FireEye Network Threat Prevention Platform (NX Series) Integration with ForeScout CounterACT™

Risk Mitigation and Threat Defense

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- **Enhanced Network Visibility.** Provides real-time intelligence about the devices and risks on your network, including unauthorized devices and BYOD endpoints owned by employees, guests, and contractors.
- **Reduced Attack Surface.** Decreases enterprise risk by ensuring that endpoints have up-to-date security defenses. Continuously monitors and mitigates security gaps on endpoints connecting to your network.
- **Advanced Threat Detection.** Enables organizations to detect malware, APTs, and zero-day attacks that evade traditional security controls. Scans for IOCs on endpoints connecting to the network to accurately determine the extent of the infection.
- **Expedited Incident Response.** Enables rapid response to threats on the network to limit lateral propagation and protect against data breaches. Quarantines infected endpoints and automates other risk mitigation actions.

OVERVIEW

Enterprise mobility and IT consumerization are the "new norm" for business, but they also introduce more security and privacy issues.

Customers face an unprecedented diversity of users, devices, and applications on their networks — guests, contractors, partners, and employees using their personal or corporate laptops, tablets and smartphones. Each requires access to a different set of network resources to remain productive.

Most organizations are unaware of a significant percentage of the endpoints on their networks because of the proliferation of mobile, personal, transient, and virtual devices. As a result, customers are blind to the vulnerabilities and security gaps on these devices. IT professionals must protect their networks from unsanctioned, rogue, and compromised mobile devices to prevent malware propagation, data leakage and compliance violations.

THE CHALLENGE

The security challenges facing IT professionals can be summed up by the following:

Visibility. Any serious attempt to manage security risk must start with complete knowledge of who and what is on your network, including visibility to whether the devices on your network are compliant with your security standards.

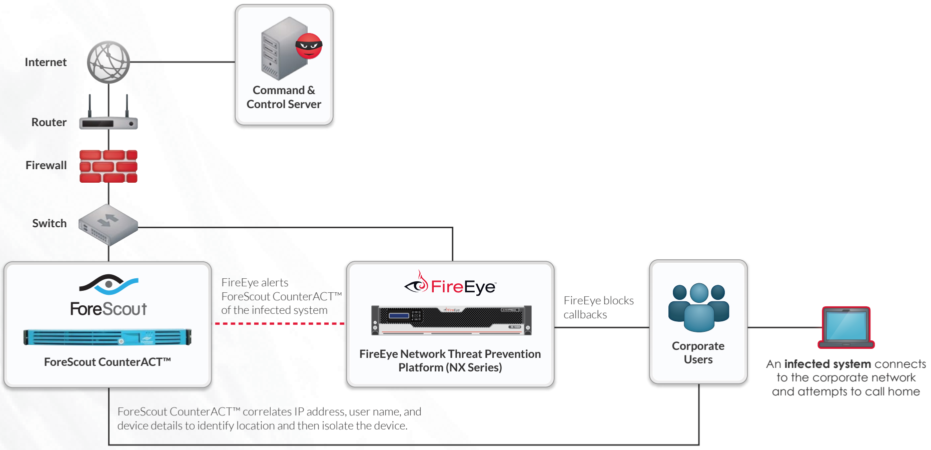
Threat Detection. Today's cyber attacks are more sophisticated than ever. Multi-vectored, stealthy, and persistent threats easily evade traditional security defenses such as firewalls, intrusion prevention systems, anti-virus platforms, and secure web and email gateways.

Automation. Increasing network complexity, the mobility and BYOD phenomenon, and today's targeted attacks are creating a perfect storm for any security program. Without an automated system to monitor, install, reconfigure, and reactivate security agents on managed systems, valuable time is lost performing these tasks manually.

THE INTEGRATED SOLUTION

FireEye has partnered with ForeScout to deliver a unique and powerful solution for risk mitigation and threat defense. With this joint solution, you can rapidly identify security risks and advanced threats, automate mitigation actions to prevent malware propagation, and reduce mean time to resolution of security and compliance issues. As a result, you can reduce breaches, data loss, and reputation risk while preempting costly investigation and remediation tasks.

ForeScout CounterACT™ and FireEye Network Threat Prevention Platform (NX Series) work together to leverage the best-of-breed capabilities of each solution and provide a holistic approach to risk mitigation and threat management. The joint solution provides real-time visibility and compliance management of devices on your network, effective response to APTs and zero-day threats, and automation to efficiently and accurately mitigate endpoint risks and advanced threats.


Internet
Router
Firewall
Switch
Command & Control Server
ForeScout
ForeScout CounterACT™
FireEye alerts ForeScout CounterACT™ of the infected system
FireEye
FireEye Network Threat Prevention Platform (NX Series)
FireEye blocks callbacks
Corporate Users
An infected system connects to the corporate network and attempts to call home
ForeScout CounterACT™ correlates IP address, user name, and device details to identify location and then isolate the device.

FIREEYE PRODUCT AND VERSION

FireEye Network Threat Prevention Platform (NX Series)

FORESCOUT PRODUCT AND VERSION

ForeScout CounterACT™ v7

HOW THE JOINT SOLUTION WORKS TOGETHER

When deployed inline, FireEye Network Threat Prevention Platform (NX Series) Series blocks outbound callbacks and informs CounterACT about the infected system, the threat severity, and the indicators of compromise (IOCs).

When CounterACT receives this information, it automatically takes appropriate actions as defined by policy, including:

- Quarantine the endpoint using ACL, VLAN reassignment, port blocking, or ForeScout's patented Virtual Firewall technology.
- Send endpoint configuration and security posture details to SIEM (Security Information Event Management) Systems, including FireEye Threat Analytic Platform (TAP).
- The information can include the name of the user logged on, missing patches, antivirus status, running processes, applications installed, external devices connected, endpoint location, IP address, and device type.
- Trigger a 3rd party scan including FireEye Endpoint Threat Prevention Platform (HX Series) endpoint agent to validate the system is compromised using the specific IOCs from FireEye Network Threat Prevention Platform (NX Series).
- Initiate CounterACT remediation to install the FireEye Endpoint Threat Prevention Platform (HX Series) endpoint agent or a patch.
- Notify the end-user and/or administrator via email or SMS.

In addition to taking actions on infected endpoints reported by FireEye, CounterACT™ also stores the IOC information received from FireEye in its IOC database. Based on policy, CounterACT™ can take additional actions including:

- Scan other endpoints that are connecting or connected to the network for the presence of the same infection.
- If CounterACT detects additional endpoints that have been compromised, it can quarantine them to prevent malware propagation and/or take additional actions as previously listed.

THE VALUE OF THIS PARTNERSHIP

The combination of FireEye intelligence and ForeScout's CounterACT tool enable customers to protect themselves from various attacks, such as APTs, malware, unauthorized access, and unauthorized devices.

CounterACT integrates with the customer's network, security, and identity infrastructure to assure the right users and their devices gain appropriate access. In the joint solution, CounterACT determines whether or not to grant access by applying FireEye Network Threat Prevention Platform (NX Series) intelligence and hunt rules gathered from the frontline incident response activity to customer log data.

The FireEye Network Threat Prevention Platform (NX Series) also allows customers to develop custom rules to monitor areas of concern, streamlining incident investigations through integrated workflow management and reporting.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000

ABOUT FORESCOUT

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT appliance dynamically identifies and evaluates network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners.

For more information contact CSC@fireeye.com.

FireEye