FORESCOUT

# ForeScout Extended Modules for FireEye® Products

## Improve real-time visibility over devices while automating network access control and threat response

ForeScout Extended Modules for FireEye® provide dynamic endpoint visibility, profiling, access control and remediation capabilities. With these Extended Modules, ForeScout CounterACT® can integrate bi-directionally with FireEye products to strengthen your overall network security. The alliance of ForeScout and FireEye enables contextual sharing of endpoint and threat intelligence and automates response workflows to help defend against threats. This gives you superior visibility and control of both managed and unmanaged endpoints and protects networks from those that are non-compliant or malware-infected.

### See

- Detect devices the instant they try to access your network
- Profile and classify personally owned and corporate devices, without relying on agents
- Scan unmanaged Windows devices to identify malware and missing or non-compliant agents

### Control

- Identify and fix corporate devices with missing, disabled or misconfigured FireEye Endpoint Security agents
- Allow, deny or limit network access based on device posture and security policies
- Restrict and remediate infected or high-risk devices to reduce the attack surface

### Orchestrate

- Use the combined intelligence of FireEye Network Security and ForeScout CounterACT to improve overall security posture
- Receive contextual threat information from FireEye, allowing security components to operate as a cohesive system
- Automate response workflows using ForeScout CounterACT and FireEye to reduce risks from non-compliant or infected endpoints

### The Challenges

**Securing what you can't see.** According to industry experts, the vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. Identifying and profiling unmanaged, personally owned, guest and Internet of Things devices can be challenging for even the most sophisticated security platforms. These systems are often unpatched, lack security agents and use unauthorized applications. For these reasons, they can serve as launching points for malware. The challenge is to close these security gaps and become aware of the entire attack surface.

**Controlling network access and reducing risk.** Protecting today's enterprise network means knowing the security posture of systems when giving them network access and taking immediate action to reduce the attack surface. If an endpoint becomes infected and poses a threat to your network, you need to quickly identify and contain the source of the attack.

**Automating threat response.** Threat intelligence changes in real time. New threat data must be automatically shared across security solutions, allowing them to operate as a cohesive system. An automated security system helps you continuously monitor and remediate vulnerabilities and security gaps based on the latest threat intelligence. This is essential for responding to attacks and security breaches quickly—before malware can propagate and exfiltrate data.

### ForeScout Extended Modules for FireEye

ForeScout Extended Modules for FireEye take full advantage of the superior capabilities of the following FireEye products and ForeScout CounterACT:

- **FireEye Endpoint Security (HX Series)** detects threats from the network core to the endpoint. This helps you enhance system visibility and enable a flexible, adaptive defense against known and unknown threats on Microsoft Windows endpoints.
- **FireEye Email Security (EX)** protects against phishing attacks as well as malicious file attachments and URLs in emails. These threats routinely bypass email security that uses conventional, signature-based defenses, such as antivirus and spam filters.

- **FireEye Network Security (NX Series)** protects against known and unknown advanced attacks. FireEye Network Security uses sandboxing techniques to observe and record zero-day threats and informs ForeScout CounterACT about infected systems and indicators of compromise (IOCs).
- **ForeScout CounterACT** is an agentless security appliance that dynamically identifies and evaluates network devices and applications, determining the user, owner and operating system. It gives you visibility into configuration, software, services, patch state and the presence of security agents. It also provides remediation, control and continuous monitoring.

### Secure corporate endpoints, to help ensure compliance

ForeScout CounterACT detects and profiles devices as they connect to the network, whether managed or unmanaged, wired or wireless, mobile or traditional. CounterACT can help you determine device compliance status with or without a FireEye Endpoint Security agent installed.

If the connecting system is a corporate Windows or Mac endpoint with a FireEye Endpoint Security agent installed, CounterACT gains information about its compliance from the FireEye solution. If no FireEye Endpoint Security agent is installed, CounterACT will inspect the system to determine its compliance status. If it is compliant except for the missing FireEye Endpoint Security agent, or if the agent is not functioning properly, CounterACT will allow the device on the network and, based on corporate policy, will either:

- Initiate installation of the agent
- Redirect the user to a website for manual installation
- Notify the user or IT staff about the missing agent for manual remediation

When the device is admitted to the network, FireEye Endpoint Security determines whether it has become noncompliant. FireEye Endpoint Security can be configured to tag the system and immediately report its noncompliance to CounterACT, which can isolate it until remediation has been performed. CounterACT also continually monitors the device to see if its behavior becomes threatening. If it does, CounterACT may isolate it, disable the USB port, shut down an unauthorized application or take another appropriate action.

### Protect corporate users against email threats

Paired with FireEye Email Security, CounterACT can help prevent phishing attacks or damage from malicious links or attachments within email.

When a corporate Windows endpoint tries to connect, CounterACT identifies and classifies it. If corporate policy dictates that the FireEye Email Security agent is required, CounterACT can determine if the agent is installed and working properly. If it is, the system is allowed on the network. If it isn't, CounterACT can take the appropriate next steps based on the corporate policy, and can initiate installation of the agent. When this is installed and the system is considered compliant, CounterACT allows it on the network.

When the device joins the network, FireEye Email Security scans incoming email for IOCs, phishing threats, malicious links or inappropriate attachments. If detected, FireEye Email Security isolates these threats, notifies CounterACT and sends an update to the FireEye Network Security. Providing the details of the threat allows FireEye Email Security to scan for known IOCs within arriving email. It also allows CounterACT to identify the threat on other devices as they connect to the network, and to take appropriate remediation actions under corporate policy.

### Strengthen network security and prevent zero-day exploits

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

When deployed inline, FireEye Network Security blocks outbound callbacks to malicious servers. It then informs CounterACT about the infected device, the threat severity and the IOCs associated with the threat. When CounterACT receives this information, it can take several actions based on policy. Typically, CounterACT will isolate the device, initiate remediation actions and then scan other endpoints on the network to help ensure that the threat has not propagated.

When the IOCs are contained, the information is stored in CounterACT's contextual database. That way, it can scan any endpoint attempting to connect to the network and initiate remediation actions before the endpoint attempts an outbound call.

## Two Sets of Eyes Provide a More Complete Picture

When installed together, FireEye products and ForeScout CounterACT provide a stronger security platform. Integration with ForeScount CounterACT through our Extended Modules makes that security even more effective, closing existing security gaps and combining the strengths of each product.

CounterACT gives you visibility into systems on the network, network access control, continuous monitoring, compliance information and, most importantly, orchestration among multiple security products.

FireEye provides threat detection and response, email protection, threat analytics and incident response.

Together, ForeScout and FireEye deliver prioritized, context-aware incident response, superior endpoint protection and the ability to gather more information on IOCs.

FireEye has ownership of the entire threat lifecycle and kill chain and offers forensics expertise and investigative tools. ForeScout makes the invisible visible. It identifies the full context of systems on the network as well as those attempting to connect to the network, and enables policy-based access and controls. The interaction between the two platforms provides for an automated response to detected threats before and after devices connect to the network. That helps you remediate threats faster, freeing IT and security staff to work on other high-priority concerns.

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