ForeScout

Highlights

- Agentless discovery and profiling of virtual and physical devices, including unmanaged BYOD, guest and IoT
- Comprehensive, real-time device data is automatically correlated and efficiently sent to Splunk
- More than 500 device properties can be added to Splunk for context-rich analytics and incident response policies
- Device data can be transferred without IP address for broader discovery and analytics
- Data feeds are Splunk Common Information Model (CIM)-ready for faster time to insight
- Closed-loop workflows from device and threat discovery to threat response and results reporting
- ForeScout supports integration with Splunk Enterprise and Splunk ES

Benefits

- Collect real-time device and network insight to continually reduce risk and refine policies
- Improve long-term trend analysis, anomaly detection and incident investigation
- Automate system-wide incident response to rapidly mitigate and remediate threats
- Prioritize incidents more easily and develop granular security policies using greater contextual insight
- Optimize time to insight, compliance enforcement and overall IT security operations efficiency

ForeScout Extended Module for Splunk®

Gain in-depth networked device insight, improve situational awareness and automate incident response

Splunk® Enterprise makes it simple to collect, analyze and act on the untapped value of big data generated by your technology infrastructure, security systems and business applications-giving you needed insight to drive operational performance and business results. Splunk Enterprise Security (ES) runs on top of Splunk Enterprise to provide an analytics-driven security information and event management (SIEM) solution to quickly detect and respond to internal and external attacks.

The ForeScout Extended Module for Splunk provides bi-directional integration between the ForeScout platform and both Splunk Enterprise and Splunk ES. The ForeScout Extended Module for Splunk combines ForeScout's agentless device visibility, broad array of controls and automated response capabilities with Splunk Enterprise and ES's powerful data correlation, rich analytics, incident management and search features. This integration helps you better understand your organization's overall security risk posture and rapidly respond to mitigate and remediate a range of security incidents. The integration also enables incident response workflows that leverage the Splunk Adaptive Response framework. The ForeScout-Splunk integrated solution provides closed-loop workflows that help enhance insight, reduce risk and improve operational performance.

The Challenges

Visibility. Serious attempts to manage security risk must start with full visibility of what and who is on your network, where they are and if devices are compliant with security standards. Most organizations are unaware of their overall attack surface because a significant percentage of devices on the network might be missed by periodic scans or unseen by corporate endpoint management tools, such as:

- Guest, Bring-Your-Own-Device (BYOD), and Internet of Things (IoT) devices
- Managed devices with missing, disabled, misconfigured or broken agents
- Transient devices undetected by periodic scans
- New IPv6 connected devices and/or network-connected devices such as Operational Technology (OT) that might not have an IP address
- Devices from different locations with overlapping IP addresses
- Orphan or underutilized Virtual Machine (VM) instances

Threat Detection. The vast majority of successful attacks exploit well-known vulnerabilities and security gaps on connected devices. Today's cyberattacks are targeted, multi-vector and stealthy. They are focused on acquiring sensitive personal information, intellectual property or insider information. Threats can easily evade traditional security defenses. Corporate or BYOD devices can acquire

> **ForeScout helps drive the intelligence of the SOC and integrates data feeds with all of our core security products."**
>
> **— Nick Duda, Principal Security Engineer HubSpot**

infections from public networks or USB peripherals. Many unmonitored threat vectors also exist on IoT devices. To limit threat propagation through enterprise networks, organizations need the ability to continually assess security posture, identify compliance gaps and scan for indicators of compromise (IOCs) on devices as they connect to the network.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, create a perfect storm for incident response programs. Without automated correlation, analysis and response capabilities, operations teams lose valuable time prioritizing and responding to incidents manually. Real-time device context, including device attributes, user profiles, security posture, applications, network and location information, provides essential insight for prioritizing incidents and determining appropriate response. Additionally, creating closed-loop threat mitigation and remediation is vital for automating incident response and refining policies to better combat cyberthreats, security breaches and data exfiltration.

ForeScout Extended Module for Splunk

The ForeScout platform provides continuous visibility of devices, including guest, BYOD, IoT and OT devices, as they connect to the network. It can also enforce policies with automated system and network controls per policy. ForeScout Extended Module solutions orchestrate information sharing and automate workflows between ForeScout and disparate security and IT management tools.

The ForeScout Extended Module for Splunk is a ForeScout extension that creates additional functionality by providing a bi-directional integration with Splunk Enterprise and Splunk Enterprise Security (ES). The ForeScout-Splunk integration gives you unparalleled insight and incident response capabilities across managed and unmanaged devices, regardless of connection point or network tier. The ForeScout Extended Module for Splunk enables you to:

- Store ForeScout data in Splunk Enterprise for long-term trend analysis, visualization and incident investigation
- Correlate high-value device context from ForeScout with other data sources to better identify and prioritize anomalous behavior and events
- Accelerate incident response by initiating ForeScout network and/or endpoint actions from Splunk through the Adaptive Response framework
- Increase valuable user and location context by resolving overlapping IT addresses and layering tenant ID with IP address in meta data

The comprehensive information sent from ForeScout to Splunk includes:

- Real-time inventory of connected devices on the network-from traditional PCs, servers and mobile systems to virtual machines to BYOD, IoT and OT, including devices with IPv6 and those with no IP address
- Endpoint information, such as device type, classification, network connection, operating system, applications, users, peripherals and more
- Device security posture and compliance gaps
- Authentication, access, tenant ID and network location information
- Threat indicators on devices detected by IOC scanning

The ForeScout App and Add-ons for Splunk, available on Splunkbase™, pair with Splunk Enterprise and Splunk ES and the ForeScout Extended Module for Splunk. The ForeScout App and Add-ons accelerate time to insight and time to respond and establish efficient communications between Splunk Enterprise and the ForeScout platform.

The ForeScout Technology Add-on for Splunk is a required component to streamline data transfer between ForeScout and Splunk Enterprise. This Add-on maps ForeScout device properties to the Splunk Common Information Model (CIM) and extracts events based on ForeScout data. The ForeScout Technology Add-on also maintains ForeScout credentials for communications between ForeScout and Splunk Enterprise.

The ForeScout App for Splunk provides customizable, out-of-the-box queries and dashboards to visualize ForeScout data in Splunk, displaying a wealth of information, including:

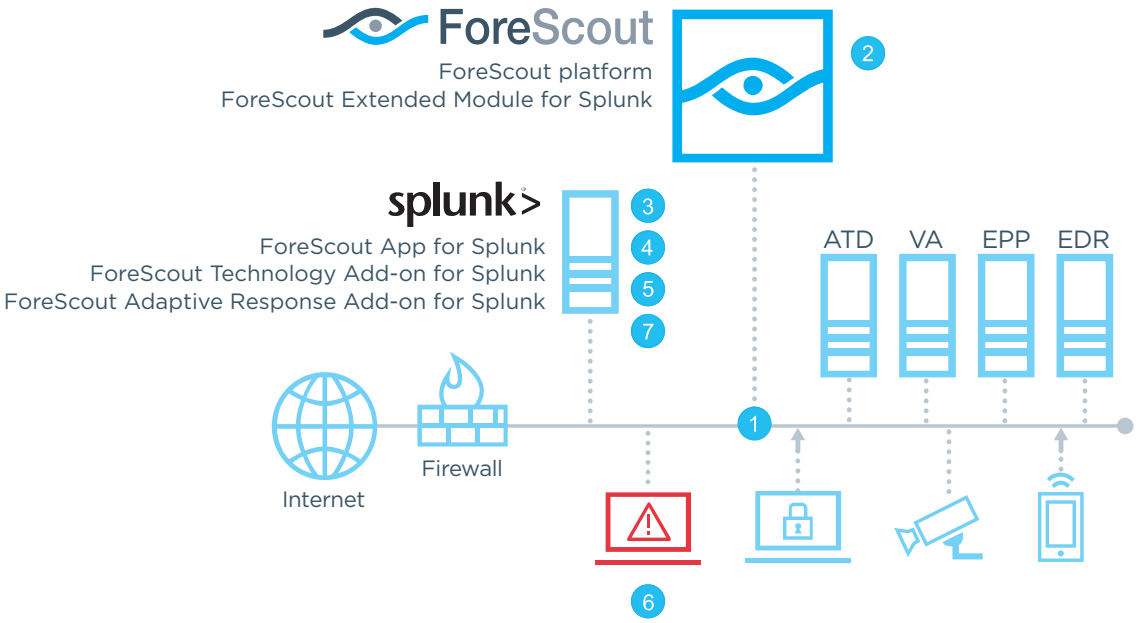
- Endpoint compliance status
- User types (registered corporate users or guests)
- Device types connected to the network, and connection details
- Patterns of network access over time
- Policy trends
- ForeScout system health information
- Incident response action status

The ForeScout Adaptive Response Add-on, in combination with the ForeScout Extended Module for Splunk, allows you to capitalize on the Splunk Adaptive Response framework. The ForeScout Adaptive Response Add-on lets you use the ForeScout App for Splunk Response Action Dashboard and/or Splunk ES's Alert Mitigation Center to visualize searches executed and actions taken. The ForeScout Adaptive Response Add-on also allows you to delegate Adaptive Response actions to ForeScout through Splunk ES and/or execute policy-driven actions through the ForeScout App for Splunk with Splunk Enterprise. The ForeScout Adaptive Response Add-on also facilitates reporting of ForeScout actions taken to Splunk Enterprise and ES. This provides a complete analysis of incident status and helps with policy refinements. Having closed-loop incident response workflows allows you to streamline security operations and minimize business risk.

ForeScout Extended Module Licensing

The ForeScout Extended Module for Splunk is an extension to the ForeScout platform that is sold and licensed separately. It is one of many ForeScout Extended Modules that enable the ForeScout platform to exchange information, automate multivendor workflows and accelerate system-wide response. For details on ForeScout's licensing policy, see www.forescout.com/licensing.

The ForeScout App and Add-ons for Splunk are available in Splunkbase™ (splunkbase.splunk.com).



1. ForeScout discovers, classifies and assesses devices as they connect to the network.
2. ForeScout sends real-time, pre-correlated device data, including networking context, in a single message packet to Splunk for long-term storage and easier correlation with other data sources, richer insight and more complete compliance information.
3. ForeScout App for Splunk visualizes ForeScout data for trend analysis, monitoring and reporting.
4. Splunk leverages device context from ForeScout and correlates with other data sources to identify and prioritize incidents.
5. With the ForeScout Adaptive Response Add-on and Splunk ES, Splunk operators can initiate actions using ForeScout based on alert severity.
6. Through the Extended Module for Splunk, the ForeScout platform can automate incident response to Splunk alerts, performing policy-driven actions on non-compliant, vulnerable or suspicious endpoints, and report action status back to Splunk. Actions can include orchestration with other security or management systems that leverage ForeScout Extended Modules for those systems.
7. Splunk operators can see the complete alert and response action lifecycle via the Spunk ES Alert Mitigation Center or ForeScout App for Splunk Response Action Dashboard within Splunk Enterprise.

Learn more at
www.ForeScout.com

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

Version 4_18