

Cisco and Splunk Integration

Integrated Solutions for Enhanced Security Automation

Today's cybercriminals are becoming more innovative than ever as they work to compromise business networks and extract as much valuable data as they can. Meanwhile, the numerous security vendors have only contributed to security silos in many customer environments. Multiple security products from multiple providers create security blind spots and roadblocks to seamless, holistic threat protection.

This is where the partnership between Cisco and Splunk can deliver immense value to customers, helping to alleviate these challenges and simplify threat defense efforts. Cisco is collaborating with Splunk in their [Adaptive Response Program](#), which targets the kill chain through coordinated mitigation actions. Splunk Adaptive Response leverages the Cisco network for threat response and investigation via integration with Cisco pxGrid and also extends into the cloud for threat investigation with Umbrella

Investigate. Combining this on- and off-network breadth provides a far-reaching "kill switch" in the kill chain.

Additionally, the Cisco® Security Suite for Splunk provides a single-pane-of-glass view of threat telemetry to Splunk. This integrated solution uses custom applications to create a composite cross-product dashboard of security events within Splunk. Specifically, this solution combines the analytics-driven security capabilities of Splunk Enterprise and the add-ons integrated with the full range of Cisco security solutions.

Splunk enables security analysts to take a proactive stance to investigation and response – from monitoring and triage, verifying and escalating, to responding to a breach or infection, across the range of data from Cisco products correlated more broadly across your entire infrastructure.

"Cisco is pleased to expand our collaboration with Splunk by coupling our integrated threat defense portfolio with Adaptive Response. To defend against aggressive adversaries we must streamline remediation by making security simple, open and automated. By integrating Adaptive Response with Cisco's open platforms such as ISE (Identity Services Engine) and Cisco Umbrella Investigate, mutual customers have the tools to help respond to threats throughout the network and in the cloud in real time, enabling protection everywhere."

- Jeff Samuels, vice president of security marketing, Cisco



Security Component Integration Overview

The Cisco and Splunk technology partnership allows Splunk Enterprise platform to ingest and analyze threat data from wide range of Cisco Security technologies.

Cisco Technology	Description	SplunkBase URL
Cisco Security Suite	The Cisco Security Suite provides a single-pane-of-glass interface into Cisco security data. It supports the full Cisco security portfolio.	https://splunkbase.splunk.com/app/525/
Cisco Firepower® Management Center	This Splunk add-on for the Cisco Firepower Management Center uses data collected by Cisco eStreamer for Splunk. It allows a Splunk admin to analyze and correlate reports from Cisco through the Splunk Common Information Model.	https://splunkbase.splunk.com/app/1808
Cisco Umbrella	You can automatically enrich security alerts inside Splunk to discover the connections between the domains, IPs, and file hashes in an attacker's infrastructure.	https://splunkbase.splunk.com/app/3324/
Cisco Identity Services Engine (ISE)	This Splunk app collects data from ISE through syslog and provides Adaptive Network Control (ANC) mitigation actions through Cisco pxGrid.	https://splunkbase.splunk.com/app/1589/ https://splunkbase.splunk.com/app/1915/
Cisco Cloudlock	The Cloudlock Cloud Access Security Broker (CASB) harnesses crowd-sourced, actionable cybersecurity intelligence to enable enterprises to securely use the cloud.	https://splunkbase.splunk.com/app/3043/ https://www.cloudlock.com/blog/tag/cloudlock-for-splunk/
Cisco eStreamer	The eStreamer log collection and comprehensive selection of dashboards is optimized for Sourcefire System 5.2+ and Splunk 6.	https://splunkbase.splunk.com/app/1629/
Cisco eStreamer eNcore	Cisco eStreamer eNcore Add-on for Splunk is an eStreamer client with a Splunk plugin that provides comprehensive event forwarding from all 6.x versions of Firepower Management Center.	https://splunkbase.splunk.com/app/3662/
Cisco Firepower eNcore App	Cisco Firepower eNcore App for Splunk provides charts, graphs, metrics and a geolocation map for all of the main Firepower eStreamer event types for users running Firepower Management Center 6.x a	https://splunkbase.splunk.com/app/3663/
Cisco Intrusion Prevention System (IPS)	The Splunk add-on for Cisco IPS allows a Splunk software administrator to consume, analyze, and report on Cisco IPS data that conforms to the Security Device Event Exchange (SDEE) standard.	https://splunkbase.splunk.com/app/1903

Cisco Technology	Description	SplunkBase URL
Cisco Cloud Web Security	This Splunk add-on allows a Splunk administrator to analyze and correlate Cisco Cloud Web Security log data through the Common Information Model in Splunk Enterprise.	https://splunkbase.splunk.com/app/2791
Cisco Email Security Appliance	This Splunk add-on allows the Splunk software administrator to use the text mail, HTTP, and authentication logs of the Cisco Email Security Appliance.	https://splunkbase.splunk.com/app/1761
Cisco AnyConnect® client	The Cisco AnyConnect Network Visibility Module (NVM) app for Splunk allows IT administrators to analyze and correlate user and endpoint behavior in Splunk Enterprise.	https://splunkbase.splunk.com/app/2992/
Cisco Adaptive Security Appliance (ASA)	This Splunk add-on allows a Splunk software administrator to map Cisco ASA devices, Cisco PIX® security devices, and Cisco Firewall Services Module (FWSM) events to the Splunk Common Information Model.	https://splunkbase.splunk.com/app/1620

For further details: Contact your local Cisco or Splunk sales representative.

About Cisco Systems.

Cisco Systems (NASDAQ: CSCO) is an industry leader in security solutions that extend from the network to the branch and cloud. By focusing on an integrated architectural approach, Cisco provides solutions that are open to automate policy enforcement, simplify the management and scalability of security solutions, and make security more effective. This holistic security approach enables Cisco to collaborate with technology

partners to deliver a complete range of integrated cybersecurity solutions. Together, we deliver the most complete security that our customers demand.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk provides the enterprise machine data fabric that drives digital transformation. More than 12,000 customers in over 110 countries use Splunk in the cloud and on-premises.