FORESCOUT

Intel® Security Integration Module

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 Windows devices to identify malicious files or processes

Control

- Identify and fix corporate devices with missing, disabled or misconfigured McAfee 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 endpoint intelligence of McAfee ePO and ForeScout CounterACT to improve overall security posture
- Receive contextual threat information from McAfee Threat Intelligence Exchange via the McAfee Data Exchange Layer, allowing security components to operate as one cohesive system
- Automate response workflows using ForeScout CounterACT based on insights from McAfee ePO and McAfee Threat Intelligence Exchange to reduce risks from non-compliant or infected endpoints

The Intel® Security Integration Module enables ForeScout CounterACT® to integrate bi-directionally with McAfee® ePolicy Orchestrator® (ePO™) and McAfee® Threat Intelligence Exchange. This enables contextual sharing of endpoint and threat intelligence between CounterACT and Intel Security products, and automation of response workflows for risk mitigation and threat defense. As a result, Intel Security customers 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

Securing what you can't see. Many organizations utilize McAfee ePO to manage endpoint security on corporate-owned devices. But ePO can't identify or profile unmanaged or BYOD (personal) devices. These devices are often unpatched, lack security agents and include unauthorized applications. Hence, they can serve as network-attached launching points for malware. To reduce this visibility gap, you need a real-time network security solution such as CounterACT.

Controlling network access and reducing risk. According to industry experts, a majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. To harden the enterprise network, you need to know the security posture of devices when giving them network access and take mitigating actions to reduce the attack surface. If a device becomes infected and poses a threat to your network, you must be able to quickly identify and contain the source of the attack.

Automating threat response. Threat intelligence changes in real time. New threat data must be automatically shared across security solutions, allowing them to operate as a cohesive system. Additionally, you need an automated system to continuously monitor and remediate endpoint vulnerabilities and security gaps based on the latest threat intelligence, as well as to respond to attacks and security breaches to limit malware propagation and data exfiltration.

ForeScout Integration with McAfee ePO and McAfee Threat Intelligence Exchange

Unlike other NAC solutions that integrate with McAfee ePO simply to learn about antivirus status, ForeScout CounterACT deeply integrates with Intel Security products, leveraging the best-of-breed capabilities of each product. The joint solution includes four components:

- **McAfee Threat Intelligence Exchange** delivers a cohesive framework where security products collectively pinpoint threats and act as a unified threat defense system that provides security resilience and immunity to infections.
- **McAfee Data Exchange Layer** is a bi-directional communications fabric that allows multiple security components to share threat intelligence and react in real-time to changing conditions.
- **McAfee ePolicy Orchestrator** is a centralized security management system to manage security across corporate endpoints and streamline and automate compliance processes.
- **ForeScout CounterACT** is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications, determining the user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents. It provides remediation, control and continuous monitoring of these devices.

ForeScout CounterACT detects and profiles devices as they connect to the network—whether managed or unmanaged, wired or wireless, mobile or traditional laptops. Based on this inspection, CounterACT determines the device type, operating system, ownership and security posture.

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.

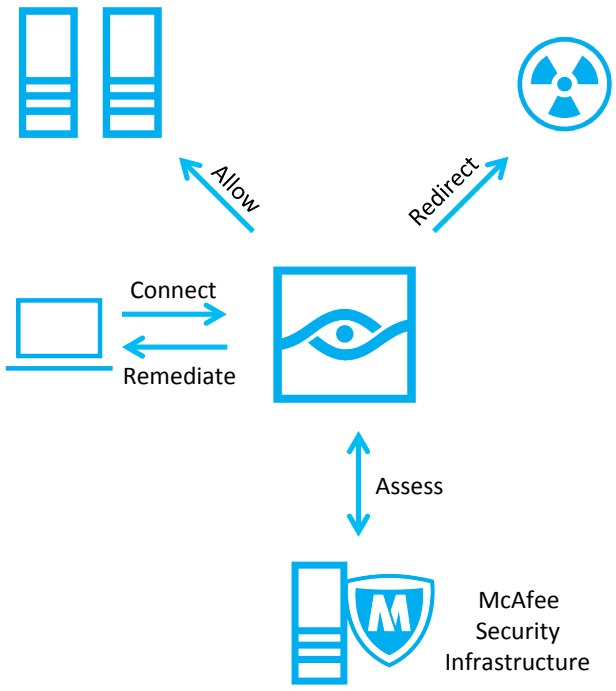

Figure 1: ForeScout CounterACT and the McAfee Security Infrastructure work in concert to Assess and remediate managed and unmanaged devices.

Enable BYOD security with CounterACT and McAfee Threat Intelligence Exchange integration

If the connecting device is a personal Windows device, CounterACT scans the system to identify all running processes, and communicates this information to McAfee Threat Intelligence Exchange via the McAfee Data Exchange Layer. McAfee Threat Intelligence Exchange responds with a threat score for each process. Based on this information, CounterACT allows devices that are free of malicious processes onto the production network. If the threat score indicates a potential malicious threat, CounterACT can terminate a process, remediate the endpoint or isolate the device until remediation can be performed.

When McAfee Threat Intelligence Exchange receives information about new malware, it broadcasts this information over the McAfee Data Exchange Layer to CounterACT. Once CounterACT receives this threat alert, it scans unmanaged Windows devices on the network to see if they contain the malicious file or process. Based upon your security policies, CounterACT can perform a wide range of control actions, including endpoint isolation, killing a malicious process or initiating other remediation actions and alerting the user.

The Intel Security Integration Module is just one of many IT system integrations that are available within the ForeScout ControlFabric® architecture. For more information about the ForeScout ControlFabric architecture and how ControlFabric can help IT security managers easily share information among security products and quickly respond to security issues, visit www.forescout.com/controlfabric.

Supported Products

- The integration with McAfee ePO requires McAfee ePO server versions 4.6 and above.
- The integration with McAfee Threat Intelligence Exchange requires McAfee Data Exchange Layer 1.1, McAfee Threat Intelligence Exchange 1.1.0 and McAfee ePO 5.3 and above

Please refer to product documentation for additional requirements and supported versions.

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

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