Cloud Security Index

Key Findings from Germany

VansonBourne

illumio

Introduction

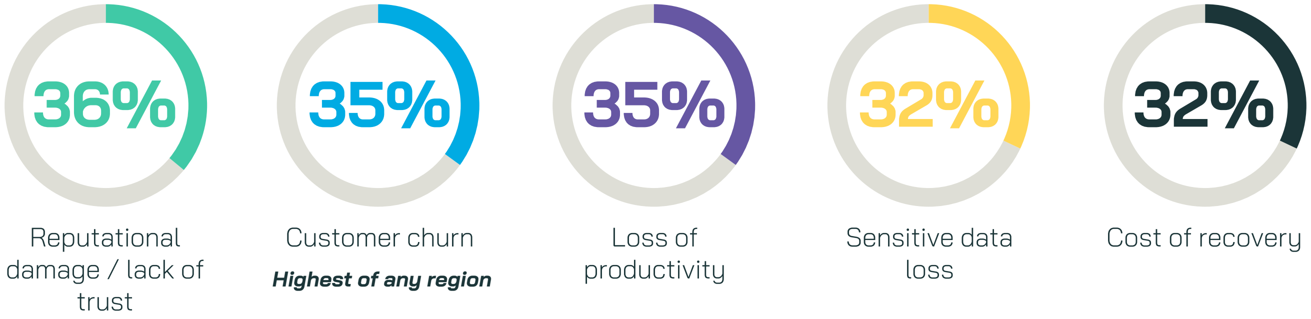
Organizations are relying on the cloud more than ever to store their highest-value assets. However, as cloud adoption increases, so does the number of cloud-based breaches and other cyberattacks. Organizations are struggling to monitor connectivity across complex cloud environments, slowing down reaction times to a breach and enabling cybercriminals to steal critical data and money and damage trust.

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 Germany-based respondents' organizations, and looks at how Zero Trust Segmentation (ZTS) can overcome cloud security gaps posed by more traditional, outdated approaches.

The Risks of Traditional Cloud Security

Despite its many benefits, cloud usage is never risk-free. During the last year, 42 percent of breaches reported by respondents originated in the cloud, resulting in an average annual loss of $7.2 million (€6.8 million) among the victims (which is much higher than the global average of $4.4 million). Given that almost all organizations are storing sensitive data (98 percent) and / or running their high-value applications (89 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 business. Notably, IT security decision-makers in Germany identified customer churn as a main impact of a cloud breach, with 35 percent acknowledging this concern compared to the global average of 28 percent.

Top five impacts of a cloud breach:



The majority (63 percent) of respondents from Germany say that cloud security at their organization is lacking and poses a severe risk. Additionally, 81 percent are concerned that connectivity between their cloud services and other environments increases the likelihood of a breach. Thirty-two percent say that a complete overhaul is required to improve their organization's reaction times to cloud breaches (which is a lot higher than the global average of 23 percent). This data point is significant because the longer it takes to respond and contain an attack, the greater the damage.

These concerns indicate that commonly used cloud security tools are failing to keep organizations 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 speed, efficiency, and reporting capabilities of their existing cloud security.

Necessary improvements to organizations' IT security include:

99% Better reaction time to cloud breaches

98% Reduce workload/ increase efficiency for SecOps (security operations) teams

98% Better exec level reporting

ZTS: The Solution for Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risk. Virtually all respondents in Germany (99 percent) believe that ZTS has the potential to greatly improve cloud security at their organization. By securing cloud services with ZTS, respondents believe it would improve three key metrics at their organization:

66%
Business continuity
Highest of any region

64%
Cyber resilience

63%
Digital trust

Respondents also acknowledge the value that ZTS would bring to their organization's cloud security posture. Germany-based respondents emphasized continuous monitoring of connectivity between cloud applications, data, and workloads as being particularly valuable (61 percent compared to 55 percent globally).

Zero Trust Segmentation improves cloud security by:

61% Continuously monitoring the connectivity between cloud applications, data, and workloads
Highest of any region

51% Containing the spread of an attack — minimizing the blast radius and incident damage from a breach

46% Providing a better understanding of connectivity from third party software

Conclusion

To offset the risks posed by hyperconnectivity and complexity in the cloud, made worse by the inadequate existing security approaches, organizations must invest strategically to boost their cloud security posture using technologies that prioritize 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 any successful attacks before they can result in greater damage to the business. ZTS allows organizations to increase their overall confidence in cloud operations and enhance cyber resilience by removing existing barriers and reducing risk 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 200 Germany-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 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.