Cisco SD-WAN and Splunk

Transform your security operations with greater monitoring and visibility

Solution

Cisco has developed a Splunk app that integrates with the Cisco® SD-WAN routers to enable visualization and analysis of the security and connection-related logs generated from SD-WAN. This integration is supported starting IOS-XE 17.10.

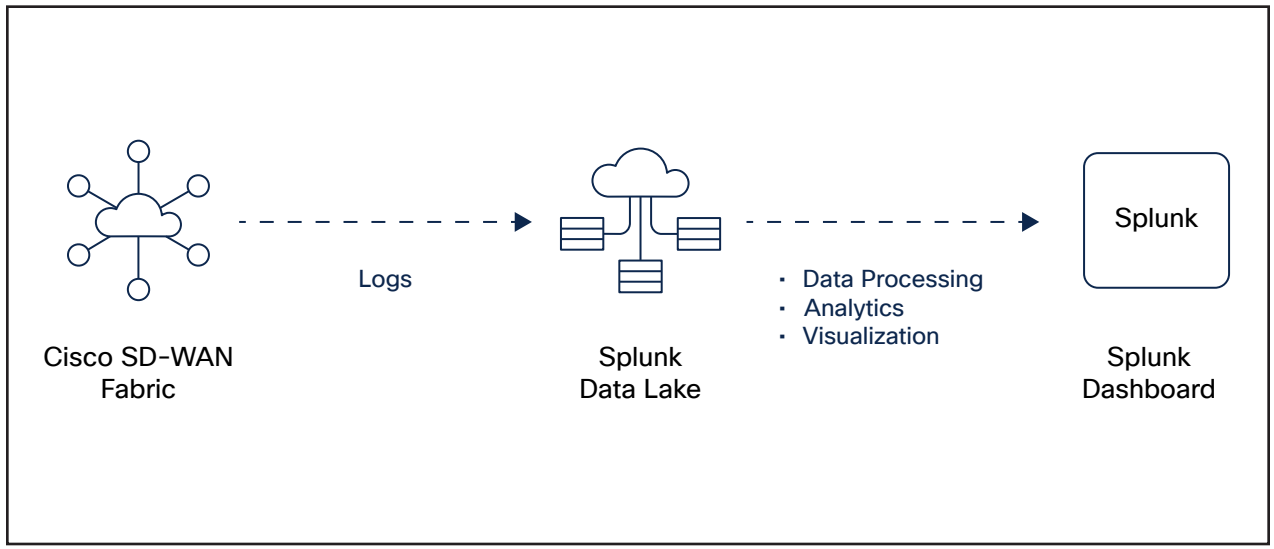

Figure 1. Cisco SD-WAN and Splunk integration for greater monitoring and visibility

The bridge to possible

Challenge

Modern enterprise networks are highly complex and unique, tailored to meet the specific needs of different markets and users. As a result, businesses often turn to multiple vendors to build a comprehensive solution. However, this approach creates challenges, particularly when it comes to monitoring and visibility. To respond quickly to security threats, it's critical for Security Operations Center (SOC) teams to have a unified console that captures and visualizes all activity across the network. Without it, businesses risk missing critical threats and leaving their network vulnerable. A streamlined monitoring and visibility solution is essential for businesses operating in today's intricate network landscape.

The bridge to possible

Benefits

- **Easy to use:** The app is available for all Cisco SD-WAN customers who have a Splunk account. Users can simply download it and start sending the SD-WAN router logs to the Splunk instance.
- **Greater monitoring and visibility:** The dashboard highlights all the information gathered by Cisco SD-WAN's security stack, providing a holistic view of all security events captured by the SD-WAN security stack. Users can easily collect actionable threat data, allowing them to respond to threats in a timely manner.
- **Historical data:** The dashboard allows customers to parse through data stored for as long as a year.
- **Efficiency:** The app automatically parses the router's security logs when they are sent to the Splunk environment and populates the data on a prebuilt security dashboard.
- **Comprehensive SOC dashboard:** The Cisco SD-WAN and Splunk collaboration enables visualization and analysis of the security and connection-related logs generated from SD-WAN, providing a common console to visualize data.

The app ingests logs from SD-WAN routers and presents actionable security analytics on a prepopulated dashboard. The actionable data presented in the dashboard allows SOC users to respond to threats promptly. The app is available for all Cisco SD-WAN customers who have a Splunk account, and users can easily download it and start sending the SD-WAN router logs to the Splunk instance. Some use cases enabled by the Splunk integration for the security operations persona are:

- A holistic view of all the security events captured by the SD-WAN security stack.
- The ability to examine any security event at the device level along with traffic patterns occurring when the security event was triggered.

The Cisco SD-WAN Splunk integration consists of two components:

Cisco SD-WAN Add-on for Splunk: Add-ons are used for data optimization and collection processes. The Cisco SD-WAN Add-on for Splunk collects a range of Cisco log data and NetFlow data and stores them in Splunk indexes.

Cisco SD-WAN Splunk Application: Using data from the add-on, the Cisco SD-WAN Application presents dashboards for Cisco logs and NetFlow data with detailed visualization, analysis, and representation.

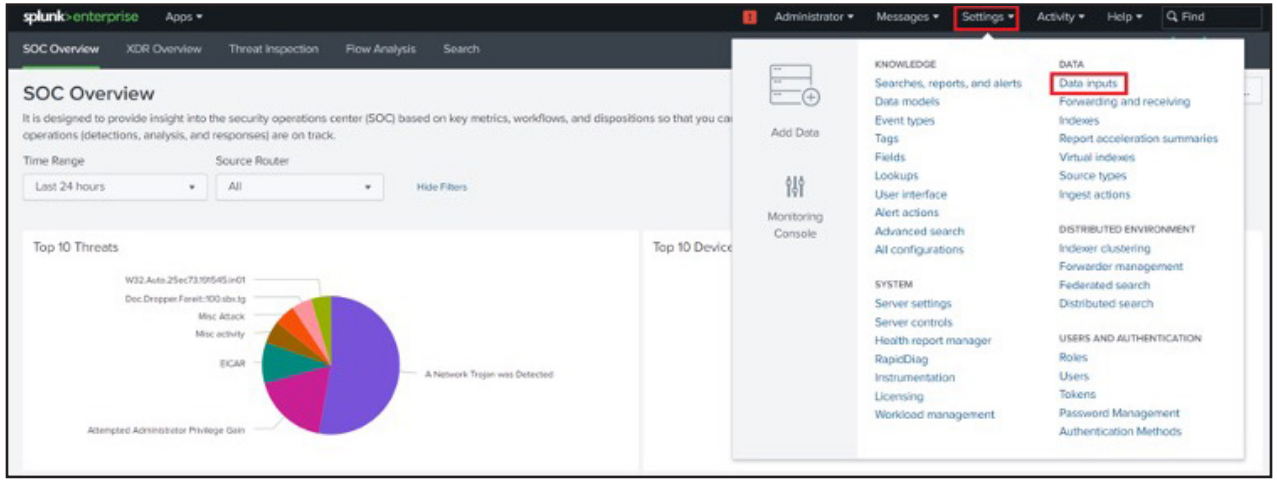

Figure 2. Cisco SD-WAN Splunk Application provides SecOps with increased visibility into threats

The bridge to possible

"At Cisco, we recognize the operational challenges IT leaders face in today's hybrid work and multicloud environment. Our collaboration with Splunk provides businesses with additional choice to monitor and secure their networks, delivering peace of mind and increased efficiency."

JP Shukla
Director, Product Management, Cisco

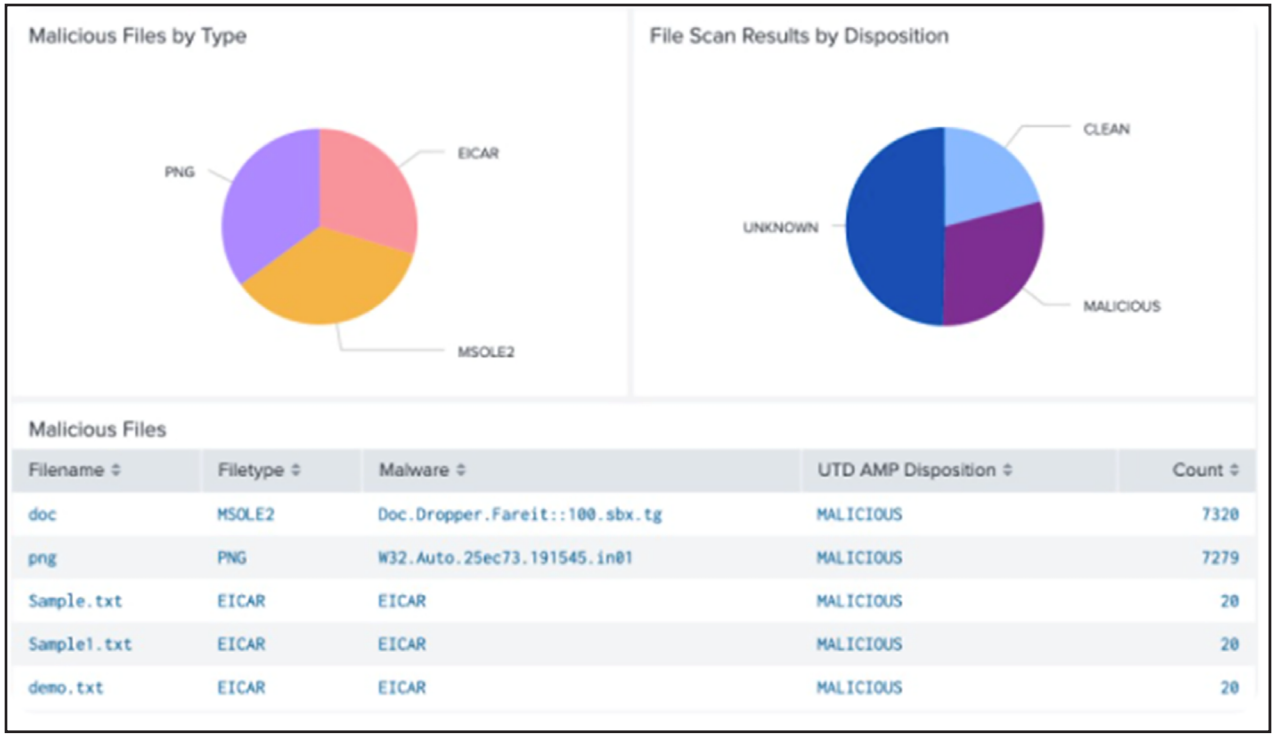

Figure 3. The Cisco SD-WAN Splunk Application provides detailed threat visibility

How it works

The Cisco SD-WAN and Splunk integration can be achieved in a few simple steps.

1. Download and install the Cisco SD-WAN Splunk Application and the Cisco SD-WAN Add-on for Splunk from the Splunk marketplace (Splunkbase), using your existing Splunk license.

[Cisco SD-WAN Splunk Application]

[Cisco SD-WAN Add-on for Splunk]

The bridge to possible

Try it now

Ready to improve your network visibility and security? Take the first step and try the Cisco SD-WAN and Splunk integration today. Download the app and app add-on from Splunkbase and follow the simple steps to get started. Need help or have questions? Contact us for a free consultation and discover how this integration can help your enterprise. **SDWAN@cisco.com**

Figure 4. Cisco SD-WAN Application on Splunkbase

2. In the app settings, add the Cisco SD-WAN IP and port number as a log source for forwarding.

3. In Cisco SD-WAN vManage, add the Splunk app IP as a log destination for forwarding.

About Splunk

Splunk is a Security Information and Event Management (SIEM) provider. The Splunk platform removes barriers between data and action, empowering observability, IT, and security teams to help ensure that their organizations are secure, resilient, and innovative.

About Cisco

Cisco is the worldwide leader in technology that powers the internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future.

C22-3607223-00 05/23