Cloud Security Index

Key Findings from Australia

VansonBourne

illumio

Introduction

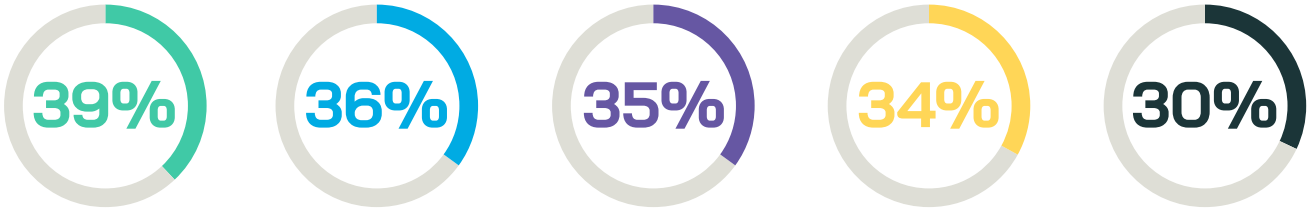
Increasingly, organisations are relying on the cloud to run their applications and store their most valuable assets. However, the growth in cloud usage is causing cloud-based breaches and ransomware attacks to skyrocket. This surge shows us that cybercriminals are successfully exploiting cloud vulnerabilities stemming from ill-equipped security practices — leading to business disruptions and a loss of critical data, trust, and financial resources. Survey respondents in Australia would benefit from a greater understanding of the connectivity of their third-party software in a way that is not cumbersome for their security operations teams to mitigate the risks.

The data from the 2023 Cloud Security Index, conducted by independent research company Vanson Bourne, reveals how there are significant cloud-based security weaknesses in organisations according to the surveyed Australia-based respondents. It also examines how Zero Trust Segmentation (ZTS) can address the security gaps of conventional cloud security approaches.

The Risks of Traditional Cloud Security

Despite its many benefits, cloud usage is never risk-free. Over the past year, 47 percent of the breaches reported by survey participants originated in the cloud, resulting in an average annual loss of more than $3 million (A$4.9 million). Considering that nearly all organisations (96 percent) store their sensitive data and/or operate their high-value applications (89 percent) in the cloud, the potential risks and financial consequences of a successful breach can be staggering. And the harm caused by a successful breach isn't limited to financial costs; it can also result in ongoing repercussions throughout the organisation.

Top five impacts of a cloud breach:



The majority (61 percent) of respondents in Australia say that cloud security at their organisation is lacking and poses a severe risk. Additionally, 91 percent are concerned that connectivity between their cloud services and other environments increases the likelihood of a breach.

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 their organisation needs to improve the efficiency, controls, and scalability of their existing cloud security.

Necessary improvements to organizations' IT security include:

97% Reducing workload / increasing efficiency for SecOps (security operations) teams

97% Setting and enforcing consistent security and compliance policies

97% Security that scales with the speed of cloud adoption

The Solution to Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risk. Nearly all Australia-based respondents (98 percent) believe that ZTS has the potential to improve cloud security at their organisation. By securing cloud services with ZTS, respondents believe it would improve three key metrics at their organisation:

62%
Business continuity

60%
Digital trust

60%
Cyber resilience

Respondents also acknowledge the value that ZTS would bring to their organisation's cloud security posture. Respondents in Australia emphasised improved understanding of connectivity from third party software as being particularly valuable (50 percent compared to 45 percent globally).

Zero Trust Segmentation improves cloud security by:

Continuous monitoring of the connectivity between cloud applications, data, and workloads

Containing the spread of an attack and minimising the blast radius and incident damage from a breach

Enabling least privilege (network) access between cloud resources

Improve understanding of connectivity from third party software

Conclusion

To offset the risks from hyperconnectivity and complexity in the cloud, made worse with inadequate security, organisations must strategically invest to strengthen their cloud with technologies that provide usability, scalability, and efficiency. Zero Trust Segmentation is essential for true cloud security. ZTS provides crucial visibility and can proactively contain a breach before it results in greater damage, so that organisations can decrease their security risks and elevate the resiliency of their cloud operations.

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 organisations in the public and private sector were interviewed in September 2023. This report provides insights from the 200 Australia-based respondents who took part.

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 organisations 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.