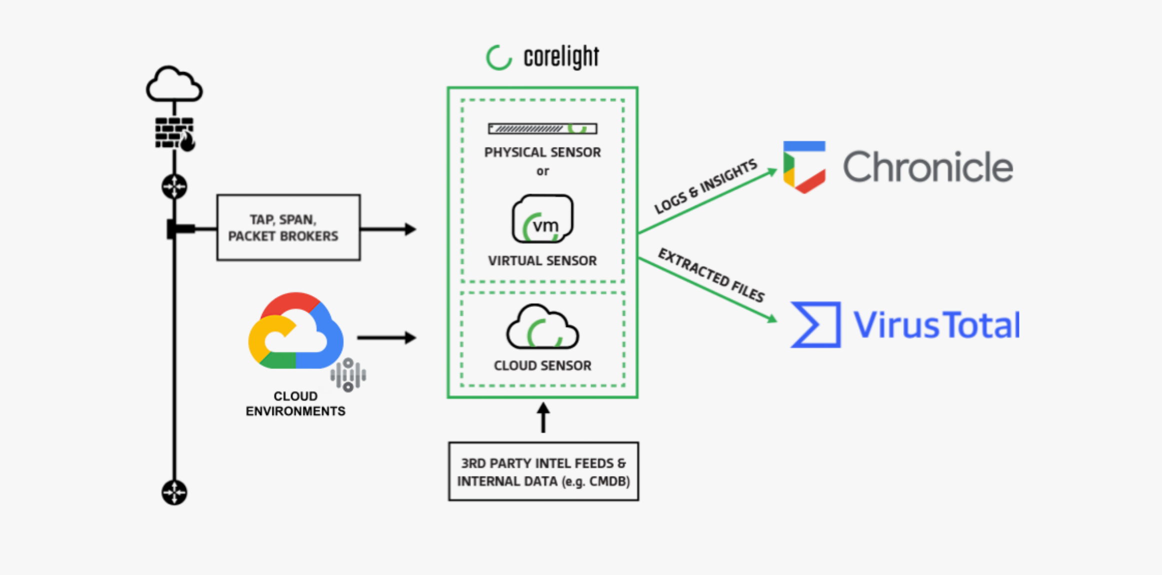
Joint Solution

Overpower network threats instantly with Google Cloud Security + Corelight

Superior network data from Corelight helps incident responders and threat hunters using Chronicle work faster and more effectively.

Imagine if your SIEM had the power and scale of Google, and the same network security evidence as the world's most advanced blue teams. You could detect attacks, hunt for threats, and investigate incidents with incredible power and speed. But there's no need to imagine it. You can get it today from Corelight and Google Cloud Security.

The Google Cloud Security and Corelight solution:



Corelight's evidence is a powerful pairing with Chronicle's capabilities. Corelight Sensors deploy as a physical appliance or as a Google Cloud VM image instance which ingests traffic directly via Google Cloud's Packet Mirroring service or from 3rd party packet-forwarding agents

Chronicle, now part of Google Cloud Security, is a global security telemetry platform for detection, investigation and threat hunting within an enterprise network. Chronicle brings unmatched speed and scalability to analyzing massive amounts of security telemetry. Built for a world that thinks in petabytes, Chronicle can support security analytics against the largest customer networks with ease.

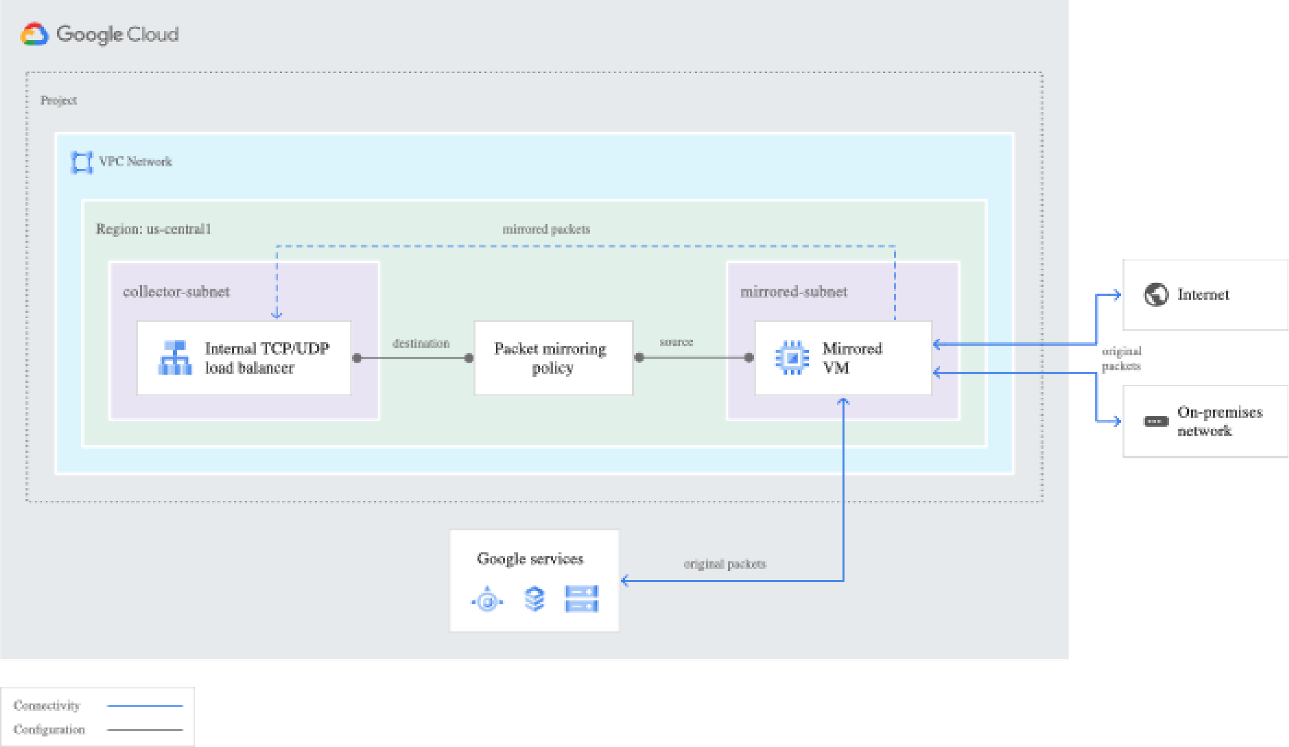
Corelight provides your security team with the world's best network evidence so they can understand network activity over time. That means they can close investigations quickly, even when incidents go back years, and find adversaries before they achieve their objectives — creating a durable, unfair advantage over attackers. Your SOC can benefit tremendously by adding Corelight's comprehensive, interlinked, lightweight evidence to Chronicle.

Corelight, powered by the open source Zeek, gives you exceptional visibility with logs, extracted files, and custom insights in Chronicle including network connection data, DNS queries and responses, HTTP transactions, as well as file hashes for every file seen on the network. Corelight's high-throughput, de-duplicated file extraction capabilities also prepare files for upload into VirusTotal.

Google Cloud users can also use Google Cloud's Packet Mirroring service, a virtual tap that copies the network traffic and streams it to Corelight for processing. It's a native Google Cloud service, and can be enabled on Google Cloud machines, with no additional CPU consumption , for non-sampled traffic across all payloads, which allows for complete visibility.

Unprecedented visibility into cloud networks

Security and network engineering teams need evidence. To capture it, it's important to mirror all of your traffic for comprehensive inspection of network flows. Because attacks can span multiple packets, security teams need visibility into all packets for each flow. Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination, including all traffic and packet data - including payloads and headers - not just the traffic between sampling periods.



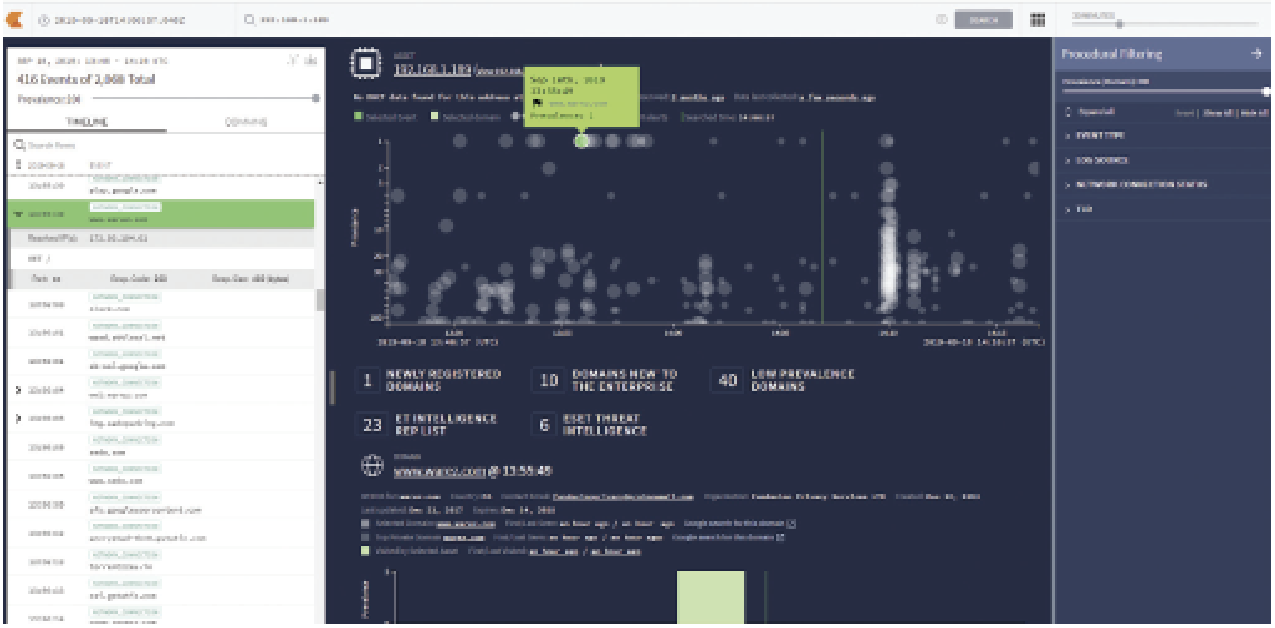
Comprehensive network insight in Google Cloud

The creators of Zeek designed the Corelight Cloud Sensor to transform Google Cloud traffic into rich logs, extracted files, and custom insights that accelerate incident response and unlock new threat hunting capabilities. The Corelight Cloud Sensor provides visibility into Google Cloud to monitor scalable cloud applications, dynamic workloads, and more. Corelight's best-in-class Zeek platform in a Google Cloud format includes:

- Enterprise support, maintenance, and software updates
- Built-in Zeek packages for detection, monitoring, and data enrichment
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Kafka, Syslog, JSON, REDIS, and SFTP
- High performance, efficient file extraction
- Comprehensive REST API for configuration and monitoring
- World-class support from the Zeek experts

Unparalleled detection and analysis

Corelight, a Google Cloud Security partner, helps detect modern threats by delivering security data to a private cloud within the Chronicle platform. That data is then automatically correlated with intelligence from global sources like VirusTotal and endpoint activity to find both known and late-breaking threats.


416 Events of 2,888 Total
TIMELINE
192.168.1.189
Procedural Filtering
1 NEWLY REGISTERED DOMAINS
10 DOMAINS NEW TO THE ENTERPRISE
40 LOW PREVALENCE DOMAINS
23 ET INTELLIGENCE REP LIST
6 ESET THREAT INTELLIGENCE
www.wanzz.com @ 13:55:49

Rich network telemetry from Corelight enables easy identification of outliers in Chronicle.

Hunt for threats and resolve incidents faster

Corelight collects hard-to-obtain network telemetry data (such as DNS response queries missing from server logs) and sends it to Chronicle, which offers a real-time graphical interface to increase analyst productivity. The solution streamlines threat analysis by stitching together data from multiple sources (e.g., a POST from a HTTP log and a user from a DHCP log.)

High value for MSSPs

Corelight and Chronicle together deliver significant value for managed security service providers (MSSPs) and other managed solution providers. Out of the box, you'll gain visibility across your customer environments including network data from Corelight as well as endpoint, system and application logs from other sources. This solution provides insights into abnormal traffic, encrypted insights, and network-based TTPs in the ATT&CK framework. Network telemetry can be sent to the managed Chronicle instance as well as the customer's on-premise SIEM with optional fork and forward capability.

Google Cloud Security

Chronicle, part of Google Cloud Security, is a security analytics platform that enables enterprise security teams to detect, investigate and hunt threats at the speed of search. Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate. Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.

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