Cloud Security Index

Key Findings from the Middle East

VansonBourne

illumio

Introduction

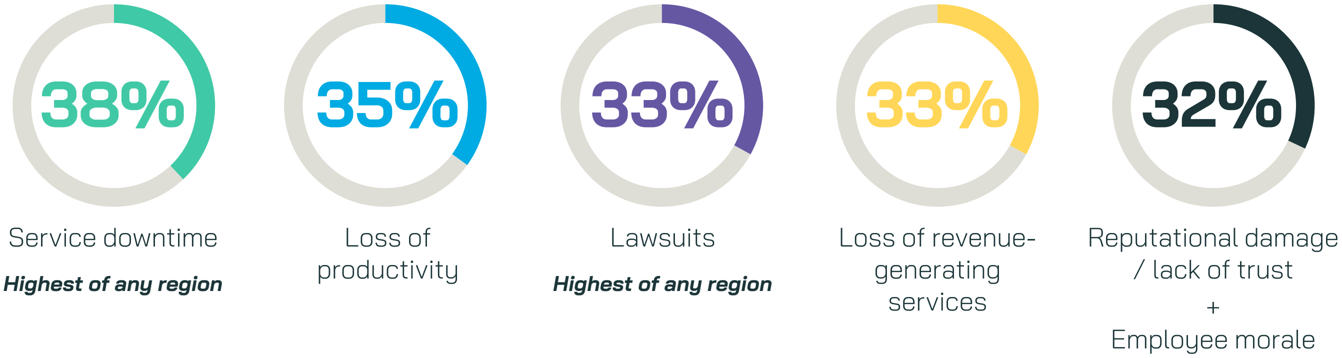
Organisations require the cloud more than ever to store their highest-value assets. However, as cloud adoption grows, so are the number of cloud breaches and other cyberattacks. The recent increase in these attacks highlights how cybercriminals are taking advantage of the security gaps caused by inadequate cloud security practices, causing organisations to lose critical data, trust, and money.

The data from the 2023 Cloud Security Index, carried out by independent research firm Vanson Bourne, identifies the major cloud-based security weaknesses of the surveyed Middle Eastern respondents' organizations, and looks at how Zero Trust Segmentation (ZTS) can overcome cloud security gaps posed by traditional, outdated approaches.

The Risks of Traditional Cloud Security

Despite having many benefits, cloud usage is never risk-free. During the last year, 54 percent[1] of the breaches reported by respondents in the Middle East originated in the cloud, resulting in an average loss of over $2.3 million annually[2]. Given that all organizations are storing sensitive data (100 percent), and the majority are running their high-value applications (76 percent) in the cloud, the potential risks and financial impacts from a successful breach can be astronomical. Unfortunately, the damage that a successful breach can cause is not only limited to the financial costs – there can also be serious long-standing consequences across the organisation. Respondents in the Middle East were particularly concerned about lawsuits (33 percent compared to 21 percent on average globally). Service downtime was also more commonly identified as a top impact of a cloud breach (38 percent compared to 29 percent globally), which may imply that their IT infrastructure is more vulnerable to cyberattacks, especially ransomware and extortion.

Top five impacts of a cloud breach:



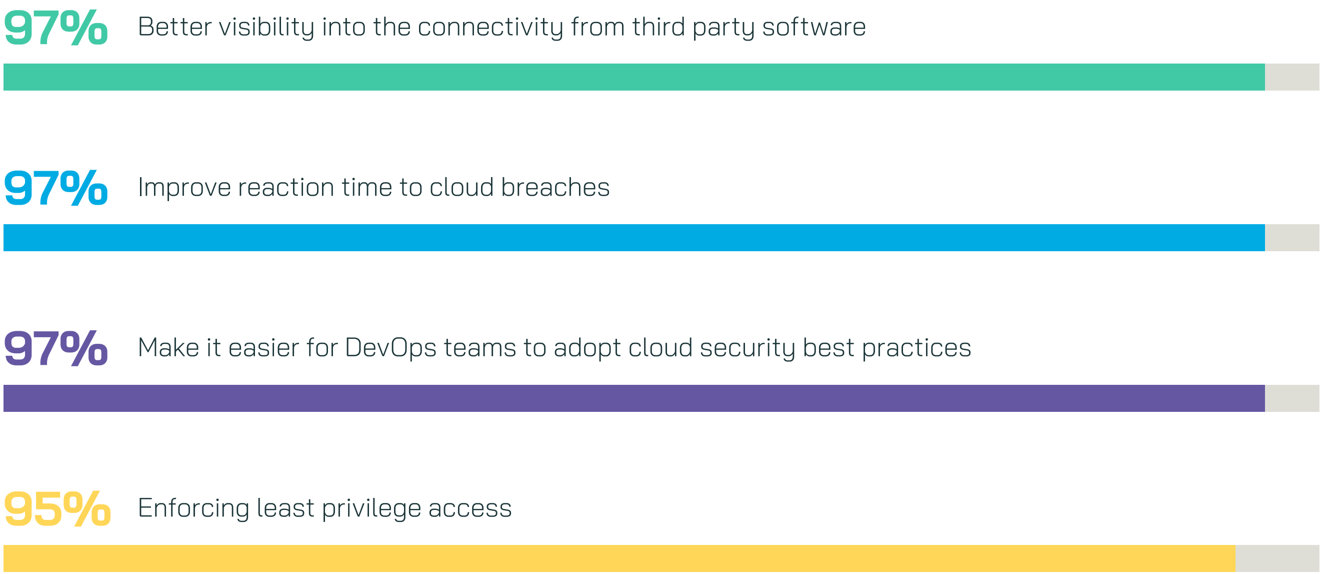
The majority (70 percent) of IT security decision makers based in the Middle East say that cloud security at their organization is lacking and poses a severe risk, which is the highest of all the regions interviewed (the global average is 63 percent). This indicates lower levels of confidence in cloud defences compared to other regions. Concerningly, 42 percent say it would be easy for attackers to move laterally across their organisation, which is much higher than the global average of 31 percent. Additionally, 98 percent are concerned that the connectivity between their cloud services and other environments is increasing the likelihood of a breach. Eighty-two percent say that the security function at their organisation slows down cloud adoption, which is higher than the global average of 74 percent and most likely is hindering the cloud migration plans of organisations.

[1] - Low base size (17 Middle East respondents whose organization experienced a breach in the past year). Results are indicative only.

[2] - Low base size (17 Middle East respondents whose organization experienced a breach in the past year). Results are indicative only.

These concerns indicate that commonly used cloud security tools are failing to keep organisations safe. To identify potential security risks before a compromise, hybrid and multi-cloud environments need connections that are monitored in real-time. Respondents reported that improvements are required for the visibility, reactivity, and ease-of-use of their existing cloud security.

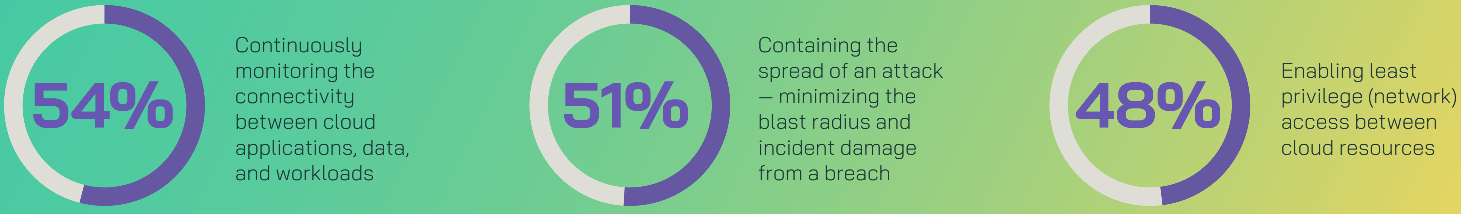
Necessary improvements to organizations' IT security include:



ZTS: The Solution for Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risk. The vast majority of respondents in the Middle East (89 percent) believe that ZTS has the potential to greatly improve cloud security at their organisation. By securing cloud services with ZTS, respondents believe it would improve digital trust (50 percent) and business continuity (50 percent). Respondents also acknowledge the value that ZTS would bring to their organisation's cloud security posture, with all (100 percent) citing at least one benefit.

Zero Trust Segmentation improves cloud security by:



Conclusion

To help manage the risks posed by hyperconnectivity and complexity in the cloud, made worse by the inadequate existing cloud security approaches, organisations must invest strategically in bolstering their cloud security posture using technologies that prioritise visibility, consistency, and control. Zero Trust Segmentation is essential to cloud security and is proven to proactively mitigate the risks posed by potential breaches and reactively contain an attack before it can result in greater damage to the organisation. In turn, organisations can increase the overall confidence in their cloud operations and enhance digital trust by removing any existing cyber security weaknesses and reducing risks as the business scales.

To find out more about the state of cloud security and the ways to employ an effective Zero Trust strategy, read the *full global report*.

Methodology

Illumio partnered with technology research specialist Vanson Bourne to assess the current state of cloud security. A total of 1,600 IT security decision makers from 500+ employee organizations in the public and private sector were interviewed in September 2023. This report provides insights from the 100 respondents in the Middle East who took part. This includes an even split of respondents from Saudi Arabia and the UAE, respectively.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit *www.vansonbourne.com*

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.