SECURING CLOUD-RESIDENT SENSITIVE DATA

Increasing Percentage of Sensitive Data Moving to Public Clouds

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

Sensitivity of Cloud-Resident Sensitive Data Remains in Doubt

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

Movement of Data to the Public Cloud Is Resulting in Data Loss

Many organizations now store data in the cloud.

Data Security Challenges Arise with Public Clouds

Organizations often experience data security issues around people, process, and technology.

Implementation Priorities Speak to Security Challenges with Cloud-Resident Data

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.

Investments in Security Controls for Cloud-Resident Data Continue

The need to move more sensitive data to public clouds is expected to continue to increase due to the benefits of increased agility and scalability that the cloud provides. The speed at which organizations are moving sensitive data to the cloud has outpaced their ability to store it securely.

Top 5 Priorities for Organizations to Implement:

- Improve discovery and classification of sensitive data and regulatory requirements
- Attract more mature access to protected sensitive data
- Build a security strategy that is aligned to secure data across on-premise and public environments
- Create a culture of security so that everyone embraces and protects sensitive data
- Invest in encryption technologies to protect cloud-resident data

Percentage of respondents reporting that over 30% of total company cloud-resident data is sensitive:

- Current: 37%
- Expected within 24 months: 67%

Percentage of respondents saying that they know that they’ve lost data:

- Only 26%

More than 20% of respondents said that MORE THAN 40% of their sensitive data is not sufficiently secured.

29% of respondents said that MORE THAN 20% of respondents said that MORE THAN 40% of their sensitive data is not sufficiently secured.

35% of respondents said that they don’t know where their sensitive data is.

35% of respondents said that they don’t know where their sensitive data is.

Download Report — Produced exclusively for Micro Focus by The Enterprise Strategy Group, Inc. 2019