EXECUTIVE SUMMARY

2023 Hybrid Cloud Security Survey

Perception vs. Reality

With 72 percent of organizations having deployed hybrid cloud infrastructure, security can be hard to get right; many of the traditional tools designed for an on-premises world simply can't sufficiently monitor and protect this modern digital infrastructure.

To uncover the true state of Hybrid Cloud Security, we analyzed the insights of over 1,000 IT and Security decision makers from across six key global markets – the US, UK, France, Germany, Australia, and Singapore. The result? A significant gap between the perception that IT and Security leaders have of their security posture, and the harsh reality. Read the full report here, or explore key insights below.

The State of Hybrid Cloud Security

The good news is that **96 percent** see cloud security as everyone's responsibility and almost all (**99 percent**) of the IT and Security leaders we surveyed across EMEA, APAC, and the US believe that, in their organizations, CloudOps and SecOps are working towards a common goal.

However, there is still significant work to be done. Vulnerability detection and response remains siloed to SecOps teams due to a lack of security-first culture for **99 percent** of respondents.

Many are also worried about a lack of true knowledge on how to secure the cloud, with over half (**52 percent**) claiming their boards don't understand the shared responsibility model.

As a result, it's hardly surprising that **93 percent** of global IT and Security leaders predict cloud security attacks to increase in the next 12 months, especially considering **90 percent** have already fallen victim to a successful cyberattack since the start of 2022.

A Growing Visibility Gap: Perception vs. Reality

31 percent of IT and Security leaders identified a breach by:

- Users experiencing slow application performance (**18 percent**) - likely due to DoS or inflight exfil
- Users were unable to access applications and digital resources (**9 percent**)
- The organization's proprietary information was leaked on the dark web (**4 percent**)

In addition, breaches are being identified too late, nearly **1 in 3** breaches are going undetected by current security and monitoring tools. Given these stark findings, it is no surprise that concerns around blind spots are increasing.

Another concerning finding is that **1 in 3** CISOs lack confidence in where their most sensitive data is stored, and how it's secured. It seems that there are a number of critical visibility gaps, compounded by a misunderstanding of the extent of blind spots; **70 percent** admit encrypted traffic runs across their hybrid cloud freely, while a further **35 percent** claim to have limited sight into containers. This presents grave business risk as encrypted traffic cannot be sufficiently analyzed, and malware threats cannot be detected with existing tools as this data traverses internally, externally, and laterally across an organization.

Here exists the perception vs. reality disparity. While **50 percent** of IT and Security leaders state they are either confident, or completely confident, that they're sufficiently secure from on-premises to cloud, the true state of hybrid cloud security is that blind spots not only exist but are prolific for organizations across the globe.

Zero Trust Buy-In but Adoption Remains Challenging

We also surveyed IT and Security leaders about Zero Trust for the third year in a row and identified a number of changing perceptions around the security framework.

It remains a key topic of discussion in the industry moving forward, as while **80 percent** of CISOs agreed Zero Trust would be a big trend in 2022, this number has risen to **96 percent** for 2023 and beyond. Further results highlight similar findings, as **87 percent** of respondents stated in 2023 that their board is discussing Zero Trust as a priority – a number that increased by **29 percent** compared with 2022.

Yet with growing discussion of the framework comes an increasing skepticism around the reality of its implementation. Many remain unsure about how to architect and deploy Zero Trust. This is showcased by a growing trend of skepticism in EMEA in 2021 where **77 percent** of IT and Security leaders saw Zero Trust as attainable, but this number dropped to **53 percent** in 2022 and is now less than half (**44 percent**) for 2023. This uncertainty is likely due to only **34 percent** of organizations having the visibility to enable Zero Trust.

Deep observability defined: Amplifying the power of traditional security and observability tools with actionable network-derived intelligence and insights to eliminate blind spots, enabling teams to proactively mitigate hybrid cloud security and compliance risk, cut costs, and reduce complexity.

The Power of Deep Observability

IT and Security leaders do recognize that achieving visibility is integral to Zero Trust. In fact, we found that while **89 percent** of respondents in 2022 saw deep observability as somewhat to strongly connected to Zero Trust, 100 percent in 2023 see the two as strongly connected.

Importantly, recognition around deep observability as a solution for securing the hybrid cloud is also growing. When shown the full definition of deep observability, **89 percent** of global IT and Security leaders in 2022 agreed it was an important element of cloud security. This number has now risen to **97 percent**, while **20 percent** more respondents claim their boards discuss deep observability as a priority to secure the hybrid cloud this year, compared to last.

The hybrid cloud is a complex space, yet with the majority of organizations embracing this infrastructure, it's crucial that IT and Security leaders have a realistic view of their security posture. The race is on to achieve visibility across all data in motion, close the gap between perception and reality, and eradicate the critical blind spots causing concern in the cloud.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Download the full report to discover the insights from your region
gigamon.com/cloud-security-survey

Gigamon®

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

07.23_01