# Cisco Security Cloud App Overview

## Cisco Security Cloud App Overview

Cisco Security Cloud App is a web application that offers a centralized platform to integrate Cisco security products with Splunk.

### Cisco Security Cloud App Benefits

The app offers these benefits:

- A unified interface to integrate Cisco security products into Splunk.
- Built-in health checks and dashboards to monitor data ingestion and resource usage.
- Guided input configuration and validation workflows.
- Simplified upgrade and maintenance processes.
- Centralized access to dashboards, data integrity checks, and metrics across Cisco products.

### List of Integrated Cisco Security Products Supported by Cisco Security Cloud App

The app supports a variety of Cisco security products, allowing ingestion and visualization of data from products such as:

- Cisco Duo
- Cisco Secure Firewall (Syslog, eStreamer, API)
- Cisco Secure Malware Analytics
- Cisco Secure Endpoint
- Cisco Secure Network Analytics
- Cisco XDR
- Cisco Multicloud Defense
- Cisco Email Threat Defense

- Cisco Vulnerability Intelligence
- Cisco AI Defense
- Cisco Secure Client NVM
- Cisco Isovalent Runtime Security
- Cisco Identity Intelligence

These integrations provide predefined input templates to streamline the configuration.

### Architecture and Data Flow

The app supports deployment on single-instance and distributed Splunk environments. Based on your deployment scale and the volume of incoming data, you can run the app on a standalone search head or distribute it across a Splunk search head cluster.

Cisco security products send events to Splunk through APIs or syslog. The app collects these events using modular inputs, each sending data to a specific index. The built-in health checks ensure inputs work properly, and dashboards display the data for detection, correlation, and investigation.

### System Requirements

Check that your Splunk Enterprise version is supported before installing or upgrading the app. Refer to the Splunkbase listing for specific version support details. View the Splunkbase listing to see which Splunk versions are supported.

Supported environments include:

- Operating Systems - Windows, macOS, and Linux.
- Supported browsers - Chrome, Microsoft Edge, and Mozilla Firefox.

Use a recent browser version and enable JavaScript for the best performance.

### API Compatibility Matrix

Refer to the API Compatibility Matrix for detailed support information, which includes product versions and endpoint coverage.