Gigamon®

2025 Hybrid Cloud Security Survey

RISK RECALIBRATION

Evolving Hybrid Cloud Security in the Age of AI

3 Introduction

4 Key Learnings

6 Methodology

6 A System Under Strain

8 AI Disruption
A New Class of Security Challenge

11 From Acceptable to Unacceptable Risk
Rethinking the Cloud

12 The CISO Perspective
Visibility is the First Line of Defense

14 The Path Forward
Deep Observability as a Strategic Reset

Introduction

From driving agility and scalability to enabling smarter, faster decision-making, cloud and artificial intelligence (AI) technologies continue to deliver business value at a pace few innovations can match. Global investment in AI is expected to grow beyond $300 billion in 2025, reaching $750 billion by 2028. This momentum shows no sign of slowing down. However, as adoption accelerates, so does the need to reassess how these innovations are secured and managed.

AI offers undeniable value, yet scaling it demands a deeper understanding of the risks—and a proactive approach to managing them. The shift toward hybrid cloud remains at the foundation of enabling these transformations. Increasingly, organizations rely on public cloud to enable the performance and flexibility needed to power AI workloads while turning to private cloud to deliver security and control. For many, these benefits still outweigh the risks, but those risks are becoming harder to ignore, and the trade-offs more difficult to manage.

Nearly all (**9-of-10**) Security and IT leaders are being forced to make unprecedented compromises when it comes to securing and managing their hybrid cloud infrastructure, often without the authority, visibility, or data quality needed to define what “acceptable risk” really means. In the 2024 Gigamon Hybrid Cloud Security report, we saw signs of growing tension between cloud-driven acceleration and security readiness. This year, that tension has reached a new level. The security cracks across hybrid cloud infrastructure are widening just as the AI wave hits, and without the right visibility, intelligence, and tooling in place, those cracks can quickly shift toward critical points of failure. It is time to redefine visibility, reassess risk, and reclaim control.

This year we surveyed over 1,000 Security and IT leaders across the globe to understand how AI is impacting hybrid cloud security. While many see AI as a path to efficiency, most also recognize it as a powerful accelerator of cyber risk—one that is reshaping their priorities and exposing new vulnerabilities.

This year's survey reveals a hybrid cloud environment under growing pressure, while an AI-driven future is advancing faster than today's cybersecurity strategies can keep pace. Breach rates have risen from **47 percent** to **55 percent** year-over-year. That represents a **17 percent** increase and highlights why many Security and IT leaders say their current security tools are failing to detect intrusions. Visibility remains inconsistent, with nearly half of surveyed organizations (**47 percent**) still lacking comprehensive insight across their environments, including lateral East-West traffic. This gap continues to outpace concerns around traditional North-South monitoring. And while AI holds the promise of transformation, it also introduces new traffic patterns, threat vectors, and data complexities that existing tools—and teams—aren't prepared to handle.

Acceptable security risk is evolving in real time, as compromises must be made to accommodate these challenges. As organizations race to deploy AI, they are leaning heavily on the cloud to support these dynamic and compute-intensive workloads; but with that comes more complexity and exposure. Not surprisingly, **1-in-3** organizations report that network data volumes have more than doubled in the past two years due to AI, and nearly half say they have seen a rise in attacks targeting large language models (LLMs). The emergence of open-source LLMs further exacerbates data concerns, potentially exposing sensitive information and presenting data exfiltration risks. Meanwhile, **46 percent** of Security and IT leaders reveal they lack clean, high-quality data to support secure AI workload deployment, hindering many organizations from fully capitalizing on the innovation that AI promises.

Security and IT leaders overwhelmingly agree that visibility gaps remain at the core of their cybersecurity challenges. As a result, deep observability—combining metric, event, log, and trace (MELT) data with network-derived telemetry, including packets, flows, and metadata—has become essential to bringing the complete risk picture sharply into focus. With **88 percent** of Security and IT leaders agreeing it is critical for securing AI deployments, deep observability is becoming the foundation for recalibrating risk and regaining control in a rapidly evolving environment.

Key Learnings

1. **Organizations are losing ground to rising threats**

   Breach rates, accelerated by AI, are on the rise. More than half (**55 percent**) of organizations report they have experienced a breach in the past 12 months. Nearly half (**47 percent**) acknowledge their current security tools are falling short in effectively detecting breaches. Compounding this challenge, **91 percent** of Security and IT leaders and **97 percent** of CISOs admit to making compromises in securing their hybrid cloud infrastructure. These compromises range from visibility across environments to data quality and tool integration, highlighting continued trade-offs in foundational areas of security.

2. **Visibility and data integrity remain the most critical and most compromised capabilities**

   Nearly half (**47 percent**) of organizations cite a lack of comprehensive visibility across their entire IT infrastructure, including lateral East-West traffic, both on-prem and in the cloud, as a top compromise. This is closely followed by **46 percent** who reveal they lack clean, high-quality data to support the deployment of new workloads, including AI. Without visibility or data integrity, organizations are flying blind in a rapidly evolving threat landscape.

3 AI is overwhelming infrastructure, and adversaries are taking advantage

Data volumes are increasing, with **1-in-3** organizations reporting their network data volumes have more than doubled over the past two years, driven by AI's strain on existing systems. This surge in data also provides attackers with more opportunities to hide large data exfiltration activities within the AI-generated noise. Nearly half (**47 percent**) of organizations report an increase in attacks specifically targeting their large language models (LLMs), while **58 percent** are seeing a rise in AI-powered attacks. As attackers grow more agile, defenders are stuck working with conventional tools, fragmented environments, and limited intelligence, resulting in nearly half of Security and IT leaders (**46 percent**) reporting that managing AI-generated threats is now their top security priority.

4 Public cloud risk perception is rising

Once regarded as a technological advantage, public cloud is now increasingly viewed as a potential risk. More than two-thirds of Security and IT leaders (**70 percent**) agree the public cloud represents a greater security risk than any other environment. Concerns around governance, data integrity, and intellectual property are prompting many organizations to reconsider their reliance on public cloud platforms, especially for AI workloads, and to reassess their public cloud security measures.

5 New technologies are reshaping the security stack

As AI-driven complexity grows, organizations are evolving their tooling strategies to meet new demands. Security and IT leaders are embracing technologies like deep observability and quantum-resistant cryptography to stay ahead of emerging threats. In fact, **73 percent** say they are preparing to implement post-quantum or quantum-resistant cryptography, reflecting a shift towards strategic investment over patchwork fixes. While **47 percent** of Security and IT leaders say their current tools could be more effective, many are looking ahead with a focus on targeted technologies built to handle the scale and complexity introduced by AI and quantum.

6 CISOs want to shape the risk agenda, not just absorb the consequences

More than one-third of CISOs (**36 percent**) are seeking greater influence over AI and security-related business decisions. As risk accelerates, many are held accountable without authority, visibility, or resources. This highlights the urgent need for CISOs to lead rather than react.

7 Real-time visibility is a top priority moving forward

Looking ahead, **64 percent** of respondents report their number one focus for the next 12 months is real-time threat monitoring and visibility across all data in motion. In an increasingly complex world, proactive security starts with gaining complete visibility and understanding of all activities across hybrid cloud infrastructure.

Methodology

The data used within this report was collated by Vitreous World, which adopted an online methodology and recruited a mix of CIOs, CISOs, CTOs, CROs and those working in Information Technology, Cybersecurity or Security Operations, Information Security and other technology roles. Interviews were conducted in Australia, France, Germany, Singapore, UK, and USA. Now in its third year, the research enables year-over-year analysis of how security priorities, perceptions, and challenges are evolving.

All respondents were guaranteed to remain anonymous as part of the study. Fieldwork was carried out between February 21–March 7, 2025.

A System Under Strain: What the Year-Over-Year Trends Tell Us

In 2023, our Hybrid Cloud Security survey uncovered a growing disconnect between confidence and control. Many organizations believed their hybrid cloud environments were secure, but visibility gaps, tooling limitations, and a continued lack of lateral East-West traffic insight painted a different picture. In 2024, we further examined their state of preparedness and found that while confidence remained high, visibility gaps persisted, with **1-in-3** breaches going undetected with current tooling.

Now, in 2025, that system is showing signs of real strain. Security and IT leaders are navigating environments that are even more complex, even more fragmented, and even less visible. Advances in toolsets are simply not keeping pace, with **1-in-2** leaders saying their tools are not as effective as they could be when it comes to detecting breaches. And nearly half (**47 percent**) still lack comprehensive visibility across their hybrid cloud environments—an issue that persists and is unchanged from last year.

1,021 Respondents

58% Work for companies with **between 501 and 1,000 employees**

42% Work for companies with **more than 1,000 employees**

60% **Senior management** (C-Suite, C-Level)

40% **Middle management** (Vice President, Director, Department Head, Senior Manager)

600+ Senior Management Respondents

39% **Chief Technology Officer**

35% **Chief Information Security Officer**

24% **Chief Information Officer**

2% **Chief Risk Officer**

161 Australia

200 France

150 Germany

160 Singapore

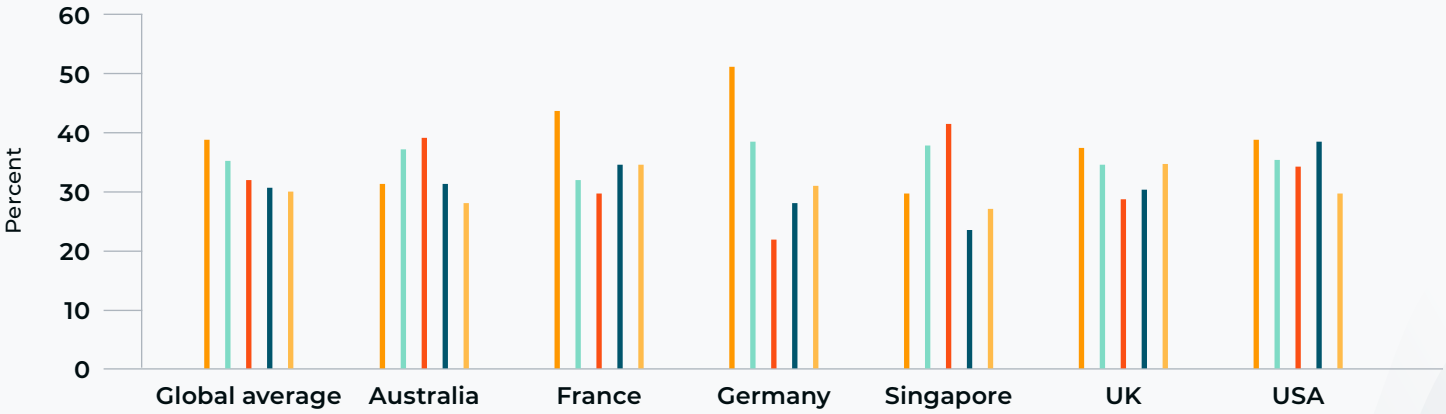
150 UK

200 USA

Compromises have become normalized. This year, **91 percent** of Security and IT leaders and **97 percent** of CISOs say they have had to make compromises in how they secure and manage their hybrid cloud infrastructure. Nearly half of respondents report lacking clean, high-quality data to support secure AI workload deployment. Just as many point to not having complete visibility, especially into lateral East-West traffic, as a capability they have had to sacrifice.

Once hailed as the engine of agility, the public cloud is now viewed by **70 percent** of respondents as the riskiest part of their infrastructure—a stark shift from the optimism that accompanied the relatively easy migration of applications just a few years ago. Concerns over governance, blind spots in encrypted traffic, and inconsistent lateral visibility are prompting a reassessment of where risk truly resides and how it should be mitigated and managed. The challenges associated with securing and managing hybrid cloud environments are not stabilizing, they are escalating. As AI adoption accelerates and infrastructure becomes harder to manage, long-standing gaps in visibility and control are being exposed. What once powered transformation is now testing its limits.

In what areas do you feel you are making compromises when it comes to securing your IT infrastructure?



- Public cloud security
- Attaining deep observability across my hybrid cloud infrastructure for all data in motion
- Securing the exponential growth of OT/IoT devices
- Having too many tools that are poorly integrated
- Lack of corporate governance surrounding AI adoption (shadow AI/IT)

CISO PERSPECTIVE

CISOs are facing heightened tension between AI innovation and security readiness. Attacks are on the rise, with **44 percent** of CISOs seeing an increase in attacks targeting their AI/LLM deployments. As a result, **86 percent** of CISOs are placing greater emphasis on having access to packet-level data and rich application metadata to unlock deeper insights and strengthen their security posture.

AI Disruption: A New Class of Security Challenge

AI is having a significant impact on hybrid cloud infrastructure, driving exponential growth in data volumes and elevating the complexity of both enabled and targeted cyberattacks.

It is also revealing where organizations are still falling short: visibility, tooling, and threat readiness. The core issue is that the infrastructure supporting AI and hybrid cloud is being overlooked, exposing vulnerabilities that threat actors can exploit. Boards are pushing for AI adoption, but the necessary conversations about how to support and secure all infrastructure layers that interact with, and host AI models, is not happening yet.

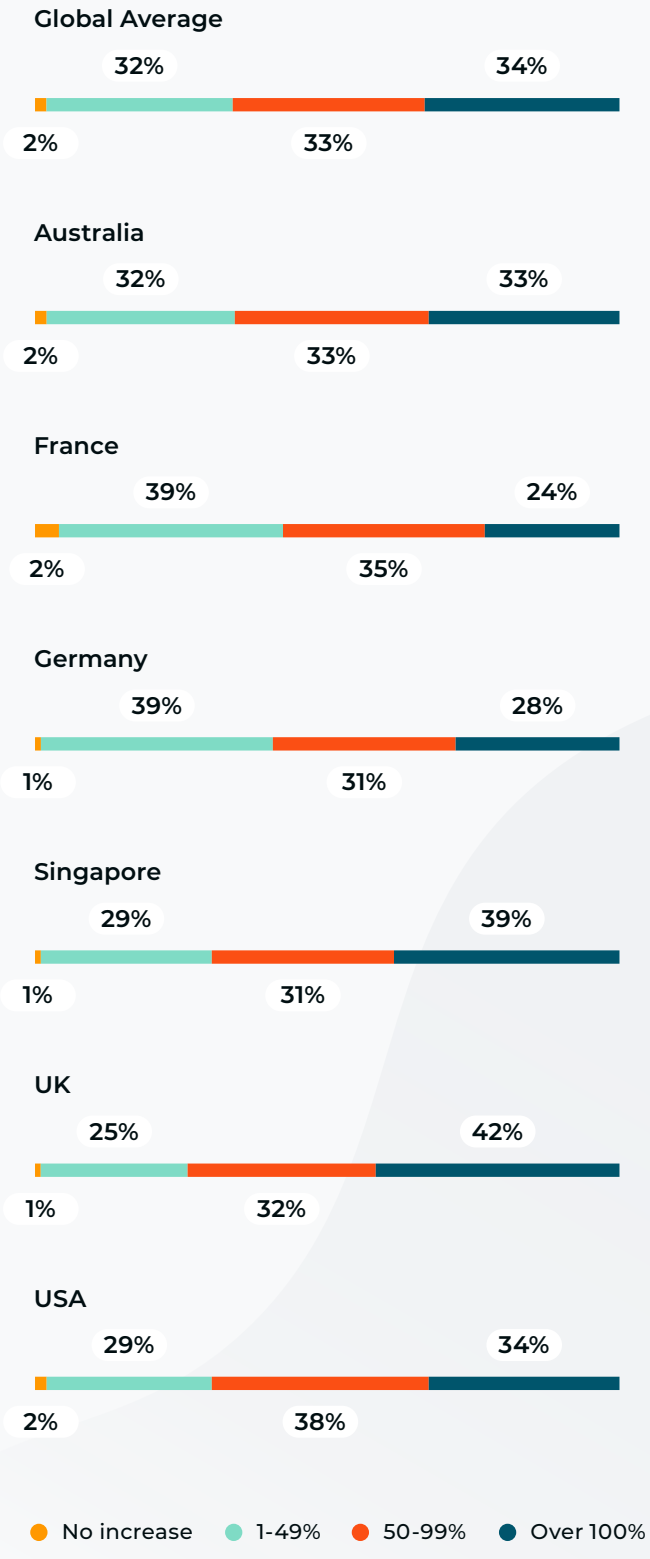
DATA VOLUME EXPLOSION

AI is pushing data volumes to—and at times beyond—new limits. Network data volumes have doubled over the past two years due to AI, according to **1-in-3** organizations. Tool-to-tool traffic is surging and overloading monitoring systems, while **46 percent** say they lack clean, high-quality data to support the deployment of new AI workloads. This problem undermines both threat detection and model accuracy.

These issues are not new, but they are rapidly accelerating. In 2024, visibility into lateral East-West traffic dropped from **48 to 40 percent** of respondents reporting a lack of visibility, underscoring that many organizations were already struggling to monitor lateral movement. With AI increasing both traffic volume and complexity, that gap has widened.

Encrypted traffic poses a significant challenge. In 2025, **55 percent** of organizations say it is less likely to be inspected—rising to **64 percent** in the USA and falling to **47 percent** in Germany. Decryption is often avoided due to time or cost, with **43 percent** citing these barriers, especially in Australia (**51 percent**) and the USA (**49 percent**). As AI drives up traffic volumes and reliance on encrypted communications between tools and services increases, inspection blind spots are fast becoming operational risks. Without clean, observable data, both AI and security performance will suffer.

How much has the volume of network data that tools monitor increased because of AI in the past 2 years?



TOOL SATURATION AND INTEGRATION STRAIN

The instinct to add new tools in response to complexity is understandable, but for many, it is having the opposite effect. More tools often mean more fragmentation, not more control.

Most deploy multiple security tools across public cloud, private cloud, and on-prem environments, with respondents reporting an average of 15 security tools in use. And while **83 percent** of leaders express confidence in their current toolsets, over half (**55 percent**) admit those tools are not as effective at detecting breaches as they could be due to limited visibility. Instead of improving performance, this growing stack often creates more noise, more fragmentation, and more blind spots. Nearly half (**47 percent**) of respondents say they are compromising on tools that integrate effectively across on-prem, public, and private cloud environments, including virtualized and container environments. The core issue remains, tools designed for a pre-AI era are struggling to keep pace with the scale, speed, and sophistication AI introduces.

ADVERSARIAL AI AND THREAT EVOLUTION

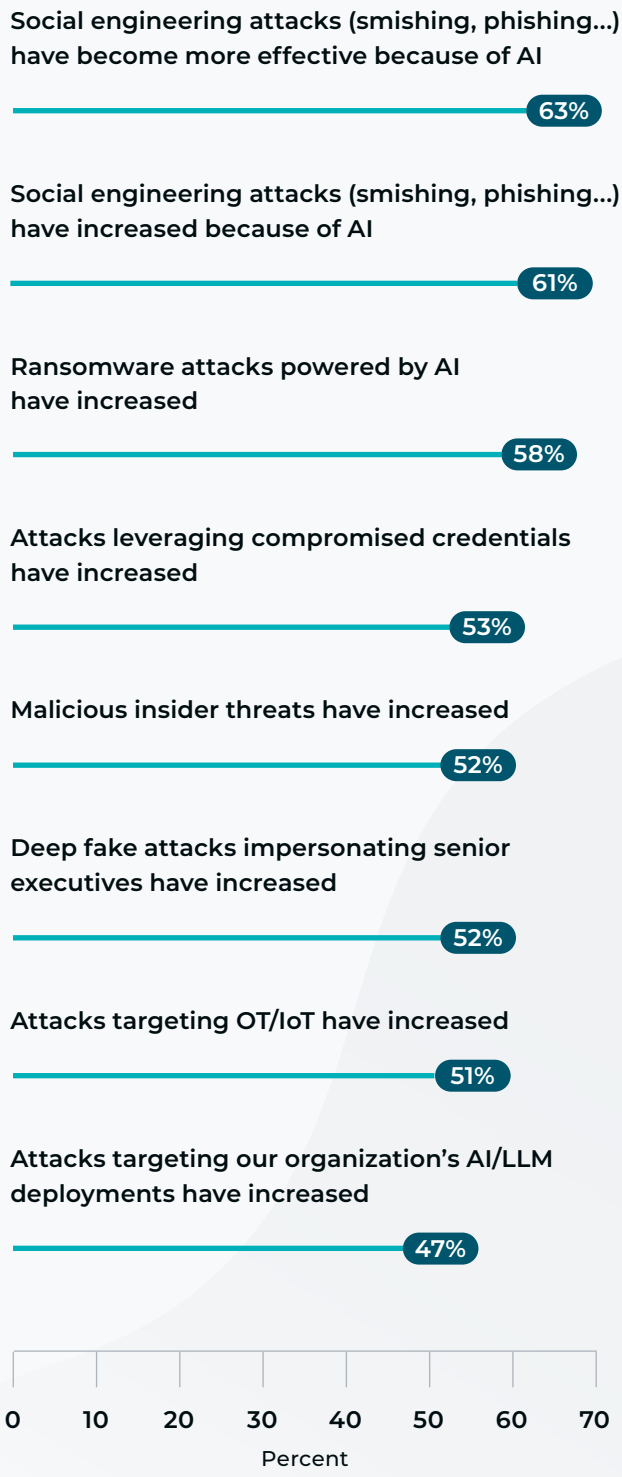
Adversarial AI is reshaping the threat landscape, giving attackers new ways to hone and scale their tactics. Last year, government agencies warned that AI will "almost certainly" increase both the volume and impact of attacks in the next two years. Unfortunately, that prediction is already playing out.

This year's results are sobering. Nearly half of organizations (**47 percent**) report an increase in attacks targeting their large language models (LLMs). Phishing and smishing attacks are becoming more convincing, and more common, with **61 percent** reporting a rise in volume and **63 percent** a rise in effectiveness. Meanwhile, **58 percent** say they have seen a surge in AI-powered ransomware—up from **41 percent** in 2024. Deepfake-based attacks are also increasing, with **52 percent** of respondents reporting exposure this year, compared to **40 percent** last year.

Regionally, concern around ransomware is highest in the USA and Australia. Deepfakes follow a similar pattern: UK (**56 percent**), USA (**56 percent**), and Australia (**55 percent**) report the highest exposure.

GLOBAL AVERAGES

Which of these threats is your organization seeing an increase in volume or effectiveness?



QUANTUM COMPUTING: A POTENTIAL PATH FORWARD

The emergence of quantum computing will drastically accelerate the risks posed by AI. It will allow malicious actors to break encrypted data far more quickly, introducing a dangerous blind spot into environments that are already under pressure.

Government agencies have issued clear and very specific guidance. The UK's National Cyber Security Centre (NCSC) has published migration timelines for post-quantum cryptography, urging organizations to begin preparing now to avoid rushed decisions later. Meanwhile, in the USA, the National Institute of Standards and Technology (NIST) has finalized a set of post-quantum encryption standards, marking a major milestone in the global shift toward quantum-resistant security. With **73 percent** of organizations in this year's survey reporting they are preparing to implement Post-Quantum Cryptography or Quantum-Resistant Cryptography, it is clear this threat is no longer hypothetical—it is on the horizon and is very real.

CISO PERSPECTIVE

For CISOs, the shift isn't just about where data lives—it's about who owns the risk. With **75 percent** now rating public cloud as the highest-risk environment, and **73 percent** re-evaluating cloud strategies and considering repatriating workloads back to private environments, CISOs are regaining control by deliberately positioning themselves at the center of risk governance.

From Acceptable to Unacceptable Risk: Rethinking the Cloud

Public cloud was once seen as an acceptable risk, particularly in post-COVID cloud migration. But with AI increasing attack complexity and scale, the public cloud is rapidly moving into unacceptable risk territory. This year, **70 percent** of organizations reveal they are considering repatriating public cloud data to the private cloud, and more than half (**54 percent**) are reluctant to deploy AI in public cloud environments due to concerns around governance and intellectual property. At the same time, **65 percent** now view lateral East-West visibility as a greater security priority than inspecting North-South traffic—slightly down from **73 percent** in 2024. While the dip suggests competing demands on security teams, regional trends still show strong focus in key markets, with prioritization reaching **75 percent** in Australia and **72 percent** in Singapore and the USA.

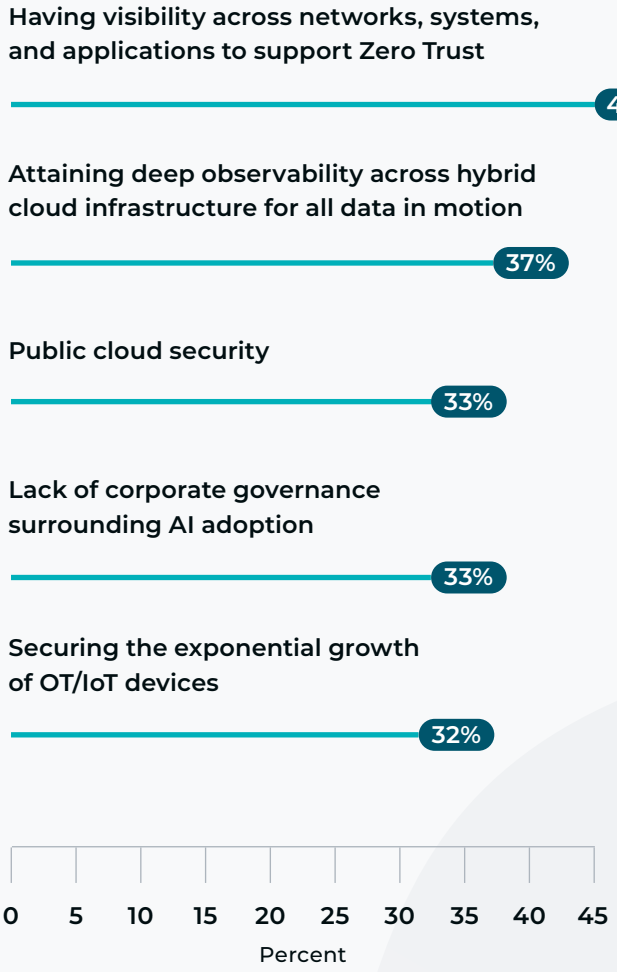
Public cloud security is now the number one concern for Security and IT leaders globally, and regional disparities highlight the extent to which it has become an unacceptable risk in some markets. In Germany, **52 percent** of leaders rank public cloud as a top challenge, compared to just **30 percent** in Singapore. That divergence suggests growing regulatory pressure and risk sensitivity in certain regions, and a widening gap in how public cloud security is being approached.

As the line between acceptable and unacceptable risk shifts, organizations are being forced to rethink their cloud strategies, not just for performance, but for security. Positively, they are doing so from a position of increased control, as **70 percent** of Security and IT leaders now say they are the final decision-makers for network and security operations in their organizations.

This growing sense of ownership is reshaping how risk is managed. The majority of Security and IT leaders (**86 percent**) now believe that cyber risk directly influences the health of the organization, pushing cybersecurity closer to the same level of board accountability as financial or legal risk.

TOP CISO CONCERNS

What are the key challenges you are most concerned about?



While public cloud may have once enabled agility, in today's AI-driven environment, it demands a more considered and deliberate approach, driving organizations to reassess where risk truly resides, and how much risk they are willing to tolerate and why.

The CISO Perspective: Visibility is the First Line of Defense

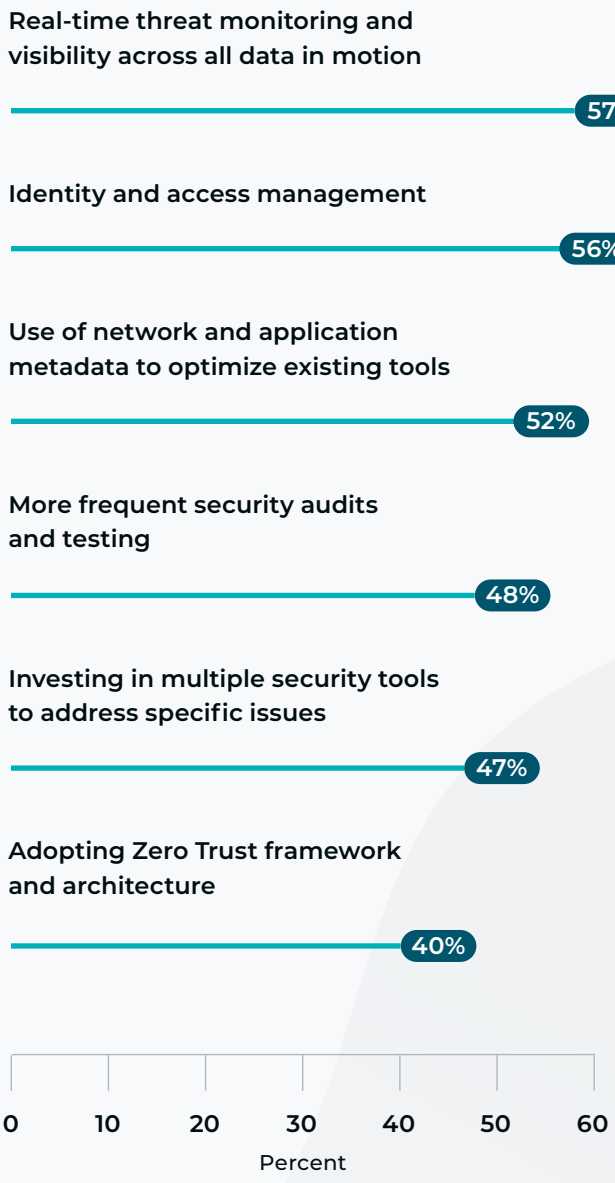
For CISOs, visibility is the foundation of security. Real-time threat monitoring and visibility across all data in motion is their number one priority in the next 12 months—a consistent trend from 2024—but one that has taken on new urgency as AI-driven complexity escalates. The mantra that "you can't protect what you can't see" continues to define the CISO mindset.

Their top concerns reflect the reality of today's security landscape. Nearly half (**45 percent**) point to network visibility for Zero Trust, **37 percent** to deep observability across hybrid cloud environments, **33 percent** to public cloud security and AI governance, and **32 percent** to securing the growth of OT/IoT devices. These are not isolated pain points, they are interconnected and complex challenges that shape how CISOs assess, contain, and respond to risk. For them it is not always about adding incremental tools. It is about making better use of their current tools, and ensuring those tools have the right data and visibility to deliver accurate, actionable intelligence and insights.

As such, CISOs are focused on data quality, not volume. Nearly half of CISOs (**47 percent**) say they are making compromises when it comes to leveraging network and application metadata to optimize tools, yet **86 percent** agree that packet-level data and rich metadata are key to strengthening security posture and unlocking deeper insights. They do not view tools as silver bullets, but rather see the value in the granularity, quality, and relevance of the data those tools are working with.

TOP SECURITY STRATEGIES

In the next 12 months, what are your top 3 priorities to optimize your defense-in-depth strategy?



CISOs are pushing visibility into the boardroom. This year, **8-in-10** CISOs (**83 percent**) believe deep observability is now integral to board-level discussions, up from **76 percent** in 2024, reflecting growing alignment between security and business objectives.

But while awareness is rising, authority still lags, as most CISOs still do not control the budget. Investment decisions are often made by CIOs (**31 percent**) or CTOs (**28 percent**), leaving CISOs responsible for managing risk—but often without the resources, influence, or authority to shape the strategy behind it. They know what needs to change. They see where the vulnerabilities lie. But without control over security investments or executive backing, even the most well-informed Security and IT leaders are left in an untenable position: referees expected to enforce the rules without a whistle, while the game plays on around them. Accountability without authority does not just limit their impact—it introduces risk the organization can't afford to ignore.

THE CISO–BOARD RELATIONSHIP

As AI accelerates complexity and expands the threat landscape, strong collaboration between CISOs and the board is increasingly seen as a strategic imperative—not just a best practice. The growing importance of cybersecurity is being recognized at the executive level, but recognition is not the same as influence. While **74 percent** of organizations say cybersecurity investment is more critical in 2025 than it was in 2024, almost half still allocate **20 percent** or less of their IT budgets to it. And despite rising engagement from boards, CISOs still feel sidelined when it comes to shaping AI and security strategy.

CISOs are clear about what needs to change. Their top five recommendations include:

1. **Enable direct CISO input into AI and security-related decisions**

   CISOs want a voice in shaping how AI is deployed and secured, not just in implementation, but in strategy and governance. Without their input, risk is often underestimated or misaligned with business priorities.

2. **Make cybersecurity a recurring board agenda item**

   Making cybersecurity a regular item on the board agenda ensures issues are tracked over time, not just addressed reactively. It also reinforces the role of security in overall business health.

3. **Strengthen board-level reporting tied to security outcomes**

   CISOs are asking for more meaningful reporting frameworks that go beyond just technical metrics and show how security performance ties to business resilience and risk reduction.

4. **Improve board education on cybersecurity fundamentals**

   A more cyber-aware board leads to better communication and better decisions. CISOs want to close the knowledge gap, so boards can be an active part of the security discussion.

5. **Establish clear breach disclosure protocols**

   Predefined breach disclosure plans can help avoid chaos during an incident. CISOs want clear, agreed-upon protocols in place to streamline incident response and ensure compliance under pressure.

These actions reflect a broader shift towards elevating cybersecurity from a technical silo to a core pillar of business strategy. While boards may be engaging, real progress will only come when CISOs are given a seat at the table. Full collaboration is key to aligning cybersecurity with business objectives and helping boards view it not as a cost center, but as a strategic business advantage.

The Path Forward: Deep Observability as a Strategic Reset

The answer to today's hybrid cloud challenges is not more data—it is better insight. As AI drives a surge in traffic and complexity, deep observability and the visibility that it is providing is emerging as the new standard of a modern security architecture, enabling organizations to shift from reactive defense to proactive control.

By integrating network-derived telemetry with MELT data, deep observability empowers threat detection, encrypted traffic analysis, and lateral East-West visibility—capabilities essential for securing AI-era hybrid clouds.

Security and IT leaders are aligned on its importance, with **88 percent** reporting access to rich network-derived telemetry is essential to the secure and efficient deployment of AI. In 2024, **84 percent** of respondents

Deep observability provides a comprehensive view of network traffic using network-derived telemetry across physical, virtual and cloud environments so organizations can better detect, prioritize, and respond to threats as they evolve. This level of visibility is essential to determine the data going in and out of AI models and mitigate the risk of data poisoning.

CHAIM MAZAL
Chief Security Officer, Gigamon

agreed that deep observability was fundamental to securing hybrid cloud environments. This year, that number is nearly **9-in-10** respondents (**89 percent**)—a view that holds strong across key markets, particularly in France, Singapore, UK, and USA.

Despite this momentum, execution remains a challenge. While **83 percent** of Security and IT leaders say deep observability is now part of board-level cybersecurity discussions, fragmented tooling and limited authority continue to hold back progress. The issue is not recognizing the value, it is building the capability to act on it.

Deep observability is not about collecting more signals, it is about regaining control. In a world where AI is reshaping infrastructure and expanding the attack surface, it offers a way to bring clarity to complexity. By integrating network-derived telemetry with MELT data, deep observability transforms fragmented signals into actionable intelligence—making risk visible, measurable, and manageable for today's challenges and what comes next. It is the strategic reset for which Security and IT leaders have been waiting.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

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

04.25_01