corelight

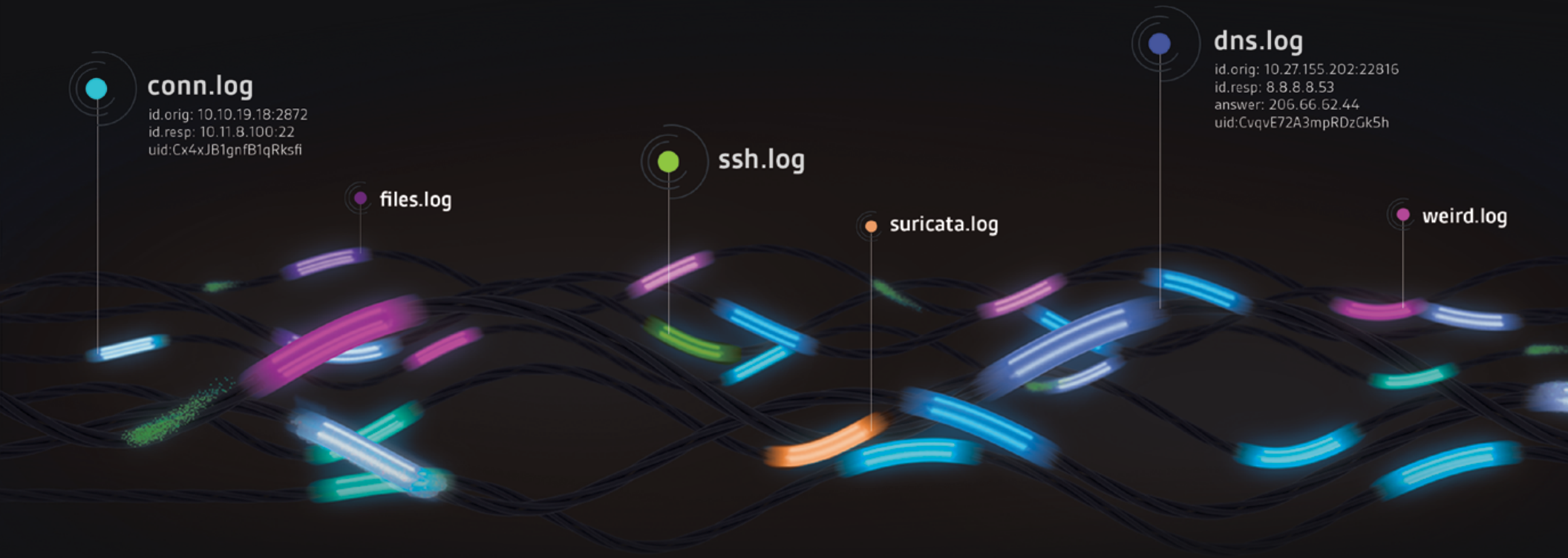
DISRUPT ATTACKS WITH NETWORK EVIDENCE

NETWORK DETECTION & RESPONSE | ON-PREM AND CLOUD

Corelight transforms **network and cloud activity into evidence** to keep you ahead of **ever-changing attacks.**

See and understand your network fully through **uncompromising visibility** and **powerful new analytics**. With our open NDR platform, **your team can track down incidents quickly** and **hunt like never before.**

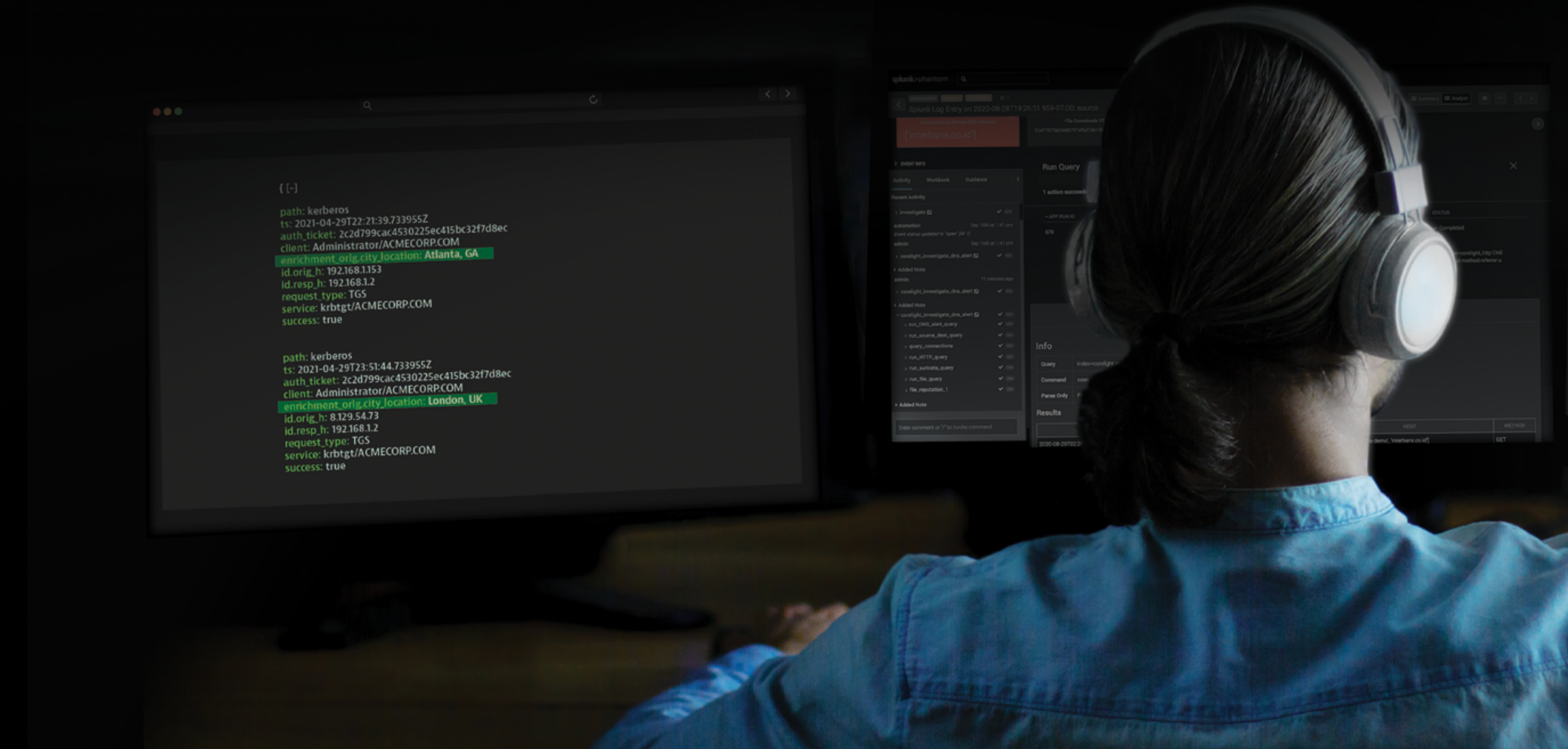
Corelight's comprehensive, correlated evidence is ready for your SIEM:



See everything that matters on your network.

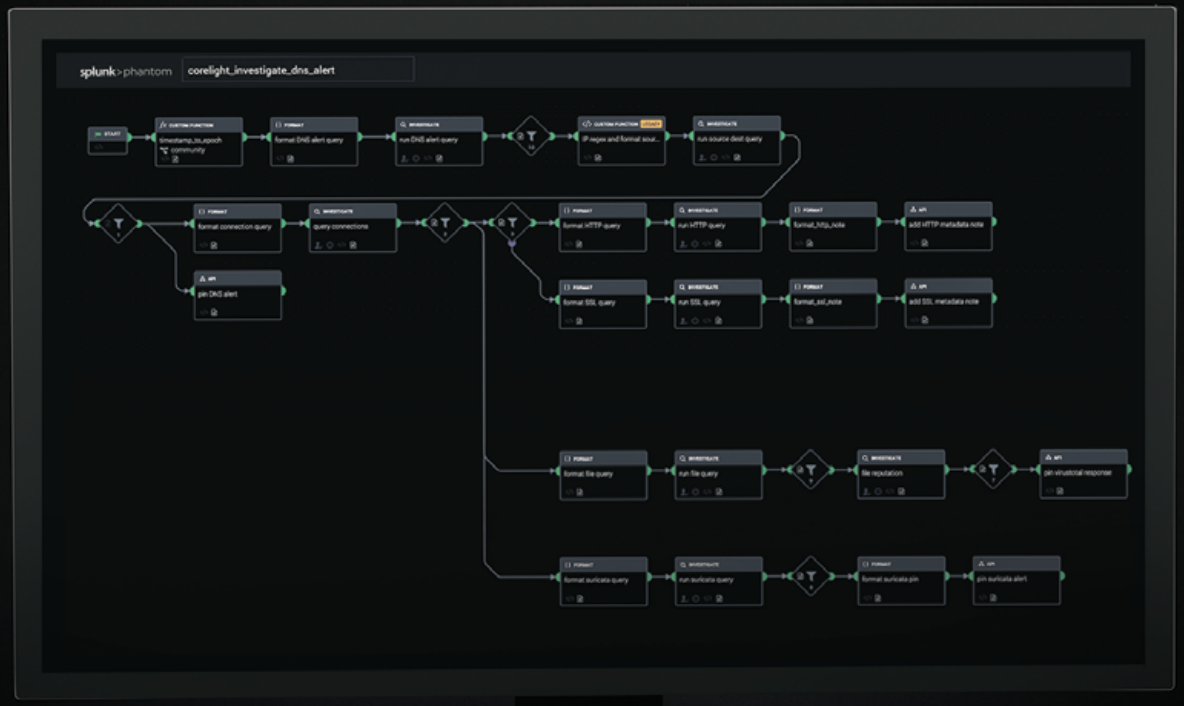
COMPLETE VISIBILITY

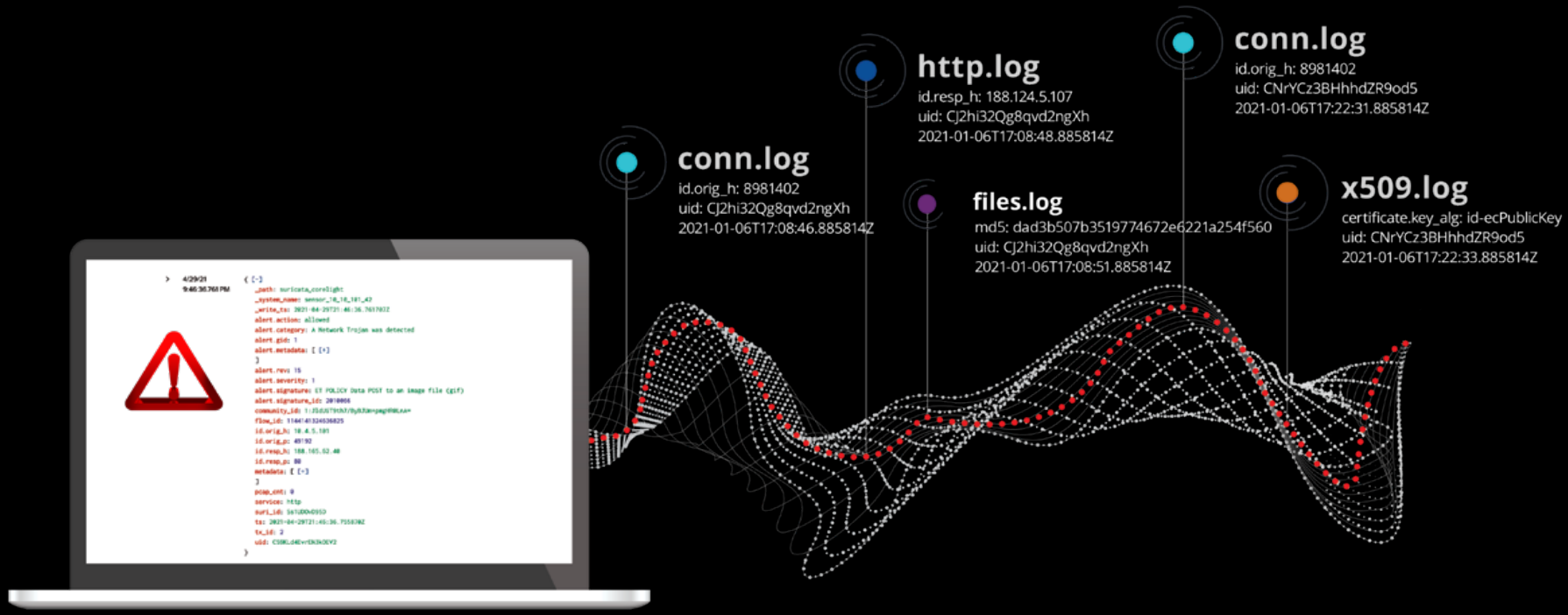
Corelight illuminates your network, including previously hidden areas, to provide context so you can understand more of your assets. Rapidly gain a commanding view of your organization and all devices that log onto your network—with access to details such as DNS responses, file hashes, SSL certificate details, and user-agent strings—without relying on other teams to respond to data requests.



NEXT-LEVEL ANALYTICS

Corelight's high-fidelity, correlated telemetry is the perfect partner for analytics, AI/ML tools, and SOAR playbooks—making them far more efficient and unlocking brand new capabilities. Corelight Collections amplify your detections even further with insight into encrypted traffic, command and control, and more.



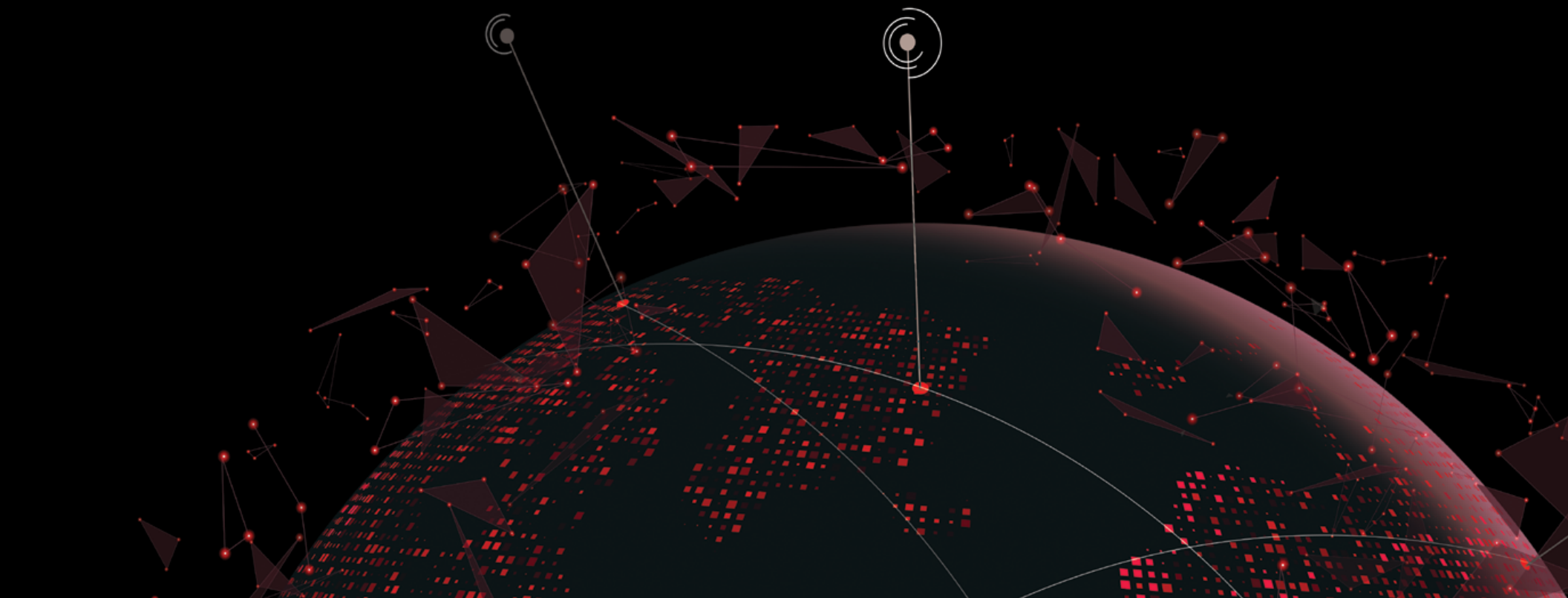


FASTER INVESTIGATION

Open NDR speeds response by correlating alerts, evidence, and Smart PCAP so the next answer you need is just a click away. The context Corelight offers reduces false positives and slashes your alert backlog—without redesigning processes or retraining analysts—because our evidence integrates into existing workflows. What's more, our evidence is so lightweight that it allows you to capture years of activity and establish your network's baseline to reveal future anomalous activity.

EXPERT HUNTING

Hunting is the best way to find advanced attackers and deny them cover. Corelight's structured evidence is clear and complete enough to make anyone on your team an efficient hunter. It's the exact same telemetry that the world's most elite defenders use, and shows you everything from artifacts left by intruders to critical misconfigurations. When you hunt like the experts, you can disrupt attacks before they turn into your next big investigation.



THE OPEN NDR PLATFORM

Suricata

CUSTOM ALERTS
TIED TO EVIDENCE

Suricata generates alerts that we embed directly into Zeek logs, putting every detection into context to save time, cut alert backlogs, and improve analytics.

Zeek®

THE GLOBAL STANDARD
FOR NETWORK EVIDENCE

The Zeek open source network security monitor generates lightweight metadata and detections to enable threat hunting and speed incident response.

Smart PCAP

HIGHLY-FLEXIBLE, EFFICIENT
PACKET CAPTURE

Smart PCAP links logs, extracted files, and insights with just the packets you need, to reduce storage costs while expanding retention times by a factor of 10.

CORELIGHT PRODUCTS

APPLIANCE SENSORS

Model	IU size	Monitoring interface	Throughput
AP 5000	Full-depth	2 QSFP28 modules. Support for optical modules at 8 x 10G, 2 x 40G or 2 x 100G	100 Gbps
AP 3000	Full-depth	Up to 8 SFP/SFP+ or 2 QSFP interfaces Support for copper and optical modules at 1G and 10G or 40G	25 Gbps
AP 1001	Full-depth	4 SFP interfaces. Support for copper and optical modules at 100M and 1G	10 Gbps
AP 200	Half-depth	4 SFP interfaces. Support for copper and optical modules at 100M and 1G	2 Gbps

VIRTUAL SENSORS

	vCPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
VMware	4–64	16–256	500–4000	ESXi 6.5 or above	500 Mbps–8 Gbps
Hyper-V	4–64	16–256	500–4000	Windows Server 2016	500 Mbps–8 Gbps

SOFTWARE SENSOR

CPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
2–64	8–256	100–4000	Any 64-bit Linux distribution	250 Mbps–8 Gbps

CORELIGHT PRODUCTS

CLOUD SENSORS

	Instance	System requirements	Nominal capacity
AWS	M4 or M5 type AWS EC2	Amazon VPC traffic mirroring enabled OR mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps
MS AZURE	Azure Ds v3 series (D8s minimum)	Traffic mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps
GOOGLE CLOUD	GCP-E2 or N1 machine type	Google Cloud Packet Mirroring enabled OR mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps

FLEET MANAGER

- Manage hundreds of sensors
- See overall fleet health in one pane of glass; drill into individual sensor metrics with one click
- Define custom sensor groups, assign individual user roles and access levels
- Deploy custom sensor policy templates
- Demonstrate compliance using audit logs

smartPCAP

- Cut your PCAP costs by up to 50%
- Fine tune rules to capture only the packets you need
- Expand retention by 10x while reducing costs
- Access packets directly in your SIEM for faster investigations

CORELIGHT COLLECTIONS

Turnkey packages that deliver proprietary detections plus curated insights from the Zeek community.

C2 COLLECTION

50+ detections and insights into known command and control activity as well as MITRE ATT&CK® C2 techniques to find novel attacks

- Find Cobalt Strike and known malware families that run C2 over HTTP
- Detect DNS tunneling and other techniques like domain generation algorithms

ENCRYPTED TRAFFIC COLLECTION

Dozens of unique insights into SSL, SSH, and RDP connections along with encrypted insights from the Zeek community like JA3—all without decryption

- Track SSL fingerprints, soon-to-expire certificates, and more
- Track user behavior over SSH and RDP with insights that can determine if it's a human or a script behind those packets

CORE COLLECTION

Preloaded Corelight packages that help sensors scale in high-throughput environments

- Detect lateral movement mapped to MITRE ATT&CK
- Find cryptomining traffic over TCP or HTTP

MAKE YOUR DATA-FIRST STRATEGY A REALITY.

info@corelight.com | 888-547-9497