Chrome Enterprise Recommended

splunk>

# Manage Extended Security Insights from Chrome Browser and ChromeOS in Splunk

## Empower IT teams to take action against Chrome Browser and ChromeOS security detection events.

The way we work has drastically changed. With more companies adopting remote and hybrid work models, 65% of organizations have seen a measurable increase in attempted cyberattacks, which is particularly problematic since 78% say remote workers are harder to secure*. IT teams need to do everything they can to ensure their business data and employees are protected while balancing the needs for productivity, no matter where the workers are.

*Splunk State of Security Report, 2022

With security being a top priority, Chrome has partnered with Splunk on new integrations to collect, analyze, and extract insights from security events. With the Google Chrome App for Splunk and Google ChromeOS App for Splunk, users have access to prebuilt dashboards and analytics to help them investigate, automate, and respond to the most critical incidents of risky extension installs, malware transfer and unsafe site visits. Visit the Google Chrome App for Splunk getting started guide to learn more.

# Added Browser Security with Chrome and Splunk

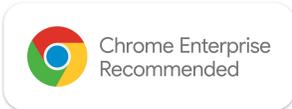## Detect and mitigate attacks, vulnerabilities and high-risk user behaviors.

Using Chrome Browser Cloud Management, you can now add Splunk as a Chrome Reporting connector to send these events to Splunk HTTP Event Connector. The Google Admin console and APIs allow administrators to configure which events are sent to Splunk Cloud (or Splunk Core) through custom filtering. With the extended security insights you get from Chrome browser in Splunk, your IT or security team can make better informed decisions.

## Get visibility on these risky events within managed browsers:

Malware downloads

Content transfer*

Unsafe site visit

Password reuse

Password change

Extension Installs

Unscanned content transfer*

Sensitive data transfer*

* Available to BeyondCorp Enterprise customers

→ Learn more about Splunk

Chrome Enterprise
Recommended

splunk>®

# Getting Started with the Google ChromeOS App for Splunk

## Investigate and respond to security-related events from ChromeOS endpoints

With employees spending more time interacting with ChromeOS endpoints, the chances of risky behavior impacting enterprise resiliency increases. Fortunately, the Google Chrome Add-on and Google ChromeOS App for Splunk are able to help address these risks by:

- Sending Chrome Threat and Data Protection events into Splunk and mapping them to the Splunk Common Information Model (CIM) to allow for easy correlation with other data sources and maximum efficiency at search time.

- Providing pre-built dashboards and analytics to help investigate the most critical incidents of suspicious logins, device and session/endpoint activities.

## Get visibility on these risky events within ChromeOS:

Multiple failed login attempts on a device

USB peripherals added to an endpoint

Unaffiliated or unauthorized users added to a device or system

Multiple Chrome Remote Desktop sessions on a device

Logins from a guest or unaffiliated user

Multiple screenshot attempts

→ Learn more about Splunk