VansonBourne | illumio

Cloud Security Starts **with Zero Trust Segmentation**

Today, organizations are more exposed and vulnerable than ever to cybercriminals who continue to exploit weaknesses in the cloud and across the software supply chain to wreak havoc by stealing, encrypting, and holding data for ransom.

Vanson Bourne, in partnership with Illumio, surveyed 1600 IT security decision makers to identify the shortcoming of organizations' traditional cloud security approaches and uncovered how organizations can overcome these challenges to improve business resilience and reduce risk.

Cloud Security Has Failed Us.

63%

believe that their organization's cloud security is lacking and poses a severe risk to the business.

92%

are concerned that connectivity between environments increases the likelihood of a breach.

Why aren't today's most commonly used cloud security tools enough? Organizations that use cloud-based services need more efficiency, visibility, and less complexity to reduce risks across their environments:

95%

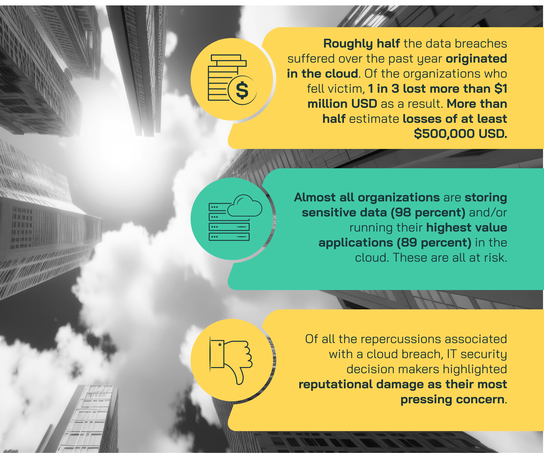
- need better visibility into connectivity from third-party software.
- need better reaction time to cloud breaches.
- need to reduce workloads/increase efficiency for security operations (SecOps) teams.

Only 24%

express high confidence in their ability to contain attacks and prevent bad actors from spreading through their environment.

Cloud Security Gaps Have Severe Repercussions.

Cloud usage, with its many benefits, is not risk-free. The rising popularity of hybrid and multi-clouds has opened up new doors for cybercriminals eager to take advantage of interconnected systems and data:



Roughly half the data breaches suffered over the past year **originated in the cloud**. Of the organizations who fell victim, **1 in 3 lost more than $1 million USD** as a result. **More than half** estimate **losses of at least $500,000 USD.**

Almost all organizations are **storing sensitive data (98 percent)** and/or running their **highest value applications (89 percent)** in the cloud. These are all at risk.

Of all the repercussions associated with a cloud breach, IT security decision makers highlighted **reputational damage as their most pressing concern**.

Stakeholder trust, while taking a long time to build up, can be destroyed in an instant by a devastating breach. Rather than waiting for this doomsday scenario to occur, an organization's best defense lies in proactively preparing for the inevitable successful attack.

Zero Trust Segmentation Effectively Mitigates the Risk.

Today, cloud resilience starts with Zero Trust Segmentation (ZTS). In a hyperconnected world, ZTS guarantees increased cloud resilience and reduced risk so that your organization can operate in the cloud confidently, securely, and with speed:

97%

believe ZTS has the potential to greatly improve cloud security at their organization

Findings reveal that the top ways ZTS improves organizations' cloud security posture are through:

- **55%** Continuous monitoring of cloud applications, data, and workloads
- **45%** Offering insights into unnecessary connectivity that could result in exposure
- **51%** Minimizing the "blast radius" of an attack

61%

say securing all cloud services with ZTS would improve **digital trust**, which increases credibility among users.

59%

state securing all cloud services with ZTS would improve **business continuity**.

61%

report securing all cloud services with ZTS would strengthen **cyber resilience**.

To learn more about redefining cloud security with Zero Trust Segmentation, please read the **full report**.