Gigamon®

Strengthening Cyber Resilience in Financial Services with Gigamon Deep Observability

Reduce risk, improve compliance confidence, and enable operational efficiency across hybrid cloud environments.

Financial services organizations face escalating cyber risk, expanding regulatory expectations, and increasing pressure to deliver always-on digital services. Encrypted, ingress-egress, lateral (East–West) traffic, and hybrid cloud traffic now carry the most sensitive data and highest-value transactions. These same areas, however, are where attackers increasingly operate, and where traditional metric, event, log, and trace (MELT) tools often lack the network context required for effective detection, investigation, and validation.

The Gigamon Deep Observability Pipeline delivers network-derived telemetry—packets, flows, and application metadata—across data center, cloud, virtualized, and container environments. By centralizing and governing access to encrypted traffic and selectively enriching and routing telemetry to existing security, observability, and compliance tools, financial institutions can:

- **Strengthen risk management and security posture**
- **Improve compliance and audit readiness**
- **Increase operational efficiency and performance across hybrid environments**

Gigamon helps financial services leaders address these challenges while serving as a strategic partner to CISOs, CIOs, and heads of risk.

Key Challenges and Market Shifts

Financial institutions are navigating several converging challenges as they adopt cloud and AI-driven services:

- **Encrypted, ingress-egress, and lateral traffic blind spots** that obscure threat activity and complicate evidence collection.
- **Hybrid and multi-cloud architectures** that expand the attack surface and fragment control coverage.
- **Complex regulatory mandates** (e.g., PCI DSS 4.0, DORA) that require continuous proof of control effectiveness, not just annual attestations.
- **Tool sprawl and rising costs,** as security and observability stacks ingest more data without sufficient context or signal quality, while adversaries increasingly exploit automation and AI to move faster than legacy visibility models.

Traditional approaches that rely solely on data from recorded logs cannot, on their own, provide the depth of insight required to fully secure and manage hybrid cloud infrastructure. Deep observability extends these tools with network-derived telemetry, often significantly improving tool efficiency, reducing data ingest volumes, and accelerating time to value.

Solution Overview

The Gigamon Deep Observability Pipeline efficiently delivers network-derived telemetry to cloud, security, and observability tools to eliminate blind spots, optimize traffic, and reduce tool costs across hybrid cloud infrastructure.

CORE CAPABILITIES

- **Complete visibility** into network communications across data center, private cloud, and public cloud, including encrypted, ingress-egress, and lateral traffic.
- **Centralized, policy-driven decryption** (Gigamon Precryption® technology and TLS/SSL decryption) that provides governed access to encrypted flows for approved tools and workflows.
- **Selective traffic delivery and enrichment,** filtering out duplicate and low-value traffic while enriching remaining flows with contextual metadata for higher-fidelity detection and faster troubleshooting.
- **Gigamon Application Metadata Intelligence (AMI)** to identify applications, services, AI engines, and dependencies critical to financial transactions and customer-facing services.

BUSINESS OUTCOMES

- **Faster identification and resolution of performance** and availability issues
- **Reduced mean time to detect, investigate, and remediate** security incidents
- **Improved reliability** of customer-facing services across hybrid environments
- **Higher analyst and operator productivity,** with less tool noise and manual troubleshooting

Gigamon helps financial services teams strengthen cybersecurity and compliance by adding network context to existing tools. Learn more here

Learn more about securing and managing hybrid cloud environments with the **Gigamon Deep Observability Pipeline** on our website.

Risk Management and Security Posture

KEY CHALLENGE

Attackers increasingly exploit encrypted, ingress-egress, and lateral traffic to hide “low and slow” campaigns, lateral movement, and command-and-control activity. In complex hybrid environments, security teams must defend with finite resources while threat actors accelerate with automation and AI.

GIGAMON OUTCOMES

- Enhanced protection of high-value assets, payment systems, and critical transaction flows
- Better detection of ransomware, lateral movement, Living Off the Land (LOTL) attacks, and Command and Control (C2) activity hidden in encrypted or lateral (East-West) traffic
- Stronger, more resilient cyber risk posture and higher confidence for boards and regulators

Compliance and Audit Readiness

KEY CHALLENGE

Financial institutions must continuously demonstrate that controls are effective across encrypted, ingress-egress, and lateral hybrid cloud communications. Gaps in visibility complicate evidence collection, slow down audits, and increase the risk of non-compliance with frameworks such as PCI DSS 4.0 and DORA.

GIGAMON OUTCOMES

- Stronger ability to prove compliance and control effectiveness on demand
- Reduced audit preparation time and disruption to business operations
- Increased confidence in meeting evolving regulatory mandates and demonstrating effective governance to boards and supervisors

> Gigamon has helped us in a number of areas: advanced visibility, performance capability, and intelligent and advanced threat management. Today we are leveraging AMI capability to help us troubleshoot performance issues and safeguard our PCI environment as we move to PCI DSS 4.0.
>
> **Waddaah Keirbeck**
> Global Chief Technology Officer
> Corpay (formerly FLEETCOR)

Operational Efficiency and Performance

KEY CHALLENGE

Hybrid cloud and containerized architectures complicate ownership of performance issues, and traditional tools often detect problems only after customers are impacted. Limited visibility into how traffic flows between users, applications, and infrastructure slows root-cause analysis and drives up tooling and operational overhead.

GIGAMON OUTCOMES

- Reduced MTTR for performance and availability issues
- Higher service reliability for digital banking, payments, and trading platforms
- Lower tool spend and extended life of existing observability investments through more efficient data ingestion and processing

By partnering with Gigamon, financial institutions can gain the deep observability required to protect digital banking services, streamline compliance, and keep critical systems performing at scale.

To learn more about how Gigamon supports financial services organizations:
Visit **gigamon.com/financial-services**,
request a meeting at **gigamon.com/contact-sales**,
or connect with your Gigamon representative
or channel partner to discuss how the Gigamon Deep Observability Pipeline supports your security, compliance, and performance initiatives.

About Gigamon

Gigamon® delivers an AI-powered Deep Observability Pipeline that provides network-derived telemetry to cloud, security, and observability tools. With AI-driven insights across packets, flows, and application metadata, organizations gain complete visibility into all data in motion to detect threats concealed in encrypted and lateral traffic, resolve network and application performance issues, and validate compliance while reducing operational cost and complexity. Gigamon is trusted by 4,000+ organizations, including 83 of the Fortune 100 and hundreds of public sector agencies and educational institutions. Learn more at **gigamon.com**.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

01.26_01