FireEye Threat Analytic Platform (TAP) with ForeScout CounterACT™ Integration

Risk Mitigation and Threat Defense

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- **Real-Time Visibility:** Obtain real-time information about endpoints on the network, including unauthorized devices and BYOD endpoints owned by employees, guests, and contractors.
- **Fast Response to Security Breaches:** Respond immediately to compromised devices on the network. The moment that FireEye Threat Analytic Platform (TAP) flags an endpoint that may have been compromised, ForeScout CounterACT can quarantine the endpoint and, optionally, initiate endpoint remediation.
- **Discover and Block APTs, Malware:** FireEye Network Threat Prevention Platform (NX) and ForeScout Active Response work together to help you detect and block a very high percentage of APTs, regardless of whether they are incoming, propagating, or actively exfiltrating data.

INTEGRATED SOLUTION

- **Context Aware Automation:** Upon detection, ForeScout applies pre-defined policies to automatically remove or isolate non-compliant or compromised devices from the production network.
- **Boosts Intelligence with Context Aware Security Data:** Adds context to FireEye-generated alerts to provide a broader perspective of the business risk and impact.

OVERVIEW

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

Customers are facing 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 number of the endpoints on their networks because of the proliferation of mobile, personal, transient, and virtual devices. These devices are not under customer management, have broken agents, or are not detected between the periodic scans. 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.

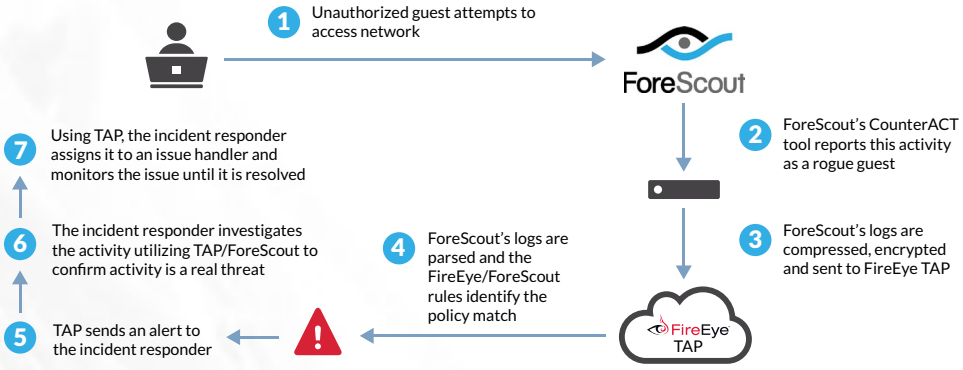
THE CHALLENGE

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 the network and be compliant with the corporate 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. These targeted attacks, originating from highly motivated and well-funded threat actors and nation states, are focused on acquiring sensitive personal information, intellectual property, or insider information. As the attackers have gained the upper hand, organizations are being compromised at an accelerating rate.

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.



FIREEYE PRODUCT AND VERSION

Threat Analytics Platform (TAP) 12.01 and later versions are supported

FORESCOUT PRODUCT AND VERSION

CounterACT™ v7

THE INTEGRATED SOLUTION

ForeScout has partnered with FireEye to deliver a unique and powerful solution for risk mitigation and threat defense. The FireEye Threat Analytics Platform (TAP) creates a cross-enterprise threat protection fabric using a next-generation threat detection engine and dynamic threat intelligence. The FireEye Network Threat Prevention Platform (NX) stops attacks from the web or via email that traditional security controls miss. FireEye Network Threat Prevention Platform (NX) blocks outbound malware activity and informs CounterACT of the affected system and the threat severity. CounterACT then takes action.

HOW THE JOINT SOLUTION WORKS TOGETHER

FireEye and ForeScout work together to leverage the best-of-breed capabilities of each solution. The joint solution provides real-time visibility and compliance management of all devices connected to your network, effective response to APTs, malware, and zero-day threats, and automation to efficiently and accurately mitigate threats.

When FireEye and CounterACT are working together on the same network, FireEye sends CounterACT the IP address of any system that it suspects has been compromised. When CounterACT receives this information, it automatically takes whatever actions the customer has pre-programmed into the CounterACT policy manager. This could be to quarantine the endpoint or report information about the endpoint to other systems such as SIEM systems. This response can include the name of the logged on user, missing patches, antivirus status, running processes, applications installed, external devices connected, the location of the endpoint, IP address, and device type.

THE VALUE OF THIS PARTNERSHIP

The combination of FireEye intelligence and ForeScout 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. By employing FireEye Threat Analytic Platform (TAP) intelligence and hunt rules gathered from the frontline incident response activity and applying that to customer log data this integration is achieved.

FireEye Threat Analytic Platform (TAP) 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, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**