FORESCOUT

ForeScout Extended Module for FireEye® NX

Improve defenses against and automate response to advanced network threats

ForeScout Extended Module for FireEye® NX protects your network by identifying zero-day threats through the use of sandboxing techniques. It then informs ForeScout CounterACT® about infected endpoints and devices as well as indicators of compromise (IOCs), while also assessing the severity of the threats. CounterACT uses this information to enforce policy-based actions. These may include isolating devices, initiating remediation actions and scanning other systems to minimize threat propagation. CounterACT stores the latest IOC information in its database and scans devices attempting to connect to the network. It also performs remediation actions before the endpoint attempts an outbound call to a malicious server.

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Classify and profile devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

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 Network Security to prevent lateral malware propagation
- Scan endpoints connecting to your network for IOCs identified by FireEye Network Security
- Automate system-wide response using out-of-the-box or customized policies to quickly mitigate threats and data breaches

The Challenges

Visibility. According to industry experts, the 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:

- Unmanaged, personally owned devices
- Guest or Internet of Things (IoT) endpoints
- Systems with disabled or broken agents
- Transient devices undetectable by periodic scans

As a result, organizations aren't aware of the attack surface on these systems.

Threat Detection. Today's cyberthreats are more sophisticated than ever before and can easily evade traditional security defenses. These multivector, stealthy and targeted attacks are focused on acquiring sensitive personal information, intellectual property or other 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 don't rely on signatures alone, but instead use a behavior-based approach.

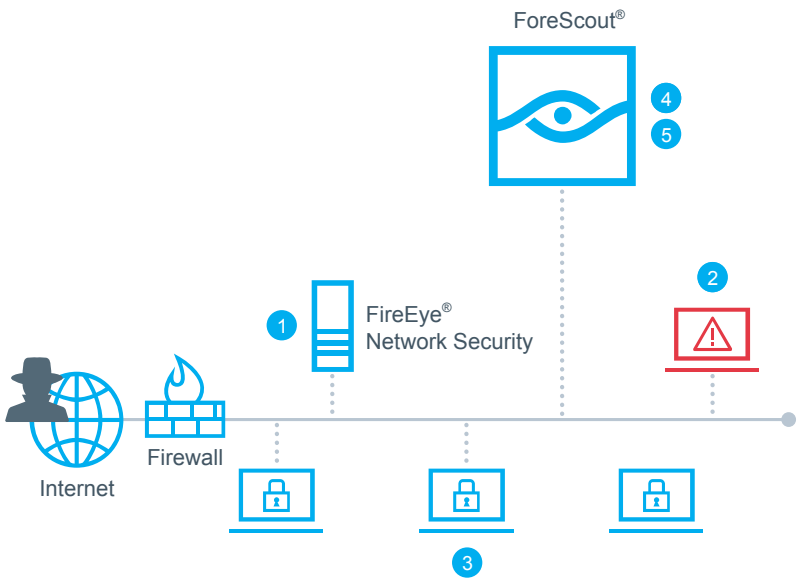
Response Automation. The velocity and evasiveness of today's targeted attacks are coupled with increasing network complexity and mobility, along with growing numbers of personally owned devices on the network. These factors are creating the perfect storm for IT security teams. To protect your organization, you need an automated system to continuously monitor and mitigate endpoint security gaps. Automating these tasks is critical, as valuable time is lost when IT teams perform them manually. 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 it Works

The Extended Module for FireEye NX, ForeScout CounterACT and FireEye Network Security (NX Series) can work together to quickly detect advanced threats and IOCs, and contain infected endpoints.

ForeScout CounterACT is a network security appliance that helps IT organizations see devices, including non-traditional ones, when they connect to the network. CounterACT provides policy-based control of these devices. It also works with ForeScout ControlFabric® Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

1. FireEye Network Security discovers a zero-day threat and blocks the outbound "call home."
2. CounterACT receives an alert from FireEye Network Security and isolates the infected system.
3. CounterACT initiates a scan of the other endpoints for the same IOC.
4. CounterACT isolates other infected endpoints.
5. CounterACT initiates remediation steps for infected endpoints based on your corporate policies.



ForeScout Extended Modules

The Extended Module for FireEye NX is an add-on module for ForeScout CounterACT and is sold and licensed separately. It's one of many ForeScout Modules that enable CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response.

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

FireEye Network Security doesn't rely solely on signatures to identify and block threats in real-time, but takes a behavior-based approach instead. ForeScout CounterACT uses threat information from FireEye to help you to scan the network for IOCs, determine the extent of infection on your network and contain infected endpoints. This helps you break the cyber kill chain.

When deployed inline, FireEye NX Series blocks outbound callbacks to malicious servers and informs CounterACT about the infected system, the threat severity and IOCs. Based on your policy, CounterACT uses the IOC information from FireEye to scan other endpoints that are attempting to connect or are already connected to your network for the presence of infection. Infections on other endpoints may have occurred:

- On outside networks
- On unmonitored corporate networks
- Via non-network pathways, such as USB devices

After discovering infected endpoints, CounterACT can automatically take policy-based mitigation actions to contain and respond to the threat. Depending on the severity or priority of the threat, various actions can be performed. For example, you can:

- Quarantine endpoints
- Initiate direct remediation
- Share real-time context with other incident response systems
- Initiate a scan by another third-party product
- Notify the end user via email or text message

These custom-defined actions can be performed manually or automatically.

To classify the types of threats detected, the Extended Module for FireEye NX draws from a comprehensive list of properties stored in the contextual database on the CounterACT system. This detailed data helps you determine whether remediation or isolation must occur immediately, or whether it can be done at a later time so as not to impact the end user.

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