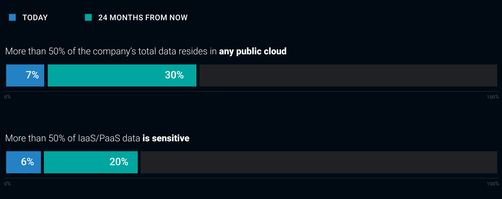
Enterprise Strategy Group
by TechTarget

SECURITY CONSIDERATIONS
for Cloud Data Transfers

In an era where the cloud is now the epicenter for data and applications, and data is continually moving, IT's focus must be on data security. Now that the cloud is becoming the main data repository, it represents an emerging threat vector for ransomware and viruses. Infected files can lead organizations to potentially lose data, customers, and revenue, all of which pose risk to the business. Additionally, cybercriminals are getting smarter when finding ways to access sensitive data.

Large Amounts of Cloud-resident Sensitive Data Are Insufficiently Secured

Data, especially sensitive data, continues to be migrated to public clouds as organizations leverage the efficiencies of massive on-demand analytics applications and data-processing power. The complexity of the cloud, combined with the volume, velocity, and variety of data, makes it difficult for organizations to classify and secure their sensitive data.



70%
of organizations reported that discovering sensitive data requires **reading 100% of the data.**

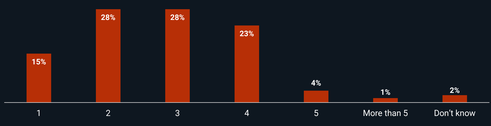
59%
said that more than 30% of their IaaS/PaaS sensitive data is **insufficiently secured.**

Loss of Cloud-resident Sensitive Data Is Common and Suspected

Unfortunately, organizations are losing cloud-resident sensitive data and experiencing multiple data loss events throughout the year. Data loss occurs in every cloud storage architecture for a multitude of reasons, including misconfiguration, policy violations, and access controls. Of great concern is that 20% of organizations likely don't have the tooling or expertise in place to detect and prevent data loss.

» LOSS OF CLOUD-RESIDENT SENSITIVE DATA IN THE LAST 12 MONTHS

» NUMBER OF TIMES LOSS, OR SUSPECTED LOSS, OF CLOUD-RESIDENT SENSITIVE DATA HAS OCCURED IN THE LAST 12 MONTHS



» TYPE OF DATA STORES ORGANIZATIONS EXPERIENCED CLOUD-RESIDENT SENSITIVE DATA LOSS FROM

34% Data warehouse
34% Raw object stores
34% Data lake
32% Data lakehouse
31% File stores
21% Block stores

» TOP CONTRIBUTORS TO CLOUD-RESIDENT SENSITIVE DATA LOSS

Data exposure from misclassification:
33%

Misconfiguration of IaaS/Paas services:
32%

Ransomware Attacks Are Pervasive and Impactful

47% of organizations are routinely (daily, weekly, monthly) targeted with ransomware. Malware and ransomware affect endpoints—local and cloud storage alike—and deliver financial gains for the attackers and debilitating results for victims. While paying ransom may enable an organization to recover some of its data, it also encourages attackers to come back for more.

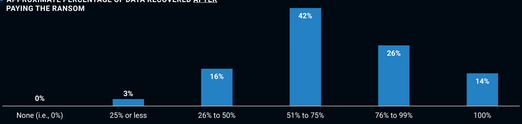
41%
of organizations have been the victim of a successful **ransomware attack.**

32%
of organizations have been the victim of a successful ransomware attack **more than once.**

56%
of organizations **paid a cyber ransom** to regain access to its data, applications, and/or systems.

61%
of organizations experienced additional extortion attempts or other fees beyond the initial ransomware demand, **and paid more.**

» APPROXIMATE PERCENTAGE OF DATA RECOVERED AFTER PAYING THE RANSOM



The Benefits of Securing Data Transfers

Securing data transfers can result in several benefits for organizations, including:

Visibility into data security blind spots.

An understanding of the data an organization has to aid in data loss prevention.

Assurance to customers that the data they're using is clean and trustworthy.

Risk mitigation to prevent repeat incidents.

Meeting compliance requirements (e.g., SOC2, HIPAA, etc.).

Job security for employees responsible for data security.

Reputational damage prevention (i.e., staying out of the headlines).

Prevention of productivity gaps, monetary loss, and fines by reducing the risk of breach.

Secure Data With Cloud Storage Security

Unsecured data creates risk for organizations as they move more of their data to and within the cloud. These organizations can effectively reduce their data security risk by classifying the data across their cloud data stores as well as ensuring they scan data to prevent infection and transmission of malware, viruses, and ransomware.

Cloud Storage Security (CSS) provides an easy way to incorporate security scanning into managed file transfers so organizations can protect their data in dynamic cloud environments. The CSS platform protects organizations from advanced threats, providing antivirus scanning, data classification, and assessments for storage in the cloud.

The solution installs and runs within an organization's AWS account so that data never leaves the environment or region. CSS flexibly supports any workflow with multiple ways to scan the data. In addition, users can automatically discover and scan data in AWS storage for threats using multiple industry-leading detection engines.

LEARN MORE

CLOUD STORAGE SECURITY

This Enterprise Strategy Group Infographic was commissioned by Cloud Storage Security and is distributed under license from TechTarget, Inc.

Source: Enterprise Strategy Group Complete Survey Results, *The Cloud Data Security Imperative*, April 2022.
Source: Enterprise Strategy Group Complete Survey Results, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

© 2023 TechTarget, Inc. All Rights Reserved.