# Cloud Security Index

Key Findings from the
United States

VansonBourne

illumio

# Introduction

Organizations are relying on the cloud more than ever to store their highest-value assets. Yet, as cloud adoption increases, so too are the number of cloud-based breaches and other ransomware attacks. The recent increase in cyberattacks shows that cybercriminals are taking advantage of the security gaps caused by inadequate cloud security practices to wreak havoc on organizations, causing them to lose critical data, trust, and money to bad actors.

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 U.S. respondents' organizations and looks at how Zero Trust Segmentation (ZTS) can overcome cloud security gaps posed by traditional, more antiquated approaches.

## The Risks of Traditional Cloud Security

Despite its many benefits, cloud usage is never risk-free. During the last year, 46 percent of the breaches reported by respondents originated in the cloud, resulting in 61 percent losing more than $500,000 USD annually. Given that almost all organizations are storing sensitive data (99 percent) and / or running their high-value applications (91 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.
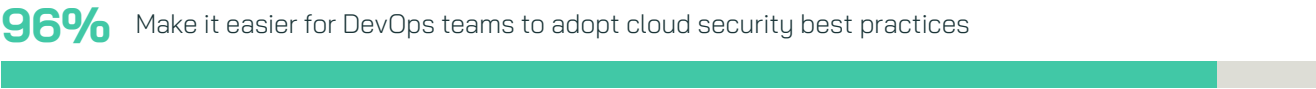
### Top five impacts of a cloud breach:

| 38% | 36% | 35% | 32% | 32% |
|-----|-----|-----|-----|-----|
| Reputational damage/lack of trust | Sensitive data loss | Loss of revenue-generating services | Loss of productivity | Cost of recovery |

IT security decision makers based in the U.S. are the most likely to understand their organization's cloud-security risk exposure very well (55 percent compared to 47 percent globally). Despite this, the majority (61 percent) say that cloud security at their organization is lacking and poses a severe risk. Additionally, 94 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 efficiency, usability, and reactivity of their existing cloud security.

## Necessary improvements to organizations' IT security include:

**96%** Make it easier for DevOps teams to adopt cloud security best practices

**96%** Improve reaction time to cloud breaches

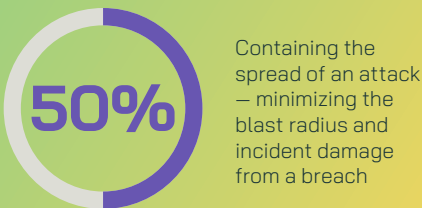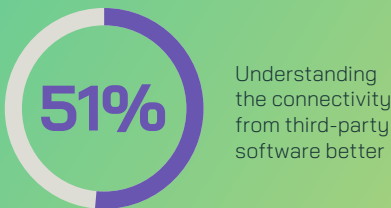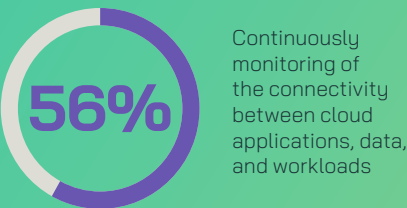**95%** Reduce workload / increase efficiency for SecOps team

## The Solution to Improved Cloud Security

Zero Trust Segmentation (ZTS) increases cloud resilience and reduces risk. Nearly all U.S. respondents (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:

**70%**
Digital trust
(The highest of any region)

**64%**
Business continuity

**67%**
Cyber resilience
(The highest of any region)

Respondents also acknowledge the value that ZTS would bring to their organization's cloud security posture. U.S. respondents emphasized an increased understanding of connectivity from third-party software as being particularly valuable (51 percent compared to 45 percent globally).

## Zero Trust Segmentation improves cloud security by:

**56%** Continuously monitoring of the connectivity between cloud applications, data, and workloads

**51%** Understanding the connectivity from third-party software better

**50%** Containing the spread of an attack — minimizing the blast radius and incident damage from a breach

## Conclusion

To offset the risks posed by hyperconnectivity and complexity in the cloud, made worse by inadequacies of existing cloud security approaches, organizations must invest strategically in bolstering their cloud security posture using technologies that prioritize visibility, consistency, and control. Zero Trust Segmentation is essential to cloud security, 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. In turn, organizations can increase their overall confidence in cloud operations and enhance cyber resilience by removing existing barriers while 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 400 U.S. 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.