Gigamon®

Financial Services Industry Insights: The Visibility Imperative in the Age of AI

INDUSTRY SUMMARY

2026 Hybrid Cloud Security Survey

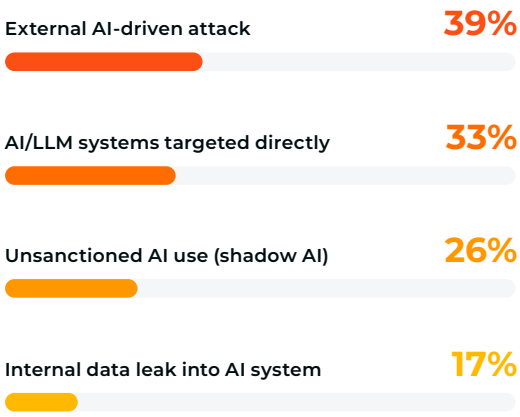
Financial institutions have never invested more in cybersecurity, yet many still struggle to answer a fundamental question: **Can you prove you can see the risks that threaten your business?**

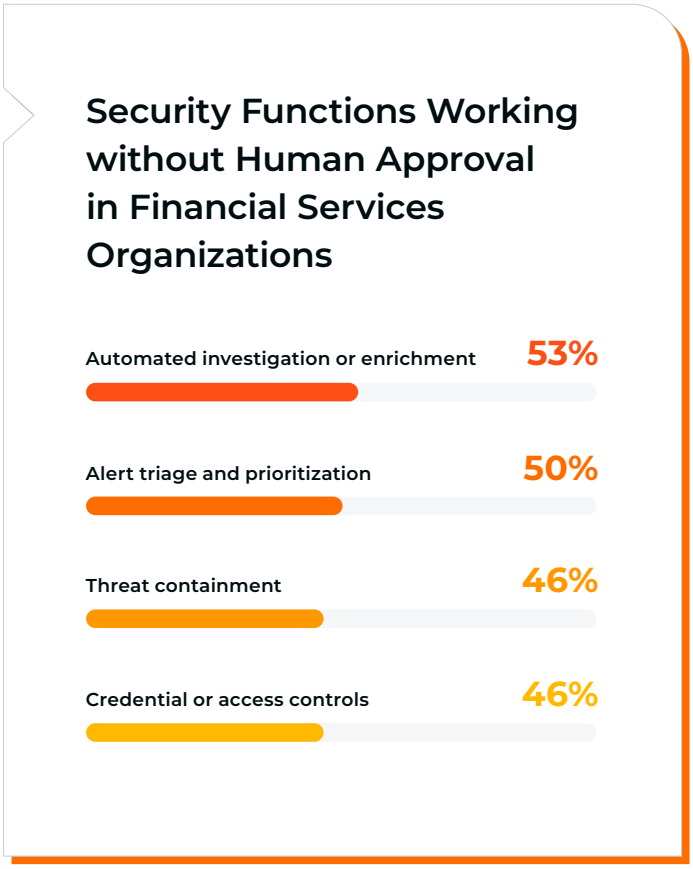
As AI adoption accelerates and hybrid cloud environments become increasingly complex, visibility has emerged as one of the most critical challenges facing financial services organizations. In the **Gigamon 2026 Hybrid Cloud Security Survey**, we surveyed Security and IT leaders in financial services organizations across the globe to better understand their AI adoption, security priorities, and emerging challenges. The results reveal a growing disconnect between perceived security and provable security, one that carries significant implications for operational resilience, regulatory compliance, and financial performance.

While **65 percent** of organizations globally experienced a data breach in the past year, and **83 percent** reported AI involvement in those breaches, financial services leaders are confronting a unique set of challenges. As financial institutions accelerate modernization initiatives and embrace AI to drive efficiency and innovation, concerns around AI-powered attacks, cloud risk, and data exposure continue to rise amid regulatory and compliance demands. Against this backdrop, **more than half** (52 percent) rank AI-powered attacks as one of their top security challenges, reflecting the growing complexity of managing risk in the age of AI.

At the heart of these challenges is a growing gap between perceived security and provable security. As AI reshapes how data moves across hybrid cloud environments, Security and IT leaders are finding that traditional indicators of security maturity do not always translate into clear evidence of control. Visibility is becoming the foundation for understanding, validating, and ultimately managing risk.

AI Security Incidents Span Multiple Risk Categories





With **95 percent** of financial services leaders reporting that security depends on complete visibility across all data in motion, it is clear that visibility is no longer simply a technical capability. In one of the world's most regulated industries, it has become foundational to managing business risk.

AI Adoption is Accelerating Risk Faster in Financial Services

For financial services organizations, cybersecurity failures have consequences that extend beyond technical disruption. They can impact customer trust, operational continuity, regulatory standing, and ultimately financial performance.

At the same time, these organizations are embracing AI at a rapid pace. **More than nine in 10** (91 percent) stated they have introduced automation and AI-powered tools to strengthen data security, while **two-thirds** (66 percent) report that AI-driven automation is already initiating security functions without human interaction, significantly higher than the **53 percent** of global respondents.

This drive toward automation and efficiency is accelerating faster than the broader market, but it also increases the need for visibility and governance. As AI becomes more deeply embedded in security operations, organizations must be able to understand how data moves, how AI systems interact with sensitive information, and whether security controls are performing as intended.

Yet visibility continues to challenge Security and IT teams, with **94 percent** of financial services organizations reporting they have invested in new security technologies to improve detection and visibility, while **42 percent** report it is taking longer to detect breaches. More tools are generating more data, but not necessarily more understanding. As AI, cloud, and encrypted traffic expand the attack surface, organizations are discovering that technology adoption alone does not create security outcomes. The differentiator is the ability to observe, validate, and understand risk across data in motion.

Risk is Increasing Faster Than Visibility

The survey found that financial services organizations are among the most concerned about AI-driven attacks, cloud risk, and data exposure.

Nearly half (47 percent) of financial services organizations reported an increase in attacks targeting their AI/LLM deployments, and **more than half** (54 percent) reported an increase in social engineering attacks, such as smishing and phishing, powered by AI.

These findings reinforce an important reality: security investments alone do not guarantee security outcomes. The effectiveness of any security strategy ultimately depends on the ability to observe how risk develops across data, applications, and infrastructure. As threats increasingly move laterally across hybrid cloud environments and exploit encrypted traffic, organizations need visibility into how data moves and not just where it resides. Without visibility into East-West traffic, encrypted communications, and cloud workloads, attackers can operate undetected for extended periods, increasing both business and financial risk.

Visibility challenges become even more pronounced when encrypted traffic enters the equation. **More than one in three** (36 percent) financial services organizations consider encrypted traffic their biggest risk, while **88 percent** report "harvest now, decrypt later" attacks as a major concern.

As global standards bodies and industry experts warn that encrypted data harvested today may be decrypted in the future as quantum computing capabilities mature, financial services leaders are increasingly focused on long-term exposure. In fact, **93 percent,** more than any other industry we surveyed, say visibility into encrypted traffic is critical to post-quantum cryptography (PQC) readiness.

For financial services organizations, the challenge is no longer limited to what can be seen today. It also includes understanding what could be exposed tomorrow. The combination of encrypted traffic, long-lived financial data, and advancing quantum capabilities is elevating visibility from an operational requirement to a strategic imperative.

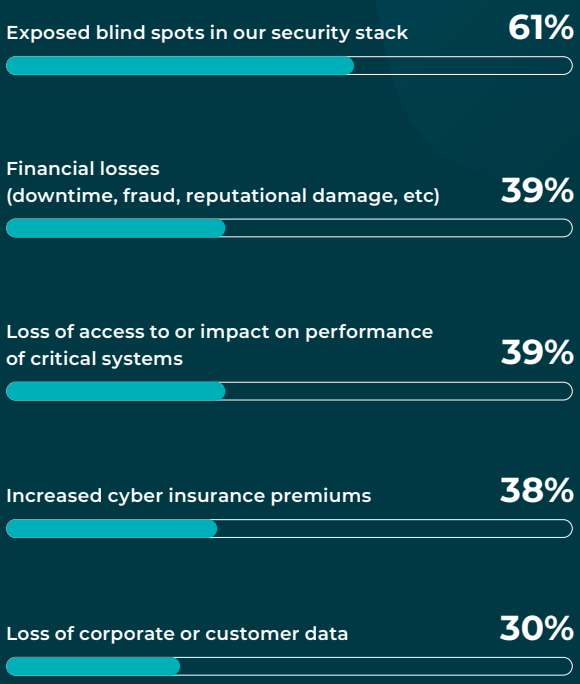
Threat actors are increasingly leveraging encrypted channels and lateral movement techniques to evade traditional security controls. Without comprehensive visibility into all data in motion, organizations are often forced to investigate incidents after damage has occurred rather than identifying risk before it impacts operations.

The findings reinforce a simple reality: organizations cannot effectively manage risks they cannot see, validate, or explain.

Financial services organizations are investing heavily in cybersecurity, but investment alone does not create control. **The findings make it clear that visibility has become foundational to modern cybersecurity.** Without a complete understanding of how data moves across hybrid cloud environments, organizations cannot validate security outcomes, demonstrate compliance, or confidently manage risk.

SHANE BUCKLEY
President and CEO, Gigamon

Impact of Breaches on Financial Services Organizations



Compliance is No Longer a Reporting Exercise

The business consequences of cyber attacks are becoming increasingly difficult to ignore. Among financial services organizations that experienced a breach, **98 percent** reported material impact, including increased cyber insurance premiums, regulatory penalties, operational disruption, and data loss.

At the same time, regulatory expectations continue to evolve beyond documentation and periodic audits. Regulators increasingly expect organizations to demonstrate continuous oversight of risk, operational resilience, and security controls. It is no longer sufficient to document that controls exist. Organizations must be able to demonstrate that those controls are operating effectively across increasingly complex hybrid cloud environments.

Financial institutions face mounting pressure from frameworks such as DORA, PCI DSS, SEC cybersecurity disclosure requirements, and evolving data protection regulations. Security leaders are increasingly concerned that governance and security readiness may not be keeping pace with the rapid adoption of AI and the complexity of modern hybrid cloud environments.

As accountability moves higher within organizations, cybersecurity is becoming a board-level issue. Visibility is no longer simply a security requirement. It is becoming a foundational element of compliance, audit readiness, governance, and the ability to provide evidence that risk is being managed effectively.

Shifting Data Strategies in Financial Services

Financial services organizations have historically been among the early adopters of technologies that improve speed, scale, and operational efficiency. Today, many are reassessing where AI data should reside and how it should be secured.

Public cloud environments are considered riskier for AI deployments by **84 percent** of financial services leaders, reflecting growing concerns about data exposure, intellectual property protection, and operational control. As AI workloads expand, financial organizations are reassessing where sensitive data should reside and whether visibility and governance can keep pace in increasingly distributed environments.

As a result, many leaders are considering data lakes as an alternative. **Nearly two-thirds** (62 percent) believe data lakes represent the most secure environment for critical data. Confidence grows even further when network-derived telemetry is used to enrich visibility across data in motion. In fact, **94 percent** of financial services organizations believe network-derived telemetry improves the security of their data lakes.

Network-derived telemetry, in the form of metadata, packets, and flows, complements metrics, events, logs, and traces (MELT) data to provide a more complete understanding of data in motion. Together, these insights help security teams connect previously fragmented views of activity, improving their ability to investigate threats, validate controls, and understand how risk develops across hybrid cloud environments. The result is deep observability, providing the context needed to transform disconnected signals into a coherent, actionable understanding of risk.

Financial services leaders agree. **More than 90 percent** of these organizations say deep observability is foundational to securing their AI deployments. Deep observability helps organizations understand how data moves across systems, observe how AI systems interact with that data, and identify threats as they emerge.

Single Biggest Risk for Financial Services Leaders Ranked

1. Public Cloud
2. Private AI/LLM Environments
3. Lateral (East-West) Traffic
4. Encrypted Traffic
5. Data Lakes/Private Cloud/OT and IoT Environments

Performance, Efficiency, and Security Must Work Together

Financial institutions operate in environments where performance matters. Whether supporting customer transactions, digital banking platforms, payment processing systems, or trading operations, delays and inefficiencies can have direct business consequences.

Yet many organizations continue to address emerging threats by adding more tools, creating increasingly disparate security architectures. This is particularly challenging for financial services, where **more than half** (52 percent) of the leaders cited fragmented security tools as their biggest challenge in securing their hybrid cloud infrastructure.

More tools often generate more data, but not necessarily more understanding. When visibility is fragmented across platforms, teams can see individual events but struggle to understand how they connect, making it harder to identify threats, investigate incidents, and make informed decisions.

The issue is not a lack of data. It is a lack of context that allows organizations to connect individual signals into a complete picture of risk.

Security leaders increasingly recognize that complete visibility across data in motion is essential to improving security outcomes because it provides the context needed to transform data into actionable insight. By enriching existing security, observability, and operational tools with network-derived telemetry, organizations can reduce complexity, improve incident response, accelerate troubleshooting, and gain greater value from existing investments.

Top Challenges for Today's Financial Services Security and IT Leaders Ranked

1. **Fragmented security tools**
2. **Visibility gaps**
3. **Shortage of cloud security expertise**

From Security Confidence to Security Proof

Financial services organizations operate in one of the world's most highly regulated and frequently targeted industries. As AI transforms how applications, users, and data interact, leaders need more than additional tools and alerts, they need evidence.

Organizations that can observe how data moves across hybrid cloud environments, identify threats hidden within encrypted traffic, and validate security outcomes through deep observability will be better positioned to reduce risk, strengthen compliance, and maintain operational resilience.

Today's financial services organizations recognize the growing challenge of validating security in increasingly complex environments. Their focus on visibility, encrypted traffic inspection, AI governance, and post-quantum readiness reflects a broader shift from relying on assumptions toward building security strategies grounded in evidence.

In an industry where trust is the foundation of every transaction, visibility has become more than a security capability. It has become the foundation for proving that systems are secure, controls are effective, and risk is being managed with confidence.

Methodology

The data presented in this report was compiled by Vitreous World. Fieldwork was conducted using an online methodology, recruiting a mix of Chief Information Officers, Chief Information Security Officers, Chief Technology Officers, Chief Risk Officers and those working in information technology, cybersecurity or security operations, information security and other technology roles were recruited. Interviews were conducted across Australia, France, Germany, Singapore, the UK and the USA. All 1,023 respondents, of which 139 are in the financial services industry, were guaranteed to remain anonymous as part of the study. Fieldwork was carried out between February 16-17, 2026.

About Gigamon

Gigamon® protects the hybrid cloud networks and data of the world's most complex organizations. The AI-powered Gigamon Deep Observability Pipeline delivers complete visibility into all data in motion by providing trusted, network-derived telemetry directly to cloud, security, and observability tools. With AI driven insights across packets, flows, and application metadata, organizations can detect threats concealed in encrypted and lateral traffic, resolve network and application performance bottlenecks, and validate compliance while reducing cost and complexity. Gigamon is trusted by over 4,000 organizations worldwide, including 83 of the Fortune 100, major mobile network operators, and public sector agencies at every level. Learn more at gigamon.com.

Download the report at
gigamon.com/2026-cloud-security

Gigamon®

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

06.26_01