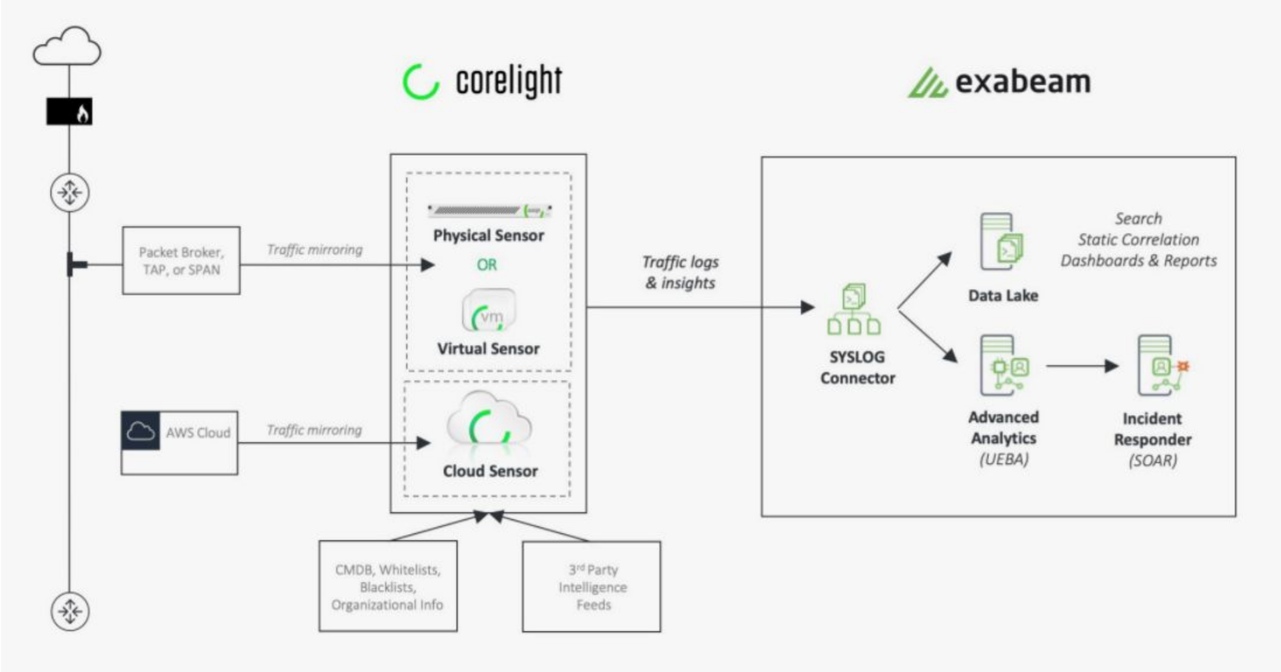
exabeam corelight

Joint Solution

Transform traffic into actionable security Insights

Since nearly all attacks must cross the network, it’s an essential source of truth, yet common logs like Netflow or DNS records provide scant detail and often leave security operators in the dark, unable to see critical events. Full packet capture, while comprehensive, is cost-prohibitive to store at scale and ultimately slow to search. Packets don’t let you move at the speed of attack. Corelight, however, transforms raw traffic into rich, protocol-organized logs that comprehensively summarize network events at less than 1% the size of full traffic capture.

The Corelight / Exabeam solution:



Corelight has partnered with Exabeam, the Smarter SIEMTM company, to combine Corelight's proven network security monitoring (NSM) capabilities with Exabeam's advanced user and entity behavior analytics (UEBA) and automated incident response capabilities. This integrated solution streams Corelight's rich logs directly to Exabeam so security teams can obtain faster, more actionable network insights, and use the rich data as a building block for advanced security analyses via the Exabeam platform.

The joint solution pairs deep network traffic analysis from Corelight with powerful log management and security analytics from Exabeam, allowing organizations to get rapid, precise answers to critical security questions about their environment. Exabeam ingests logs and insights from Corelight via TSV or JSON over TCP and combines them with existing log data, third party tools, and contextual data from identity and authentication tools to establish a baseline of normal behavior for all assets in an organization — including communication patterns, ports and protocols used, and operating activity.

Corelight

Corelight Sensors operate out-of-band, run in physical, virtual, and cloud environments, and leverage the power of the open-source Zeek network security monitor to transform raw traffic into rich logs, extracted files, and custom security insights. Corelight extracts over 400 fields of data from network traffic, which comprise 50+ network log types covering 35+ protocols. Corelight's logs are interlinked with unique connection IDs, timestamps, and file hashes that allow security analysts to effortlessly pivot across protocol activity and make fast sense of traffic so they can move at the speed of attack. Security teams can ingest Corelight's logs and network insights directly into their Exabeam platform via a few simple export configurations in the Corelight Management Console.

Corelight Sensors offers powerful capabilities beyond open-source Zeek, including:

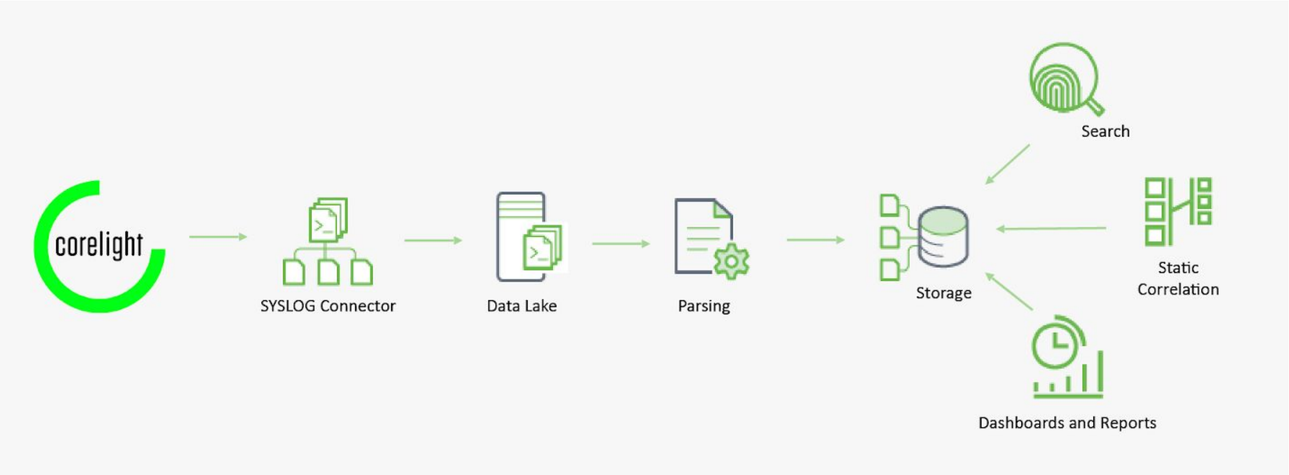
- 5-10x peak performance, with up to 25 Gbps of monitored traffic per sensor
- Simplified 15 minute deployments
- Rich management capabilities via a web-based management console
- Comprehensive API
- Detailed sensor performance and health monitoring
- Flexible support options, including data formats, filtering and forking
- Support for the creators and builders of Zeek

Corelight Sensors provide a complete history of what happened on your network, but with storage costs that are just a small fraction of the equivalent cost of storing full packets in a form factor that's dramatically fast to search and analyze. The comprehensive nature of Zeek logs enables faster incident response times and unlocks more powerful threat hunting and analytics capabilities through richer, more complete network evidence.

Exabeam

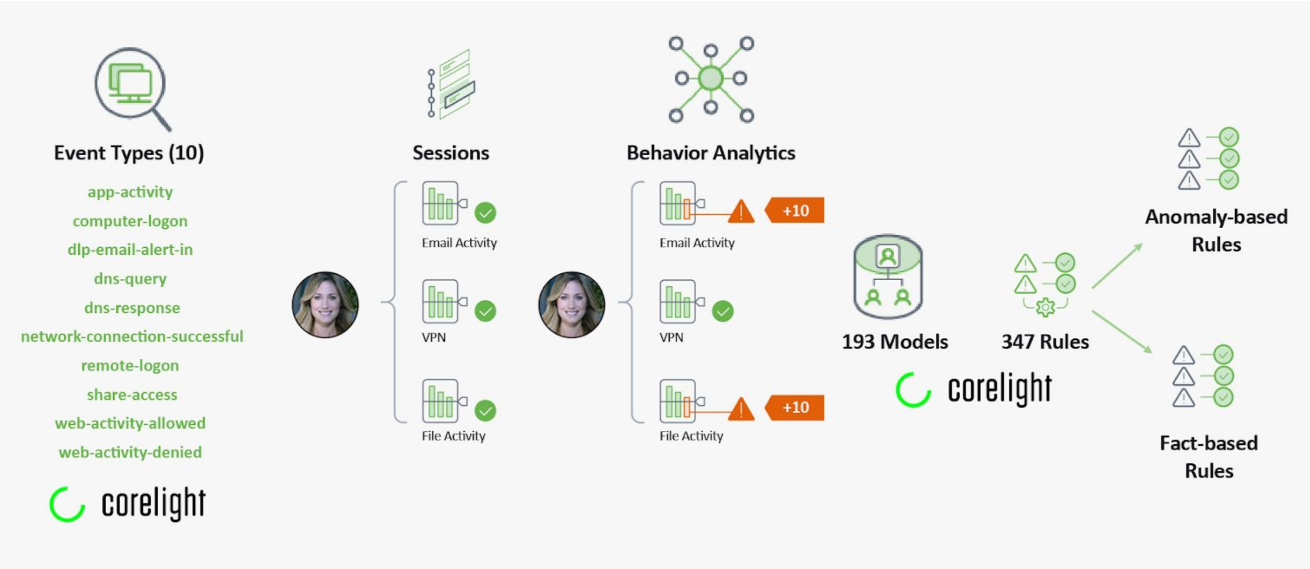
Exabeam data lake

Data lake provides an unlimited security data lake—at a flat, predictable price—with contextual log parsing to help your team quickly find the information they need, without combing through a sea of raw logs. The enhanced log view highlights the security relevant information of specific log types such as user and source IPs from VPN logs to easily view security risks instead of combing through raw logs. Guided search assists analysts by auto completing their search requests.



Advanced analytics

Advanced Analytics baselines normal behavior for all users and entities in an environment, then automatically detects the behaviors indicative of a threat. It fully integrates with Exabeam Threat Intelligence Services (TIS) to provide real-time actionable intelligence into potential threats in your environment by uncovering indicators of compromise (IOC) and malicious hosts.



Incident responder

Security teams responding to an incident can use hundreds of tools, resulting in an inefficient "swivel-chair" response. Incident Responder provides centralized security orchestration and automated response (SOAR) that amplifies SOC team productivity.The Incident Responder prebuilt APIs connect and integrate all your systems, IT, and security tools, whether it's email servers, active directory (AD), or your firewall, for a rapid automatic response using response playbooks.

exabeam

Exabeam is the Smarter SIEMTM company. We empower enterprises to detect, investigate and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com.

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