ForeScout

Highlights

See

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor endpoints on the network, including corporate, BYOD, guest and IoT

Control

- Allow, deny, change or limit network access based on user, network segment, application, device profile and security posture
- Initiate threat mitigation actions on non-compliant, vulnerable and compromised endpoints
- Improve compliance with industry and government mandates and regulations

Orchestrate

- Share high-value endpoint context with Splunk to enhance correlation and prioritize incidents
- Improve long-term trend analysis, anomaly detection and incident investigation
- Automate system-wide incident response to quickly mitigate threats and data breaches

ForeScout Extended Module for Splunk®

Gain greater in-depth endpoint insight, improve situational awareness and automate incident response

Splunk® Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results. Splunk Enterprise Security (ES) extends the power of Splunk Enterprise, enabling security teams to harness data and gain organization-wide visibility and security intelligence.

The ForeScout Extended Module for Splunk enables bi-directional integration of ForeScout CounterACT® with Splunk Enterprise and Splunk ES. It combines ForeScout's endpoint visibility, access control and automated response capabilities with Splunk's powerful correlation, analysis and search features. This helps security teams better understand their overall security risk posture and respond more quickly to mitigate a range of security issues.

Forescout and Splunk customers can also leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency.

The Challenges

Visibility. Serious attempts to manage security risk must start with knowledge of who and what is on your network, including visibility into whether the devices on your network are compliant with your security standards. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

- Unmanaged guest or Bring-Your-Own-Device (BYOD) endpoints
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

As a result, organizations are often left unaware of the attack surface on these devices.

Threat Detection. According to industry experts, the vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network. Today's cyberattacks are targeted, multivector and stealthy. They are focused on acquiring sensitive personal information, intellectual property or insider information. These threats can easily evade traditional security defenses, as corporate or BYOD endpoints can get infected on public networks through USB peripherals or through unmonitored threat vectors. To limit threat propagation through the network, organizations need the ability to assess security posture, identify compliance gaps and scan for indicators of compromise (IOCs) on devices as they connect to the network.

> **Leveraging the ForeScout Extended Module for Splunk via Adaptive Response, we can increase our holistic data defense and security to minimize the impact of malware and data breaches."**
>
> **— Clayton Colwell, Associate Security Engineer, Brown-Forman Corporation**

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating a perfect storm for incident response programs. Without automated correlation, analysis and response capabilities, IT teams lose valuable time prioritizing and responding to incidents manually. Accurate and up-to-date endpoint context—including device classification, user identity, software inventory, security posture, network connection and location information—is essential for prioritizing incidents. And closed-loop remediation and threat mitigation are vital for automating incident response and combating cyberthreats, security breaches and data exfiltration.

Extended Module for Splunk

ForeScout CounterACT is a network security solution that gives you the unique ability to see devices, including non-traditional devices, when they connect to the network. CounterACT provides policy-based control of these devices. It works with ForeScout ControlFabric® Architecture to orchestrate information sharing and automate workflows among disparate security and IT management tools, including Splunk Enterprise and Splunk ES.

Paired with CounterACT, the ForeScout Extended Module for Splunk and ForeScout App for Splunk allow bi-directional communication with Splunk Enterprise and Splunk ES, which gives customers unparalleled visibility into endpoints on the network, including BYOD, IoT and guest devices. You can also leverage endpoint context from CounterACT to improve correlation and prioritize incidents within Splunk solutions, and take precise, automated endpoint remediation actions based on correlated security data.

With ForeScout and Splunk, security teams can:

- Store CounterACT data in Splunk solutions 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 to identify and prioritize incidents
- Initiate CounterACT network and host actions from Splunk to automate incident response, remediation and threat mitigation

The ForeScout Extended Module for Splunk sends CounterACT data to Splunk solutions for long-term storage, trend analysis, correlation and incident prioritization. This also helps you comply with log retention mandates. 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
- Device information, such as device type, classification, network connection, operating system, applications, users, peripherals and more
- Device security posture and compliance gaps
- Authentication, access and network location information
- Threat indicators on devices detected by IOC scanning

The ForeScout App for Splunk and relevant add-ons are available on Splunkbase and install on Splunk Enterprise or Splunk ES. They provide customizable, out-of-the-box queries and dashboards to visualize CounterACT data in Splunk. These dashboards display a wealth of information, including:

- Endpoint compliance status
- User types (registered corporate users or guests)
- Device types connected to the network, and connection details
- Patterns of network access over time
- Policy trends
- CounterACT system health information

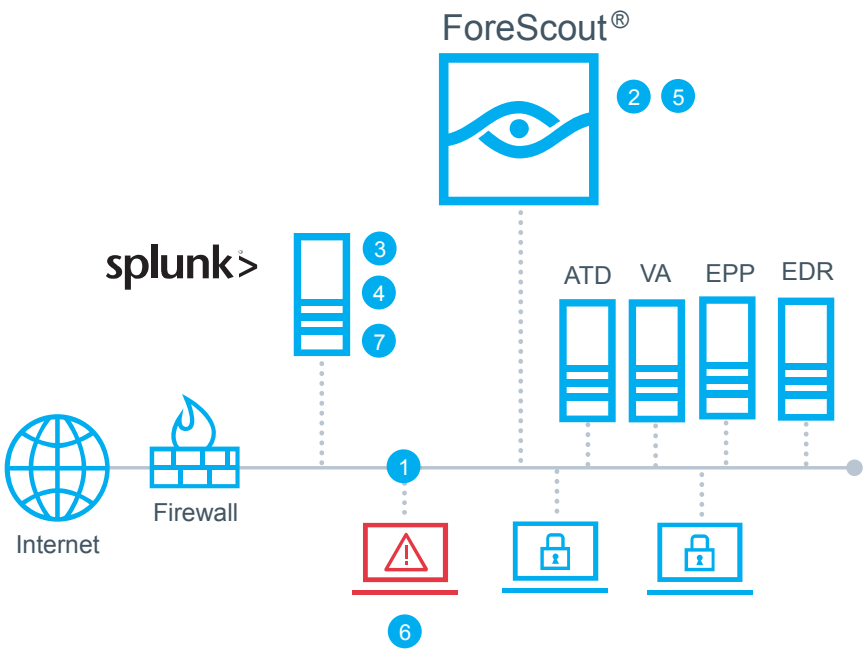
When an alert is raised by Splunk solutions, either based on CounterACT data or correlated data from multiple sources, the ForeScout Extended Module for Splunk enables incident response teams to initiate CounterACT actions to mitigate threats. For example, if the threat is related to a vulnerable, non-compliant or suspicious endpoint, Splunk can prompt CounterACT to isolate the endpoint and initiate remediation actions.

Splunk ES customers can use the Alert Mitigation Center to review alerts, delegate adaptive response actions to CounterACT and review response results. Incident response teams can streamline security operations and minimize business risk by implementing closed-loop response, remediation and threat mitigation.

ForeScout Extended Modules

The ForeScout Extended Module for Splunk is an add-on module for ForeScout CounterACT that is sold and licensed separately. It's one of many ForeScout Modules that enables CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response.

The ForeScout App for Splunk and relevant add-ons are available on Splunkbase (splunkbase.splunk.com).



1. CounterACT discovers, classifies and assesses devices as they connect to the network
2. CounterACT sends up-to-date device context to Splunk for long-term storage and correlation, including device connection, classification and compliance information
3. ForeScout App for Splunk visualizes CounterACT data for trend analysis, monitoring and reporting
4. Splunk leverages device context from CounterACT and correlates with other data sources to identify and prioritize incidents
5. Splunk operators initiate adaptive response actions using CounterACT based on severity of the alert
6. CounterACT triggers policy-based mitigation and remediation actions on non-compliant, vulnerable or suspicious endpoints and reports action status back to Splunk
7. Splunk Enterprise operators can review response action status and results using the ForeScout App. Splunk ES customers can see the complete alert and response action lifecycle in the Alert Mitigation Center.

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