2025 HYBRID CLOUD SECURITY SURVEY

AI is doubling your network traffic. NOW WHAT?

1 IN 3 organizations report network data volumes have more than doubled in the past two years due to AI.

91% of Security and IT leaders admit they are making trade-offs just to keep up.

AI Broadens the Cyberattack Surface

Ransomware, phishing, and deepfakes are scaling with AI.

46% say defending against AI-generated threats is now their #1 priority.

47% of organizations report an increase in attacks targeting their AI/LLM models.

AI Relies on High-Quality Data

46% of Security and IT leaders lack clean, high-quality data needed to secure AI traffic. That means AI tools underperform and increase risk.

WITHOUT HIGH-QUALITY DATA, THREAT RISK RISES AND THE VALUE OF AI DECLINES.

Visibility Gaps Reduce Tool Effectiveness

1 IN 2 organizations report that their security tools are not as effective as they could be, creating blind spots.

47% lack full visibility into hybrid cloud.

55% say tools fail to detect breaches.

57% prioritize real-time visibility—but don't have it.

Deep Observability Resets the Rules

Combine MELT and network-derived telemetry to get the deep observability you need to eliminate blind spots.

89% of Security and IT leaders say deep observability is essential to hybrid cloud security and AI.

AI changed the game.

GET DEEP OBSERVABILITY

As threats evolve and tools fall short, visibility isn't optional. It's foundational to securing the hybrid cloud.

Get insights from 1,000+ Security and IT leaders. Download the report: GIGAMON.COM/CLOUD-SECURITY-SURVEY

Gigamon®