FORESCOUT

Datasheet

ForeScout Extended Module for FireEye® EX

Improve defenses against advanced email threats and automate threat response

The Forescout Extended Module for FireEye® EX prevents targeted phishing attempts and protects networks from threats hidden in malicious links and attachments in email. These threats routinely bypass email security that uses conventional, signature-based defenses, such as antivirus and spam filters. However, with this module, 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, 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 either:

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

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

Threat Detection. Today's cyberthreats are more sophisticated than ever and are built to evade traditional security defenses. Many of these threats arrive through stealthy, targeted email focused on acquiring sensitive personal information, intellectual property or other insider information. These email attacks can result in compromised endpoints and data breaches that can often remain undetected for weeks or months. To detect these vulnerabilities in email, you need new, advanced security controls that don't rely on signatures alone, but instead use a behavior-based approach to analyze and isolate these threats.

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 a way to continuously monitor email and endpoints, detect threats, share intelligence and mitigate these security issues. 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

Using the Extended Module for FireEye EX, ForeScout CounterACT and FireEye Email Security products (FireEye EX series) can work together to quickly detect advanced threats and IOCs that are delivered through phishing attempts via email attachments and embedded malicious links. Once identified, the email message is quarantined, effectively breaking the cyber kill chain.

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 helping to ensure devices have up-to-date security defenses
- Initiate remediation using out-of-the-box or customized policies and risk mitigation actions on malicious or infected endpoints

Orchestrate

- Quarantine emails with malicious email links or attachments identified by FireEye Email Security
- Scan devices for IOCs identified by FireEye Email Security to prevent malware from propagating
- Automate system-wide response using out-of-the-box or customized policies to quickly mitigate threats and data breaches

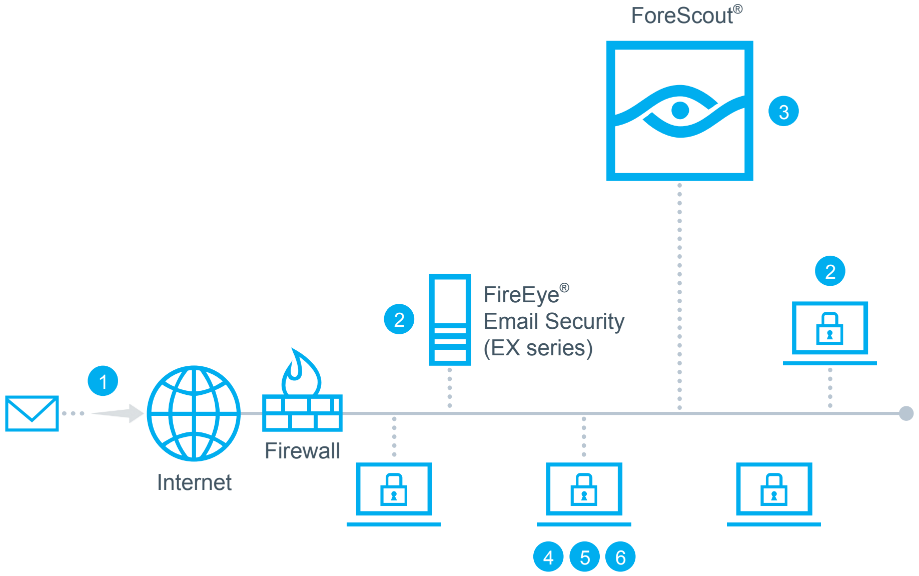
1. Inbound email arrives destined for user endpoint.
2. FireEye Email Security detects potential malware embedded in email, then analyzes and gathers intelligence on IOCs in a sandbox, recording and observing IOCs generated when the malware executes.
3. After analyzing and gathering intelligence on IOCs, FireEye Email Security alerts CounterACT about the new malware.
4. CounterACT enables a scan of other endpoints for identified IOCs.
5. CounterACT isolates systems that show multiple IOCs and takes action on them based on your corporate policies.
6. CounterACT scans systems for known IOCs as they connect to the network.

ForeScout Extended Modules

The Extended Module for FireEye EX 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.

Learn more at
www.ForeScout.com



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

FireEye Email Security secures against advanced email attacks. As part of FireEye Network Security, FireEye Email Security does not rely solely on signatures. Instead, it uses a behavior-based approach to analyze potentially malicious emails and attachments and successfully quarantine them, blocking threats in real time. ForeScout CounterACT uses threat information obtained from FireEye Network Security to help you:

- Scan endpoints on your network for IOCs
- Determine the extent of infection
- Contain the security threat

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

FireEye Email Security identifies spear-phishing emails by analyzing attachments and URLs to provide an accurate picture of potential attacks. Based on your policy, CounterACT uses the information from FireEye Network Security to scan other corporate endpoints that may contain the identified threat. It also extends visibility to other threat vectors outside of the corporate network, such as personal email, cloud storage accounts, smartphone text messages and other sources of malicious files that can be introduced into your network.

When FireEye Email Security detects an infected email, it will quarantine the email and provide contextual information to CounterACT. CounterACT can automatically take policy-based mitigation actions to contain and respond to that threat. Various actions can be performed depending on the severity or priority of the threat. These include scanning endpoints on the network, quarantining infected endpoints, initiating direct remediation, sharing real-time context with other incident response systems or notifying the user via email or text message. These custom-defined actions can be performed manually or automatically.

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