Gigamon®

# CISO Empowerment in the Age of AI Risk

CISO INSIGHTS

## 2026 Hybrid Cloud Security Survey

## Introduction

AI is rapidly reshaping how organizations operate, compete, and innovate. As adoption accelerates, risk is increasing just as quickly. In many cases, it is outpacing the ability to measure, validate, and mitigate it.

For CISOs, this creates a defining challenge. They are responsible for securing environments that are more distributed, more dynamic, and more difficult to observe. Hybrid cloud architectures, decentralized AI usage, and encrypted data flows have changed how risk develops and how it must be managed.

This is not just a technology issue. It is a visibility and proof issue.

The scale of this challenge is clear. In the past 12 months, **83 percent** of global organizations reported AI-related security incidents. These included external attacks involving AI at **41 percent**, internal leaks at **30 percent,** unsanctioned use of AI at **30 percent**, and direct attacks on AI or LLM systems at **33 percent**.

At the same time, many CISOs still lack the visibility needed to respond with confidence. **Nearly half** say it is taking longer to detect breaches, while **46 percent** report that AI-driven traffic is making breaches harder to identify and investigate.

CISOs are being held accountable for risk they cannot fully see and cannot fully prove. In that environment, visibility becomes a source of empowerment. It gives CISOs the clarity to act decisively, the evidence to communicate credibly, and the confidence to lead with authority.

This perspective is based on insights from **307 CISOs** who participated in the **2026 Hybrid Cloud Security Survey**, reflecting the experience of security leaders across the globe operating at the front lines of AI-driven risk.

## Accountability Without Proof

AI and hybrid cloud adoption have fundamentally changed how data moves. Applications now span environments. Workloads shift constantly. Traffic is encrypted by default. Systems interact in ways that are difficult to trace using traditional approaches.

Visibility gaps driven by cloud complexity are now the **top challenge** CISOs face. They see how risk develops within East-West traffic, across hybrid cloud environments, and inside AI-driven processes. They know that governance models, data security controls, and AI-specific skills are not keeping pace with how quickly these environments are evolving.

But awareness is not the same as proof.

Without a consistent view of data in motion, security teams lack the ability to validate what is happening across their environment. They cannot reliably detect threats within encrypted or lateral traffic. They cannot always establish clear root cause. And they cannot consistently provide evidence to support reporting and decision making.

This creates a structural imbalance. CISOs are expected to answer critical questions without always having the data required to answer with confidence.

### CISOs View Challenges Differently, Focusing on Structural and Operational Weaknesses

| CISO | CHALLENGES | ALL OTHER RESPONDENTS |
|---|---|---|
| 1 | Visibility gaps due to cloud complexity | 2 |
| 2 | Shortage of cloud security expertise | 3 |
| 3 | Fragmented security tools | 5 |
| 4 | Complexity driven by AI adoption | 4 |
| 5 | Increase in AI-driven attacks | 1 |

## A Perception Gap That Elevates Risk

While CISOs recognize these limitations, the broader business often sees a different picture. **Nearly 40 percent** of organizations report that they operate at an integrated level of AI security maturity. **Sixty percent** believe their data governance frameworks are robust and well established. On the surface, this suggests confidence and control.

The underlying data tells a different story.

The percentage of organizations experiencing a data breach has risen from **47 percent** in 2024[1] to **65 percent** in 2026. Insider threats are increasing. AI is now involved in most incidents. Visibility gaps remain across hybrid environments.

This disconnect between perception and reality is widening.

**Nearly half** of C-level executives surveyed believe the root cause of security incidents can be identified within 72 hours. In contrast, only **about one-quarter** (27 percent) of CISOs agree, with **nearly half** reporting that identification actually takes up to seven days. CISOs report a slower and more complex reality, with another **23 percent** reporting it can take up to 30 days to determine root cause or restore operations, compared with just **8 percent** of other C-suite executives.

CISOs, working directly with incident data, understand the time and complexity involved in tracing activity across systems. Other executives often rely on summarized reporting that does not reflect that same level of detail. The result is a more optimistic view of performance than the underlying reality supports.

This gap has consequences. When organizations believe they are recovering faster and more completely than they are, they are more likely to reinforce existing approaches rather than address root causes.

Visibility challenges make this worse. Over **a third** of CISOs identify East-West traffic as the area of greatest risk. Among other C-level executives, that figure drops to **26 percent**, reinforcing the gap between those closest to the data and those relying on summarized views. This traffic often remains encrypted and is currently under-monitored. It is also where attackers can persist and where insider threats can spread.

The same issue applies to AI. **Three in four** CISOs (76 percent) say limited visibility into AI-driven traffic is a major barrier, allowing AI adoption to outpace their organization's ability to secure data. As AI becomes more embedded in operations, the inability to observe how it interacts with data creates further uncertainty.

## Biggest Breach Risk Across Infrastructure

RANKED IN ORDER OF CISO'S CONCERNS

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

## Why More Tools Are Not Solving the Problem

In the 2025 survey[2], **nearly half** (46 percent) of CISOs identified tool fragmentation and integration challenges as their biggest area of compromise. In response, organizations continue to invest in security technologies to address rising threats, with **9 in 10** CISOs (93 percent) reporting they've deployed new tools to improve detection and visibility over the past year. Yet breaches have increased by **18 percent** year over year.

This reflects a deeper issue. Security tools depend on the quality and completeness of the data they consume. When telemetry is fragmented across environments, when visibility into encrypted traffic is limited, and when data sources lack consistency, even advanced tools cannot deliver reliable outcomes.

Many organizations fall into a familiar cycle. A breach exposes a gap. New tools are deployed. Visibility remains incomplete. Yet the same issues return in future incidents.

Breaking this cycle requires a shift in focus. The priority is not adding more tools. It is improving the visibility and integrity of the data that supports them.

## Rising Stakes for the CISO

As risk increases, so does accountability. It is also becoming more personal.

More than **one in four** CISOs are concerned about losing their job following a serious incident. This reflects the growing expectation that security leaders can explain what happened, why it happened, and how it will be prevented going forward.

Regulatory pressure is also increasing. In the United States, SEC cybersecurity disclosure rules have raised expectations for timely and accurate reporting. In Europe, NIS2 expands accountability to management bodies, including CISOs. Similar trends are emerging across the Asia-Pacific region, where frameworks emphasize due diligence and board-level responsibility.

Cybersecurity is now treated as a governance issue, not just a technical one.

CISOs also face a set of persistent challenges, including securing data across public cloud environments, closing the AI-related skills gaps, managing unsanctioned AI use, gaining visibility into East-West traffic, and supporting teams under increasing pressure.

Each of these challenges ties back to a common issue. Organizations lack a clear understanding of how data moves, how AI is used, and where risk develops.

**80 percent** of CISOs say that inadequate corporate governance around unsanctioned use of AI presents the top challenge to securing data today. To address this concern, **41 percent** put corporate governance at the top of their security priorities list.

## What CISO Empowerment Actually Requires

If accountability continues to rise, empowerment must rise with it. For CISOs, empowerment means having clear, reliable visibility into how data moves, how AI is used, and where risk develops  along with the authority and resources to act on that insight.

**CISOs identify three capabilities as most critical to their success:**

- Access to accurate network-derived telemetry
- Comprehensive visibility into all data in motion
- Sufficient resources to scale teams and operations

CISOs are already taking action. **Nearly half** (47 percent) plan to use AI-powered tools to augment their teams and workflows, while **43 percent** are strengthening governance to ensure AI is used safely and appropriately. At the same time, **45 percent** are prioritizing improved visibility into AI-drive data flows across hybrid cloud environments.

Together, these priorities point to a shift toward deep observability.


Deep observability brings together network-derived telemetry, including metadata, packets, and flows, with metrics, events, logs, and traces (MELT) data. This creates a unified view of data in motion across hybrid cloud environments and provides the context needed to understand how systems interact and how risk develops. It also enables CISOs to align security decisions with business outcomes, improving the speed, accuracy, and credibility of risk reporting at the executive level.

With this level of visibility, CISOs can move beyond fragmented insight toward a more complete understanding of their environment.

They can detect threats earlier and with greater precision. They can trace activity across systems to establish root cause. They can validate the effectiveness of controls and identify gaps before they lead to incidents. And they can support reporting with clear, defensible evidence.

This changes how security operates. It replaces assumptions with observable data. It allows decisions to be guided by evidence rather than inference.

It also strengthens the role of AI. When visibility is incomplete, AI can reinforce gaps and create a false sense of confidence. When visibility is strong, AI can enhance detection, accelerate analysis, and improve decision making.

Empowerment, in this context, comes from clarity.

## Redefining the CISO Role

Greater visibility does more than improve operations. It changes how CISOs lead.

**Seven in 10** CISOs say a lack of board-level understanding is a major barrier to securing AI adoption. Bridging this gap requires more than technical expertise. It requires the ability to communicate risk in a way that aligns with business priorities.

When CISOs have access to clear, reliable data, they are better positioned to align security with business outcomes. CISOs also point to improved reporting as the most important step in strengthening alignment with the board, helping translate technical risk into clear business impact. When they can explain risk in concrete terms, CISOs can demonstrate the value of security investments and build trust as strategic advisors.

As AI becomes more central to how organizations operate, this shift is essential. Security must be integrated into broader business decision making, not treated as a separate function.

## From Visibility to Confidence

The challenge facing CISOs is not a lack of investment, but a lack of clarity.

As AI accelerates risk, perception gaps continue to widen and accountability increases. Yet without a consistent way to observe and validate what is happening across hybrid cloud environments, organizations remain exposed.

Progress will not come from deploying more tools. It will come from achieving deep observability, establishing a consistent and comprehensive view of data in motion across their environment.

When CISOs can see how data moves, how systems interact, and where risk develops, they gain more than visibility. They gain proof.

And with proof comes the confidence, not just to respond to risk, but to explain it, guide the business, and lead with authority. This is what empowers CISOs to meet the demands of an AI-driven world.

### How CISOs Can Strengthen the CISO-Board Relationship

1. **Improving board-level reporting by demonstrating security alignment with business outcomes**
2. **Ensuring cybersecurity is a critical element on the board's risk agenda**
3. **Support for CISOs when it comes to responsibility and accountability for security posture**
4. **Establish agreed criteria for disclosure and accountability should a breach occur**
5. **Establish regular CISO-board meetings to discuss risk and strategy**

## 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

1 Gigamon, 2024, Hybrid Cloud Security Survey: Closing the Cybersecurity Preparedness Gap

2 Gigamon, 2025, Hybrid Cloud Security Survey: Evolving Hybrid Cloud Security in the Age of AI

Gigamon®

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



04.26_01