Subscription Overview

Subscribers get regular, feature-rich updates, sensor health and performance monitoring, and dedicated customer support from world-class Zeek experts.

Subscription Overview

A Corelight subscription delivers monitored, supported, and continually-updated software that transforms traffic into rich logs, extracted files and custom insights. Built on a proprietary, enterprise-grade version of open-source Zeek, Corelight Sensors deploy in under 15 minutes, offer 10x peak performance capabilities, and run in cloud, virtual, and physical environments. Corelight subscription benefits include:

SOFTWARE UPDATES

- Multiple, feature-rich software updates delivered each year
- New, actionable content focused on detection & data enrichment
- Automatic sensor updates with offline support available

SUPPORT

- Secure cloud monitoring of sensor performance and health
- Hardware and software support, with remote access for direct fixes
- Technical support delivered by industry-leading Zeek experts

CUSTOMER SUCCESS

- A Corelight subscription provides customers with access to a Technical Account Manager (TAM) who serves as their strategic partner
- Technical guidance on package development, data tuning and more
- Dynamic Health Check alerts Corelight for proactive support

Software Updates

Connectivity to the Corelight Cloud Service (CCS) enables sensor content and configuration management via hourly database check-ins so Corelight can enhance sensors with new inputs like MaxMind GeoIP database updates and new Zeek packages. Included in every subscription, Corelight also delivers a number of major software releases each year that substantially expand product capabilities via new detection content, protocol parsers, data enrichment features, and more. Customers with

Subscription Overview

CCS-connected sensors enjoy automatic upgrades and Corelight can also support air-gapped networks with offline sensor updates. New features shipped in recent Corelight software releases include:

- SSH client brute force detection
- SSH client keystroke detection
- SSL certificate monitoring
- Lateral movement detection
- Community ID support
- Log fork and filter support

Support

A Corelight subscription includes a standard support package with an array of services including technical support, software upgrades, and access to online resources. Technical support is available via phone and email with a next business day response guarantee. For customers with mission-critical environments that require round-the-clock support, Corelight offers an enterprise support tier with 24 x 7 availability and 1 hour response SLA for P1 issues. Both support tiers offer CCS-connectivity for proactive monitoring and hardware replacement, and enterprise support customers also receive advanced replacement hardware if critical issues like disk failures are detected. Customers can also view detailed sensor health and performance metrics in Corelight's cloud management console or via their SIEM, providing visibility into areas such as:

- Hardware telemetry, such as disk status, operating temperatures, and power supply status
- Aggregate statistics around monitored traffic, including data volume and packet drops
- Installed Zeek packages, Zeek log names, and installed licenses
- And more...

Lastly, CCS-connectivity allows Corelight to directly fix problems for customers and not just talk them through issues via a screen share. With customer permission, Corelight's support team can remotely log into sensors for troubleshooting to remediate issues. Remote access is disabled by default and Corelight alerts customers when remote management is initiated and uses a new instance in the CCS for every remote session to prevent data leakage or contamination across customers.

Customer Success

A Corelight subscription also provides customers with access to a Technical Account Manager (TAM) during their onboarding and early deployment. Corelight TAMs provide customers with technical guidance around sensor implementation and configuration and on advanced use cases such as custom package development or tuning for a specific environment. A key feature of the CCS is the (optional) Dynamic Health Check Service that automatically alerts Corelight TAM and support teams if sensor health or performance anomalies are detected. This allows proactive customer outreach on issues such as:

- Export anomalies that can indicate SIEM data ingestion problems
- Internal component failures, like hard drives
- Highlighting potential capacity problems

Together, Corelight's TAMs and support team represent an industry-leading group of Zeek experts and talent with an impeccable track record of supporting the world's largest and most sophisticated organizations.

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497