cPacket

CASE STUDY

Leading US Airline Accelerates Threat Investigations by Adding Packet-Level Evidence to Corelight NDR Workflows

The Customer

A leading global airline operates a large, distributed enterprise network where operational resilience and security are mission-critical. With complex infrastructure spanning many locations and supporting a multitude of operational and passenger-facing systems, the organization depends on security teams to detect threats quickly and respond with confidence—without disrupting the systems that keep global air travel moving. This urgency is escalating: IBM reports cyberattacks on the aviation industry are up 74% since 2020, and Thales reports ransomware attacks in the aviation sector increased 600% year-over-year (based on observed activity from January 2024 to April 2025).

For malicious actors, aviation infrastructure offers a uniquely broad attack surface: interconnected IT and operational technology environments, plus IoT systems that touch everything from passenger processing to baggage operations. The industry also carries systemic risk—single points of failure in shared systems can disrupt operations for days, and heavy dependence on third-party providers means an incident can cascade across multiple systems and stakeholders, amplifying impact beyond the initial intrusion.

To strengthen detection and response, the airline had already adopted a modern security approach using packet broker infrastructure and Corelight NDR. But as threats evolved, the team needed deeper evidence and historical context to validate suspicious activity, perform forensics, and meet audit requirements—without forcing a rip-and-replace of the existing security stack.

The Challenges

The airline's security teams faced a common modern dilemma: detection signals existed, but packet-level evidence and historical data did not. Without packet capture, investigations often lacked the "ground truth" required to confirm what happened and understand scope and impact.

Key challenges included:

- **Evolving Threat Pressure:** The organization needed to identify and respond to security threats faster as attacker techniques continued to evolve across broad attack surfaces.
- **No Packet Capture Foundation:** The initially deployed solution provided sampled data without packet capture, the team had limited ability to support deep investigations, audit workflows, or retrospective threat hunting.
- **Limited Historical Context:** The team needed longer retention and rapid retrieval to investigate incidents that unfold over time—not just in the moment.
- **Preserve Existing Security Workflows:** The airline wanted to add forensic depth while continuing to leverage its existing packet broker environment and Corelight-based NDR operations.

The Solution

The airline's strategy was to extend—rather than replace—its existing security architecture. cPacket was deployed to add a packet capture and retention layer that complements the organization's current packet broker deployments and integrates directly with Corelight NDR workflows.

This approach gave the security team a clear path from detection to evidence: use Corelight for NDR-driven context and detection signals, then pivot to cPacket packet capture for deeper investigation, forensics, auditing, and historical lookback.

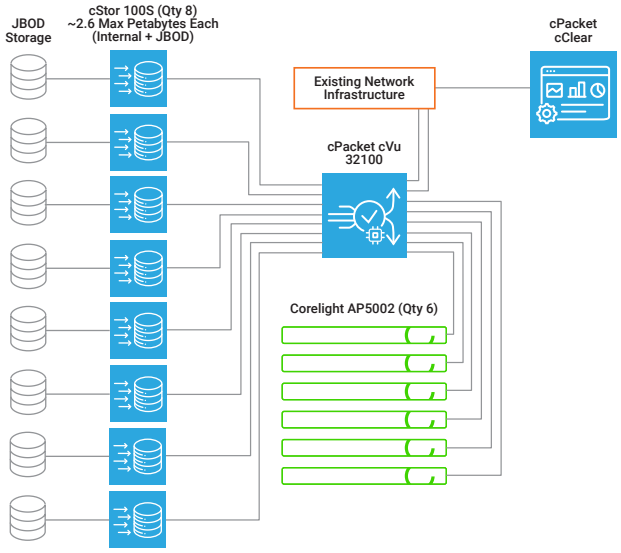
> *"The integration of packet-level intelligence into Corelight's NDR platform expedited our threat investigations and gave us better data without toggling between multiple dashboards and tools."*

Platform Components Deployed

- **cVu 32100AG:** Packet visibility and capture enablement aligned with enterprise deployment needs.
- **cStor 100S:** High-scale packet capture storage designed for longer retention, indexing, and fast recall to support security investigations, auditing and compliance.
- **cClear:** Central management and access for packet workflows and evidence retrieval across the environment.

Integration:

Corelight NDR + cPacket: Corelight provides detection and NDR context, while cPacket provides packet capture, historical retention, and indexed recall so investigators can validate events with packet truth. cPacket & Corelight fully integrate at the API level reducing detection and resolution times.



Key Benefits

- **Forensic Evidence on Demand:** Packet capture adds the missing forensic layer behind NDR detections—enabling deeper investigations, post-incident reconstruction, and stronger audit support with defensible packet truth.
- **Long-Term Historical Lookback at Scale:** With large-scale packet capture capacity (up to ~30PB) the airline can retain 30+ days of packet history, making it possible to investigate incidents that unfold slowly, validate scope after the fact, and support retrospective threat hunting beyond short rolling buffers.
- **High-Fidelity, Not Sampled:** The deployment supports lossless capture at full line rate, ensuring investigators aren't making decisions from partial evidence due to packet drops during peak conditions—critical when validating security events and proving timelines.
- **Faster Investigation Workflows via Indexed Recall:** Indexed packet recall compresses time-to-truth by letting teams pivot from "what Corelight flagged" to "here are the packets" quickly—reducing manual effort and eliminating delays caused by fragmented capture methods.
- **Stronger NDR + Compliance Workflows Through Integration:** Corelight integration and API-driven access allow detections to be enriched with packet evidence and historical recall—supporting forensic analysis tied to compliance and regulatory requirements while keeping established NDR workflows intact.

The Results

By adding packet capture, long-term retention, and fast packet recall to its existing packet broker and Corelight NDR environment, the airline strengthened its ability to respond to evolving threats with speed and confidence. Security teams gained the forensic and historical depth needed to validate suspicious activity, support audit requirements, and perform retrospective analysis—without disrupting the tools and workflows already in place.

This deployment established a scalable foundation of packet-evidence that improves the airline's security posture today and provides a strong platform for future expansion into broader network and observability initiatives.

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