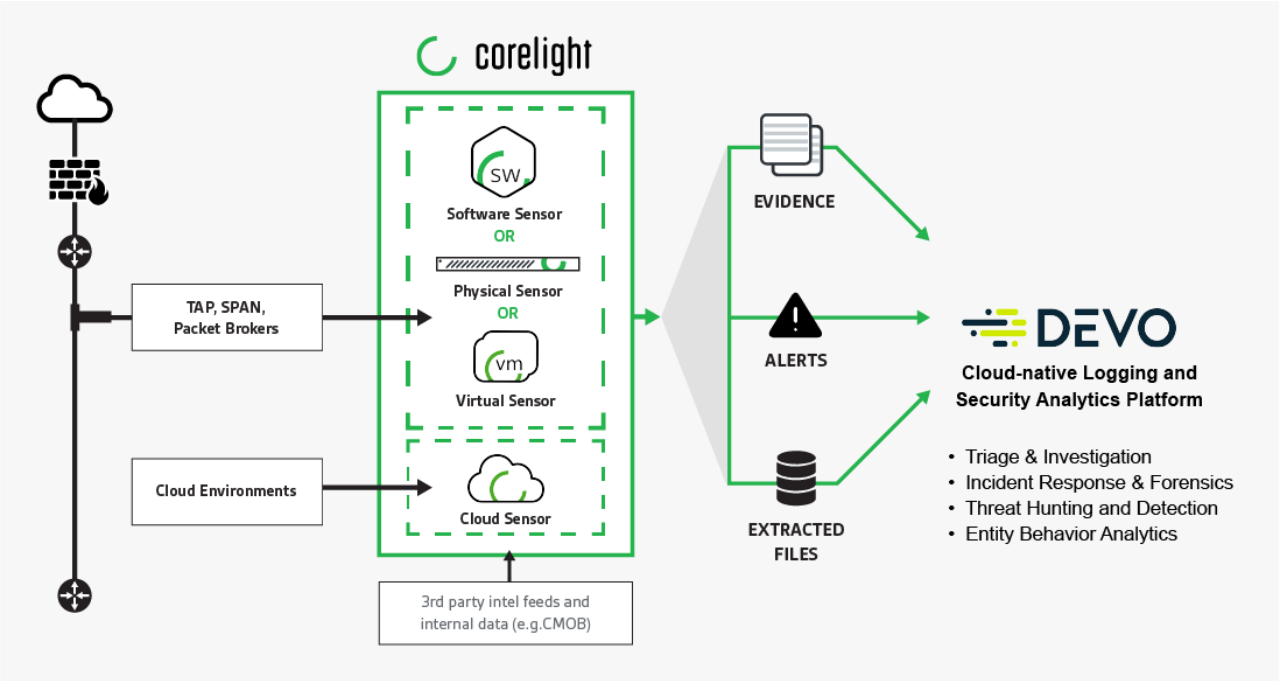
Joint Solution

Close the visibility, detection, and response gap with Corelight + Devo

Legacy SIEM and log management solutions are failing to meet the needs of security operations centers (SOCs) thanks to a rapidly expanding attack surface and adversaries who go from initial access to lateral movement in minutes. SOC teams are flooded with too many false positives, broken workflows, and speed, scale and performance issues that hinder effectiveness.

The Corelight / Devo solution:



This powerful integration pairs Network Detection and response from Corelight with the Devo Platform, a cloud-native logging and analytics platform. Devo provides unrivaled scale to collect all your data without compromise, speed to give you immediate access and answers, and clarity to focus on signals that matter.

Skilled analysts, who are in short supply, are burdened with determining what's important to investigate, analyzing large volumes of data, and piecing together the workflow from detection to response. This leads to analyst burnout, missed threats, and greater risk to businesses.

Transform today's SOC

Corelight and Devo integration benefits:

- Investigate potential threats uncovered using Zeek data with pre-packaged visual analytics and using the Devo no-code query capability for faster mitigation of threats.
- High-fidelity alerts generated from Corelight logs are automatically enriched to include entity context and threat intelligence to reduce MTTR.
- Hunt across all Corelight data and join it with other key security data sources to gain a complete understanding of IOCs.
- Analyze files (e.g. pcap, binaries) using the integrated DFIR toolkit and include findings directly within the investigation enabling investigators to centralize deeper evidence in one location.
- Ability to truly have real-time network visibility

The Devo Platform is built on a no-compromise, cloud-native multi-tenant architecture. This enables enterprises to overcome the compromise of legacy security solutions to:

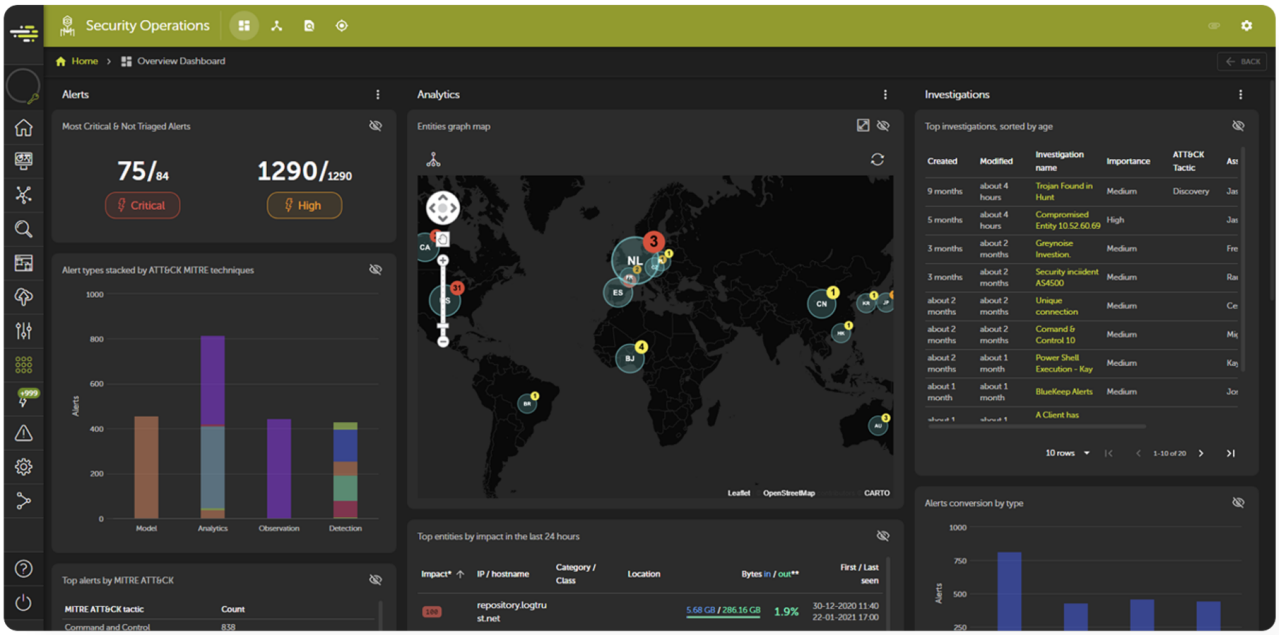
- Ingest all their data by scaling from GBs to TBs to PBs of data per day with no rearchitecting required
- Search and retain all data—data is kept always hot and for retained for 400 days by default
- Analyze and visualize the full breadth of data in real time without needing to learn a cumbersome query language
- Spend less time on solution data management and more time realizing impactful analytics

Devo Security Operations

Devo Security Operations, an application available for subscribers to the Devo Platform, empowers security teams to protect their organizations by closing the visibility gap, defending against advanced cyber-threats with quick detection and investigation, and enabling analysts to be more effective and punch above their weight. This improves operations in the SOC through:

- Triage and investigation: Analyze all real-time and historical data and improve response speed
- Incident response and forensics: Quickly prioritize and investigate with automatically enriched alerts
- Threat hunting and detection: Increase detection capabilities by hunting across 100% of data
- Entity behavior analytics: Automate and enhance insights with machine learning

Devo serves as the central hub for all data and processes within the SOC and leverages powerful data analytics, automation, and a practitioner mindset to start analysts on context-rich investigations and close the gap between detection and response which can help reduce analyst burnout.



Devo Security Operations allows analysts to easily pivot from alert triage and investigation to threat hunting in an intuitive way.

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.

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.

Joint Solution: Corelight and Devo

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

To learn more about the Devo and Corelight integration, please visit either the Devo Market **www.devo.com/partners/corelight** or the Corelight website **corelight.com**

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Headquartered in Cambridge, Mass., Devo is backed by Insight Partners, Georgian, and Bessemer Venture Partners. Learn more at www.devo.com.

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