SECURING CLOUD-RESIDENT SENSITIVE DATA

INCREASING PERCENTAGE OF SENSITIVE DATA IS MOVING TO PUBLIC CLOUDS

Organizations are storing more data in public clouds in conjunction with the use of SaaS applications and IaaS/PaaS platforms.

Respondents reporting that **over 30% of their company's total cloud-resident data is sensitive:**

CURRENTLY
37%

EXPECTED GROWTH WITHIN 24 MONTHS
67%

SECURITY OF SENSITIVE CLOUD-RESIDENT DATA REMAINS IN DOUBT

The speed at which organizations are moving sensitive data to public clouds exceeds their ability to store it securely.

75% of respondents said that
MORE THAN 20%
of their sensitive data is not sufficiently secured.

24% of respondents said that
MORE THAN 40%
of their sensitive data is not sufficiently secured.

MOVEMENT OF DATA TO THE PUBLIC CLOUD IS RESULTING IN DATA LOSS

Many organizations suspect that they've lost data stored in a public cloud-based application or platform.

50%
of respondents said that they know that they've lost data.

ONLY 26%
of respondents can say with certainty that they have not lost cloud-resident data.

DATA SECURITY CHALLENGES ABOUND WITH PUBLIC CLOUDS

Organizations cited a range of cloud data security issues aligned around people, process, and technology.

35%
Employees using cloud apps/services without IT approval

30%
Discovering/classifying data to address privacy concerns and compliance regulations

30%
General organizational knowledge of cybersecurity threats

29%
Trusting employees to follow organization's data usage policies

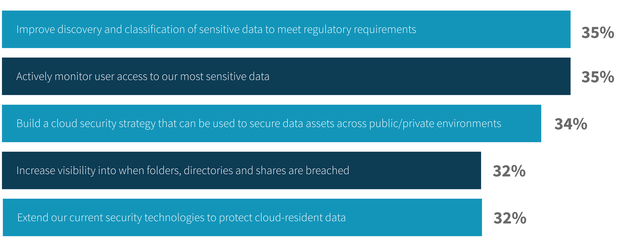
28%
Detecting data breaches in real-time

28%
Understand the shared security responsibilities in securing cloud resident data

IMPLEMENTATION PRIORITIES SPEAK TO SECURITY CHALLENGES WITH CLOUD-RESIDENT DATA

The ability to more easily meet regulatory requirements, actively monitor user access to sensitive data, and build a hybrid cloud approach to data security are key areas of focus.

Top 5 priorities for organization's to implement:



INVESTMENTS IN SECURITY CONTROLS FOR CLOUD-RESIDENT DATA CONTINUE

The volume of sensitive data moving to public clouds is expected to continue to increase. Given legitimate concerns about data loss within those environments, it's important to retool data security strategies and invest in the data security controls that best support those approaches.

This includes investing in data discovery and classification solutions that will make it easier to address regulatory compliance challenges and data encryption technology that can ensure data is protected should it fall into the wrong hands.

DOWNLOAD REPORT >

MICRO FOCUS

Produced exclusively for Micro Focus by The Enterprise Strategy Group, Inc. 2019
Source: ESG Master Survey Results, *Trends in Cloud Data Security*, December 2018