SURVEY REPORT

2023 Hybrid Cloud Security Survey

Perception vs. Reality

Table of Contents

Introduction

While we are witnessing a modest slowdown in cloud migration due to rising costs and economic uncertainty, it remains that a multitude of organizations now have a hybrid infrastructure in place. According to Forrester analysts,[1] this is deemed very much the norm and reports show **72 percent** of organizations exist in the hybrid cloud.[2] This is because enterprises will likely have paired their own data center/private cloud with one or more public clouds as a result of acquisition or to reap a number of benefits: Cisco, for example, identified **42 percent** of organizations believe they achieve a more agile and scalable development environment within the hybrid cloud, alongside **40 percent** who realize accelerated business agility and innovation.[3]

However, there are also various considerations around hybrid cloud security that have emerged as top priorities for CISOs, CIOs, and their teams, given the sharp rise in cloud-based security threats and breaches.

This latest report from Gigamon highlights that everything may not be exactly as it seems on the surface when it comes to hybrid cloud security. In fact, the research revealed there is a perception vs. reality gap for securing this infrastructure. On an initial questioning, IT and security leaders including CISOs, cloud architects and cloud security analysts across the globe confidently stated that their security tools and processes provide them with complete visibility and insights into their hybrid cloud infrastructure. Not just a few respondents made this claim – an overwhelming **94 percent** affirmed it. Yet, when we delved deeper to further investigate precise levels of deep observability, critical visibility gaps began to appear, from encrypted traffic, laterally moving data and 'unknown' blind spots.

For example, **half** of the global IT and Security leaders surveyed stated they are confident or completely confident they are sufficiently secure across their hybrid cloud infrastructure from on-premises to cloud, yet **90 percent** admitted to having suffered a data breach in the last 18 months. Therefore, we've revealed a significant disparity between how secure organizations believe their hybrid cloud infrastructure to be, and how protected their data truly is.

The reality is that almost all respondents of this 'Hybrid Cloud Security: Perception vs. Reality' report had experienced a data breach and, most worryingly, many breaches went undetected by IT and Security professionals. The feedback spanning six key global markets – the UK, France, Germany, the USA, Australia and Singapore – also highlighted that the perceived fears of security leaders, those that are making headlines such as the skills gap and lack of cyber investment, are not necessarily what really keeps them up at night. Underpinning all of this is the reality that gaining real-time insight across all data in transit – i.e., deep observability – has never been more important.

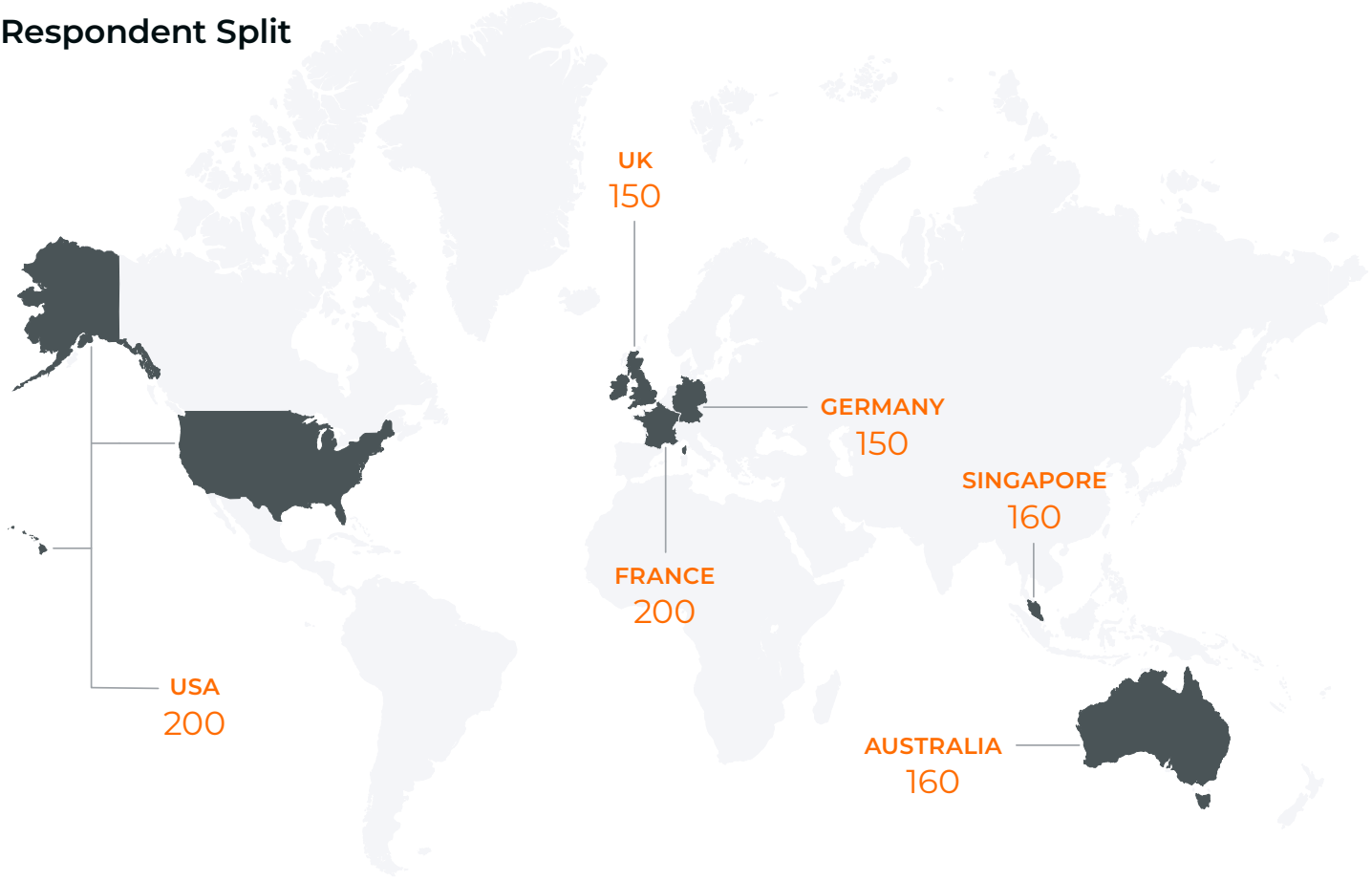
By 'deep observability' we mean amplifying the power of traditional security and observability tools with actionable network-derived intelligence and insights. This not only eliminates security and performance blind spots, it enables teams to proactively mitigate hybrid cloud security and compliance risk, while also enabling them to deliver a superior digital experience and contain the runaway cost and complexity associated with managing hybrid and multi-cloud infrastructure. In a time where cloud-based attacks are anticipated to increase, this enhanced visibility will prove indispensable.

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, COOs, cloud security analysts, cloud engineers, cloud architects, VPs of Information Security and other networking titles. Interviews were conducted in the UK, France, Germany, the USA, Australia, and Singapore. All respondents were guaranteed to remain anonymous as part of the study. Fieldwork was carried out between 19th April and the 2nd May 2023. The sample comprised of the following professionals:

- **1,020 respondents** split across the UK (150 respondents), France (200 respondents), Germany (150 respondents), USA (200 respondents), Australia (160 respondents), and Singapore (160 respondents).
- **42 percent** work for companies with between 501 and 1,000 employees, and **58 percent** work for companies with more than 1,000 employees.
- Job titles include: Chief Information Officer (**15 percent**), Chief Technology Officer (**5 percent**), Chief Information Security Officer (**12 percent**), Cloud Engineer (**7 percent**), Cloud Security Analyst (**4 percent**) and VP of Information Security (**5 percent**).

Respondent Split



Key Learnings

1. The perception of hybrid cloud security doesn't match the reality

50 percent of the IT and Security leaders surveyed stated they are either confident, or completely confident, that they're sufficiently secure across their entire IT infrastructure, from on-premises to cloud. Yet at the same time, the vast majority have suffered a data breach in the last 18 months, highlighting the dangers of complacency when it comes to security.

2. Nearly 1 in 3 security breaches are going undetected by IT and Security professionals

While surface-level confidence around total hybrid cloud visibility and security is high, the reality is that nearly a third of breaches are being identified later down the line – either through data appearing on the dark web, files becoming inaccessible, or users experiencing slow application performance (likely due to DoS or inflight exfil). It's clear that traditional security and observability tools need to go much further to detect and identify threats.

3. There's a lack of awareness around blind spots and a misconception about the dangers of encrypted traffic

Unknown blind spots are keeping CISOs up at night, yet at the same time over **70 percent** of IT and Security leaders admit they let encrypted data flow freely. It seems there is a naivety across the globe on what constitutes a hybrid cloud blind spot and the resulting danger of not analyzing data simply because it's encrypted or only flows internally.

4. One third of CISOs aren't confident they know how their most sensitive data is secured

CISOs and CIOs face a number of challenges in the modern, hybrid-cloud world, and one of these appears to be lacking the basic knowledge on how their most valuable and sensitive data is being stored and secured. This lack of observability is one example in many that point towards a growing risk in organizations as a result of critical visibility gaps.

5. Collaboration across IT departments still has a way to go

Collaboration is increasing: the vast majority believe cloud security is everyone's responsibility and see CloudOps and SecOps as working towards a common goal. Yet in practice, a lack of a security-first culture is still creating siloes according to **99 percent** of respondents who are seeing SecOps doing the legwork for vulnerability detection.

6. Deep observability is central to cloud security, rising cloud costs, and Zero Trust

Following on from findings in the Gigamon State of Ransomware for 2022 and Beyond report, findings from this year's data highlight that deep observability is rapidly gaining traction in the hybrid cloud market for securing this space and becoming a foundational element of security frameworks like Zero Trust.[4] Many are also seeing the benefits of deep observability for achieving cost efficiencies in a challenging economic environment.

IT Collaboration is on the Rise

In the year since our report on the State of Ransomware for 2022, there have been a number of large-scale data breaches across the globe, including attacks on global news organizations, schools, telecoms providers, and healthcare institutions. As a result, cybersecurity has become a central topic discussed not just by boardrooms, but also government bodies. The US White House has recently launched its new National Cybersecurity Strategy[5] following on from the 2021 Executive Order (14028) that is likely to drive security strategy for the next decade.[6] Across the rest of the world, reforms for the Australian Security of Critical Infrastructure Act 2018 are underway,[7] while ransomware became a key topic in British COBRA meetings[8] and the EU proposed its own updated regulation in the form of the Cyber Resilience Act.[9]

In the enterprise, the heightened threat environment is driving higher levels of cross-departmental IT collaboration. The vast majority of IT and Security leaders across the globe (**97 percent**) agree they can collaborate across their IT organization when it comes to vulnerability detection and response, and a further **83 percent** believe they're working in a security culture of 'collective accountability'. By this they mean a culture where responsibility for security is shared across IT organizations, a concept that professionals in the US, Australia, and Singapore are more confident compared to EMEA (where **1 in 10** are still siloing accountability to security teams).

The good news in a tough cyber environment is that **99 percent** of IT and Security professionals across EMEA, APAC, and the US are seeing CloudOps and SecOps working towards a common goal. What's more, cloud security is seen as everyone's priority by **96 percent** of those asked.

Surprisingly, CloudOps is taking the lead on security strategy and preventing cyberattacks in their organization, according to **69 percent** of respondents. This is supported by **53 percent** who see SecOps doing the same. The average drops slightly for those in Singapore, who see SecOps (**38 percent**) on par with AppSec teams (**39 percent**) for driving security strategy, but still highlights CloudOps (**59 percent**) as the leading department.

Many CISOs and senior IT security leaders find they are held solely accountable when a breach occurs. What kind of security culture does your organization practice?

The good news in a tough cyber environment is that **99 percent** of IT and Security professionals across EMEA, APAC, and the US are seeing CloudOps and SecOps working towards a common goal.

A key takeaway, however, is that there is still much more work to be done to support greater collaboration. While CloudOps teams are leading on strategy, the findings highlight that SecOps professionals are 'doing the doing' when it comes to vulnerability detection. A high **99 percent** of respondents state a lack of a security-first culture means that vulnerability detection can often be siloed within the SecOps team.

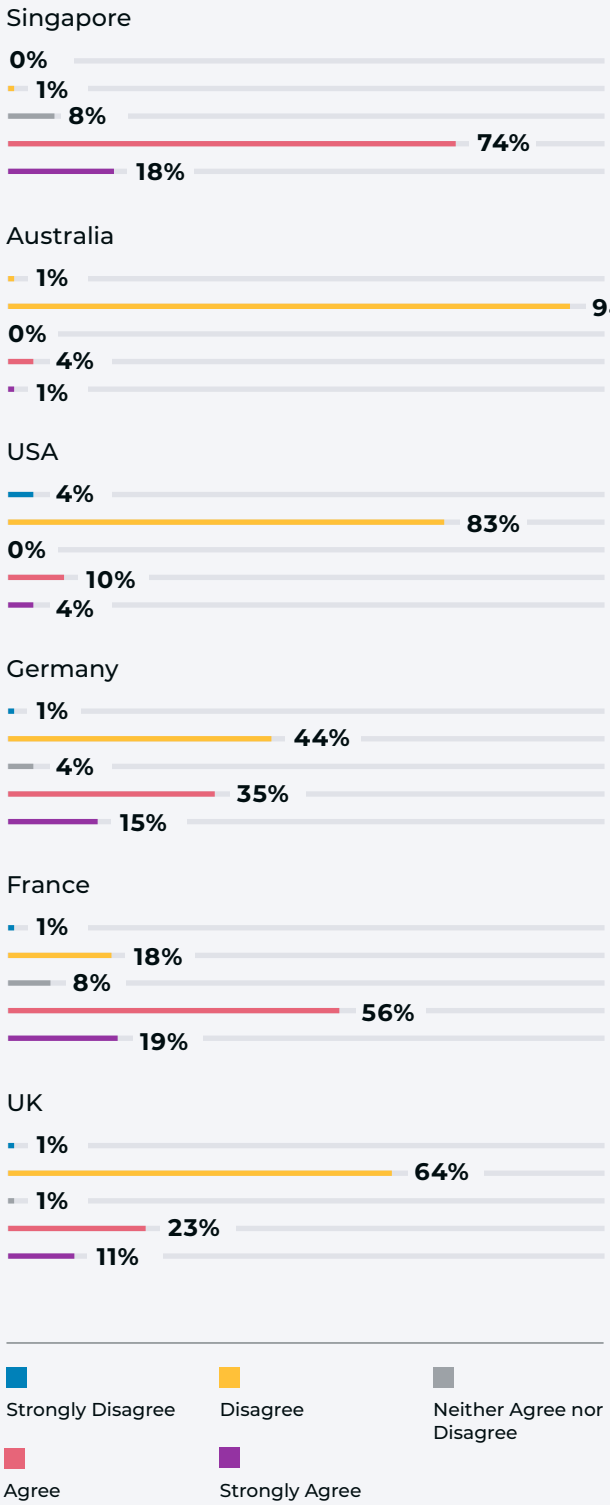
Cloud Security Remains a Key Concern

It's clear that CloudOps and SecOps are collaborating more because they recognize the escalating risk in securing hybrid cloud infrastructure. Shifting workloads to the cloud has been front and center for many organizations' digital transformation initiatives in recent years – yet most of the security and monitoring tools designed for an on-premises world simply cannot properly protect a virtual or hybrid environment.

The first issue is it seems there's not complete cloud security agreement across IT leadership. While **30 percent** of global CISOs are completely confident that they can safely advance cloud migration initiatives to the desired levels of security, those more likely to be leading the teams that are actioning this migration are less so (only **12 percent** have complete confidence).

There seems to be something of a disconnect between the Board/CISOs and other leaders in the IT and Security space, compounded by the fact that over half of global respondents (**52 percent**) claim their boards still don't understand the shared responsibility model for the cloud. This is primarily a result of **95 percent** of IT and Security leaders from Australia and **87 percent** from the US being worried their boardrooms don't fully understand the model – while France and Singapore are far more confident they do. This lack of understanding is a worrying risk, but it also highlights that the way decision makers across the globe perceive the responsibility of their cloud security is not necessarily the reality.

Given that we're seeing an increase in cloud-based security threats, to what extent do you agree the shared responsibility model inherent to the cloud is fully understood by the Board?



There seems to be something of a disconnect between the Board/ CISOs and other leaders in the IT and Security space, compounded by the fact that over half of global respondents (52 percent) claim their boards still don't understand the shared responsibility model for the cloud.

What's more, **93 percent** of IT and Security leaders predict cloud security attacks will increase in the next 12 months. Given their history, it's hard to question these predictions; **90 percent** have experienced a data breach in the last 18 months, with **59 percent** suffering a successful cyberattack in the last 7-9 months.

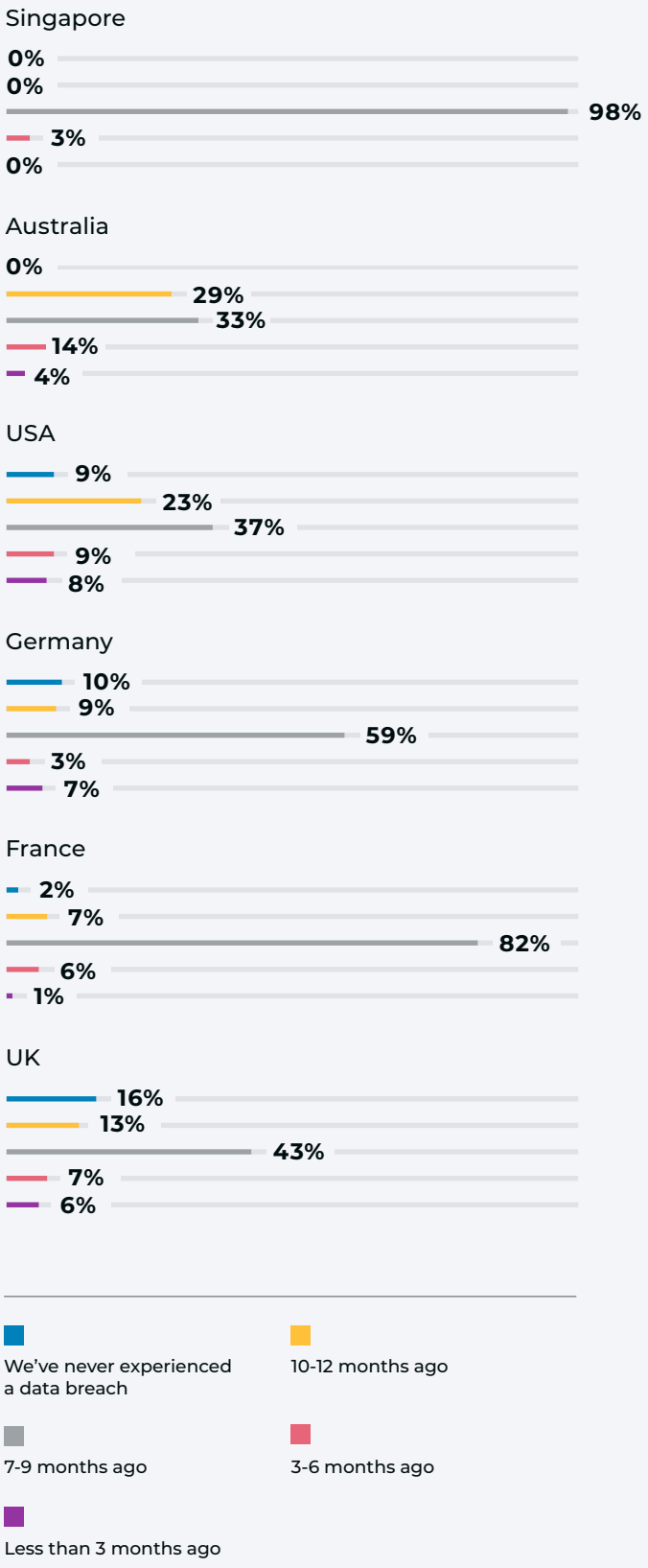
So, while these teams could agree that they practiced good levels of collaboration to ensure visibility, only **16 percent** can say they are completely confident about securing their hybrid cloud infrastructure. Here we see the perception vs. reality gap emerge. Surface level confidence is high, but further investigation digs up a number of issues and cloud security concerns that professionals may or may not be fully aware of.

93 percent of IT and Security leaders predict cloud security attacks will increase in the next 12 months. Given their history, it's hard to question these predictions; **90 percent** have experienced a data breach in the last 18 months.

This is certainly a global issue, but one that respondents from Singapore reflect most acutely; while more than one quarter (**26 percent**) of IT and Security leaders in this region state they are completely confident in securing their entire IT infrastructure (and another **66 percent** are 'confident') all have been breached in the last 9 months. France follows shortly behind Singapore, with **81 percent** either confident or completely confident that they're sufficiently secure across their entire IT infrastructure, from on-premises to cloud, and Germany slightly less so with **55 percent**. It is only in the UK (**36 percent**), Australia (**18 percent**) and the US (**17 percent**) that confidence levels are lower. Perhaps these findings signify that formerly vulnerable organizations have made significant changes to bolster their security since their last attack, but it should also highlight the danger of hybrid cloud security complacency.

The answer must lie in achieving deeper levels of observability from on-premises to cloud, according to **96 percent** of respondents that agree cloud security is dependent on gaining visibility across all data in motion.

Have you experienced a data breach in the last year?



Security Teams Struggle with Visibility Gaps

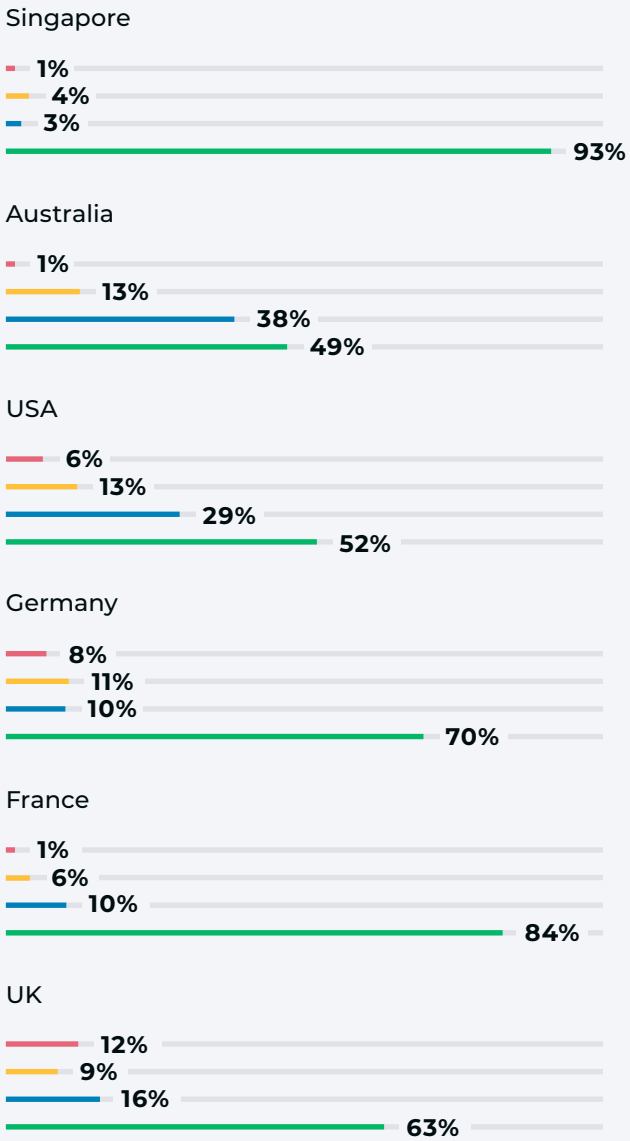
Even though visibility is cited as a key solution for hybrid cloud security concerns, many are struggling to achieve it. Most worryingly, when we asked respondents around the world who have previously suffered a breach exactly how they detected this breach, only **69 percent** were able to do so with security and observability tools. The other **31 percent** stated either:

- Users experienced 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**)

These findings highlight that almost **1 in 3** breaches are going undetected by IT and Security professionals and their tools, a number that rises to a worrying **48 percent** in the US, and **52 percent** in Australia. Across EMEA, we also found that almost **1 in 5** (**18 percent**) were unable to identify the root cause of the breach suffered by their organization.

50 percent of respondents lack confidence when it comes to knowing where their most sensitive data is stored and how it's secured.

How were you able to detect the data breach?



It seems that visibility gaps create a number of issues when detecting breaches and remediating issues following an attack. And when we questioned levels of observability across the hybrid cloud to prevent further attacks, more worrying findings came to light.

According to global IT and Security leaders, **50 percent** lack confidence when it comes to knowing where their most sensitive data is stored and how it's secured. This same data highlighted that **1 in 3** CISOs/CIOs are only slightly confident in this knowledge.

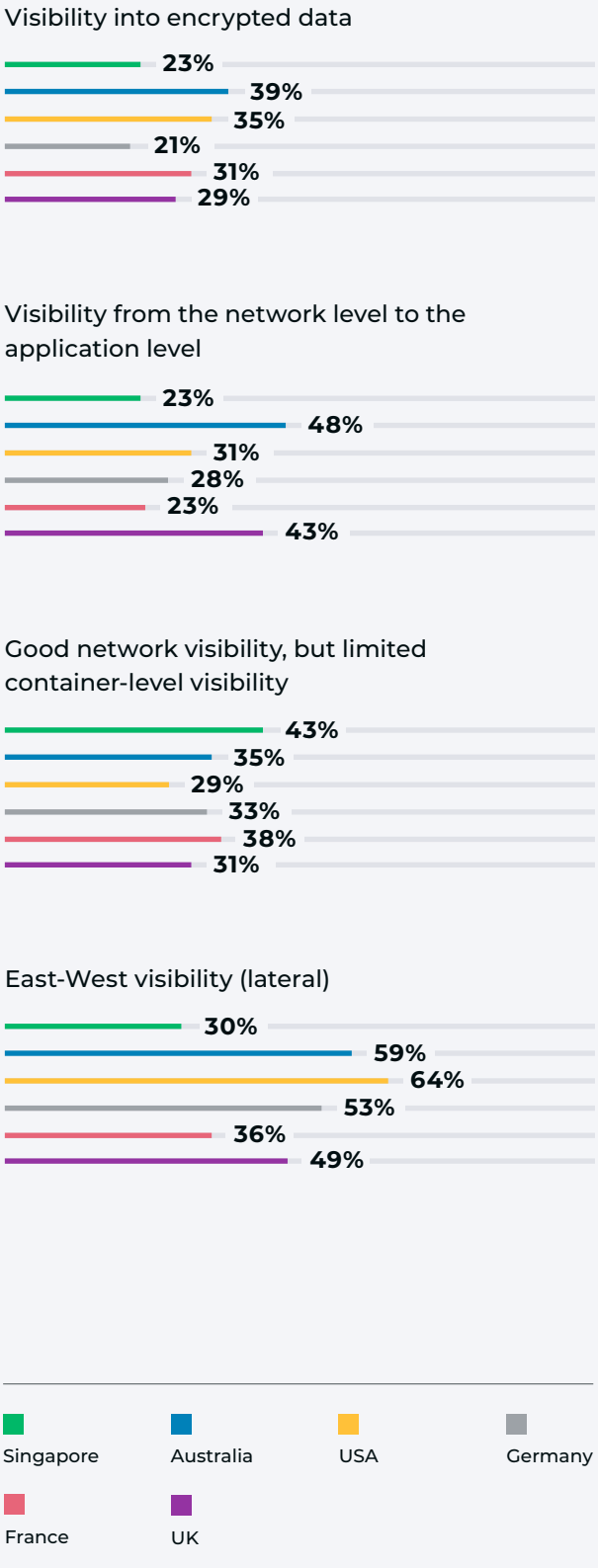
While the surface-level perception of **94 percent** of respondents is that their security tools and processes provide them with complete visibility and insights into their hybrid cloud infrastructure, the reality is their strategy is failing them if they can't be certain on how and where their most critical data exists or how it's secured.

When asked on a granular level about the level of visibility they have across their hybrid cloud infrastructure, we found that:

- **35 percent** have good network visibility, but limited sight into containers (a number that rises to **38 percent** in France and **43 percent** in Singapore)
- Only **30 percent** have visibility into encrypted data, decreasing to only **21 percent** in Germany
- Just under half (**48 percent**) have sight across laterally moving data – otherwise known as East-West traffic. The US leads the market in this space, with **64 percent** achieving East-West visibility, while Singapore falls behind with **30 percent.**

According to Ian Farquhar, Security CTO at Gigamon, East-West visibility needs "re-defining". He states, "The original concept of East-West traffic vs. data that flows from North-South references a perimeter-focused, on-premises network which simply doesn't exist anymore in the hybrid cloud world. Today's modern infrastructure means deep observability across laterally moving data is just as important as visibility into traffic coming from external sources."

What level of visibility do you currently have across your IT infrastructure?



The original concept of East-West traffic vs. data that flows from North-South references a perimeter-focused, on-premises network which simply doesn't exist anymore in the hybrid cloud world. Today's modern infrastructure means deep observability across laterally moving data is just as important as visibility into traffic coming from external sources.

IAN FARQUHAR
Security CTO, Gigamon

56 percent of respondents claimed undiscovered blind spots being exploited is the leading concern making them restless.

We can take from these findings that while the majority of IT and Security teams lack critical visibility across data in motion from on-premises to cloud, they may not perceive these blind spots as an issue simply because they're unable to recognize them as 'blind spots'.

The reality is that blind spots are defined as segments across a network and cloud where security and monitoring tools may not reach, meaning data cannot be sufficiently analyzed and therefore areas become hidden. East-West traffic (data moving laterally within an organization) is typically not perceived as significant a threat as North-South traffic (external to internal), and therefore security and monitoring tools may ignore it altogether. The same can be said for encrypted traffic; it's possible that organizations are neglecting to recognize the key danger that this data can pose, despite studies that have identified **93 percent** of malware hides behind encryption.[10]

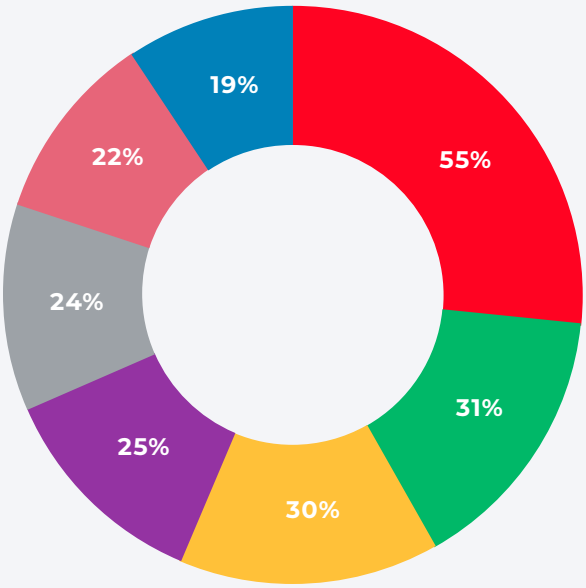
Unexpected Issues Keeping CISOs Up at Night

Given this situation, it is no surprise that blind spots are a leading concern for CISOs, CIOs and other leaders across the IT and security space. In fact, **56 percent** of respondents claimed undiscovered blind spots being exploited is the leading concern making them restless.

Respondents from France seem less concerned about this issue, with only **36 percent** stating blind spots keep them up at night – yet it is still their leading stressor. For the UK in particular, **40 percent** are kept up by worries around not having the tools/visibility to properly secure their organization.

It also comes as a surprise that the issues often making headlines in recent years, those perceived as the traditional primary pain points, are not such a key concern for the IT and Security leaders of 2023. Alongside blind spots, legislation (**34 percent**) and attack complexity (**32 percent**) are key stressors, while problems like a lack of cyber investment (**14 percent**) and the ongoing skills gap (**20 percent**) are much less concerning. France is again the outlier, with over a quarter (**26 percent**) of respondents in this region expressing worries about a lack of investment in cybersecurity.

In the current climate, CISOs and senior IT security leaders are heavily under the spotlight for their accountability for cyber incidents. What are the key factors keeping you up at night?



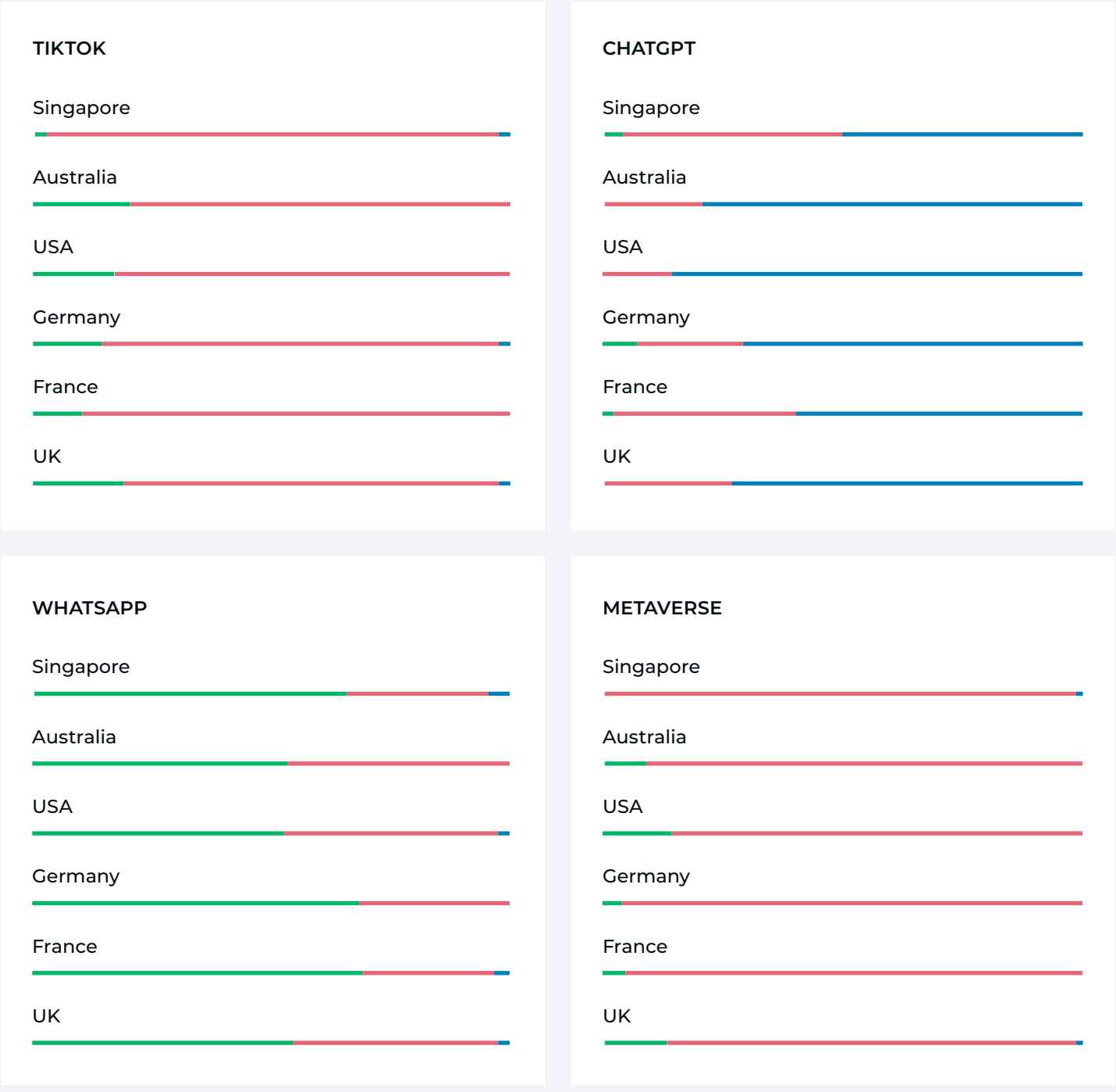
- Blind spots being exploited that you didn't know were there
- Increasing sophistication and complexity of attacks
- Not having the tools / visibility required to secure the organization
- Insufficient cybersecurity investments
- New, more focused and consequential cybersecurity legislation to comply with
- Pressure from the Board
- Lack of experienced cybersecurity personnel (skills gap)

In fact, skills are barely a global consideration when it comes to securing the hybrid cloud, with only **19 percent** claiming effective security education for staff is a crucial factor for gaining confidence in IT infrastructure security, alongside only **15 percent** pointing to the need to have access to skilled people in the cloud. It is only in France and Germany that closing the skills gap seems to be a higher priority, with **23 percent** and **25 percent** respectively stating that access to skilled people in the cloud is a crucial factor in their confidence levels that their hybrid cloud infrastructure is as secure as possible.

Evolving legislation, on the other hand, is a particular issue for the UK and Australia – **41 percent** of UK IT and Security leaders, and a high **59 percent** for those in Australia, are seeing changes in cyber law and compliance as a key concern moving forward, and it seems that the EU Cyber Resilience Act is causing the most headaches globally. In a time where the consequences of non-compliance are becoming increasingly severe (the EU's Digital Operational Resilience Act mandates organizational fines or even jail time), it is little surprise this is a key issue on security leaders' minds.

While only **24 percent** of global enterprises have banned or are looking into banning ChatGPT, **100 percent** are concerned about TikTok and the Metaverse . . . In fact, **60 percent** of global enterprises have already banned the use of WhatsApp due to cybersecurity concerns – a number that rises to **67 percent** in Germany and **69 percent** in France.

Are you concerned about the use of the following apps, tools or technologies in your organization due to cybersecurity issues?



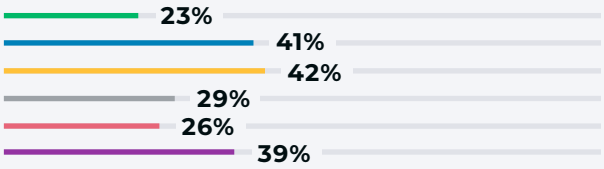
- Yes, we have already banned the use of this due to cybersecurity concerns.
- Yes, we are currently evaluating the cybersecurity risks associated with this and will make a decision soon.
- No and we do not currently plan to ban the use of this due to cypersecurity concerns.

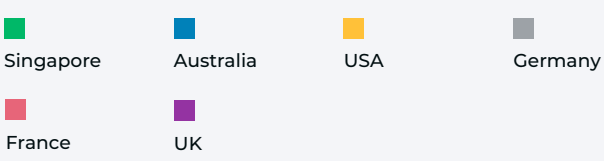
Finally, the perception of AI as a central threat concerning security professionals does not match up to the reality. ChatGPT and other generative AI technologies have been dominating headlines in 2023, yet our data found that while only **24 percent** of global enterprises have banned or are looking into banning ChatGPT, **100 percent** are concerned about TikTok and the Metaverse, alongside **99 percent** that are worried about WhatsApp. In fact, **60 percent** of global enterprises have already banned the use of WhatsApp due to cybersecurity concerns – a number that rises to **67 percent** in Germany and **69 percent** in France.

These findings signify that while AI may be front of mind for innovation, the reality is there are many other evolving technologies keeping cyber leaders awake at night.

This security framework, that aims to eradicate implicit trust across organizations and automate security response mechanisms, has long been a priority for IT and Security leaders across the globe.

Do you currently have visibility across networks, systems, and applications to support Zero Trust?





Zero Trust is on the Security Roadmap

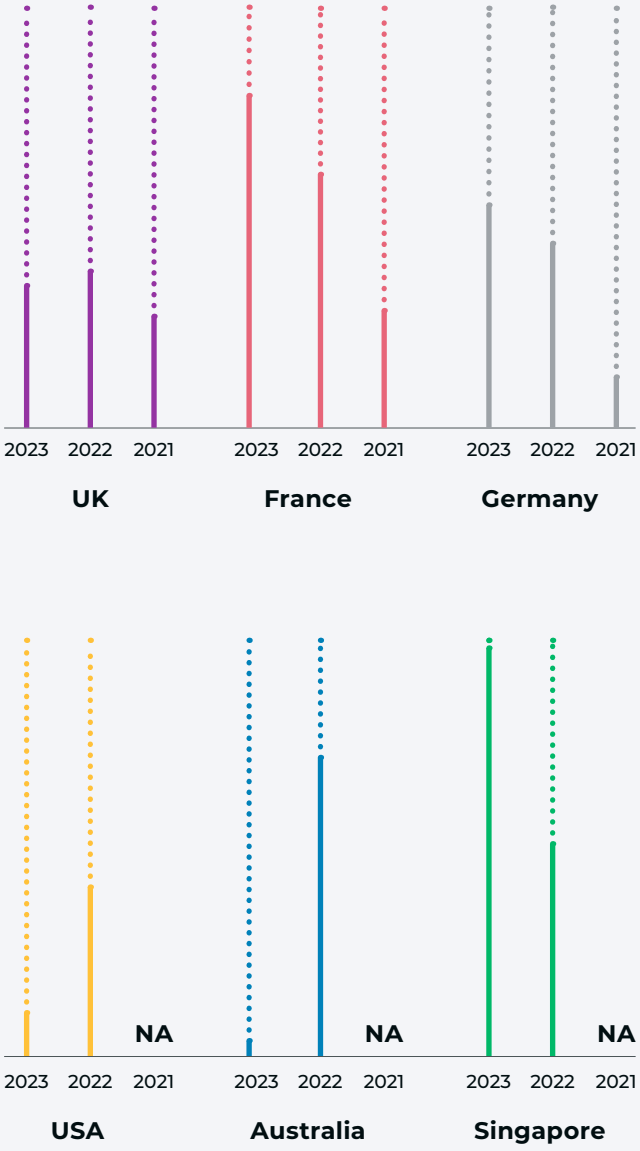
Another area where visibility needs improvement is in the world of Zero Trust. This security framework, that aims to eradicate implicit trust across organizations and automate security response mechanisms, has long been a priority for IT and Security leaders across the globe. While **80 percent** of CISOs/CIOs agreed it would be a big trend in 2022 (as identified in our Gigamon State of Ransomware for 2022 Report), **96 percent** now believe the same for 2023 and beyond.

Yet while half of all respondents to this year's survey stated that Zero Trust is crucial to boosting confidence levels that their organization is secure, the reality is that many teams simply do not have the visibility to enable it. This may be a result of Zero Trust initiatives being driven from board-level, yet those implementing the change do not yet have the investment or capacity to make it work.

According to our data, only **34 percent** of global respondents have visibility across networks, systems, and applications to support Zero Trust. It seems that the UK (**39 percent**), the US (**42 percent**) and Australia (**41 percent**) are leading the market when it comes to achieving the visibility required to enable this framework, while France (**26 percent**), Germany (**29 percent**) and Singapore (**25 percent**) fall behind.

The good news is that understanding and awareness of exactly what Zero Trust entails is growing. There has been an upward trend in how much Zero Trust is spoken about openly at a board level – if we take the UK as an example, **53 percent** agreed the boardroom discussed Zero Trust in 2021, a number that rose to **67 percent** in 2022 and **85 percent** in 2023. On a global scale, discussions increased from **58 percent** to **87 percent** across the last year. What's more, while three quarters of respondents saw Zero Trust as a journey rather than a tick box exercise in 2022, this has increased to **96 percent** in 2023.

To what extent do you agree or disagree that Zero Trust is completely unattainable?



But much like we noticed in last year's global report on ransomware, with this growing understanding of Zero Trust comes a skepticism around its complexities and the reality of implementation. Many are still nervous about how to deploy the framework, possibly due to the lack of guidance that has been published by government organizations. Across EMEA in 2021, **77 percent** saw Zero Trust as attainable, but this number dropped to **53 percent** in 2022 and is now less than half (**44 percent**). In fact, for France, only **20 percent** are confident this security approach is attainable.

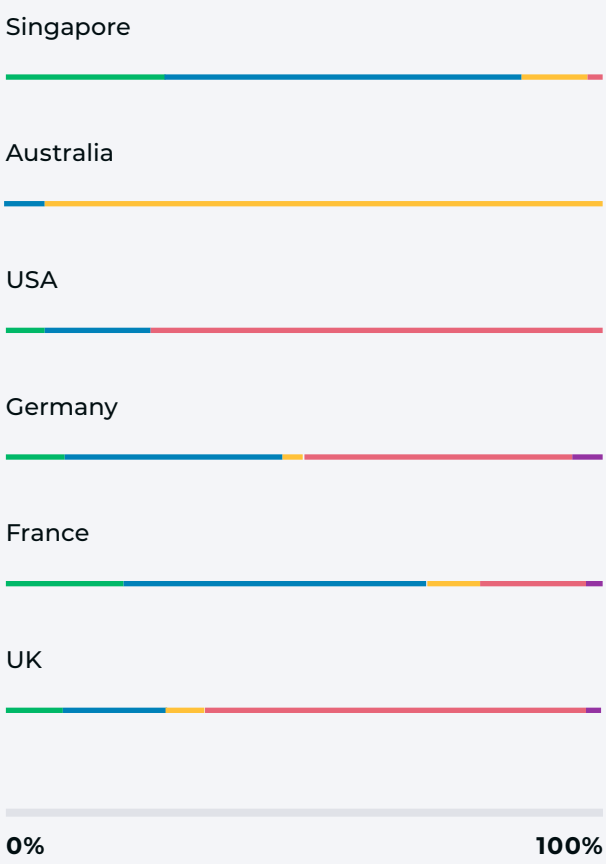
The 'unattainability' of Zero Trust is possibly a reflection of the level of investment required to architect the framework for positive outcomes. Two years ago, only **21 percent** of EMEA IT and Security leaders believed that Zero Trust required too much insight and resource to make it worthwhile, but this rose to **44 percent** in 2022, and now **53 percent** in 2023 – spearheaded by France's skepticism (**76 percent**).

It seems there is a significant divide across the globe, in which some regions are far more confident and comfortable with the future of Zero Trust than others – and it's not the same as previous years. Australia, for example, has become far more supportive of Zero Trust potential; while **48 percent** believed it wasn't worth investing in due to the insight/resource required in 2022, this has now reduced to only **7 percent.** It's a similar case for the US, with the number of skeptics dropping from **21 percent** last year, to **12 percent** this year.

Singapore and France tell a different story. In Singapore, the results are most damning: **91 percent** see Zero Trust as unattainable (a rise of **63 percent** from 2022), and **96 percent** believe it requires too much oversight.

This regional divide also creates a split decision when we asked respondents this year whether Zero Trust is simply a buzzword. **45 percent** of respondents chose yes, while **53 percent** said no – with results driven by Australia and US backing this approach to security as realistic and achievable, while Singapore and France remain uncertain.

To what extent do you agree or disagree that Zero Trust is more a buzzword than a reality?



Deep Observability is More Valuable Than Ever

Uncertainty around Zero Trust likely stems from a lack of clarity around how this framework can work in practice. According to Ian Farquhar, a true Zero Trust framework is still "work in progress". He argues, "as security teams look to implement a Zero Trust architecture, they are quickly realizing it is not a simple solution. Many organizations are still on the journey, especially now that the US is mandating Zero Trust for federal agencies with Executive Order 14028. We are seeing definitively that Zero Trust is a strategic element of security and it's the best option organizations have to substantially improve their security resilience while maintaining business agility."

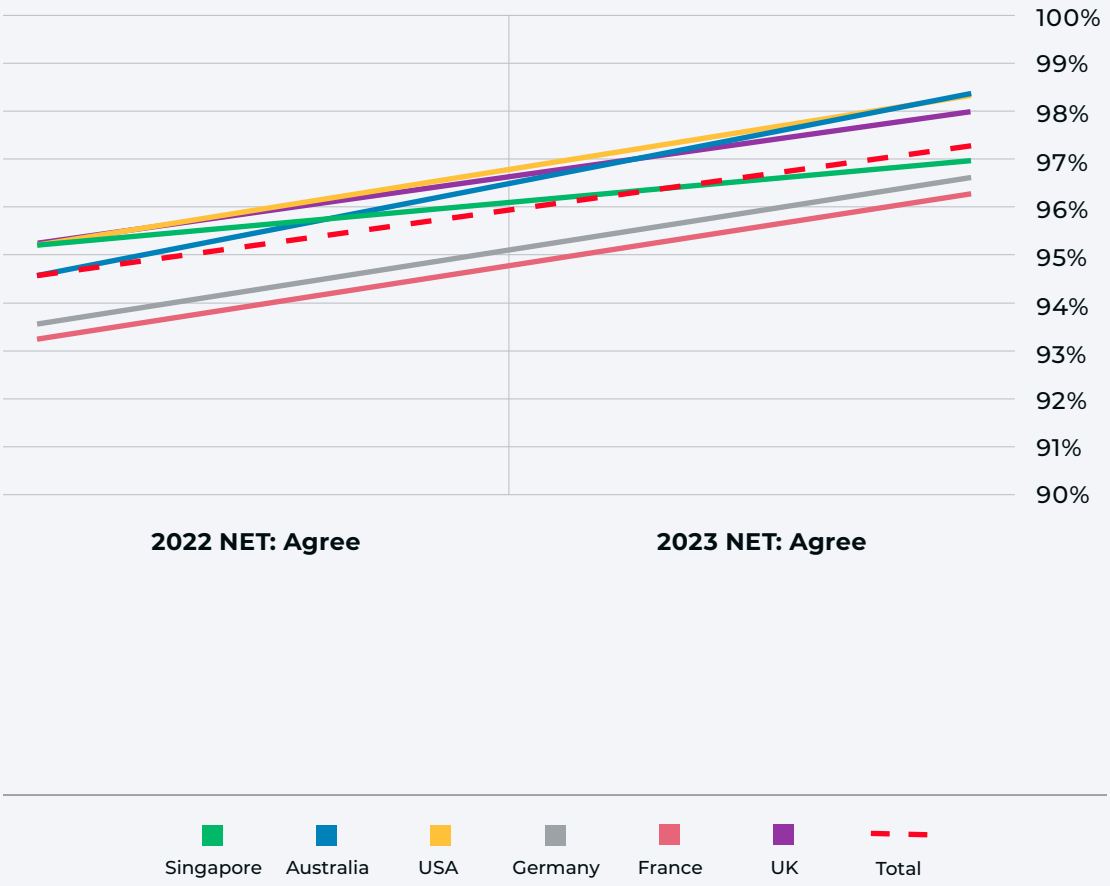
Fortunately, it seems that every IT and Security professional surveyed recognizes where to start and build a solid foundation for Zero Trust. While **89 percent** of respondents in 2022 stated they see deep observability as somewhat to strongly connected to Zero Trust, **100 percent** in 2023 see the two as strongly connected.

This is likely because deep observability goes beyond traditional log-based tools designed for an on-premises world, to provide actionable network-derived intelligence into the critical visibility gaps highlighted here by IT and Security leaders from around the world. While the term is relatively new to the market, awareness of its value is growing quickly – especially when it comes to securing hybrid cloud infrastructure. We showed survey respondents in 2022 the full definition of deep observability, leading to **89 percent** agreeing it as an important element of cloud security. This number has now risen to **97 percent** in 2023. What's more, when shown the deep observability definition, **98 percent** say it is now being discussed by the board as a priority to better secure the hybrid cloud, an increase of **20 percent** from last year.

A true Zero Trust framework is still "work in progress". As security teams look to implement a Zero Trust architecture, they are quickly realizing it is not a simple solution. Many organizations are still on the journey, especially now that the US is mandating Zero Trust for federal agencies with Executive Order 14028. We are seeing definitively that Zero Trust is a strategic element of security and it's the best option organizations have to substantially improve their security resilience while maintaining business agility.

IAN FARQUHAR
Security CTO, Gigamon

To what extent do you agree that deep observability is a foundational element of cloud security?



Finally, deep observability has been cited not only for securing hybrid cloud infrastructure, but also for managing costs. It's no secret that the unforeseen spiralling costs of cloud computing have now become a significant stumbling block. Yet enhancing visibility into the hybrid cloud means only the relevant traffic is sent to the relevant tools, significantly reducing agent, bandwidth, and data movement costs. According to our research, deep observability will play a key role in supporting **50 percent** of global IT and Security leaders and their teams that lack confidence they can effectively manage security tools costs around their hybrid and multi-cloud infrastructure.

The growing awareness of deep observability and the value of amplifying traditional security and monitoring tools is positive given the prominence of blind spots highlighted in this report. The first stage to bolstering hybrid cloud security is recognizing that many organizations are suffering from a perception vs. reality gap. Complacency may breed vulnerability and this report highlights a number of areas, from East-West traffic to encrypted data, that need greater attention. Fortunately, once IT and Security leaders across the globe truly understand the extent of this problem, bridging the gap will be made far easier with deep observability.

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. For more information about the Gigamon Platform or to contact a local representative, please visit: gigamon.com.

1 Forrester, Explore Seven Pitfalls To Avoid In Your Push To Modernize Cloud, https://www.forrester.com/resources/cloud-strategy/modernize-cloud-pitfalls-webinar/

2 Flexera, 2023 State of the Cloud Report, https://info.flexera.com/CM-REPORT-State-of-the-Cloud

3 Cisco, 2022 Global Hybrid Cloud Trends Report, https://www.cisco.com/c/en/us/solutions/hybrid-cloud/2022-trends.html

4 Gigamon, State of Ransomware for 2022 and Beyond, https://www.gigamon.com/resources/resource-library/white-paper/wp-gigamon-report-state-of-ransomware.html

5 The White House, National Cybersecurity Strategy, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

6 The White House, Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

7 Cyber and Infrastructure Centre, Security of Critical Infrastructure Act 2018, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure

8 The Record, Ransomware incidents now make up majority of British government's crisis management 'Cobra' meetings, https://therecord.media/ransomware-incidents-now-make-up-majority-of-british-governments-crisis-management-cobra-meetings

9 European Cyber Resilience Act, https://www.european-cyber-resilience-act.com/

10 Help Net Security, The hidden picture of malware attack trends, https://www.helpnetsecurity.com/2023/04/06/malware-attack-trends-q4-2022/

Gigamon®

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

06.23_1