



CASE STUDY

Global Bank Eliminates Kubernetes Blind Spots for Faster Incident Evidence with Packet-Level Observability

The Customer

One of the world's ten largest banking institutions is modernizing critical application infrastructure as part of a broader platform transformation, moving key services into Red Hat OpenShift / Kubernetes. As these applications transition into containerized environments, the bank's IT organization must maintain the same level of operational control, performance assurance, and incident-response readiness expected in high-stakes financial services.

In this environment, application availability and performance are non-negotiable. When issues occur, teams need defensible evidence fast – especially inside Kubernetes clusters where traditional visibility approaches often break down. The organization's focus is ensuring its Kubernetes foundation is operationally ready for mission-critical workloads, not just technically functional.

The Challenges

As Kubernetes adoption accelerated, the bank encountered a familiar modernization barrier: limited insight into east-west traffic inside the cluster. Without packet-level evidence, teams faced slower investigations, more frequent escalations, and increased risk during migration.

Key challenges included:

- **Kubernetes East-West Blind Spots:** Limited packet visibility into pod-to-pod traffic created investigation gaps for critical application teams.
- **Slow Time-to-Capture:** Traditional approaches relying on physical instrumentation can take significant time to deploy, reducing the ability to capture evidence when incidents recur.
- **Critical vs. Non-Critical Needs:** The bank required a model that supports always-on visibility for top-tier applications while enabling rapid, on-demand capture for less critical workloads.
- **Resource Efficiency Requirements:** Any in-cluster approach must operate within strict performance guardrails to avoid impacting production services.
- **Operational Workflow Fit:** Visibility data must align with established operational processes—so packet evidence can be used consistently across teams, not only by specialists.

The Solution

To close the Kubernetes visibility gap and support migration readiness, the bank evaluated cPacket's observability platform based on one central question: can packet truth be operationalized inside Kubernetes without unacceptable performance overhead?

The strategy focused on validating packet-level observability for east-west traffic in a way that aligns with how the bank actually works – incident workflows, operational naming conventions, and integration into existing tools and processes. Rather than requiring disruptive architectural changes, the evaluation emphasized practical deployment, measurable efficiency, and repeatable evidence generation.

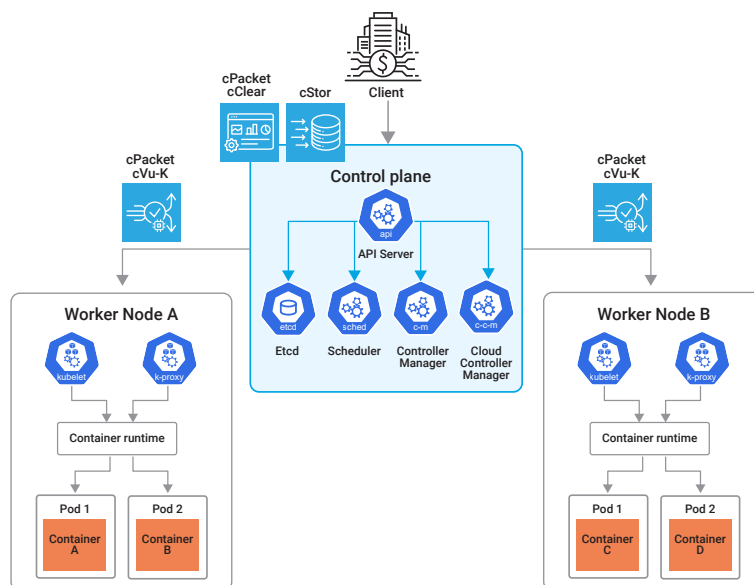
The solution needed to meet four key criteria:

- Provide packet-level visibility into Kubernetes east-west conversations inside the cluster
- Run efficiently inside Kubernetes environments and remain within acceptable resource overhead limits
- Enable fast packet recall and indexing to support time-sensitive investigations
- Fit operational workflows and support broader team adoption through integration and standardization

"cPacket was the only solution that allows us to manage and monitor Kubernetes east-west conversations and provide visibility into the cluster conversations."

Solution Components

- **cVu-K Packet Broker:** Uses an eBPF-based approach to enable packet visibility for Kubernetes east-west traffic. This provides in-cluster access to packet data and metrics, with the ability to selectively mirror relevant flows for investigation.
- **cStor Packet Capture:** Captures and stores packet data while supporting indexing for faster retrieval – helping teams move from symptom to evidence without extended manual effort.
- **cClear Control Center:** Provides centralized management and access control for capture workflows and supports operational alignment through consistent visibility and evidence packaging.



Key Benefits

- **Kubernetes Visibility:** Packet-level insight into pod-to-pod traffic reduces cluster blind spots and supports migration confidence.
- **Faster Evidence Collection:** Indexed capture and rapid recall help teams retrieve the right traffic quickly during investigations.
- **Operational Readiness for Critical Workloads:** Supports models for always-on visibility for high-value services and rapid on-demand capture when needed.
- **Efficiency Guardrails:** Designed to validate low-overhead operation suitable for production environments.
- **Workflow Alignment:** Built to support consistent operational processes, improving the likelihood of adoption beyond a small expert group.

The Results

The bank's evaluation proved that Kubernetes east-west packet visibility can be deployed efficiently and used operationally to support critical application migration. cPacket's Unified Network Observability Platform achieves the bank's objectives:

- Verifying that in-cluster packet visibility can be delivered without disrupting service performance
- Validating packet capture, recall, and indexing effectiveness for real investigation workflows
- Establishing a repeatable operational model for Kubernetes east-west evidence collection
- Validation Workflow and Integrations with Existing Support and Operations teams tools.

After a successful PoV, the bank intends to begin with a small-scale deployment at one site, expand into a major US data center, and then scale internationally as Kubernetes migration efforts broaden.

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