FORESCOUT

See

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

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Orchestrate

- Share contextual insight with McAfee ePO about unmanaged endpoints and rogue devices
- Automatically evaluate information from McAfee ePO to apply security policies against any device
- Accelerate system-wide response to quickly mitigate risks and data breaches

The ForeScout-McAfee ePO Joint Integration

Supplement McAfee ePO with real-time visibility over managed and unmanaged personal devices and automated network access control.

The ForeScout ePO Integration Module allows ForeScout CounterACT® to integrate with McAfee ePO. This integration provides IT security managers with superior visibility and control of both managed and unmanaged endpoints on the network. In addition, this integration helps organizations save time by automating the installation of security agents, including those from McAfee, and assuring those agents are healthy and up-to-date.

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 not managed (BYOD, guest and IoT), 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 cyber threats 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 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 cyber threats to propagate within your network and exfiltrate data.

How it Works

Ensure corporate device security with CounterACT and McAfee ePO integration

If the connecting device is a corporate device and has a McAfee agent installed, ePO tells CounterACT what it knows about the endpoint compliance status of the device. If the device does not have a McAfee 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 a McAfee agent is missing or broken, CounterACT alerts ePO to install or repair the agent. If this is unsuccessful, CounterACT will either attempt to install the McAfee agent directly, or, it will capture the endpoint's browser and will send the user to a self-remediation page. CounterACT also notifies the ePO Rogue System Detection about unauthorized or non-compliant devices.

Once admitted to the network, if ePO determines that the endpoint has become non-compliant, ePO can be configured to tag the system 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.

1. Device connects to the network
2. CounterACT informs ePO of device status
3. If non-compliant, ePO remediates the device
4. CounterACT allows or denies access based on ePO's assessment

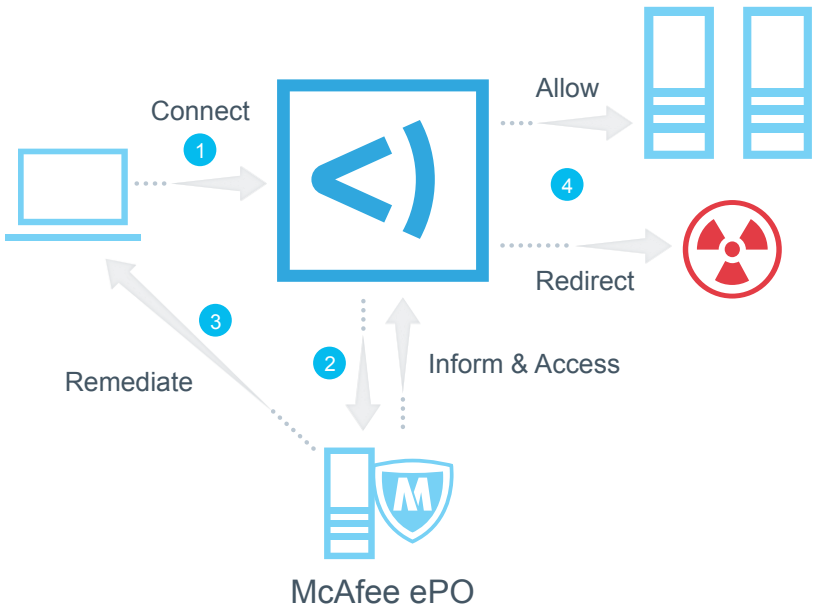

Figure 1: ForeScout CounterACT and the McAfee ePO work in concert to assess and remediate devices as they access the network.

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