

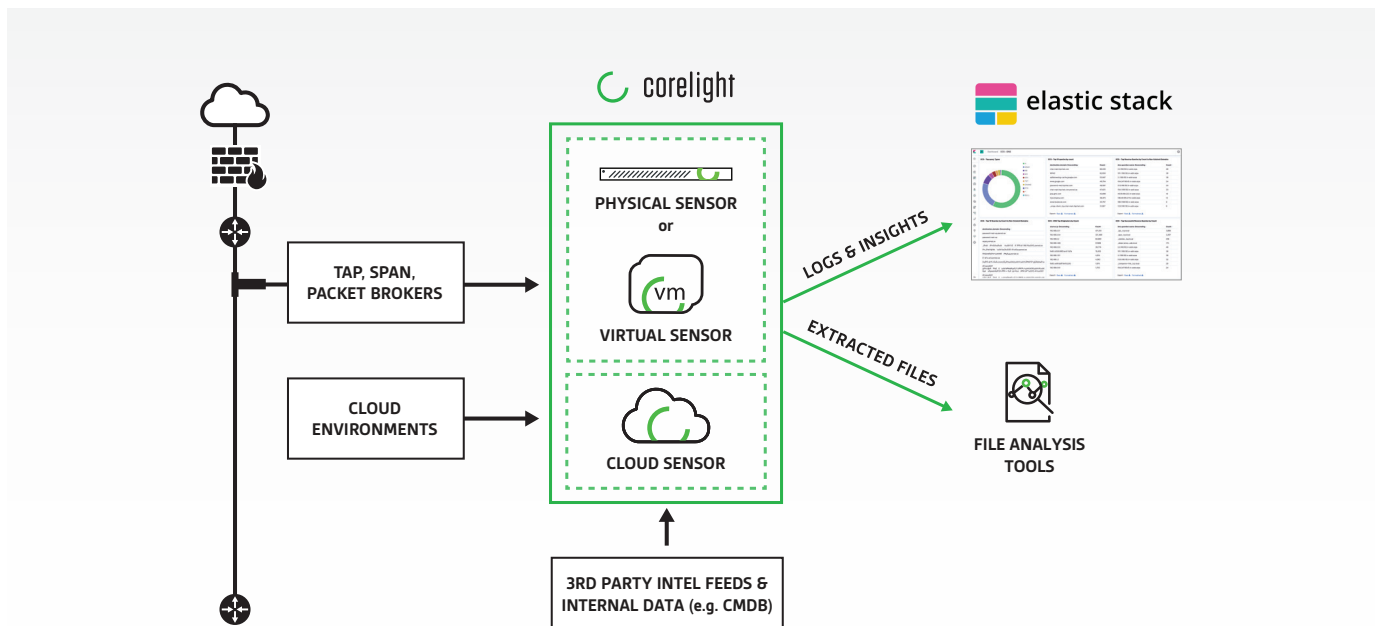
Get to the network truth faster with Corelight + Elastic

Security professionals can't do their jobs without quickly making sense of threats and the context around them. Many choose the Elastic Stack (previously known as the ELK Stack) as the preferred environment for threat detection and response.

Corelight's comprehensive network data in the Elastic Stack dramatically accelerates incident response and unlocks new threat hunting capabilities. Nearly all attacks must cross the network, but default sources of network data (like Netflow or DNS records) lack critical security context, often leaving analysts in the dark. Corelight, powered by open-source Zeek (formerly Bro), details network activity across dozens of protocols, reassembles and extracts hundreds of file types and enables custom security insights to preserve this key source of truth.

Superior network data from Corelight helps incident responders and threat hunters using the Elastic Stack work faster and more effectively.

Corelight's integration with the Elastic Stack:



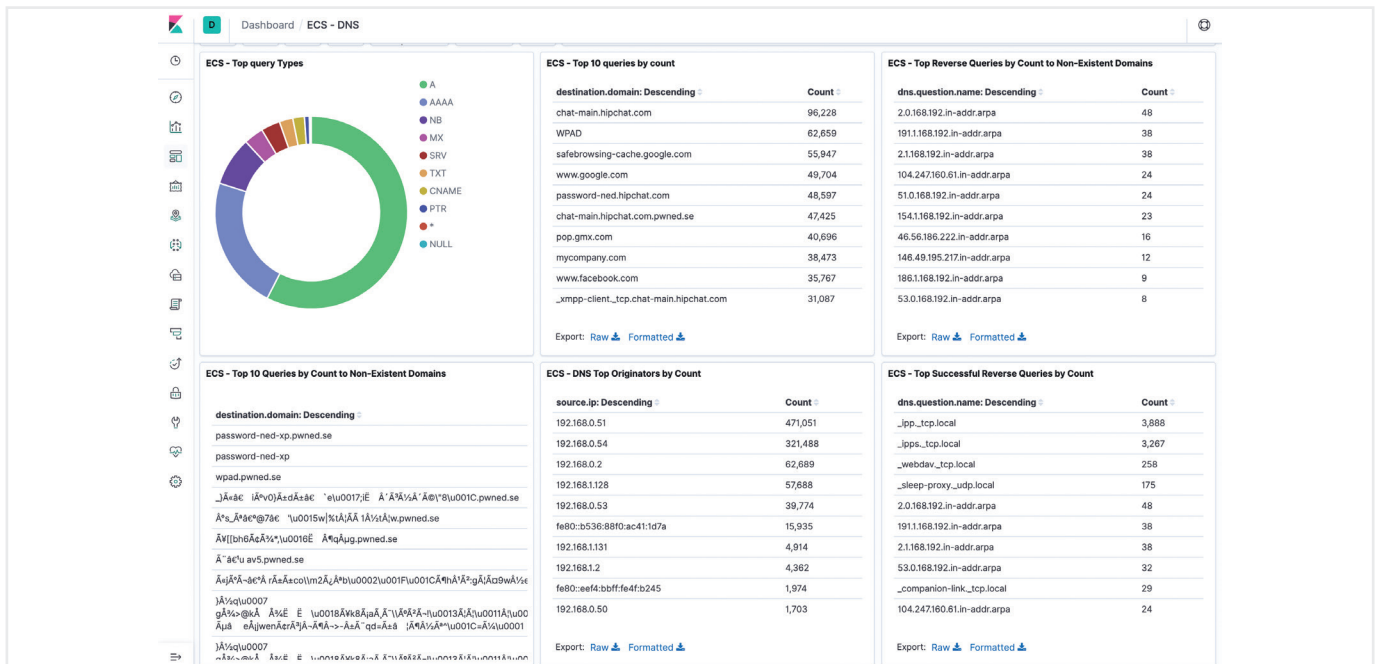
This powerful integration pairs deep network traffic analysis and logging from Corelight with Elastic's distributed search, analytics, and visualization capabilities.

Close network visibility gaps and accelerate incident response

Corelight automatically streams rich network data to Elastic Security, providing security teams faster, deeper, and more actionable insights that can reduce incident response time by up to 20x. This data serves as a centralized source of truth to investigate and rapidly respond to security incidents, replacing Netflow and augmenting low level server logs spread across different business units outside the security team. Support for the Community ID standard further accelerates incident response by enabling analysts to quickly pivot within the Elastic SIEM from a third-party data source like a Suricata alert into the associated Corelight data. Support of the Elastic Common Schema (ECS) format facilitates the unified analysis of data from Corelight and other diverse sources so that content such as dashboards and machine learning jobs can be applied more broadly, searches can be crafted more efficiently, and field names can be recalled by analysts more easily.

Find advanced network threats

Corelight has developed a set of ECS-compliant Kibana dashboards to provide a launch point for threat hunters and incident responders using Elastic Security. The dashboards provide answers to important questions, such as: What are the top DNS queries to non-existing domains? Are there any self-signed certificates on our network? Have user generated keystrokes been used in any SSH sessions? These answers unlock new hunting capabilities that can identify potential command and control attacks with integrated machine learning.



Corelight passively captures comprehensive information about DNS queries and responses (along with information about dozens of other protocols, applications, and data) without DNS server logging or involvement by server sysadmins.

Zeek: The gold standard for network security.

Corelight runs on Zeek, the powerful, open-source network analysis tool that has become a global standard. Thousands of the world's most critical organizations use Zeek to generate actionable, real-time data to help defend their networks.




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, including TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. Zeek logs are structured and interconnected to support threat hunters and incident responders. Elastic users have the flexibility of choosing to collect all or a portion of this data in Elasticsearch and take action on it using Elastic Security.

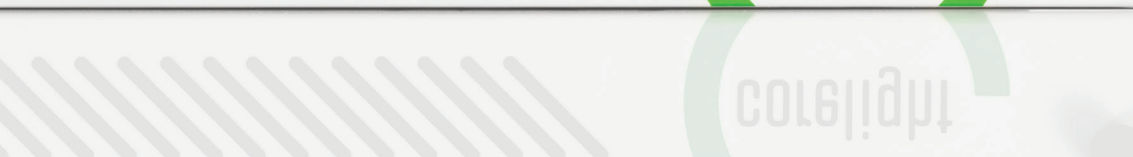
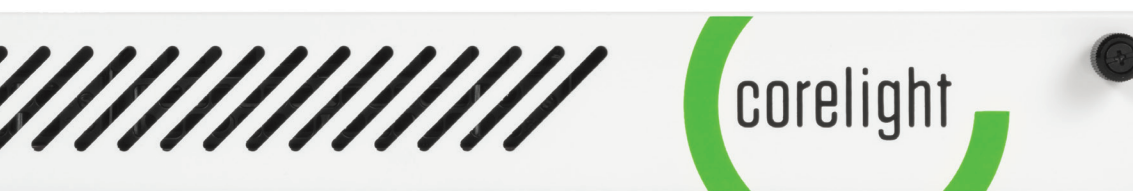
Corelight Sensors—available in physical, cloud and virtual formats—vastly simplify the challenges deploying open-source Zeek. They offer excellent performance, combine the capabilities large organizations need with high-end, out-of-band hardware and a specialized version of the open-source Zeek network security monitor.

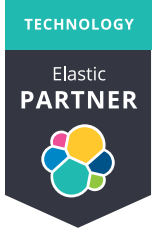
Corelight Sensor capabilities include:

- Up to 25 Gbps+ of monitored traffic per sensor
- 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 generates 50+ network 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 | |





Elastic is a search company. As the creators of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds self-managed and SaaS offerings that make data usable in real time and at scale for search, logging, security, and analytics use cases. Since its founding in 2012, there have been more than 350 million cumulative downloads of Elastic software. Elastic is a distributed company with more than 1,000 Elasticians in 30 countries. Learn more at elastic.co.



Corelight delivers powerful network traffic analysis (NTA) solutions that help organizations defend themselves more effectively by transforming network traffic into rich logs, extracted files, and security insights. Corelight Sensors are built on Zeek (formerly called "Bro"), the open-source NTA framework that generates actionable, real-time data for thousands of security teams worldwide. Zeek has become the 'gold standard' for incident response, threat hunting, and forensics in large enterprises and government agencies worldwide. Corelight makes a family of physical, cloud and virtual network sensors that take the pain out of deploying open-source Zeek and expand its performance and capabilities. Corelight is based in San Francisco, California and its global customers include numerous Fortune 500 companies, large government agencies, and major research universities. For more information, visit corelight.com.

For more information:

info@corelight.com

888-547-9497

510-281-0760

corelight.com

 **[@corelight_inc](https://twitter.com/corelight_inc)**