ForeScout

Datasheet

ForeScout Extended Module for FireEye® HX

Detect and respond to endpoint threats in real time

FireEye HX Extended Module

ForeScout Extended Module for FireEye® HX provides automated detection, containment and remediation of advanced threats and indicators of compromise (IOCs) by orchestrating security processes between ForeScout CounterACT® and FireEye Endpoint Security (HX Series). Upon receiving notification from FireEye HX, CounterACT isolates malware-infected endpoints and devices to stop lateral propagation of threats. CounterACT also stores and uses IOC information from FireEye HX to scan systems that are attempting to connect or are already connected to the network for the presence of infections. This reduces your attack surface, disrupts the cyber kill chain, limits malware propagation and helps minimize data breaches.

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 systems on their network because they are:

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

As a result, organizations aren't aware of the attack surfaces on these devices.

Threat Detection. Today's threats 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 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 threats to propagate within your network and exfiltrate data.

How it Works

The FireEye HX Extended Module, ForeScout CounterACT and FireEye Endpoint Security (HX Series) can work together to quickly detect and contain advanced threats and IOCs. This approach also helps you maintain compliance on Windows workstations.

ForeScout CounterACT is a network security appliance that helps IT organizations see systems, including non-traditional ones, when 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.

Highlights

See

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

Control

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

Orchestrate

- Scan devices connecting to your network for known IOCs and quarantine infected systems
- Validate Microsoft Windows endpoints to help ensure FireEye HX endpoint security is installed and operating properly
- Automate system-wide response using out-of-the-box or customized policies to quickly mitigate threats and data breaches

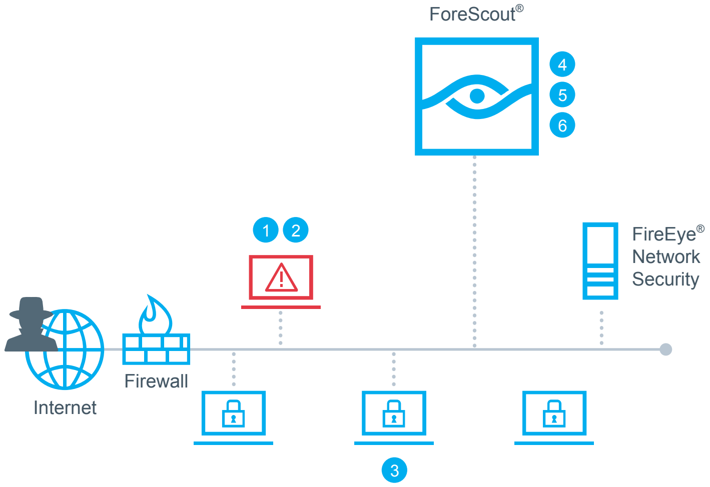
1. FireEye HX identifies and classifies an IOC on a Windows endpoint.
2. CounterACT receives an alert from FireEye HX and isolates the infected system.
3. CounterACT initiates a scan of other endpoints for the same IOC and isolates infected endpoints.
4. CounterACT initiates remediation steps for infected endpoints based on corporate policies.
5. CounterACT scans Windows endpoints as they enter the network looking for IOCs and a properly functioning FireEye HX client.
6. If necessary, CounterACT initiates installation of the FireEye Endpoint Security (HX) client on Windows endpoints.

ForeScout Extended Modules

The Extended Module for FireEye HX is an add-on module for ForeScout CounterACT and is sold and licensed separately. It's one of many ForeScout Extended 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.

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



The FireEye HX Series secures against advanced endpoint threats and malware. Rather than relying solely on signatures, it uses a behavior-based approach to analyze potentially infected endpoints and successfully block threats in real time.

ForeScout CounterACT uses threat information obtained from the FireEye Network Security to help you:

- Scan endpoints on your network for IOCs
- Determine the extent of infection
- Install the FireEye HX agent on Windows workstations
- Contain infected endpoints.

This disrupts the cyber kill chain and helps prevent attackers from propagating additional threats and exfiltrating data.

The FireEye HX Series provides threat detection capabilities from the network core to the endpoint. This helps you enhance system visibility and enable a flexible and adaptive defense against known and unknown threats.

CounterACT uses 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
- Through non-network pathways, such USB devices

CounterACT can also initiate the installation of the FireEye HX client on Windows endpoints where it is missing, deactivated or out of date.

When CounterACT discovers infected endpoints, 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
- Notify the user via email or text message

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

The Extended Module for FireEye HX draws on a comprehensive list of properties stored on the CounterACT system to classify the type of threats detected. 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 user.