

Joint solution

Streamline investigations with native Splunk integration



Splunk is a recognized leader in helping security teams make sense of massive amounts of data collected from across their environments. Unfortunately, however, one data set that is often missing is the rich network telemetry that can provide crucial insights into operational and adversarial activities occurring within the network. Without it, users have limited visibility into what is happening across the environment, which severely handicaps their threat detection and response capabilities.

Corelight overcomes this challenge with rich network evidence that can greatly improve detection coverage and accuracy to accelerate incident response, while amplifying your investment in Splunk automation. With native Common Information Model (CIM) support, Corelight data integrates seamlessly into Splunk Enterprise and Splunk Enterprise Security (ES) environments by automatically populating fields in common Splunk data models, such as Network Traffic, Network Resolutions (DNS), Network Sessions, Certificates, Web, and Email. The result is much faster and effective detection and response.

How much time can this native integration save? One mutual Splunk and Corelight customer described it as “like Google for your network” and saw a 95% reduction in average incident response time. Read the case study [here](#).

INTEGRATION HIGHLIGHTS

Seamless ingestion of data with native Common Information Model (CIM) support

Out-of-the-box support for Splunk ES correlation searches

Simplified data filtering for faster investigations

Quick time to value with linked data and Corelight analytics

The Corelight App for Splunk accelerates deployment for new Splunk users

Advanced network evidence for Splunk

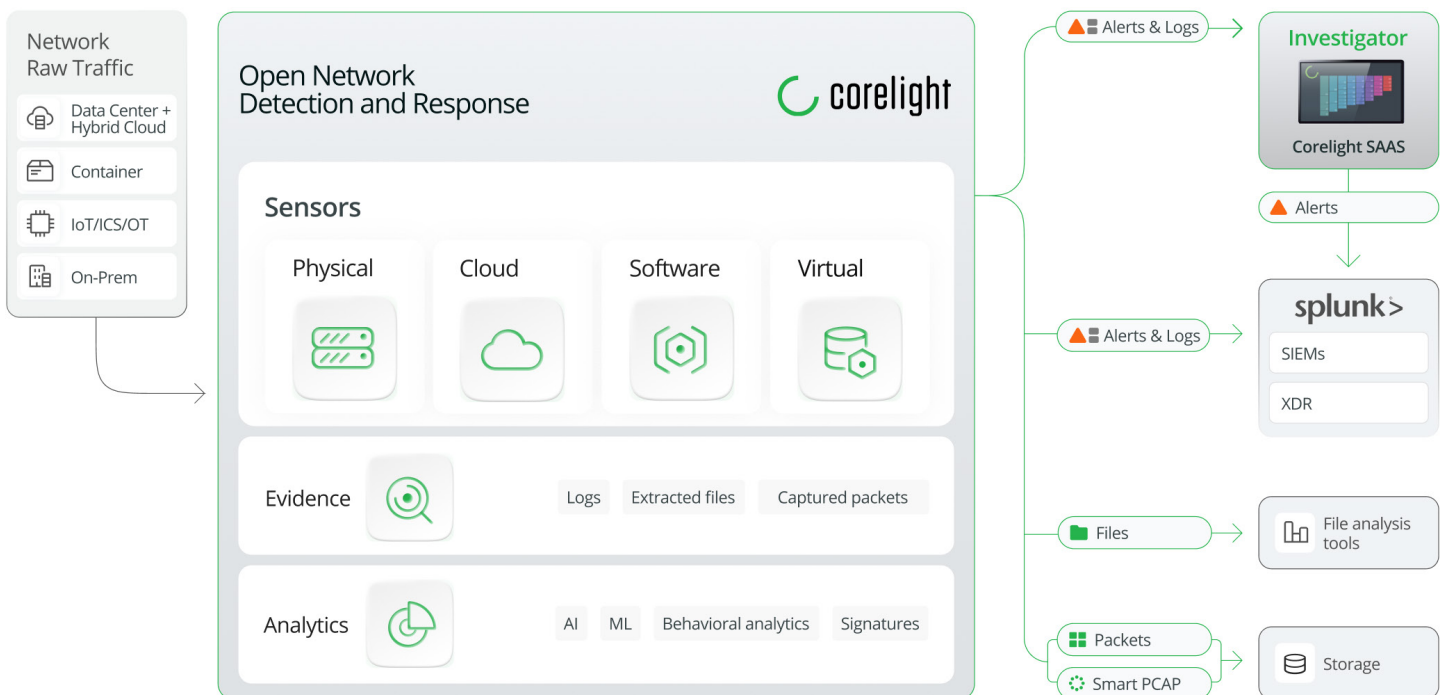
By generating detailed, correlated log data, alerts, and analytics through passive network monitoring, Corelight gives Splunk analysts a complete and contextual view of all the activity across the enterprise. This elevated visibility across on-premise, cloud, and multi-cloud environments greatly accelerates threat investigations and reduces the stress of over-extended Security Operations Center (SOC) teams.

Joint solution

For organizations interested in forwarding only network alerts, the Corelight Investigator SaaS offering can ensure that only critical events are sent to Splunk. So whether forwarding just alerts from Investigator or alerts and rich, correlated evidence, Corelight data is available to help optimize the value of your Splunk environment. Moreover, Corelight data is there to power [Splunk SOAR playbooks](#), allowing SOC teams to automate tasks and keep them focused on high-value activities.

Accelerate time to value with the Corelight App for Splunk

The Corelight App for Splunk brings clarity and guidance on where to focus by providing insights from real-time network telemetry that helps analysts quickly and easily determine the most interesting threats across the environment. By providing intuitive dashboards and insights, as well as direct links to relevant details on the most pressing threats, the App enables security teams to streamline investigations, accelerate response times, and boost analyst productivity.



To learn more about the Splunk integration, request a demo at

<https://corelight.com/contact>

info@corelight.com | 888-547-9497