ForeScout

Solution Brief

ForeScout Extended Modules for Endpoint Security Platforms

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

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Classify and profile devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

Control

- Identify and fix corporate devices with missing, disabled or broken 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 or EDR platform to improve overall security posture
- Verify if the security agent is installed and operational on-connection before allowing network access
- Trigger real-time malware scans based on third-party threat intelligence

ForeScout Extended Modules for endpoint security platforms enable contextual sharing of endpoint and threat intelligence between ForeScout CounterACT® and your existing EPP and EDR platforms. 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) devices. 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 and EDR 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 security agent
3. If the agent is installed and functional, and the endpoint is compliant, it is allowed on the network.
4. If the agent is missing, or the device is non-compliant, it is isolated until remediation actions can be performed.
5. If the security agent is 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.

Supported Products

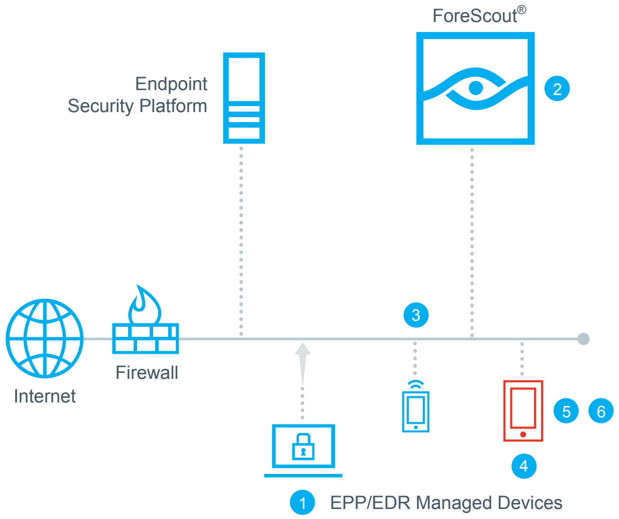
Products supported by Extended Modules for EPP and EDR platforms include:

- McAfee® ePO™
- Symantec™ Endpoint Protection

Learn more at
www.ForeScout.com

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



Unlike other Network Access Control (NAC) solutions that integrate with your endpoint protection platform (EPP) or endpoint detection and response (EDR) platform to simply learn about antivirus status, ForeScout CounterACT deeply integrates with your endpoint security platform, 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 agent installed, CounterACT validates the security posture and compliance status before allowing network access.

If the security agent is not installed or broken, CounterACT alerts the endpoint management platform to install or repair the agent. If this is unsuccessful, CounterACT will capture the endpoint's browser and send the user to a self-remediation page. CounterACT also notifies the endpoint security platform about unauthorized or non-compliant devices.

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

The ForeScout Extended Modules for endpoint security are add-on modules that are licensed and sold separately. Like other ForeScout Modules, they enable CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response.

For details on our licensing policy, see www.forescout.com/licensing