Cloud Security Index

Key Findings from the United Kingdom

VansonBourne

illumio

Introduction

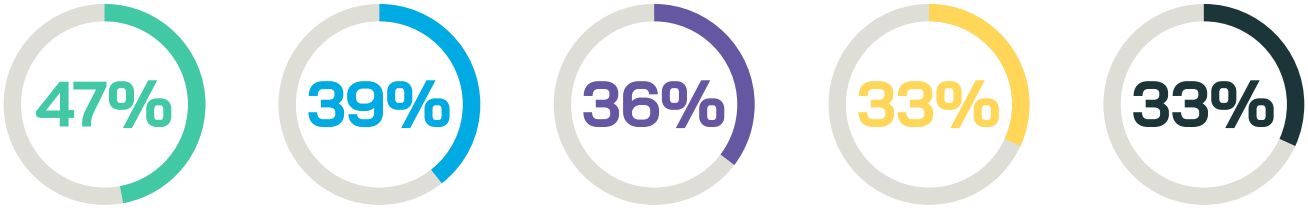
Organisations are increasingly dependent on the cloud to run their applications and store their most valuable assets. Unfortunately, with the growth in cloud services, cloud-based breaches and ransomware attacks are skyrocketing. This surge shows us that cybercriminals are successfully exploiting cloud vulnerabilities stemming from insufficient security practices — leading to business disruptions and loss of critical data, trust, and financial resources. The potential reputational damage of a cloud breach was particularly concerning to U.K. survey respondents compared to the global findings.

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 U.K. 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, 45 per cent of the breaches reported by survey participants originated in the cloud, resulting in 46 per cent incurring annual losses exceeding £405,250 GBP. Considering that nearly all organisations store their sensitive data (96 per cent) and/or operate their high-value applications (89 per cent) 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. In the U.K., IT security decision-makers are most likely to recognise reputational damage as a major consequence of a cloud breach (47 per cent compared to 39 per cent globally). They are also more likely to report that cloud breaches highly impact operations — making them impossible (58 per cent compared to 48 per cent globally).

Top five impacts of a cloud breach:



The majority (68 per cent) of U.K. respondents say that cloud security at their organisation is lacking and poses a severe risk. Additionally, 89 per cent 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 improvements are required for the usability, scalability, and efficiency of their existing cloud security.

Necessary improvements to organizations' IT security include:

93% Setting and enforcing consistent security and compliance policies

93% Security that scales with the speed of cloud adoption

92% Make it easier for DevOps teams to adopt cloud security best practices

The Solution to Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risk. Nearly all U.K. respondents (98 per cent) 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:

65%
Cyber resilience

57%
Digital trust

50%
Business continuity

Respondents also acknowledge the value that ZTS would bring to their organisation's cloud security posture. U.K. respondents emphasised insights into unnecessary connectivity that could result in exposure as being particularly valuable (50 per cent compared to 45 per cent globally).

Zero Trust Segmentation improves cloud security by:

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

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

Offering insights into unnecessary connectivity that could result in exposure

Conclusion

To offset the risks from hyperconnectivity and complexity in the cloud, made worse with inadequate security, organisations must invest strategically 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 organizations in the public and private sector were interviewed in September 2023. This report provides insights from the 200 U.K. 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 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.