

Case Study

German Private Bank

Network Visibility That Pays Off

How a Bank Detects Network Incidents Faster, Analyzes Them More Efficiently, and Optimizes Operations Long-Term

Industry: Financial Services

Customer: Leading German Bank

Challenge: End-to-end visibility down to the packet level for network issues, anomalies, and security-related events

When issues arise within an IT network, every second matters. Full visibility into network traffic, down to the packet level, is essential for responding effectively when incidents occur. A leading German bank chose Allegro Packets to ensure reliable data recording and fast access to the insights they need to investigate.

Challenge: When Every Second Counts

The customer required continuous recording of network traffic. Network issues and anomalies needed to be extracted from a defined time window for retrospective analysis. The goal was to quickly identify where anomalies first appeared, how they propagated across business-critical systems such as payment processing and core banking platforms, and whether recurring patterns could be detected, all based on raw packet-level data.

Previously, the bank relied on the built-in packet recording functionality of a security solution vendor. However, that product's maintenance costs were disproportionate to the limited analytical capabilities provided. Rather than renewing the existing maintenance agreement, the bank sought a more cost-effective alternative that offered greater value.

Key Challenges:

- ⚡ Limited traceability of network activity within financial data traffic
- ⚡ Limited forensic analysis capabilities for security-related incidents
- ⚡ Delayed root cause analysis of disruptions affecting business-critical systems such as payment processing and core banking
- ⚡ Challenges in meeting compliance and audit requirements
- ⚡ Significant manual effort required for ad hoc packet captures during incident investigations
- ⚡ High costs of the existing solution despite limited analytical functionality

Solution: Better Insights Through Complete Network Transparency

The bank selected the Allegro Network Multimeter 3500 to ensure comprehensive network visibility, especially in time-critical situations. One of the key advantages is its integrated packet ring buffer: network data is continuously recorded and remains available for retrospective analysis. This enables the IT team to access historical network data at any time without requiring manual captures or advance preparation.

The flexible and scalable storage architecture allows recording capabilities to be tailored precisely to the bank's requirements. Data can be filtered with great granularity, by packet size or specific traffic flows, for example. At the same time, built-in security features such as AES-256 encryption and redundant storage ensure secure, compliant, and auditable data retention.

The Allegro Network Multimeter integrates seamlessly into the existing infrastructure and supports flexible data acquisition methods, whether directly in the data path, through SPAN ports, or across sites using ERSPAN.

When analysis is required, the IT team benefits from an intuitive workflow. Relevant traffic flows can be visualized and exported as pcap files in just a few clicks, significantly accelerating detailed packet-level investigations.

Results: Lower Costs, Greater Planning Reliability

With the Allegro Network Multimeter, the bank fully achieved its primary objective: reliable recording and rapid analysis of packet-level data immediately before and after anomalies and security-related incidents.

Continuous access to historical data now enables the IT team to investigate incidents significantly faster and with greater accuracy, without relying on preconfigured captures or reactive measures. Critical information is always available exactly when it is needed.

The solution also delivered clear financial benefits. Compared to maintaining the previous infrastructure, the investment paid for itself within two years, based on a planned lifecycle of five years.

As a result, the bank benefits not only from greater visibility but also from a substantially improved cost structure and long-term budget predictability.

Case Study

German Private Bank

Key Benefits at a Glance:



- Audit-ready network forensics through complete packet recording
- Significantly faster investigation of security incidents and anomalies in financial data traffic
- Reduced downtime of business-critical applications such as payment processing and trading systems
- Lower risk of compliance violations and reputational damage
- More efficient use of IT resources
- Predictable and optimized long-term cost structure

Conclusion: An Investment That Delivers Value

The bank now operates a powerful, future-proof network visibility platform capable of supporting high-performance data center environments with bandwidths of up to 200 Gbit/s.

At the same time, the solution provides a foundation for further optimization. Additional analysis capabilities are already available and can be activated as needed, further improving troubleshooting efficiency and accelerating investigations.

This positions the bank not only to meet current requirements but also to continuously evolve its network strategy. The result is a shift from reactive troubleshooting toward a more proactive and strategic approach to network analysis.

About Allegro Packets

Allegro Packets, a German-based company, offers portable and rack-mount solutions for network analysis and packet capturing. The brand is setting new benchmarks by combining high performance, reliability, active development, relentless support, and fair pricing in its all-in-one proposition. Allegro Packets' solutions are recognized and utilized by service providers, government organizations, healthcare institutions, and enterprises worldwide.

Website: www.allegro-packets.com