VERITAS

The Not-So-Silver Lining of Cloud Service Providers' Tools

2022 Research Report on Securing Your Enterprise in a Multi-Cloud Environment

GLOBAL OUTLOOK

Exploring the layers of cloud operations and the gaps CSP tools create in enterprise data visibility and security.

How much are enterprises using CSP backup and recovery tools?

99%

99% of respondents said they use CSP backup and recovery tools to some degree

48% use these tools "all of the time"
46% use them "most of the time"

Smaller companies use these tools slightly more – **51%** of those companies with fewer than 5,000 employees use them all of the time, compared to **41%** of those with 5,000 or more employees

Why do companies use CSP backup and recovery tools?

- Cost-Effective
- Easy to Use
- 24/7 Support Available

How much is IT complexity increasing from digital transformation and migration to the cloud?

96%

96% of respondents said some improvements are needed to track their organizations' entire data footprint

59% of respondents said they have "complete visibility" into data stored within cloud environments

To what extent do enterprises understand their cloud data protection responsibilities?

94%

of respondents do **NOT** understand their cloud data protection responsibilities

"The CSP protects the infrastructure only; the customer is responsible for protecting their applications, and data."

Just **6%** of respondents identified the correct statement above, based on their understanding of the cloud shared responsibility model.

What are the consequences of using CSP backup and recovery tools?

89% experienced a ransomware attack on data they hold within cloud environments

53% have lost data as a result of using CSP backup tools

Top impacts organizations have experienced as a result of a ransomware attack on cloud-based data:

- 41% Exposure of Sensitive Data
- 39% Financial Losses From Data Recovery
- 39% Organizational Downtime
- 36% Permanent/Temporary Loss of Data

How aware are IT leaders of the dangers of using CSP backup and recovery offerings?

"The current offering from public service cloud providers fall short of my organization's security need."

76% respondents agree

64%

of respondents said they agree that relying solely on CSP tools puts their organization at risk

In what ways are enterprises ensuring data protection and disaster recovery?

Just **11%** of respondents said their organization performs backup of it's data continuously

46% backup their data less frequently than every 12 hours

In the past 2 years, organizations have experienced the following, which have resulted in downtime:

- 27% Natural Disaster
- 43% Hardware or Software Outage
- 40% Cloud Provider Outage

Organizations can mitigate the effects of ransomware, outages, natural disasters, and other checkpoints if they have visibility into:

- Reliance on CSP data protection offerings
- Business-critical data in the cloud
- Protective measures in place for data and applications
- Security, performance and cost advantages with a robust, holistic solution

HEADQUARTERS
2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827 | veritas.com

For more information visit:
veritas.com

Follow us on Twitter at @veritastechllc

VERITAS

V1700 11/22