# Risk thrives in uncertainty.
# The best defense is evidence.
# The best evidence is packet data.

## Eliminate blind spots for faster threat detection and response.

While logs, flows, and traces are often used to monitor network health and security, packet-level telemetry is the evidentiary gold standard. cPacket cVu packet brokering solutions deliver the most accurate, comprehensive, and real-time view of network activity to Corelight's Open NDR Platform, which transforms this rich network data into actionable security insights, leveraging its powerful analytics and evidence-based detections to identify sophisticated threats across the network.

Together, cPacket and Corelight eliminate blind spots with indisputable evidence to accelerate threat hunting, diagnostics, and attack containment. This evidence helps SecOps dramatically reduce the time to respond and resolve incidents.

The combination of packets, precision, and performance have made cPacket the solution-of-choice for the most demanding networks in the Financial Services, Healthcare, Government, SaaS, and other markets.

## Corelight and cPacket: The best line of defense for cloud and hybrid networks

Another challenge is detecting  threats and analyzing large volumes of data across hybrid topologies with both physical and cloud deployments. Unlike the black box of CSP monitoring tools that are prone to dropped packets and offer limited insights, cPacket's Cloud Suite provides end-to-end visibility of all packets across hybrid environments. cPacket's agentless architecture makes it cost-effective and easy to deploy virtual packet broker and capture appliances in Azure, AWS, and Google Cloud instances. The cVu-V virtual packet proker can provide inline packet acquisition or enhance CSP native packet mirroring capabilities, to enable Corelight's Open NDR platform with complete visibility into cloud workloads.

### INTEGRATION HIGHLIGHTS:

- Delivers full-fidelity packets to Corelight sensors, enabling improved visibility and threat detection.
- Line-rate packet processing and analytics on every port enhances incident detection, troubleshooting, and resolution.
- Centralized view of cloud and hybrid environments with agentless cloud observability for all major CSPs.
- Rich, correlated network logs and evidence-based detections accelerates investigations and response.
- Integration of Corelight Sensor and cVu-V virtual packet broker streamlines Azure and other CSP deployments.
- Flexible network observability platform scales cost-effectively with security, traffic, and performance requirements.
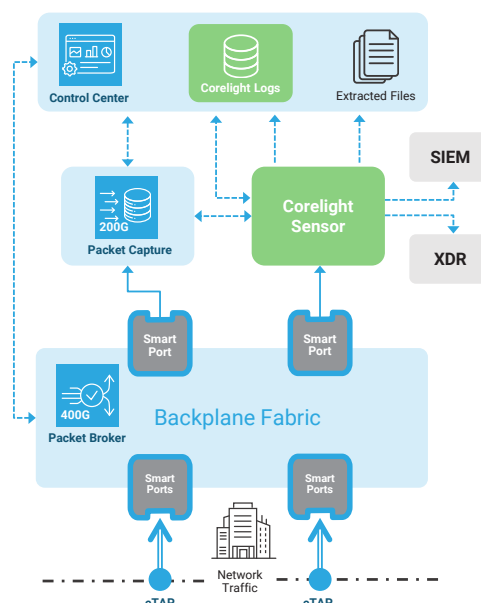
## Solution Benefits

### Complete Visibility

Quickly detect cyberattacks and potential threats across hybrid and multi-cloud environments. Corelight's rich, correlated logs – combined with cPacket's high-performance packet broker fabric on-prem and integrated cloud solution – enable easy, automated deployment using Terraform in distributed CSP workloads.

### Faster Investigation

Only cPacket's line-rate packet processing (including timestamping, smart filtering deduplication, and string search), enriched security insights, and flexible encrypted traffic analysis not only accelerate incident detection, but provide analysts with indisputable evidence for root cause analysis.

### Next Level Analytics

Corelight sensors generate Zeek logs and detections that provide response teams with a comprehensive view of all network traffic – enabling them to resolve incidents up to 20x faster. In addition to surfacing network health metrics (latency, re-transmissions, server performance, etc.), cPacket's continual and on-demand packet capture and network analytics can enhance incident forensics with full packet indexing, replay and real-time searchability of historical data.

### Ultimate Scalability

As your business grows and security requirements evolve, the combination of Corelight's Open NDR Platform and cPacket's Cloud Suite (with native CSP autoscaling) scales with you – supporting fluctuating cloud traffic patterns without sacrificing performance, resiliency, compliance, and ROI.

### 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.

"The combination of **cPacket's virtual packet broker** with **Corelight VMs** is the Terraform solution we were looking for. It enabled full automation across dozens of our Kubernetes clusters to improve security inspection and exfiltration detection."

– Leading Generative AI Company

### About cPacket

cPacket Networks powers hybrid-cloud observability through its Intelligent Observability Platform. It reduces service outages through network-centric application analysis, strengthens cybersecurity through high-resolution network data for threat detection, and accelerates incident response through network forensic analysis. The result is increased service agility, experience assurance, and transactional velocity for the business. cPacket solutions are certified for 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.**

SB-CL-060425