint is allowed on the network and given access to the protected information.



Unlike other NAC solutions that integrate with Endpoint Protection Platforms to simply learn about antivirus status, Forescout CounterACT deeply integrates with your EPP, leveraging the best-of-breed capabilities of each product. CounterACT detects and profiles devices as they connect to the network—whether managed or unmanaged, wired or wireless, mobile or traditional. Based on this inspection, CounterACT determines the device type, operating system, ownership and security posture.

If the connecting device is a corporate device and has an EPP agent installed, the agent tells CounterACT what it knows about the endpoint compliance status of the device. If the device does not have an EPP agent, CounterACT will inspect the device to determine its compliance status. If the device is compliant and the user is authorized, CounterACT allows the device to access the appropriate network resources, according to your policy.

If an EPP agent is missing or broken, CounterACT alerts the EPP system to install or repair the agent. If this is unsuccessful, CounterACT will either attempt to install the EPP agent directly or it will capture the endpoint's browser and send the user to a self-remediation page. CounterACT also notifies the EPP about unauthorized or non-compliant devices.

Once admitted to the network, if the EPP determines that the endpoint has become non-compliant, the EPP can be configured to tag the endpoint and immediately report its non-compliance to CounterACT, which can isolate the endpoint until remediation has been performed. CounterACT also continually monitors the endpoint to determine if its behavior becomes threatening. For example, CounterACT may isolate the endpoint, disable the USB port, or kill an unauthorized application.

Forescout Extended Modules for EPP are optional modules for Forescout CounterACT and are sold separately. When used in conjunction with your existing EPP system, Forescout CounterACT and these Extended Modules provide automated response to maintain compliance of endpoints while providing a dynamic threat detection approach to security, thereby reducing the attack surface of your network.

Supported Products

Products supported by Extended Modules for EPP include:

- McAfee ePO
- Symantec Endpoint Protection

Learn more at
www.Forescout.com

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