cPacket corelight

SOLUTION BRIEF

See Everything.
Detect Anything.
When Packet Analytics Meet Evidence-Based NDR.

Accelerate alert-to-answer with streamlined workflows and on-demand network insights.

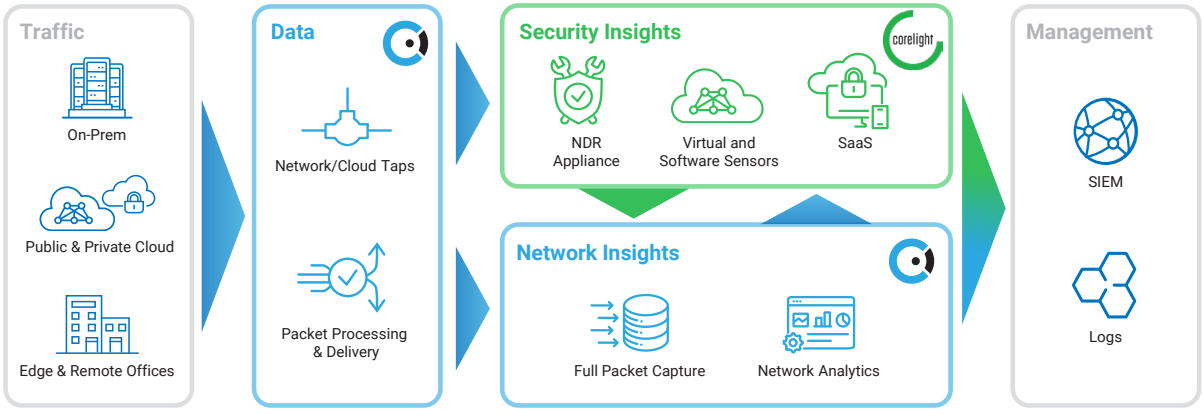
Detecting, diagnosing, and resolving threats across hybrid environments often require security analysts to analyze large volumes of network traffic data from physical and cloud infrastructure. While logs, flows, and traces are often used to monitor network health and security, packet-level telemetry is the evidentiary gold standard.

Together, cPacket and Corelight eliminate blind spots and friction to accelerate threat hunting, diagnostics, and attack containment. Unlike the black box of CSP monitoring tools that are prone to dropped packets and offer limited insights, cPacket's Unified Observability solutions deliver the most accurate and complete view of network activity to Corelight's Open NDR Platform – in real time.

With a history of successful deployments in the most demanding environments, Corelight and cPacket offer a solution to provide customers with the best combination of data and insights to streamline workflows.

SOLUTION HIGHLIGHTS:

- One-click access to packet data and packet capture reports (PCAPs) within the familiar Corelight UI accelerates detection-to-response workflows.
- Deep network insights on demand from Corelight Investigator enhances forensics, file reconstruction, and root cause analysis.
- Real-time evidence provides valuable information so triage and response teams can quickly limit lateral movement and mitigate threats.
- Centralized view of cloud and hybrid environments with agentless cloud observability for all major CSPs.
- Deployment of Corelight sensors and cVu-V virtual packet brokers simplifies Azure, GCP, and AWS deployment.



cPacket data and insights are sent to the Corelight Open NDR Platform for advanced security insights

Solution Benefits

Complete Visibility

Analysts can quickly detect cyberattacks, exfiltration, and potential threats across hybrid and multi-cloud environments. Corelight's rich, correlated logs – combined with cPacket's unified observability fabric – enable deployments using Terraform in distributed CSP workloads.

Faster Investigation

cPacket's line-rate packet processing (including timestamping, smart filtering, deduplication, and string search), and real-time analytics (including encrypted traffic, TCP flow, sessions, etc.) enable SoC teams to act quickly to identify the root cause and impact – often in minutes instead of hours or days.

Next Level Analytics

Corelight's Zeek-based logs and multi-layer detections accelerate investigations with up to 20x faster resolution. With continual and on-demand packet capture, cPacket surfaces additional network health metrics (latency, re-transmissions, server performance, etc.), that allow incident response teams to quickly isolate and mitigate threats.

Streamlined Workflows

SOC teams can quickly access real-time packet data and deep network analytics within their familiar interface, which streamlines detection, triage, investigation, and response – without jumping between dashboards and tools.

Audit-Ready Proof

When full packet capture is required, cPacket provides indisputable evidence for regulatory and legal compliance. cStor solutions offer continuous capture at up to 200Gpbs and the industry's fastest indexing, search, and retrieval times to streamline reconstruction and forensics.

Simple Licensing Model

Both Corelight and cPacket offer transparent licenses that allow customers to focus on threats, not upgrades and renewals. cPacket's licenses include all features from day one, and are based on instance throughput (measured in Gbps or Terabytes per Day) rather than number of instances.

> "Knowing my NDR tools are using the best data gives me peace of mind. But using an integrated solution gives me back time in my day and makes investigations much easier."
>
> – Security Analyst for a global airline

About cPacket

cPacket is modernizing network observability for the AI era. Built on trusted packet data, the company's Unified Network Observability Platform delivers complete visibility, real-time analytics, and explainable AI insights across hybrid and multi-cloud environments. The result is faster detection and resolution of performance issues, stronger security posture, and greater operational resilience. Global finance, healthcare, and technology enterprises and government agencies rely on cPacket to ensure network reliability and business continuity at scale. Built for the world's fastest, most demanding networks — solutions are certified for SOC 2 (Type I and II), FIPS 140-2 and AICPA compliance. Find out more at **www.cpacket.com**.

About Corelight

Corelight transforms network and cloud activity into evidence that security teams use to proactively hunt for threats, accelerate response to incidents, gain complete network visibility and create powerful analytics. Corelight's global customers include Fortune 500 companies, major government agencies, and large universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology. For more information, visit **https://corelight.com** or follow **@corelight_inc.**