Solution Brief

ForeScout Integration with McAfee Threat Intelligence Exchange and McAfee Data Exchange Layer

Gain real-time threat insight and rapidly mitigate risks from unmanaged and BYOD endpoints

See

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

Control

- Grant, deny or limit network access based on device posture and security policies
- Quarantine malicious or high-risk BYOD endpoints
- Automate remediation of BYOD endpoints to reduce attack surface

Orchestrate

- Leverage the McAfee Data Exchange Layer to share information between CounterACT and McAfee Threat Intelligence Exchange
- Evaluate running processes on BYOD Windows devices and determine threat profile
- Receive threat data from McAfee Threat Intelligence Exchange and inspect all BYOD Windows devices across the enterprise network

ForeScout CounterACT® now provides bi-directional information sharing with McAfee® Threat Intelligence Exchange over the McAfee Data Exchange Layer. With this integration, customers can leverage system-wide threat intelligence from all McAfee security components, and protect their networks from unmanaged and personally owned (BYOD) Windows devices.

The Challenges

Visibility. Any serious attempt to manage security risk must start with knowledge of who and what is on your network, including visibility to whether the devices on your network are compliant with your security standards. 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. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network.

Threat Detection. Today's cyber attacks are more sophisticated than ever. Multi-vectored, stealthy and targeted threats easily evade traditional security defenses such as firewalls, intrusion prevention systems, anti-virus platforms, and secure web and email gateways. Originating from highly motivated and well-funded threat actors and nation states, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. As the attackers have gained the upper hand, organizations are being compromised at an accelerating rate. In order to effectively detect and block these sophisticated threats, new security controls that do not rely on signatures are needed.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating a perfect storm for any incident response program. Without an automated system to monitor, install, update and reactivate security agents on managed systems, valuable time is lost performing these tasks manually. Without the ability to apply security controls to unmanaged endpoints (BYOD, guest and IoT), you are increasing your attack surface and putting your infrastructure at risk. And without a system 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

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

The combined Intel Security/ForeScout solution includes three 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.
- **ForeScout CounterACT®**, the industry's leading agentless cybersecurity appliance, 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. CounterACT is the first third-party solution to integrate with McAfee Threat Intelligence Exchange and McAfee Data Exchange Layer.

This integrated solution allows you to assess the security posture of unmanaged Windows devices, quarantine or limit network access of those devices that are determined to be risky or malicious, and initiate remediation actions when necessary on unmanaged Windows devices. It addresses two previously unmet needs:

1. Device connects to the network and CounterACT scans device and gathers list of running processes
2. CounterACT communicates information to McAfee TIE via McAfee DXL
3. If non-compliant, CounterACT allows or denies access based on threat score from TIE
4. CounterACT terminates malicious processes or remediates the endpoint

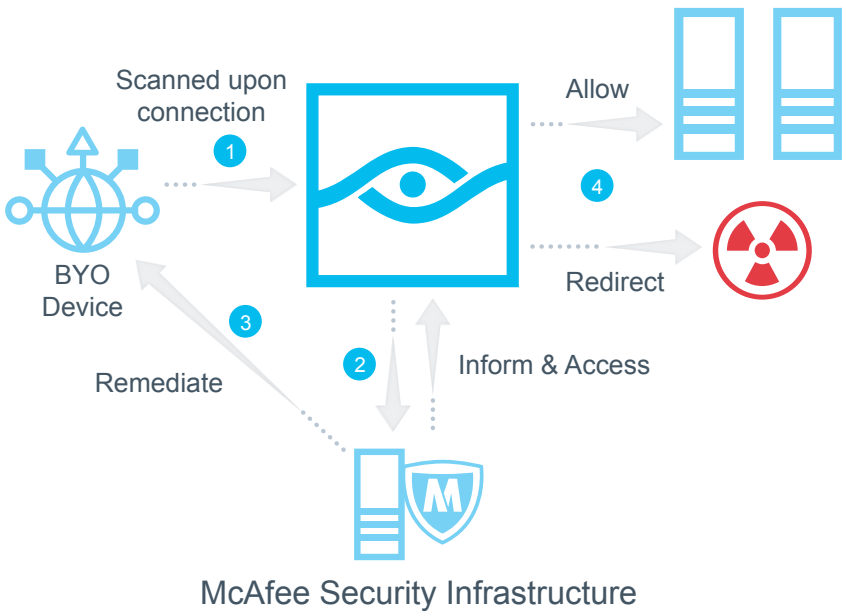

Figure 1: ForeScout CounterACT and McAfee Threat Intelligence Exchange share real-time security context, resulting in more timely and accurate detection, assessment and remediation of unmanaged Windows devices on corporate networks.

Assess and secure unmanaged Windows BYOD devices on network admission

McAfee Threat Intelligence Exchange constantly receives and analyzes the latest contextual threat data from third-party feeds, McAfee Global Threat Intelligence and other McAfee security solutions. Upon receiving threat intelligence about a new malicious file or process:

1. The McAfee Threat Intelligence Exchange server broadcasts this information over the McAfee Data Exchange Layer to CounterACT, which continuously listens for these broadcasts.
2. Upon receiving the alert, CounterACT scans all unmanaged Windows devices on the network to see if they contain the malicious file or process.
3. Based on your security policies, CounterACT can perform the same wide-range of control actions as in the first use case. It can allow, limit or quarantine a compromised endpoint from the network, kill a malicious process on the endpoint, initiate other remediation actions and notify the user.

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