Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab Review

ForeScout CounterACT and FireEye: Visibility, Control, and Shared Contextual Insight

Date: July 2017 **Author:** Tony Palmer, Senior Lab Analyst

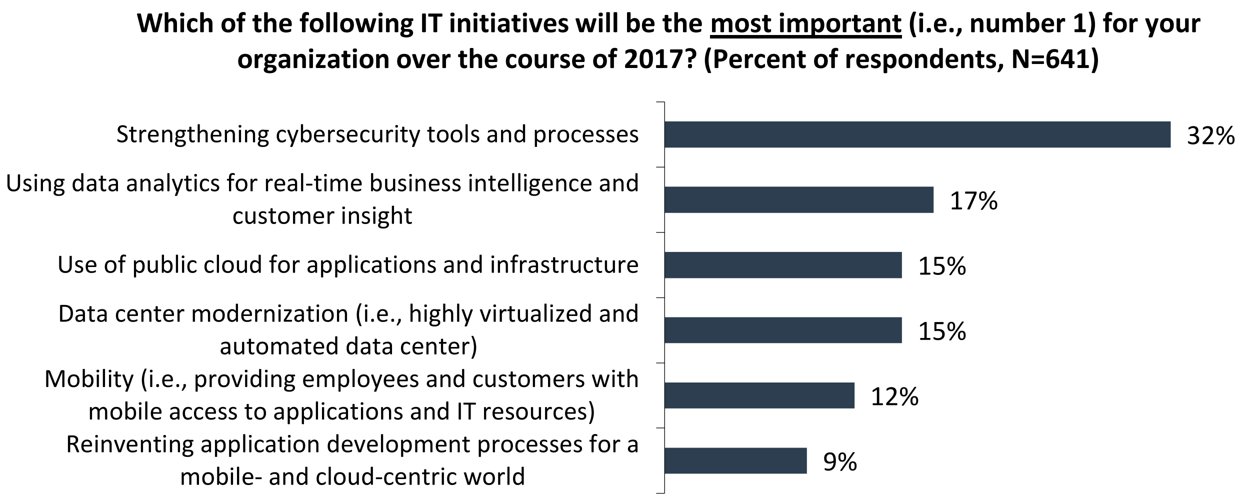
Abstract

This report provides a first look at the key benefits of bi-directional workflow integration between ForeScout CounterACT and FireEye solution platforms for network, endpoint, and email. The focus is on how endpoint and threat intelligence data can be shared between CounterACT and FireEye products. This bi-directional data exchange provides users visibility and control of both managed and unmanaged endpoints.

The Challenges

According to ESG research, cybersecurity initiatives were cited by 32% of respondents as their most important IT initiative in 2017.[1] This is hardly surprising, considering the multitude of cyber security incidents organizations are experiencing. In a 2016 research project conducted by ESG and the Information Systems Security Association (ISSA), 39% of cybersecurity professionals say that their organization has experienced one or more incidents resulting in the need to reimage one or more endpoint or server, 27% have experienced a ransomware incident, and 20% have experienced at least one security incident that disrupted a business application.[2]

Figure 1. Most Important IT Initiatives for 2017



Source: Enterprise Strategy Group, 2016

Adding to these challenges is an increasing skills gap in cybersecurity. Forty-five percent of organizations claim that they have a problematic shortage of cybersecurity skills, the most cited response by a wide margin.[3]

The increase in mobile, personal, transient, and even virtual devices leaves many organizations unaware of a significant percentage of the endpoints on their networks. These devices are either not under management, have non-functional agents, or are only detected during intermittent scans.

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

[2] Source: ESG/ISSA Research Report: Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II). December 2016.

[3] Source: ESG Research Report, 2017 IT Spending Intentions Survey, March 2017.

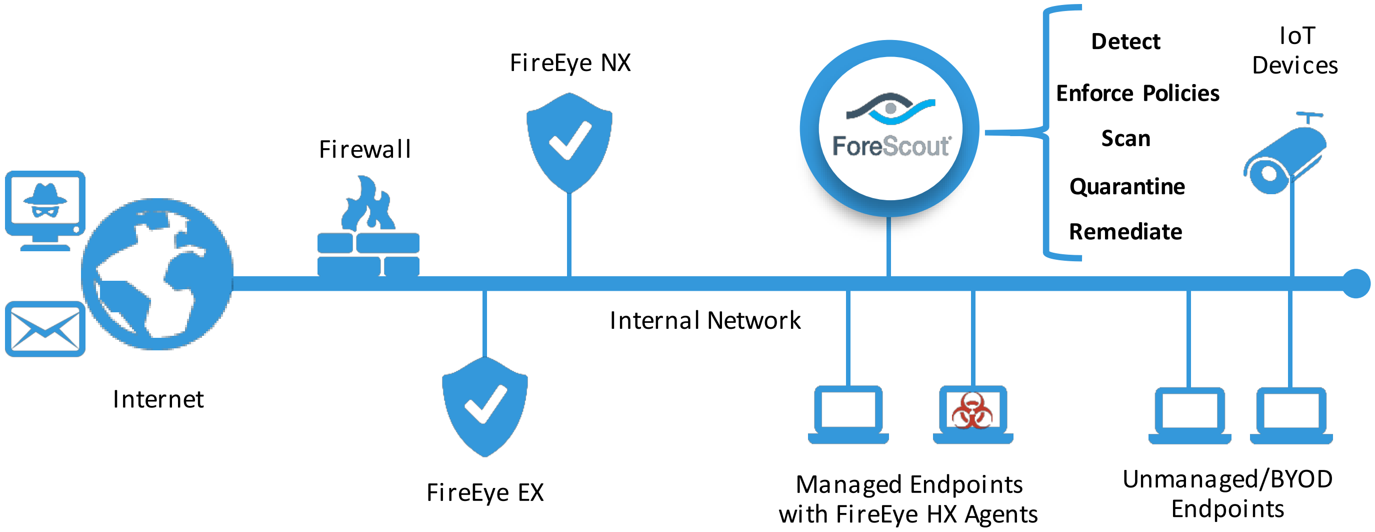
The Solution: ForeScout Extended Modules for FireEye

Unmanaged, bring-your-own-device (BYOD), guest, and Internet of Things (IoT) endpoints are often unpatched, lack security agents, and include unauthorized applications. Hence, they can serve as network-attached launching points for malware. By combining ForeScout's endpoint visibility, access control and automated response capabilities with FireEye's advanced threat detection techniques, security teams can gain a clearer understanding of their threat exposure and respond more quickly to malware and security breaches.

ForeScout CounterACT integrates with FireEye via three Extended Modules: FireEye Endpoint Security (HX Series), FireEye Email Security (EX Series), and FireEye Network Security (NX Series). FireEye HX and EX Series are designed to detect and stop advanced and targeted attacks, including ransomware and spear phishing delivered by email. FireEye Network Security (NX Series) and FireEye Endpoint Security are built to protect against known and unknown advanced attacks that traditional signature- and policy-based network technologies often miss.

ForeScout CounterACT leverages threat information from FireEye solutions to scan the network for indicators of compromise (IOCs), determine the extent of infection on the network, and contain infected endpoints to prevent further threat propagation and data exfiltration by automating threat response. FireEye does not rely on signatures alone to identify and block threats in real time.

Figure 2. ForeScout Integration with FireEye NX, HX, and EX



FireEye offers threat and behavior analysis exploit detection capabilities with FireEye Endpoint Security (HX Series), and is designed to defend against known and unknown threats. For endpoints that are found to have the presence of a known threat, CounterACT can take various actions such as: initiating built-in or third-party remediation systems, sharing real-time context with other response systems, or notifying the end-user and administrator via email or Short Message Service (SMS), and numerous other host- and network-based actions that are available within CounterACT. CounterACT can also initiate the installation or update of the FireEye Endpoint Security agent on endpoints where the agent is missing, deactivated, or out of date.

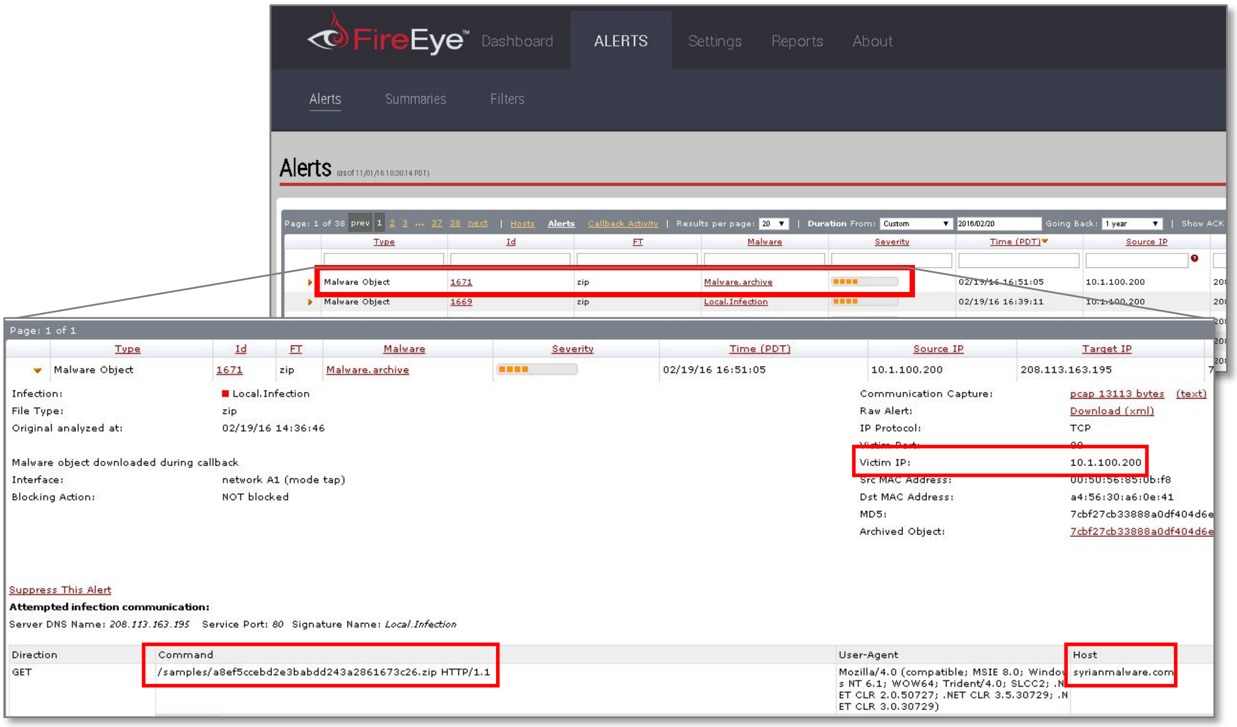
FireEye Email Security identifies advanced and targeted email threats by analyzing attachments and URLs using the MVX engine. When FireEye email security solution detects an infected email, it quarantines the email and provides contextual information to CounterACT. CounterACT then automatically takes policy-based mitigation actions to contain and respond to that threat. Depending on the severity or priority of the threat, various actions may be taken, such as scanning endpoints on the network, quarantining infected endpoints, triggering built-in or third-party remediation systems, or notifying the end-user via email or SMS.

ESG Lab Tested

ESG Lab walked through ForeScout CounterACT's integration with FireEye Network Security to validate the ability of the joint solution to detect advanced threats and IOCs, automate containment of infected endpoints based on threat level, scan endpoints that reside on the network for the presence of known threats, and scan endpoints when they connect to the network for the presence of threats.

First, ESG Lab configured the integration between ForeScout CounterACT and FireEye Network Security in just two steps. CounterACT's IP address was added as a target for notifications from FireEye Network Security via syslog, in JSON format. In CounterACT, the FireEye Modules were configured with the IP addresses of the FireEye Network Security appliances. The whole process took less than a minute. At this point, we were ready for our first scenario, where a corporate endpoint downloads malicious software. ESG Lab connected to a site hosting malware samples, downloaded one to the desktop, and extracted it.

Figure 3. FireEye Sending Indicator of Compromise Data to ForeScout



Alerts (as of 11/01/16 10:30:14 PDT)

Page: 1 of 38 prev 1 2 3 ... 37 38 next | Hosts Alerts Callback Activity | Results per page: 20 | Duration From: Custom 2016/02/20 Going Back: 1 year | Show ACK

Type	Id	FT	Malware	Severity	Time (PDT)	Source IP	
Malware Object	1671	zip	Malware.archive	■■■■	02/19/16 16:51:05	10.1.100.200	20
Malware Object	1669	zip	Local.Infection	■■■■	02/19/16 16:39:11	10.1.100.200	20

Page: 1 of 1

Type	Id	FT	Malware	Severity	Time (PDT)	Source IP	Target IP
Malware Object	1671	zip	Malware.archive	■■■■	02/19/16 16:51:05	10.1.100.200	208.113.163.195

Infection: ■ Local.Infection
File Type: zip
Original analyzed at: 02/19/16 14:36:46

Malware object downloaded during callback
Interface: network A1 (mode tap)
Blocking Action: NOT blocked

Communication Capture: pcap 13113 bytes (text)
Raw Alert: Download (xml)
IP Protocol: TCP
Victim Port: 80
Victim IP: 10.1.100.200
Src MAC Address: 00:50:56:85:0b:f8
Dst MAC Address: a4:56:30:a6:0e:41
MD5: 7cbf27cb33888a0df404d6e
Archived Object: 7cbf27cb33888a0df404d6e

Suppress This Alert

Attempted infection communication:

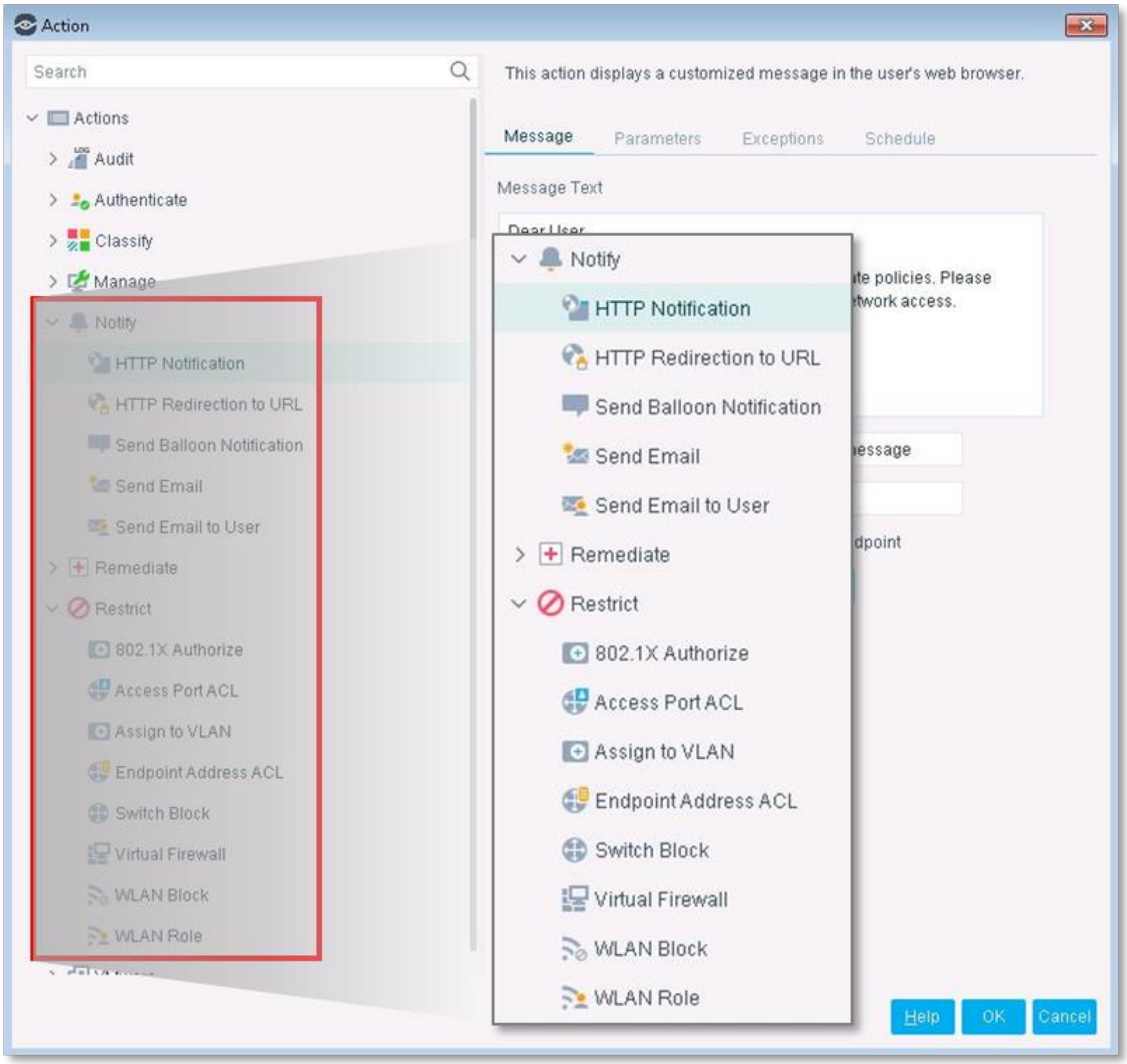
Server DNS Name: *208.113.163.195* Service Port: *80* Signature Name: *Local.Infection*

Direction	Command	User-Agent	Host
GET	/samples/a8ef5ccebd2e3babdd243a2861673c26.zip HTTP/1.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)	syrianmalware.com

As shown in Figure 3, FireEye sends an alert to CounterACT with relevant IOC information, including the endpoint that is infected. When CounterACT receives the alert, it responds according to customizable policies. In this case, when the infected executable was run, CounterACT killed the process on the endpoint and put the endpoint in a remediation vLAN. Along with this endpoint containment process, CounterACT also initiated a scan on the other endpoints that were connected to the network to detect the presence of this known threat.

Next, ESG Lab looked at a different scenario, where endpoints are trying to connect to the website or CnC address discovered as an IOC in the previous demonstration. CounterACT can leverage the data provided about the threat and can take a wide variety of host- or network-based actions, including warning the user via a pop-up http notification, killing the running process, assigning the device to a new VLAN, or applying a virtual firewall to isolate the device, as shown in Figure 4. ESG Lab attempted to connect to the DNS name of the website in the previous example using a new endpoint and CounterACT detected and blocked the malicious activity. CounterACT continuously monitors the network to automatically detect when any subsequent endpoints try to browse to a known malicious URL or connect to a known CnC address and take appropriate policy-based actions.

Figure 4. ForeScout CounterACT Policy Actions



This action displays a customized message in the user's web browser.

Why This Matters

With the rapidly evolving threat landscape, it's no wonder that cybersecurity initiatives represent the IT priority most often cited by ESG research respondents in 2017. Many organizations utilize FireEye Endpoint Security to manage endpoint security on corporate endpoints, FireEye Email Security to detect and block emails containing malicious links and attachments, and FireEye Network Security to protect against known and unknown advanced attacks hiding in internet traffic. With a significant percentage of unmanaged endpoints on organizations' networks, whether BYOD, corporate assets with non-functional agents, or IoT devices, a solution that can extend the FireEye platform to these devices could significantly reduce an organization's attack surface.

ESG Lab has validated that ForeScout CounterACT detects and profiles endpoints as they connect to the network—whether managed or unmanaged—and deeply integrates with FireEye advanced threat protection products to continuously monitor and remediate endpoint vulnerabilities and security gaps.

The Bigger Truth

The unprecedented diversity of users, devices, and applications on networks—where employees, contractors, guests, and partners often use personal devices to connect to their own sets of network resources—challenges businesses to efficiently provide appropriate network access to authorized and approved users, devices, applications, and systems.

ESG Lab was quite impressed with ForeScout CounterACT's ability to efficiently address network access, endpoint compliance, mobile security, and threat mitigation. In ESG Lab testing, CounterACT delivered real-time intelligence about devices, applications, and users on the network, with granular controls to help enforce endpoint security policy. In addition, information sharing and automation with FireEye advanced threat prevention products helped rapidly address security issues on managed and unmanaged devices.

ForeScout CounterACT demonstrated that it can provide visibility, intelligence, and policy-based mitigation of security issues by providing real-time insight into the vulnerabilities and security gaps on unmanaged devices while coordinating security controls and automating responses to rapidly contain threats and breaches.

. The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.