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

The ForeScout-FireEye™ Joint Integration

Improve defenses against advanced threats and automate threat response

The ForeScout and FireEye™ joint solution allows you to reduce your attack surface, identify advanced threats, scan for indicators of compromise (IOCs), and automate threat response. As a result, you can disrupt the cyber kill chain and limit malware propagation, minimize data breaches and avoid costly investigation and reputation risk.

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

ForeScout CounterACT™ and FireEye Network Threat Prevention Platform (NX Series) work together to quickly detect advanced threats and IOCs, contain infected endpoints, and break the cyber kill chain.

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 FireEye Threat Prevention Platform does not rely solely on signatures to identify and block threats in real-time. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence that empowers security teams to prevent, detect, analyze and respond to today's advanced

attacks. ForeScout CounterACT leverages this threat information from FireEye and enables you to scan the network for IOCs, determine the extent of infection on your network and contain infected endpoints. This disrupts the cyber kill chain and prevents further lateral threat propagation and data exfiltration.

When deployed inline, FireEye NX Series blocks outbound callbacks and informs CounterACT about the infected system, the threat severity and the indicators of compromise. Based on your policy, CounterACT leverages the IOC information from FireEye to scan other endpoints that are attempting to connect or are already connected to your network for presence of infection. Infections on other endpoints may have occurred on outside networks, on unmonitored corporate networks or via non-network pathways such as USB devices. FireEye isn't able to detect these infections at the time endpoints connect to the network.

Regardless of whether CounterACT discovers infected endpoints from FireEye 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 SMS.

1. An infected system connects to the network
2. If inline, FireEye NX blocks callback. FireEye NX alerts ForeScout CounterACT of the infected system and indicators of compromise (IOCs)
3. CounterACT isolates the infected system to prevent reconnaissance or lateral threat propagation ForeScout CounterACT scans other endpoints on corporate network for IOCs
4. CounterACT isolates other infected endpoints and initiates appropriate risk mitigation actions

Learn more at
www.ForeScout.com

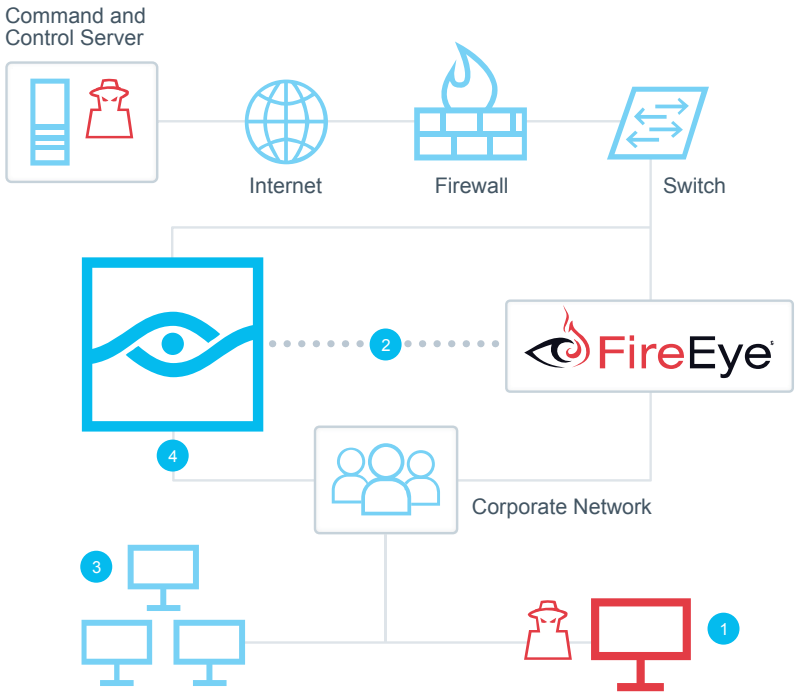

Figure 1: ForeScout CounterACT and FireEye NX Series work together to detect and mitigate advanced threats.

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

Version 1_16