FORESCOUT

# Forescout eyeExtend for Splunk®

## Improve situational awareness, prioritize incidents and accelerate response

Organizations use Splunk's data analytics to gather, analyze and correlate security information and events for security monitoring, incident investigation and compliance reporting. But the challenges to get an accurate security snapshot of the network and ability to dynamically respond to any identified incident remain for organizations. By combining the Forescout platform's complete device visibility and insight with Splunk's data mining expertise, Forescout eyeExtend for Splunk allows security managers to achieve a broader understanding of their security posture, visualize key control metrics and respond more quickly to mitigate a range of security incidents. Organizations benefit by optimizing time to insight, achieving quicker incident response and realizing strengthened network security.

## Challenges

- Gaining real-time device visibility across managed and unmanaged devices for better situational awareness
- Improving the accuracy and reliability of Splunk's trend analysis for incident investigation
- Rapidly detecting and prioritizing alerts and assessing criticality of incidents to focus resources on the most urgent security events
- Compressing incident response time to curb lateral attacks

## The Solution

Forescout eyeExtend for Splunk combines complete device visibility, broad array of controls and automated response capabilities from Forescout with Splunk's data correlation, analytics and incident management.

Through its agentless architecture and real-time continuous monitoring, Forescout eyeExtend for Splunk provides Splunk with complete device visibility and in-depth context across IT, cloud and OT networks. The comprehensive and rich contextual device data provides a complete picture of your entire enterprise attack surface, helps reduce time to insight and facilitates investigations. It also contributes to more precise trend analysis, accurate correlation and prioritization of alerts and events enabling your security team to focus their time and attention on the most critical security incidents. Forescout also helps with streamlining security operations by automating policy based actions-limiting access of the device to the network based on incident severity feed from Splunk in real time.

Put simply, Forescout eyeExtend for Splunk helps improve situational awareness, prioritize incidents and automate remediation to enhance overall IT and security operations efficiency and minimize security and business risk to an organization.

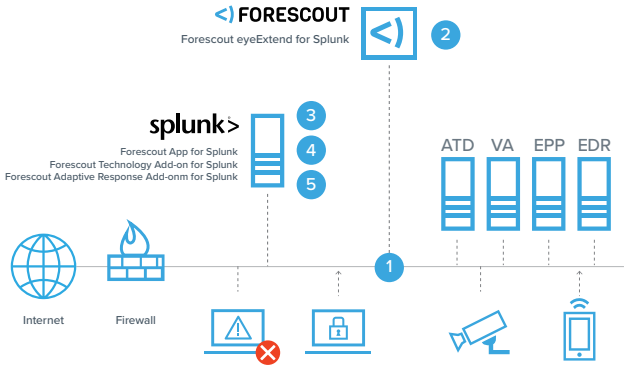
eyeExtend

### Benefits

- Reduce risk and refine security policies by collecting real-time device and network insight across all devices
- Enhance fidelity and scope of Splunk's long-term trend analysis and investigations
- Increase operational efficiency by helping prioritize incidents according to severity with Forescout's rich contextual device data
- Automate incident response to rapidly remediate threats

### Highlights

- Complete device visibility of all virtual and physical devices, including unmanaged BYOD, guest, IoT and OT devices
- Rich contextual device data in Splunk Common Information Model (CIM)-ready format
- Enhanced incident correlation and prioritization
- Automated and closed-loop incident response workflows across the entire incident lifecycle
- Workflow orchestration between Forescout eyeExtend for Splunk and Splunk® Enterprise, Splunk Cloud™ and Splunk® Enterprise Security (ES)




1. Forescout discovers, classifies and assesses devices as they connect to the network and shares this information with Splunk for long term storage and correlation with other data sources
2. Administrators view Forescout data within Splunk for anomaly detection, trend analysis, monitoring and reporting
3. Splunk leverages device context from Forescout and correlates with other data sources to identify and prioritize alerts
4. Forescout can initiate policy-based actions limiting access of the device to the network based on alert severity in real time
5. Forescout reports back action results to Splunk to close the loop for administrators to see the entire incident lifecycle in the Splunk dashboard

## Use Cases

**Rapid anomaly detection and accurate trend analysis**

Forescout discovers, classifies and assesses all IP-connected devices; compiles this information in the Splunk CIM format and shares it with Splunk. The additional device information from Forescout includes user information, device type, device configuration, network access patterns over time, network location and security posture. Splunk correlates rich contextual data from Forescout with other data sources and uses this information for long-term storage, swift anomaly detection and accurate trend analysis

**Enhanced incident correlation and prioritization**

Splunk correlates rich device context from the Forescout platform with other data sources to better identify and prioritize incidents. When Splunk receives alerts from other data sources about a suspicious activity on a device, it shares the information with Forescout. Forescout provides high-value user, network and device context to Splunk. Splunk leverages this additional insight to determine if a suspicious event is actually malicious or violates policy and escalates or reduces the severity of the event based on the device and user context, such as highly privileged or less trusted users.

**Automated closed-loop incident response**

Forescout scans all connected devices for indicators of compromise (IOCs) and policy violations in real time when alerted by Splunk. Splunk operators can initiate Forescout actions—such as isolating or quarantining potentially compromised or noncompliant endpoints—through Splunk's Adaptive Operations Framework–depending on the severity of the violation. Forescout can also dynamically trigger policy-based mitigation and response actions until the deviant device is remediated. Forescout then delivers the results back to Splunk to close the loop. Administrators can view the entire lifecycle and final outcome of the event in the Splunk dashboard.

## Forescout eyeExtend for Splunk Apps and Add-Ons from Splunkbase™

| FORESCOUT APPS AND ADD-ONS | CAPABILITY |
|---|---|
| Forescout Technology Add-on for Splunk | A required component to streamline data transfer between Forescout and Splunk. |
| Forescout App for Splunk | Provides customizable, out-of-the-box queries and dashboards to visualize Forescout data in Splunk dashboard. |
| Forescout Adaptive Response Add-on | Allows delegation of Forescout actions through Splunk's Adaptive Operations Framework. This add-on also enables reporting back the Forescout actions and results to Splunk. |

Please Note:
1. Forescout Apps and Add-Ons are included as part of Forescout eyeExtend for Splunk license.
2. Forescout eyeSight is the base product required for all use cases.
3. Forescout eyeControl product is required to facilitate Forescout actions for incident response.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com