

# Get to the truth faster with Corelight + Splunk.®

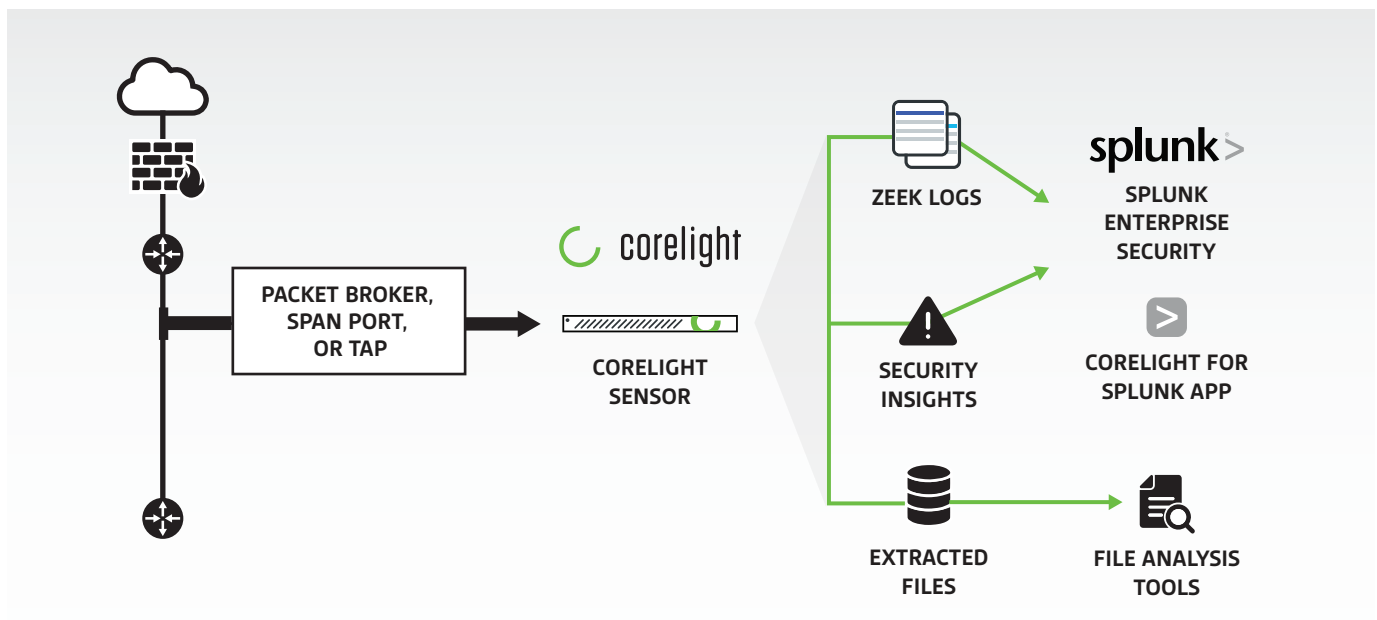
Security professionals can't do their jobs without quickly making sense of threats and the context around them. Corelight's comprehensive network data pairs with Splunk to dramatically improve incident response and threat hunting capabilities. Nearly all attacks must cross the network, but the default sources of network data (like Netflow records) lack critical details, leaving teams in the dark. Corelight, powered by open-source Zeek (formerly Bro), details network activity across 50+ logs, extracted files and insights to preserve this key source of truth.

Corelight's Splunk app and deep integration with the Splunk Enterprise Security SIEM delivers an essential part of the modern security stack. Corelight automatically streams rich network data to Splunk, and combined with the Corelight App for Splunk, provides security teams faster, deeper, and more actionable insights.

How much faster? One Splunk/Corelight customer described the integrated solution as "like Google for your network" and saw a 95% reduction in average incident response. Read more here: <http://www3.corelight.com/Education-First-Use-Case>

**Superior network data from Corelight helps incident responders and threat hunters using Splunk Enterprise Security work faster and more effectively.**

## The Corelight / Splunk solution



Corelight Sensors use the Splunk Universal Forwarder, ensuring seamless data ingestion in Splunk. The joint solution gives organizations rapid, precise answers to critical security questions.



# Zeek: The gold standard for network security data.

Corelight solutions are built on Zeek, the powerful and widely-used open source network analysis tool. Thousands of the world's most critical organizations use Zeek to generate actionable, real-time data for their high-performance security teams.



**Zeek** extracts over 400 fields of data in real time directly from network traffic. It covers dozens of data types and protocols from Layer 3 to 7 about TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. The Zeek logs are structured, and interconnected specifically to support threat hunting and incident resolution.

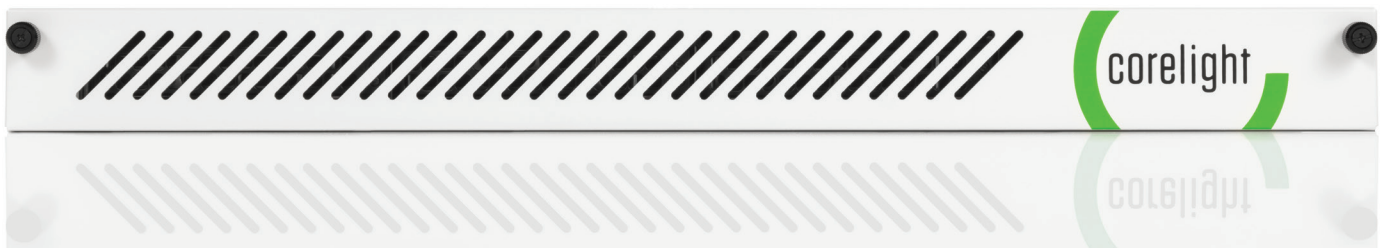
**Corelight Sensors**—available in physical, cloud and virtual formats —take the pain out of deploying open-source Zeek. They combine the integrations and capabilities large organizations need with high-end, out-of-band hardware and a specialized version of the open-source Zeek for excellent performance.

Corelight Sensor capabilities include:

- Up to 25 Gbps+ of monitored traffic
- Hardware, cloud or virtual appliance models
- A web-based sensor management GUI
- Fleet Manager to manage up to 250 Corelight Sensors
- Pre-installed collections of Zeek packages
- A comprehensive API
- On-box performance and health monitoring
- Dynamic file extraction
- Flexible export options, including popular data formats, filtering, and forking
- Shunting to handle elephant flows over 25 Gbps (AP 3000 only)
- Support from the creators and builders of Zeek

## Zeek parses 50+ logs.

- |  |  |
|--|--|
|  conn       |  radius       |
|  dce rpc    |  rdp          |
|  dhcp       |  rfb          |
|  dnp3       |  sip          |
|  dns        |  smb files    |
|  dpd        |  smb mapping  |
|  files      |  smtp         |
|  ftp        |  snmp         |
|  http      |  socks       |
|  intel    |  software   |
|  irc      |  ssh        |
|  kerberos |  ssl        |
|  mail     |  syslog     |
|  modbus   |  traceroute |
|  mysql    |  tunnel     |
|  notice   |  weird      |
|  ntlm     |  x509       |
|  pe       |  |





Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future. With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers.



Corelight delivers the most powerful network security monitoring (NSM) solutions that help large organizations defend themselves by transforming network traffic into rich logs, extracted files, and security insights. Corelight makes a family of virtual, cloud and physical sensors that take the pain out of deploying open-source Zeek and make it faster and enterprise-ready. Corelight's customers include Fortune 500 companies, government agencies, and research universities. For more information please visit [www.corelight.com](http://www.corelight.com)

## Contact us

**For more information or  
to schedule an evaluation:**

**[info@corelight.com](mailto:info@corelight.com)**

**888-547-9497**

**510-281-0760**

**[corelight.com](http://corelight.com)**