

SECURING SENSITIVE DATA IN PUBLIC CLOUDS



SECURING CLOUD-RESIDENT DATA IS A TEST FOR MANY

Organizations are storing data in public clouds at an increasing rate. However, the speed at which organizations are moving data to public cloud storage is outpacing their ability to secure it.

81%

of respondents believe that on-premises data security is more mature than public cloud infrastructure/application data security.



75%

of respondents believe that 21% or more of their organization's sensitive data that is stored in public cloud services is insufficiently secured.



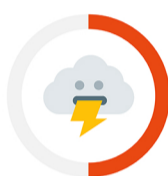
22%

of respondents *suspect* that they have lost cloud-resident data.



50%

of respondents *know* that they've lost cloud-resident data.



CLOUD DATA SECURITY CHALLENGES

The most commonly identified issues regarding the security of cloud-resident data centered around people, process, and technology.



Trusting employees to follow data usage policies



Ability to detect data breaches in real time



Identifying when data is being accessed via stolen credentials



Identifying culprits of data loss

CLOUD SECURITY LACKS IN IMPORTANT AREAS

ESG asked respondents to identify which specific areas of cloud security are coming up short, and what level of improvement they feel is needed.

Needs SIGNIFICANT improvement (i.e., top priority)

Needs SOME improvement



Detecting data loss/breach activity in real time

20% | **49%**



Determining location of breached data

22% | **45%**



Alert on the anomalous access to and use of data

21% | **46%**



Information to help narrow suspect list

20% | **47%**



Continuous risk assessment of third-parties

19% | **48%**



Expediting investigations of actual and attempted data loss

19% | **48%**

FINDING THE RIGHT BALANCE IS KEY

There are many reasons for organizations to embrace a cloud-centric approach to IT.

As a result, organizations will continue to migrate applications and data to public clouds for the foreseeable future. So too, concerns around the security of cloud-resident data will persist until organizations employ processes and technology that can secure their data regardless of where it resides.

A key piece of any solution is data loss detection and response. This includes the ability to track data, detect early breach activity, identify attackers, and respond with countermeasures.

[LEARN MORE >](#)

