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

ForeScout Extended Modules for endpoint security platforms enable contextual sharing of endpoint and threat intelligence between the ForeScout platform and your existing EPP and EDR platforms. These integrations allow you to automate response for faster risk mitigation and stronger threat defense. You can gain superior visibility and control of both managed and unmanaged endpoints, and protect your networks from noncompliant, infected or malicious devices.

Highlights

See

- Discover managed and unmanaged 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 the ForeScout platform and your EPP or EDR platform to improve overall security posture
- Verify if endpoint security agents are installed and operational on-connection before allowing network access
- Take actions such as triggering real-time malware scans based on third-party threat intelligence

The Challenges

Incomplete 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 devices such as BYOD, guest or IoT devices. Devices may have disabled or broken agents, or are on-the-move devices that aren't detected by periodic scans. As such, they remain invisible to most security tools.

Difficulty to detect threats. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multi-vectored, 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..

Lack of automated response. 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 continuous monitoring and mitigation of endpoints, you spend valuable time performing these tasks manually. You don't have the ability to automatically and quickly respond to attacks and security breaches, thereby leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

How ForeScout Extended Modules for EPP and EDR Work

The ForeScout platform provides the unique ability to see devices, including non-traditional devices, the instant they connect to the network. It provides policy-based control of these devices, orchestrates information sharing and automates operations among disparate security and IT management tools.

Unlike other network security solutions that integrate with your endpoint protection platform (EPP) or endpoint detection and response platform (EDR) to simply learn about antivirus status, the ForeScout platform deeply integrates

1. An endpoint attempts to connect to the network.
2. ForeScout scans and classifies the endpoint and looks for required security agents.
3. If agents are installed and functional, and the endpoint is compliant, it is allowed on the network.
4. If an agent is missing, or the device is noncompliant, 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

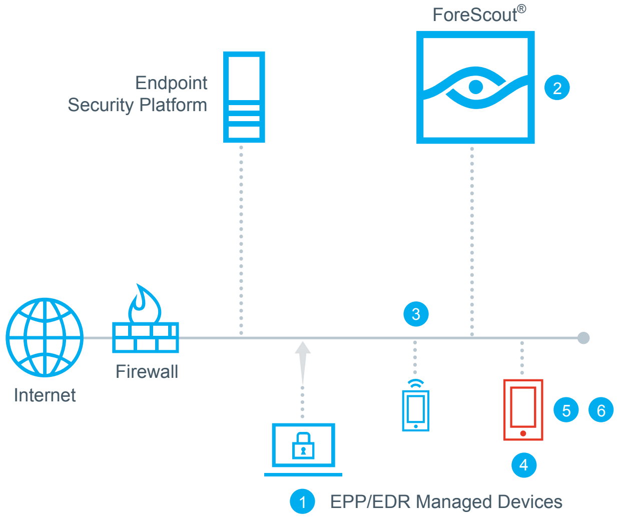
Products supported by Extended Modules for EPP and EDR platforms include:

- McAfee® ePO™
- Symantec™ Endpoint Protection
- FireEye® HX
- CrowdStrike®
- Carbon Black

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



with your endpoint security products, leveraging their best-of-breed capabilities. It detects and profiles devices as they connect to the network—whether managed or unmanaged, wired or wireless, mobile or traditional. Based on this inspection, the ForeScout platform determines the device type, operating system, ownership and security posture.

If the connecting device is a corporate device and has an agent installed, the ForeScout platform lets you validate the security posture and compliance status before allowing network access.

If the security agent is not installed or broken, the ForeScout platform alerts the endpoint management system to install or repair the agent. If this is unsuccessful, ForeScout will capture the endpoint's browser and send the user to a self-remediation page.

Our platform also notifies the endpoint security systems about unauthorized or noncompliant devices. Once admitted to the network, if the agent determines that the endpoint or the endpoint management is no longer compliant, the endpoint management platform can be configured to tag the endpoint and immediately report its noncompliance to the ForeScout platform which can isolate the endpoint until remediation occurs.

The ForeScout platform also continually monitors the endpoint to determine if its behavior is suspicious. This allows it to take different actions per policy such as quarantining an endpoint, disabling a USB port or killing 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 the ForeScout platform to exchange information with your existing security solutions, automate multivendor workflows and accelerate system-wide response.

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