

Gigamon Application Metadata Intelligence (AMI) for Security and Compliance Frameworks

Network-derived telemetry for validating controls across hybrid and multi-cloud environments

Organizations are expected to demonstrate compliance continuously, not just during annual audits. Hybrid and multi-cloud architectures, encrypted traffic, and complex application dependencies make evidence collection slow and manual. Many teams rely on logs and application metrics to demonstrate compliance, but these sources often lack the network context needed to validate how systems communicate and where sensitive data moves.

Network-derived telemetry helps close this gap. By extracting metadata directly from network traffic, organizations gain visibility into communication between systems, validate segmentation policies, and confirm encryption standards across hybrid and multi-cloud environments. This visibility helps security and compliance teams generate consistent evidence to support modern compliance frameworks.

Why Network Telemetry Matters for Compliance

The network records how data moves between users, applications, and infrastructure. This makes it a valuable source of independent evidence for security and compliance teams. Network-derived telemetry helps organizations:

Map system communications and dependencies

Identify which systems communicate and how traffic flows between regulated environments.

Validate segmentation and access controls

Confirm that sensitive systems such as payment environments, healthcare systems, or financial reporting infrastructure are properly segmented.

Verify encryption and protocol usage

Ensure data in motion is protected using approved encryption standards and identify weak or misconfigured protocols.

Produce audit-ready evidence faster

Provide consistent telemetry that supports compliance reporting and control validation.

How Gigamon AMI Supports Compliance Frameworks

Gigamon Application Metadata Intelligence (AMI), part of the Gigamon Deep Observability Pipeline, extracts network-derived telemetry from network traffic and identifies the applications, services, and dependencies communicating across the environment. This telemetry is delivered to existing security, observability, and compliance tools.

Network-derived telemetry helps teams:

- Identify applications and services communicating across the network
- Monitor encrypted and East-West traffic across hybrid and multi-cloud environments
- Validate segmentation and encryption policies
- Generate evidence for audit and regulatory reporting

Gigamon AMI helps security, risk, and compliance teams generate consistent network-derived evidence to support modern compliance frameworks and reduce audit preparation time by up to 50 percent.

Visit gigamon.com/contact-sales to learn how we can help support the frameworks you use.

How Gigamon AMI Supports Security and Compliance Frameworks

The following table highlights representative examples of how Gigamon AMI can support risk and compliance frameworks. It is not an exhaustive control mapping.

Framework / Regulation	Key Requirement Area	How Gigamon AMI Helps	Executive-Level Outcome
SOX (Sarbanes–Oxley) – Sections 404 & 409	Internal controls over financial reporting; timely disclosure of material events	Uses network-derived telemetry to continuously monitor critical systems, access patterns, and data flows that underpin financial applications	Stronger Section 404 internal control attestations and faster, evidence-backed Section 409 incident and outage disclosures
GDPR – Articles 25, 30, 32	Privacy-by-design, data mapping, and protection of personal data in transit	Validates network segmentation around systems processing personal data, maps data flows between systems, and verifies encryption protocols in use	Clear evidence of GDPR technical controls, reduced audit friction and lower regulatory and reputational risk
ISO 27001 / 27002	Information Security Management System (ISMS), control implementation, and risk processes	Provides continuous visibility into networks communications to design, implement, and monitor security controls and surface operational and security risks from network traffic patterns	Better-aligned ISMS, measurable control effectiveness, and more defensible risk registers supported by objective network evidence
ORSA (Own Risk and Solvency Assessment)	Operational risk identification and assessment	Maps network topology to reveal single points of failure, analyzes historical outage impact, tracks bandwidth and capacity trends, and identifies inter-system dependencies from traffic flows	Defensible view of reasonably foreseeable material risks supported by concrete technical evidence
NCUA Part 748.1(b) – Information Security Program	Security controls implementation; controls testing (CT-01–CT-03)	Monitors network access controls, including unauthorized access attempts and segmentation between member-facing and back-office systems, and provides continuous traffic analysis and centralized event correlation	Demonstrable evidence package for NCUA Controls Testing CT-01–CT-03 supporting a regulator-aligned security program
NCUA Part 748.2 – Cybersecurity Incident Response	Incident detection, response, and investigation	Detects network-based indicators of compromise, lateral movement, and command-and-control (C2) traffic and enables network forensics, breach timeline reconstruction, and data exfiltration analysis	Faster incident detection and containment, regulator-ready investigation records, and clearer understanding of business impact
PCI DSS 4.0 – R1, R2, R4, R5, R10–12	Security controls implementation; controls verification	Monitors network access controls, verifies encryption in use, validates in-scope networks, and confirms security guardrails	Faster compliance reporting and stronger control attestations


Worldwide Headquarters

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

© 2026 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.