Cloud Security Index

Key Findings from France

VansonBourne

illumio

Introduction

Today, organizations rely on the cloud more than ever to store their highest-value assets. That said, as cloud adoption increases, so does the number of cloud-based breaches and other ransomware attacks. Organizations are struggling with understanding the division of responsibility for security between their cloud providers and vendors. Consequently, cybercriminals are exploiting the security gaps created by insufficient cloud security practices, and damaging organizations through the loss of critical data, trust, and financial assets. The loss of revenue-generating services as a result of cloud breaches is a particular concern to survey respondents in France compared to other countries, demonstrating how much French organizations rely on the cloud for their business operations.

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and looks at how Zero Trust Segmentation (ZTS) can overcome the cloud security gaps posed by traditional, more outdated approaches.

The Risks of Traditional Cloud Security

Despite its many benefits, cloud usage is never risk-free. During the last year, 47 percent of the breaches reported by respondents originated in the cloud, resulting in an average annual loss of $2.7 million (€2.5 million) among the victims. Given that almost all organizations are storing sensitive data (98 percent) and / or running their high-value applications (90 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 to the organization. Notably, IT security decision-makers in France identified loss of revenue-generating services as a main impact of a cloud breach, with 41 percent highlighting this concern compared to the global average of 35 percent.

Top five impacts of a cloud breach:

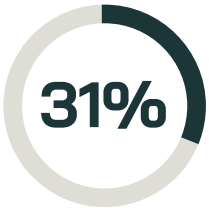
Loss of revenue-generating services

Highest of any region

Sensitive data loss

Reputational damage / lack of trust

Cost of recovery



Employee morale

The majority (61 percent) of respondents from France say that cloud security at their organization is lacking and poses severe risks. Additionally, 92 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 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 ease-of-use, scalability, and reliability of their existing cloud security.

Necessary improvements to organizations' IT security include:

98% Make it easier for DevOps teams to adopt cloud security best practices

98% Security that scales with the speed of cloud adoption

96% Set and enforce consistent security and compliance policies

ZTS: The Solution for Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risks. Nearly all respondents in France (94 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:

64%
Cyber resilience

57%
Digital trust

55%
Business continuity

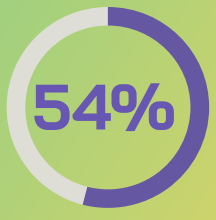
Respondents also acknowledge the value that ZTS would bring to their organization's cloud security posture. France-based respondents emphasized insights into unnecessary connectivity as being particularly valuable (56 percent compared to 45 percent globally).

Zero Trust Segmentation improves cloud security by:

Offering insights into unnecessary connectivity that could result in exposure

Highest of any region

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



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

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 by using technologies that prioritize visibility, consistency, and control. Zero Trust Segmentation is essential for cloud security and is proven to proactively mitigate the risks posed by potential breaches and contain a successful attack before it results in greater damage to the organization. ZTS allows organizations to increase overall confidence in their cloud operations and enhances cyber resilience by removing existing barriers 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 200 France-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.