FORESCOUT

Solution Brief

ForeScout Extended Modules for Advanced Threat Detection

Improve defenses against advanced threats and automate threat response

Highlights

See

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

Control

- Allow, deny or limit network access based on device posture and security policies
- Reduce attack surface by ensuring endpoints have up-to-date security defenses
- Initiate remediation and risk mitigation actions on malicious or infected endpoints

Orchestrate

- Quarantine infected endpoints identified by your ATD system to prevent lateral malware propagation
- Scan endpoints connecting to your network for IOCs identified by your ATD system
- Automate system-wide response to quickly mitigate threats and data breaches

ForeScout Extended Modules for Advanced Threat Detection (ATD) Systems

ForeScout Extended Modules for Advanced Threat Detection allow ForeScout CounterACT® to integrate with systems that are designed to detect advanced persistent threats (APTs) within your network. This integration enables IT security managers to reduce their attack surface, detect advanced threats, scan the network for indicators of compromise (IOCs), and automate incident response. As a result, you can limit malware propagation, minimize data breaches, avoid costly investigation and protect your reputation.

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) endpoints. In addition, 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 cyberattacks are more sophisticated than ever before 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 Extended Modules for ATD 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. A new IOC is identified and reported to the ATD system.
2. The ATD system notifies CounterACT about the endpoint infected.
3. CounterACT isolates the infected endpoint.
4. Using details from the ATD system such as file size, registry changes and processes spawned, CounterACT initiates remediation actions.
5. CounterACT scans other devices on the network for the new IOC and initiates remediation actions.
6. CounterACT scans endpoints for IOCs as new endpoints attempt to connect to the network.

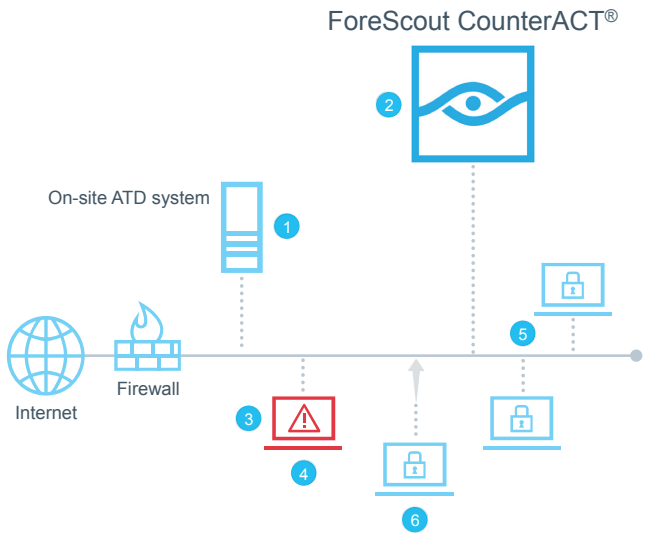

Figure 1: ForeScout CounterACT receives IOC information from ATD systems and takes threat mitigation actions.

Supported Advanced Threat Detection Systems

- Bromium vSentry version 2.4.4 or above
- Check Point Threat Prevention version r77.20, r77.30 and r80
- FireEye NX Series (Network Security) running FireEye Operating System version 7.4 or above
- Palo Alto Networks WildFire with a Palo Alto Networks Firewall running PAN-OS version 6.0 or above.

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

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

Network-based ATD systems examine ingress and egress traffic to detect malicious payloads and communication with malware command and control (C&C) centers. However, they cannot prevent systems infected on outside networks or those infected via non-network pathways (such as USB devices) from connecting to the corporate network. Host-based ATD systems protect against malware on managed corporate systems but are unable to detect infection on unmanaged systems (BYOD). Neither type of ATD system can detect the extent of infection on your network and contain the threat to prevent further internal propagation.

Through ForeScout Extended Modules, CounterACT integrates with your ATD system to detect IOCs on your network and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.

When an ATD system detects malware and suspects that a device within your network has been compromised, it informs CounterACT about the affected system(s) and IOCs. CounterACT can receive IOC data from multiple ATD systems, and also allows you to manually define IOCs directly from the console. Based on your policy, CounterACT leverages its IOC repository to scan other endpoints that are attempting to connect or are already connected to your network for presence of infection.

Regardless of whether CounterACT discovers infected endpoints from your ATD system or via IOC scanning, it can automatically take policy-based mitigation actions to contain and respond to the threat. Various actions can be performed depending on the severity or priority of the threat, such as quarantine endpoints, initiate direct remediation, share real-time context with other incident response systems, initiate a scan by another third party product, or notify the end user via email or short message service (SMS).

Extended Modules for ATD are optional modules for ForeScout CounterACT, and are sold separately. When used in conjunction with your existing ATD system, CounterACT and ATD Extended Modules offer automated response to IOCs while providing a dynamic threat detection approach to security that reduces the attack surface of your network.