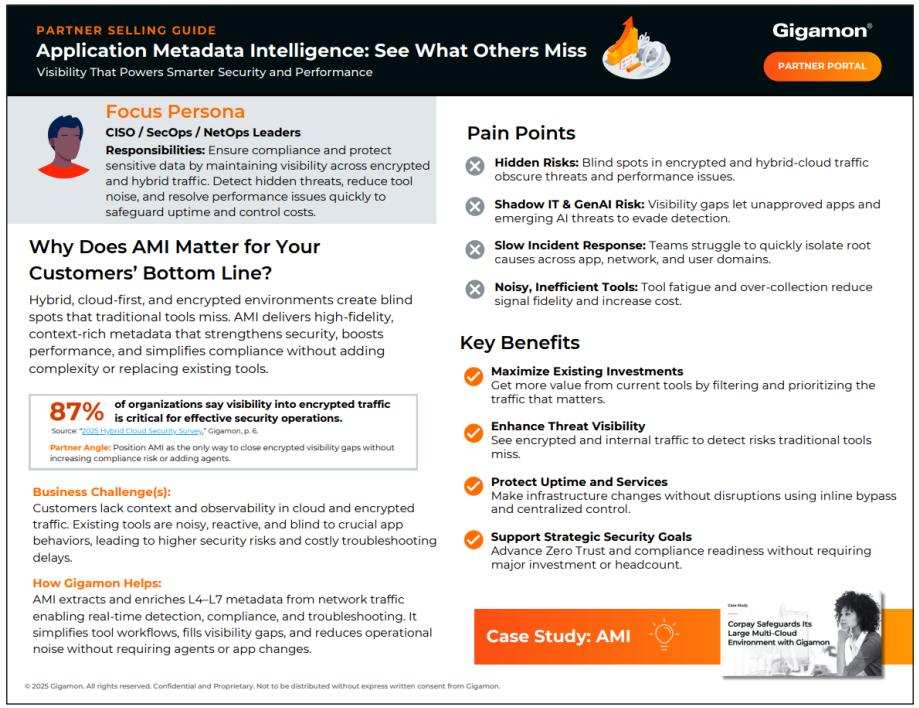
Gigamon®

Application Metadata Intelligence: See What Others Miss

Visibility That Powers Smarter Security and Performance



PARTNER SELLING GUIDE

Application Metadata Intelligence: See What Others Miss

Visibility That Powers Smarter Security and Performance

Gigamon®

PARTNER PORTAL

Focus Persona

CISO / SecOps / NetOps Leaders

Responsibilities: Ensure compliance and protect sensitive data by maintaining visibility across encrypted and hybrid traffic. Detect hidden threats, reduce tool noise, and resolve performance issues quickly to safeguard uptime and control costs.

Why Does AMI Matter for Your Customers' Bottom Line?

Hybrid, cloud-first, and encrypted environments create blind spots that traditional tools miss. AMI delivers high-fidelity, context-rich metadata that strengthens security, boosts performance, and simplifies compliance without adding complexity or replacing existing tools.

87% **of organizations say visibility into encrypted traffic is critical for effective security operations.**

Source: "2025 Hybrid Cloud Security Survey," Gigamon, p. 6.

Partner Angle: Position AMI as the only way to close encrypted visibility gaps without increasing compliance risk or adding agents.

Business Challenge(s):

Customers lack context and observability in cloud and encrypted traffic. Existing tools are noisy, reactive, and blind to crucial app behaviors, leading to higher security risks and costly troubleshooting delays.

How Gigamon Helps:

AMI extracts and enriches L4–L7 metadata from network traffic enabling real-time detection, compliance, and troubleshooting. It simplifies tool workflows, fills visibility gaps, and reduces operational noise without requiring agents or app changes.

Pain Points

- **Hidden Risks:** Blind spots in encrypted and hybrid-cloud traffic obscure threats and performance issues.
- **Shadow IT & GenAI Risk:** Visibility gaps let unapproved apps and emerging AI threats to evade detection.
- **Slow Incident Response:** Teams struggle to quickly isolate root causes across app, network, and user domains.
- **Noisy, Inefficient Tools:** Tool fatigue and over-collection reduce signal fidelity and increase cost.

Key Benefits

- **Maximize Existing Investments**
  Get more value from current tools by filtering and prioritizing the traffic that matters.
- **Enhance Threat Visibility**
  See encrypted and internal traffic to detect risks traditional tools miss.
- **Protect Uptime and Services**
  Make infrastructure changes without disruptions using inline bypass and centralized control.
- **Support Strategic Security Goals**
  Advance Zero Trust and compliance readiness without requiring major investment or headcount.

Case Study: AMI

Case Study

Corpay Safeguards Its Large Multi-Cloud Environment with Gigamon

carahsoft

For more information, contact Carahsoft or our reseller partners:

Gigamon@carahsoft.com | 703-673-3515

PARTNER SELLING GUIDE

Application Metadata Intelligence: See What Others Miss

Visibility That Powers Smarter Security and Performance

Gigamon®

PARTNER PORTAL

Focus Persona

CISO / SecOps / NetOps Leaders

Responsibilities: Ensure compliance and protect sensitive data by maintaining visibility across encrypted and hybrid traffic. Detect hidden threats, reduce tool noise, and resolve performance issues quickly to safeguard uptime and control costs.

Why Does AMI Matter for Your Customers' Bottom Line?

Hybrid, cloud-first, and encrypted environments create blind spots that traditional tools miss. AMI delivers high-fidelity, context-rich metadata that strengthens security, boosts performance, and simplifies compliance without adding complexity or replacing existing tools.

87% **of organizations say visibility into encrypted traffic is critical for effective security operations.**

Source: "2025 Hybrid Cloud Security Survey," Gigamon, p. 6.

Partner Angle: Position AMI as the only way to close encrypted visibility gaps without increasing compliance risk or adding agents.

Business Challenge(s):

Customers lack context and observability in cloud and encrypted traffic. Existing tools are noisy, reactive, and blind to crucial app behaviors, leading to higher security risks and costly troubleshooting delays.

How Gigamon Helps:

AMI extracts and enriches L4–L7 metadata from network traffic enabling real-time detection, compliance, and troubleshooting. It simplifies tool workflows, fills visibility gaps, and reduces operational noise without requiring agents or app changes.

Pain Points

- **Hidden Risks:** Blind spots in encrypted and hybrid-cloud traffic obscure threats and performance issues.
- **Shadow IT & GenAI Risk:** Visibility gaps let unapproved apps and emerging AI threats to evade detection.
- **Slow Incident Response:** Teams struggle to quickly isolate root causes across app, network, and user domains.
- **Noisy, Inefficient Tools:** Tool fatigue and over-collection reduce signal fidelity and increase cost.

Key Benefits

- **Maximize Existing Investments**
  Get more value from current tools by filtering and prioritizing the traffic that matters.
- **Enhance Threat Visibility**
  See encrypted and internal traffic to detect risks traditional tools miss.
- **Protect Uptime and Services**
  Make infrastructure changes without disruptions using inline bypass and centralized control.
- **Support Strategic Security Goals**
  Advance Zero Trust and compliance readiness without requiring major investment or headcount.

Case Study: AMI

Application Metadata Intelligence: See What Others Miss

PARTNER PORTAL

Core Use Cases

Network Detection and Response (NDR)
Turn Encrypted Traffic Into Actionable Intelligence with AMI

Reveals hidden threats in encrypted and East-West traffic, for faster, more confident security decisions — without decryption.

Learn More

Application Performance and Troubleshooting
Protect Revenue Through Application Reliability with AMI

Quickly pinpoints and fix performance issues to safeguard SLAs, user satisfaction, and revenue.

Learn More

Zero Trust
Add Continuous Behavioral Validation with AMI

Continuously monitor application and user behavior to detect misuse, anomalies, and shadow IT that policy alone can't catch.

Learn More

Compliance (PCI, HIPAA, M-21-31)
Simplify Compliance and Reduce Audit Risk with AMI

Automate encryption checks, certificate hygiene, and traffic logging to ensure regulatory readiness without adding operational burden.

Learn More

Discovery Questions:

How confident are you in detecting threats within encrypted or hybrid-cloud traffic?

Gigamon AMI delivers visibility into encrypted and hybrid-cloud traffic, turning hidden activity into actionable intelligence without decryption.

Are you getting the expected ROI and accuracy from your current security and observability tools?

Gigamon AMI enriches your existing tools with high-value metadata, improving accuracy while reducing data ingestion costs.

Objection Handling:

We Already Have Visibility Tools

Objection: "Our SIEM, EDR, and observability tools already give us full visibility."
Response: I understand — those tools are valuable. But they can't see unmanaged devices, east–west traffic, or encrypted flows without breaking encryption. Gigamon AMI feeds those blind spots into your existing stack, improving detection accuracy and maximizing the ROI of tools you've already purchased.

Too Expensive to Add Another Platform

Objection: "Budgets are tight — we can't add another tool right now."
Response: Understood — and that's why AMI isn't about replacing your stack. It makes your current tools smarter by reducing noisy data, improving correlation, and cutting ingestion costs. Many customers offset the investment in AMI through savings on existing licenses and faster incident resolution.

ALLIANCE ECOSYSTEM

Accelerate Growth with AMI Partners

These technology partners strengthen AMI—learn more or reach out to your channel account manager.

- **Splunk**
- **Elastic**
- **Cribl**
- **ExtraHop**
- **Dynatrace**
- **Sumo Logic**
- **New Relic**
- **and more partners!**

GET STARTED

Strategize or Explore A New Opportunity

Connect with your local Gigamon Channel Account Manager and get started.

CONTACT

Gigamon®

Thank you for attending this Gigamon webinar! Carahsoft is the distributor for Gigamon Cybersecurity solutions available via NASA SEWP V, NASPO ValuePoint, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Gigamon's solutions, please check out the following resources and information:

For additional resources:

carah.io/GigamonResources

For additional Gigamon solutions:

carah.io/GigamonSolutions

To purchase, check out the contract vehicles available for procurement:

carah.io/GigamonContracts

For upcoming events:

carah.io/GigamonEvents

For additional Cybersecurity solutions:

carah.io/Cybersecurity

To set up a meeting:

Gigamon@carahsoft.com or 703-673-3515