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

ESG Lab Review

ForeScout Extended Module for Splunk

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

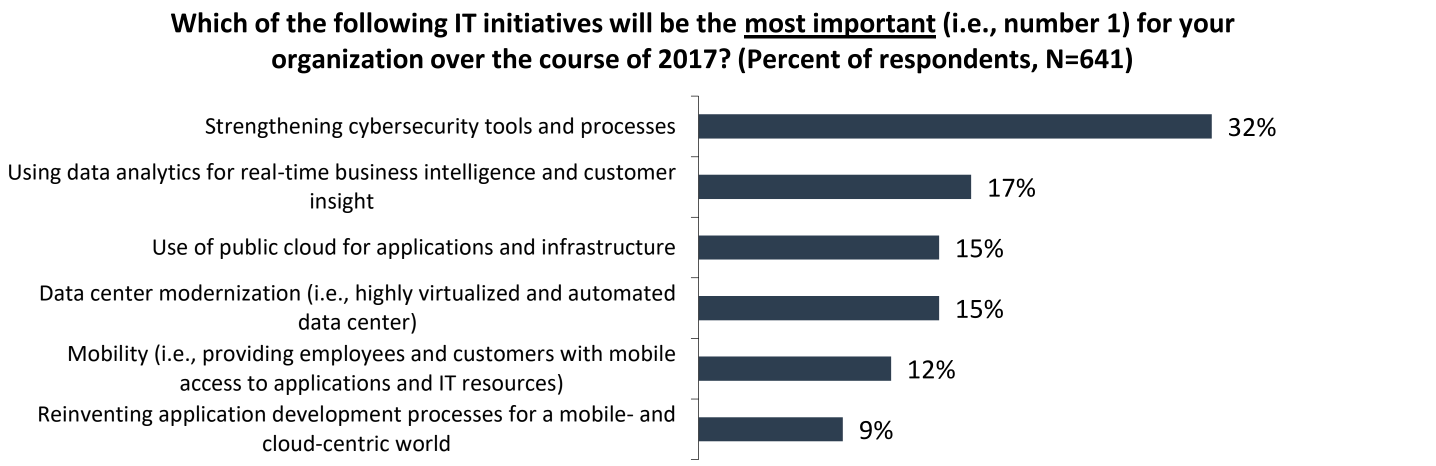
Abstract

This report provides a first look at the key benefits of ForeScout's bidirectional integration with Splunk Enterprise and Splunk Enterprise Security (ES), with a focus on how the ForeScout Extended Module can combine ForeScout's endpoint insight, access control, and automated response capabilities with Splunk's correlation, analysis, and search features. This integration provides visibility into and control of managed and unmanaged endpoints while helping security teams better understand their security risk posture and respond quickly to mitigate security issues.

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 nonfunctional 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: The ForeScout Extended Module for Splunk

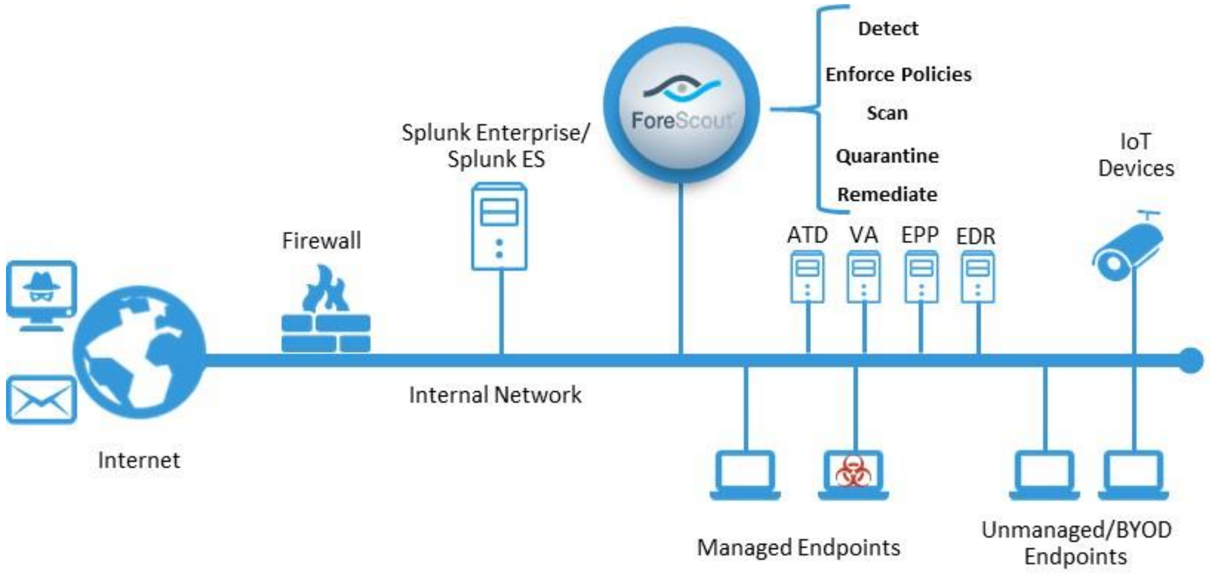
The ForeScout CounterACT platform is designed to provide continuous security monitoring and mitigation for an organization's devices, both traditional and nontraditional, when they connect to the network. ForeScout's goal is to provide IT organizations with comprehensive insight into their endpoint landscape and compliance, and to address network access and threat management challenges.

ForeScout CounterACT integrates with Splunk Enterprise and Splunk ES via the ForeScout Extended Module for Splunk. Organizations use Splunk Enterprise to obtain operational intelligence by collecting and indexing logs and machine data from their infrastructure and security tools. Splunk provides search, analysis, and visualization capabilities to help quickly discover and share insights. Splunk Enterprise Security (ES) extends the power of Splunk Enterprise, designed to streamline security operations, improve threat management, and minimize business risk.

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 threats. By combining ForeScout's endpoint visibility, access control, and automated response capabilities with Splunk ES, customers can also leverage the joint solution and Splunk Adaptive Response framework for closed-loop remediation and threat mitigation.

With this joint solution, security teams can store CounterACT data in Splunk for long-term trend analysis, visualization, and incident investigation; identify anomalous behavior and events based on CounterACT data; correlate high-value endpoint context from CounterACT with other data sources like advanced threat detection (ATD), vulnerability assessment (VA), endpoint protection platforms (EPP), endpoint detection and response (EDR) systems, and next-generation firewalls to identify and prioritize incidents; and initiate CounterACT network and host actions from Splunk to automate incident response, remediation, and threat mitigation.

Figure 2. ForeScout Integration with Splunk Enterprise and Splunk ES



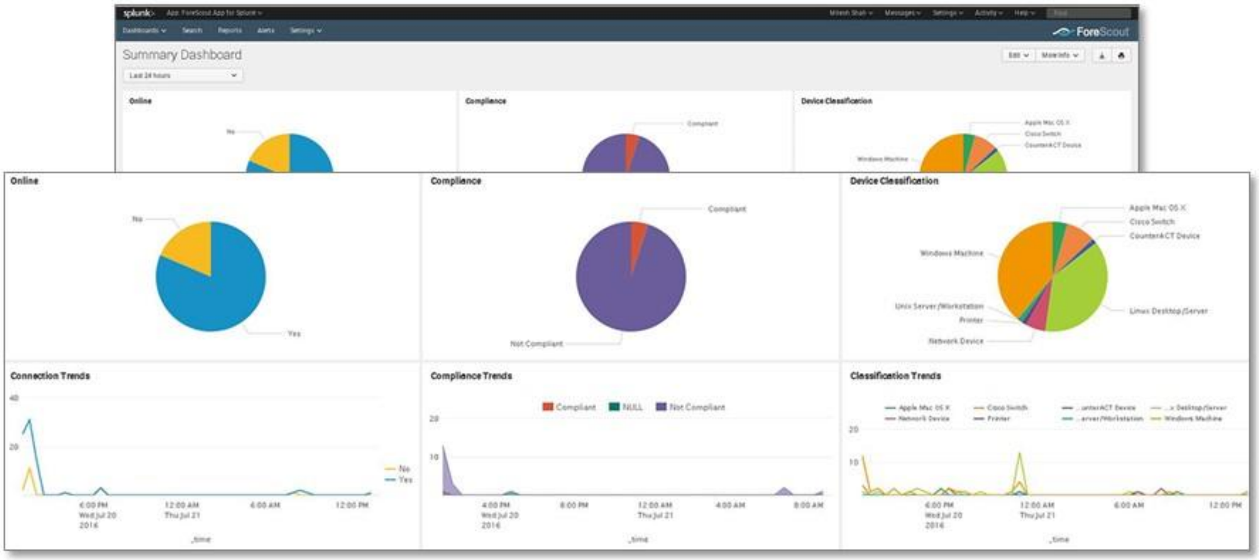
Splunk helps organizations to comply with log retention mandates buy storing the data sent to it by CounterACT. Information sent to Splunk includes real-time inventory of connected devices on the network—from traditional corporate PCs, servers, and mobile devices to BYOD and IoT devices. ForeScout sends detailed device information on device type, classification, network connection, operating system, applications, users, and peripherals, for example. Device security posture and compliance gaps are also reported, along with authentication, access, network location information, and threat indicators on devices detected by IOC scanning.

ESG Lab Tested

ESG Lab walked through ForeScout CounterACT's integration with Splunk Enterprise and Splunk ES to validate the ability of the joint solution to detect anomalies, provide context for correlation and incident prioritization, and provide automated, closed-loop incident response.

ESG Lab configured the integration between ForeScout CounterACT and Splunk in just two steps. First, ESG Lab configured the Extended Module for Splunk to connect to a Splunk HTTP Event Collector—CounterACT can also send detailed endpoint data and third-party alerts to Splunk using Syslog or REST API. Next, the ForeScout App for Splunk was configured to send alerts and messages to CounterACT. The whole process took less than a minute. At this point, we were ready for our first scenario, which ForeScout refers to as a multi-stage correlated action, where the information sharing between products results in a chain of events that helps customers limit risk factors in their environment.

Figure 3. ForeScout App for Splunk Summary Dashboard—Connection, Compliance, and Classification



CounterACT sends real-time information to Splunk for long-term storage and Splunk maintains a database of information from CounterACT and multiple other systems for analysis and correlation. Keeping that data for an extended period allows organizations to run trend and compliance reports over an extended timeframe, as shown in Figure 3.

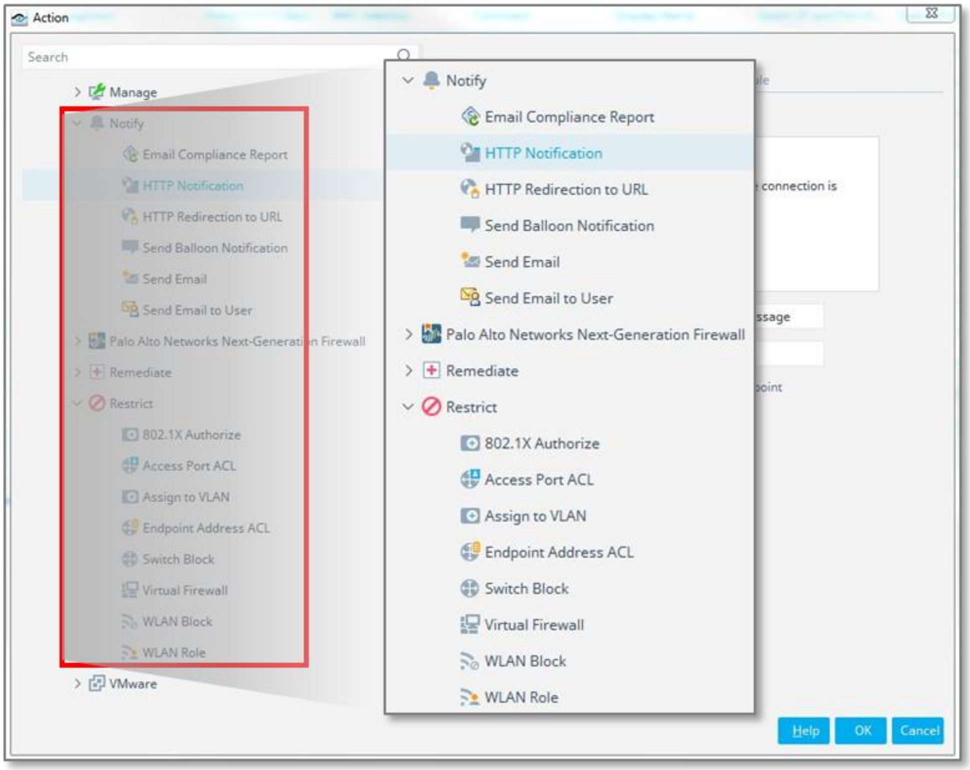
The ForeScout App for Splunk Summary Dashboard visualizes information provided by ForeScout CounterACT to Splunk. The report is divided into three sections: Online, Compliance, and Device Classification. The ***Online*** chart in the upper left shows a representation of the number of endpoints that CounterACT sees and shows how many are online versus offline. Similarly, the ***Compliance*** chart shows the endpoints' compliance status. ***Device Classification*** reports on what types of endpoints are on the network. Below all three charts are trend timelines that show how these three categories have changed over time.

ESG Lab also looked at anomaly detection. In this example, the Splunk operator created a baseline for user authentications and the deviation that would be considered an anomaly. When ForeScout forwarded data for authentication attempts that deviated from the baseline based on frequency, location, time, or system, an anomaly detection alert was generated by Splunk. Next, endpoint context was examined. In our test environment, an IPS system sent an alert to Splunk about a potentially compromised system. Splunk used the user and device context and classification to confirm whether the event was malicious, in this case escalating the severity of the event. Splunk can also reduce severity if the event is determined to be benign.

Finally, ESG Lab looked at the capability of ForeScout and Splunk to provide automated, closed-loop incident response. In this scenario, an ATD system identified an IOC and sent an alert to ForeScout and Splunk. ForeScout sent detailed endpoint context to Splunk for further analysis, and Splunk correlated the threat data from the ATD system, endpoint context from

ForeScout, and data from other threat feeds to determine which endpoints were truly compromised. The Splunk operator sent an action request to ForeScout to release non-compromised endpoints and to block compromised endpoints. CounterACT can take a wide variety of policy-based 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. ForeScout sends results data back to Splunk for review in the Incident Review dashboard, attached to the Notable Event which triggered the action requests.

Figure 4. ForeScout CounterACT Policy Actions



Why This Matters

With the rapidly evolving threat landscape growing more difficult to manage, it's no wonder that cybersecurity initiatives represented the IT priority most often cited by ESG research respondents in 2017.[4] Splunk provides the ability to collect large amounts of information from multiple sources, including security systems, network devices, users, and IoT devices. The ability to collect, store, analyze, and correlate this information is an asset but requires manual intervention. With a significant number of unmanaged endpoints on organizations' networks, whether BYOD, corporate assets with nonfunctional agents, or IOT devices, a solution that can enable organizations to automatically detect, respond to, and mitigate threats is needed.

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 Splunk Enterprise and Splunk ES to continuously monitor and remediate endpoint vulnerabilities and security gaps and provide automated, closed-loop incident response to attacks and security breaches, which improves an organizations security posture.

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

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.

Splunk Enterprise enables organizations to acquire operational intelligence through analysis of logs and machine data from their infrastructure and security tools. Search, analysis, and visualization capabilities are designed to help operators quickly discover and share insights. Splunk Enterprise Security (ES) extends the power of Splunk Enterprise, designed to streamline security operations and improve threat management, with a goal of minimizing business risk.

ESG Lab was quite impressed with ForeScout CounterACT's ability to enable organizations using Splunk 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 to Splunk, with granular controls to help enforce endpoint security policy. In addition, information sharing and automation with Splunk helped rapidly address security issues via an automatic closed-loop process.

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 managed and unmanaged devices while coordinating security controls and automating responses to rapidly contain threats and breaches. If your organization is currently using or considering Splunk for security intelligence, it would be a smart move to look at how ForeScout CounterACT can work with Splunk to drive efficiency and improve security and compliance postures.

. 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.