corelight

Why Corelight is your **best next move** in enterprise security.

Despite spending billions annually[1] on security infrastructure and services, even the most sophisticated enterprises continue to be breached, attacked, and compromised. In this high-stakes and high-risk environment, the question for most CISOs and security architects trying to stay ahead of attackers is, "What's my best next move?"

In an intensifying threat environment, assume the bad guys will get in.

It's apparent to anyone in the field that cybersecurity problems are getting worse—not better. Despite the thousands of vendors, products, and services available, CISOs and security architects continue to struggle to secure their networks. In an environment where attackers improve their techniques faster than enterprises can adapt, perimeter-based security strategies—while still essential—have proven to be less than foolproof.

Essentially all large organizations have found themselves compromised at one point. And often attacks go undetected for months or even years. In the well-publicized breach of Marriott, the attackers first gained access in 2014 but weren't detected until September 2018. In the intervening period, the data of 500 million guests became compromised.[2] There's no doubt Marriott (like most global companies) has likely spent millions on cybersecurity and operated a capable security operations team. Yet they were **still** vulnerable. This is why so many companies now operate under the assumption that breaches will happen, and so they are shifting their focus to timely detection to identify adversaries as quickly as possible. As Brian Krebs wrote in December 2018, *"The companies run by leaders and corporate board members with advanced security maturity are investing in ways to attract and retain more cybersecurity talent, and arranging those defenders in a posture that assumes the bad guys will get in."*[3]

Visibility is your best next move.

Assuming Krebs is correct (and attackers will get in), gaining complete visibility of your network traffic becomes essential. This is where deploying Corelight Sensors is the **best next move** you can you make if you're not currently using Zeek (formerly known as Bro) in your security stack. Here's why:

Network Security Monitoring with Zeek gives you near-complete visibility into network activity.

1 Gartner forecasts for information security products will be $124 billion in 2019 https://gtnr.it/2QhjS4T
2 https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html
3 https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/

Corelight Sensors running Zeek are the *single most comprehensive* next step you can take to get a fuller picture of attacks, whether they're in progress right now or occurred in the past.

It's likely every person, place, and thing in your organization touches your network, making it the best place to look for signs of adverse activity. Network Security Monitoring (NSM) with Zeek gives you near-complete visibility into network activity by extracting hundreds of pieces of security-relevant data from live network traffic 24/7, then connecting and organizing them into Zeek logs.

More than just a broad and deep set of data, the logs Zeek produces synchronize automatically to the microsecond and tie together by key fields. This allows incident responders and threat hunters to quickly follow the trail of attacks across protocols, users, data types, and sources. The data Zeek extracts comes from almost 60 different data types and protocols, covering the most important areas where attackers are likely to leave clues behind: email (and attachments), web traffic, DNS queries and responses, Windows® files & shares, DHCP, SSL, TCP connections, and many others from layers 3 to 7.

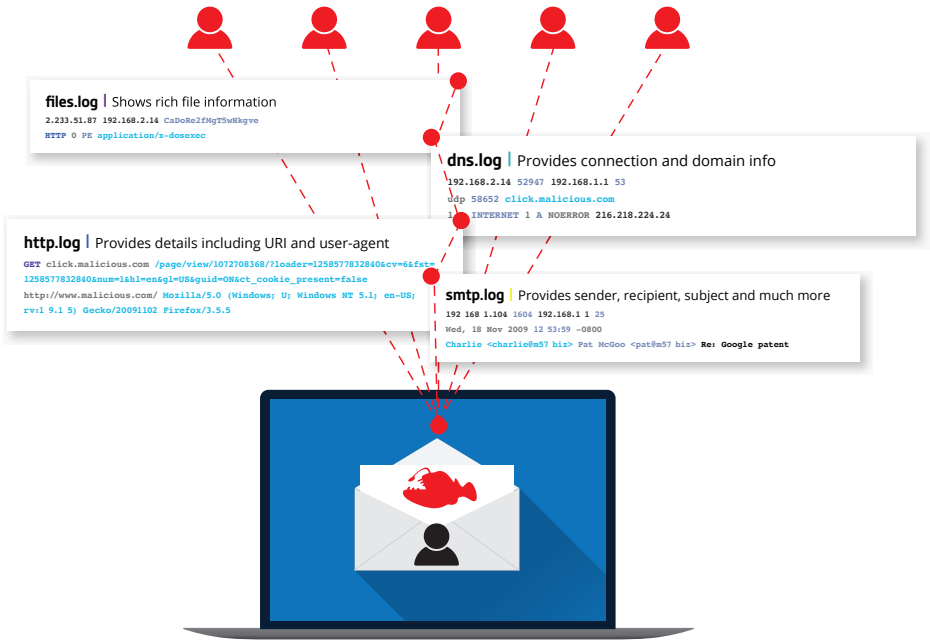
Corelight Sensors running Zeek also extract files directly out of network traffic (with the option to use MIME type filtering for example, to limit the number of files extracted), and send them to storage systems for later forensic analysis.

NSM isn't the only thing you should do—and Zeek won't single-handedly protect your organization—but deploying Corelight Sensors at strategic locations (such as the border of your organization's network) can give you almost complete visibility into traffic. Remember, *network security isn't just about your network, it's about **everything.***

Deploying Corelight Sensors is the fastest and smartest thing you can do today.

In real world terms, Corelight Sensors take about 15-25 minutes to set up and deploy, even in large enterprise networks. This is lightning-fast compared to deploying just about any other enterprise-wide security solution.

If you're familiar with open-source Zeek, the benefits of Corelight Sensors will be even more appealing. Corelight Sensors take Zeek and package it into a turnkey product that's available as a physical appliance (with 2, 10 or



An analyst can follow a phishing attempt starting with the SMTP log, pivot to HTTP or SSL logs, DNS log, FIles log, and so on to find its sources and measure the impact of the attack.

Corelight Sensors: appliance, vm, and cloud versions.

25 Gbps+ ingest capacity), virtual appliance, or cloud-deployable vm. Even sophisticated Zeek experts will have trouble building a custom Zeek sensor with more than 4 or 5 Gbps of capacity, and even then high packet loss can be a problem.

Corelight's engineering team (the same people who built Zeek over the last 20 years) spent years developing a hardened OS, selecting the right hardware, and locking down the open-source software to ensure performance under load and with custom scripts. You can try to do it yourself using the open-source software, but expect to invest months or years in the project. Many sophisticated users spend a year or two building Zeek NSM infrastructure that meets their needs.

Corelight Sensors also include tools that provide a better experience and improved threat hunting capabilities. The Core Collection is a bundle of 10 detection scripts packaged with the Sensor. Created by Corelight and third-party experts, these packages have been tested and validated by Corelight for performance. Sensors also include a modern web-based GUI, Fleet Management for multi-sensor networks, a pre-built comprehensive API, and built-in integration with Splunk, Kafka, Amazon, and others.

The least disruptive security solution provides a range of benefits.

Unlike most enterprise deployments, Corelight Sensors are non-disruptive. No one will notice—except your security team, with powerful new data at their fingertips. Corelight Sensors are:

Deployed out-of-band: Sensors typically operate by accepting a copy of network traffic from a packet broker, but can also be fed via a span port or optical tap, if preferred. Regardless, they're not intercepting primary network traffic, but inspecting a complete copy.

Stealthy: Since Corelight Sensors are out-of-band, attackers have no way of knowing they're present and therefore can't evade them. An intruder only has to make one mistake to blow their cover. Richard Bejtlich wrote about it a decade ago *"The Defender's Dilemma vs Intruder's Dilemma"* in 2009 [4] on his blog, TaoSecurity.

Comprehensive: Typical deployments are made at logical choke points in the network topology. With a single Corelight deployment, security teams gain a comprehensive view of their organization. Compared to asking permission from various operational teams in your organization (network, web applications, DNS, email, file systems, storage, etc.) to deploy agents or turn on logging, etc., it's simple. Even internal teams might not know Corelight Sensors are deployed unless you tell them (or help them resolve a breach!).

Lightweight and more efficient: Zeek logs are a fraction of total network traffic (typically 0.5% to 1%, sometimes as little as 0.1%), making the time window available for retrospective analysis massively larger (because you can store 100 to 1,000 times as much data in the same storage system you're already using, compared to PCAP).

Providers of structured, relevant data: Because Corelight Sensors produce automatically correlated and structured logs out of one appliance (or a fleet if you have multiple sensors), all logs can be easily ingested into your analytics stack removing the organizational and logistical hassles of setting up logging systems. Zeek logs also provide the most relevant data quickly and in an easily understandable format.

Compatible with your existing stack: Lastly, your SOC can keep using their current security analytics stack, whether it's Splunk, Elastic, ArcSight, Databricks, QRadar, or a similar solution. Corelight Sensors are engineered to provide data and detections that improve these SIEMs.

4 https://taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html

Make your best next move.

Cyber security threats will continue to advance and multiply, requiring companies to keep pace by deploying a wide arsenal of solutions and spending millions to protect themselves. Most large organizations have deployed endpoint security solutions, but as breaches to these systems show, this is not enough. Companies are asking, *"What's next?"*

Adding network-wide visibility is the necessary **best next move** to protect your organization. NSM with Corelight Sensors based on Zeek give a comprehensive picture of who's doing what in your organization—a solution that's quick to deploy, is among the least disruptive, economical, and hard to beat for effectiveness. When combined with the high-value data Zeek extracts from network traffic, Corelight is the next move to consider in the battle against cybersecurity adversaries. For more information, visit corelight.com.

To have someone contact you right away, just fill out the form at https://corelight.com/contact and we'll be happy to help you.

Core Collection

Detection packages:

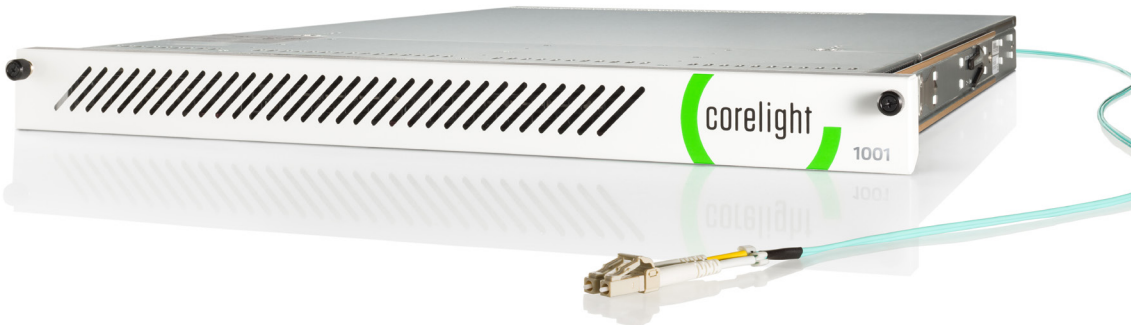
- Cryptomining detection
- SSL fingerprinting
- HTTP stalling detection
- Long connections detection
- Port scanning detection

Data enrichment packages:

- URL extraction in SMTP
- POST data capture in HTTP
- DNS hostname annotation

Operational packages:

- SSL certificate monitoring
- Traffic shunting



Contact us

For more information or to schedule an evaluation:

info@corelight.com

888-547-9497

510-281-0760

corelight.com

We make the **world's networks safer.**