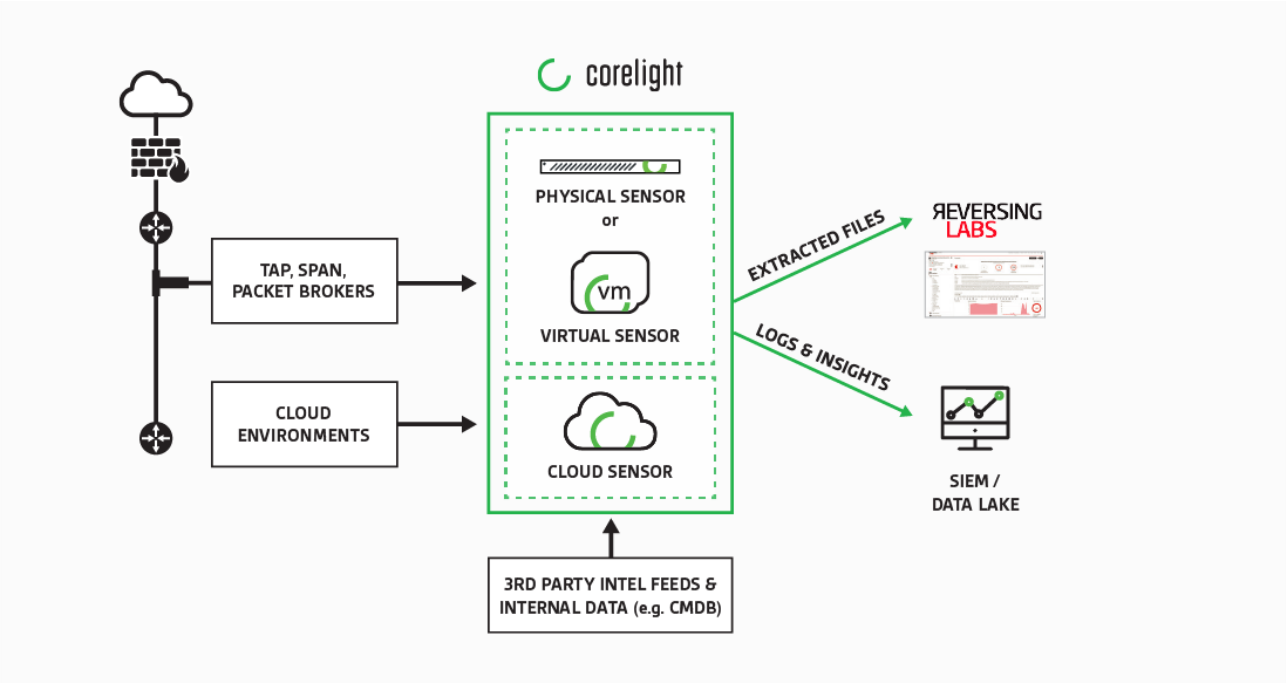
Joint Solution

Flush out malware on the network with Corelight + ReversingLabs

File-based malware can range from broad-based attacks to highly-customized, targeted payloads. Whatever their form, nearly all of these attacks must cross the network. That makes network traffic analysis an excellent tool for catching malicious files early and containing their impact. The difficulty lies in rapidly extracting and reassembling files as they cross the network, and analyzing them at scale.

With Corelight and ReversingLabs, you can overcome these challenges with automated file inspection that combines high-throughput file extraction with a hyper-scaled analysis platform. That means you can reduce risk through fast, reliable malware detection and file-based insights.

The Corelight/ReversingLabs solution:



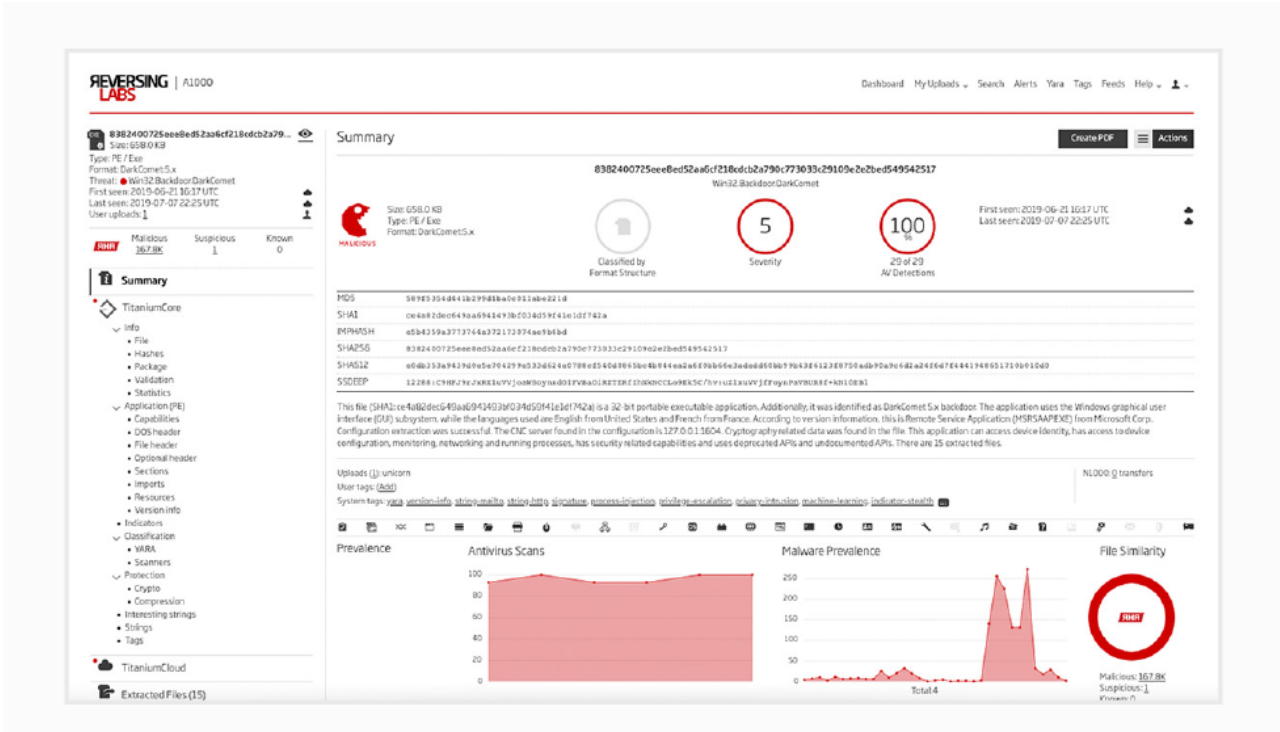
Joint Solution: Corelight and ReversingLabs

Corelight Sensors deploy out-of-band in under 15 minutes, turning raw packets into extracted files that can be streamed to ReversingLabs' powerful file analysis platform, providing quick and accurate insights into more than 4,000 file formats.

High-performance file extraction

Corelight Sensors transform raw packets into powerful evidence with open-source Zeek. Backed by decades of development and a massive, global community, Zeek empowers organizations to quickly understand traffic and defend themselves. In addition to connection-oriented logs and custom-scripted insights, Zeek can also extract hundreds of different file types directly from traffic. Corelight Sensors dramatically improve this capability, achieving extraction rates of over 10,000 files/minute in the real world through performance improvements over open-source Zeek like file deduplication. Corelight also allows customers to filter out specific file types from downstream analysis, a feature open-source Zeek lacks.

Corelight generates logs that contain 400+ fields, across 50+ log types covering dozens of protocols and data. Every file crossing the network generates a "files.log" with 25 fields of security-relevant detail such as file name, MIME type, size, and hashes. Since Corelight logs are interlinked via a unique connection ID, analysts can easily trace the origins and movement of malicious files on the network. In their SIEM, they can quickly track files across ports and protocols by pivoting from ReversingLabs insights to Corelight logs.



Enterprise-scale file analysis

ReversingLabs offers a file analysis platform that includes a massively scalable decomposition/classification design, automated static analysis engine, a file reputation service, and an

investigation web interface for incident response and threat hunting. The platform's hybrid cloud model integrates with EDR, Email, SIEM, TIP, and sandboxes. ReversingLabs delivers actionable intelligence directly to security analysts on object and malware identification and classification through their SIEM/SOAR environment.

With a repository of 10 billion files and support for 4,000 formats, ReversingLabs delivers the fastest, most accurate malware insights in the industry. The platform generates 3,000+ threat indicators for every sample and assigns five levels of classification. In addition to its expansive repository, ReversingLabs also provides customers with historical detection results across 40+ AV vendors. Customers can classify files with an advanced rules engine that supports up to 250 YARA rules per ruleset for retro-hunting.

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 about 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.

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

Through its Titanium Platform, ReversingLabs delivers automated static analysis and file reputation services that represent the fastest and most accurate insights in the industry, finding the hidden objects that are armed to destroy enterprise business value. We maintain the largest repository of malware and goodware in the industry of more than 8 billion files and objects, and are the only vendor to speed analysis of files in milliseconds. ReversingLabs seamlessly integrates at scale across the enterprise with connectors that integrate with existing security investments, reducing incident response time for SOC analysts, while providing high priority and detailed threat information for hunters to take quick action. Learn more at https://www.reversinglabs.com, or connect on LinkedIn or Twitter.

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