Chrome Enterprise Recommended

splunk>

Get Extended Security Insights in Chrome browser with Splunk

Provide IT teams the increased visibility they need within browser to make better-informed security decisions.

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.

With security being a top priority, Chrome has partnered with Splunk on a new integration to collect, analyze, and extract insights from security events through the Chrome Enterprise Connector Framework. The events can include password changes, unapproved password reuse, sensitive data exfiltration, unsafe site visits, and malware transfer events within managed Chrome browsers.

*Splunk State of Security Report, 2022

Added 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 Enterprise) 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 transfer
Content transfer
Unsafe site visit
Password reuse
Password change
Unscanned content transfer*
Sensitive data transfer*

*Available to BeyondCorp Enterprise customers

Learn more about Splunk