Cloud Storage Elevates Data Protection

Pathfinder Report

April 2022

Commissioned by

SEAGATE

SEAGATE LYVE™ Cloud

451 Research

S&P Global Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

Henry Baltazar

Research Director, Storage

Henry Baltazar is a Research Director for the storage practice at 451 Research, a part of S&P Global Market Intelligence. Henry returned to 451 Research after spending nearly three years at Forrester Research as a senior analyst serving Infrastructure & Operations Professionals and advising Forrester clients on datacenter infrastructure technologies. Henry has evaluated and tested storage hardware and software offerings for more than 15 years as an industry analyst and as a journalist.

Prior to 451 Research and Forrester, Henry spent nearly nine years working as a technical analyst for eWeek Labs, where he covered storage, server hardware and network operating systems. At eWeek Labs, he initiated the testing coverage of various technologies, including data replication, clustering, virtual tape libraries, storage virtualization, SAN management, NAS, iSCSI and email archiving. In addition, Henry was a member of eWeek's editorial board and provided content for the magazine's enterprise storage blog. Henry has been widely quoted in the press, including such media outlets as Silicon Valley Business Journal, Computerworld and SearchStorage.com.

Henry holds a BA in environmental sciences from the University of California, Berkeley.

Executive Summary

IT resiliency has always been a key goal for organizations, but it is becoming more difficult to achieve because of multiple factors. Rapid data growth is commonplace at many organizations, while storage IT budgets are growing at only a modest rate. New challenges such as the rising threat of ransomware are also giving organizations ample reason to improve and enhance their data protection toolsets and processes. One major technology disruption that has become mainstream in recent years is cloud-based data protection services such as online backup and disaster recovery as a service (DRaaS), which can take advantage of the elasticity and resources of cloud storage service providers.

Key Findings

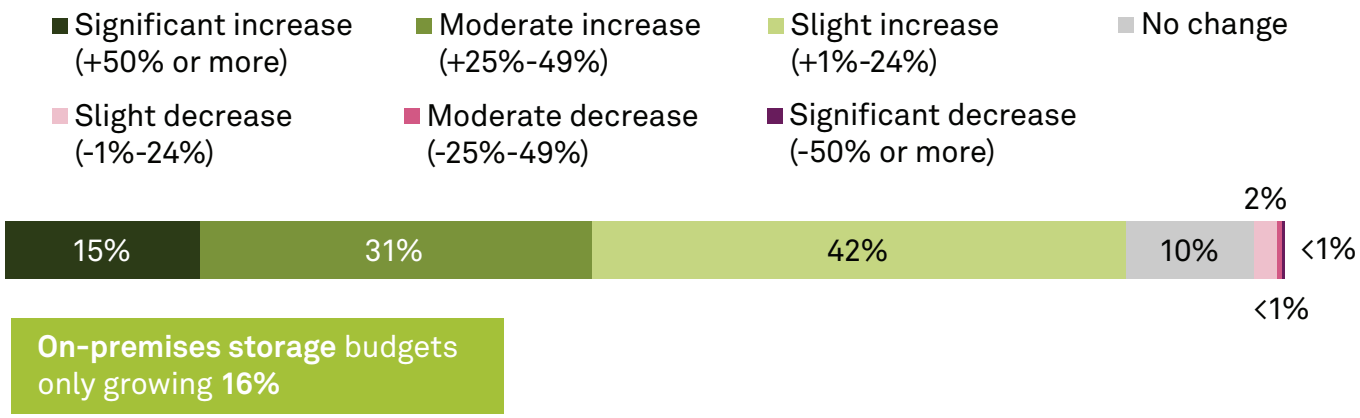
- Data growth is a top storage pain point, and this is forcing organizations to reevaluate the storage and data protection in their IT infrastructure.
- Outages have major impacts on revenue and can negatively inhibit a business in multiple ways.
- Most organizations are already leveraging cloud in their data protection strategies either in a hybrid cloud configuration or as SaaS (online backup or DRaaS).
- Egress charges and API access fees are hampering the adoption of cloud storage services.

Market Requirements and Customer Pain Points

Data Growth Is Outpacing Budget Growth

Data growth continues to be the top challenge facing organizations, and this issue is unlikely to go away. We emphasize that rapid data growth is a natural trait for organizations that are thriving and digitally transforming their operations. If anything, companies should be concerned if they are not seeing any data growth in their environments. In the Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2021 survey, less than 4% of the total respondents said they expect the data they have under management to decrease over the next 12 month, with only 10% expecting no change in the amount of data. On average, respondents expect to see their data grow by 28% in the next 12 months, which is comparable to the data growth expectations we have seen in previous studies.

Figure 1: Data Is Growing Rapidly at Most Organizations



On-premises storage budgets only growing **16%**

Q: Over the next 12 months, do you expect the amount of data your organization has under management to increase, decrease or not change?

Base: All respondents (n=458)

Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021

In contrast, respondents expect the budgets for on-premises storage to grow by only 16%. The cost of storage systems and services tends to decline over time thanks to technology advances such as higher-density hard drives and flash storage, and with data growth greatly outpacing budget growth, many organizations are looking to upgrade their storage systems and data management to maximize utilization and efficiency of their storage assets.

Organizations are using cloud storage to help alleviate the effects of data growth. In the study, 61% of respondents said they are already using public cloud storage services, and 59% said their use of public cloud storage is impacting their budgets for on-premises storage systems. For many IT professionals using public cloud resources for the first time, unstructured data archiving and data protection are attractive use cases if they're not ready to move production workloads to the cloud.

Outages Have Many Negative Consequences

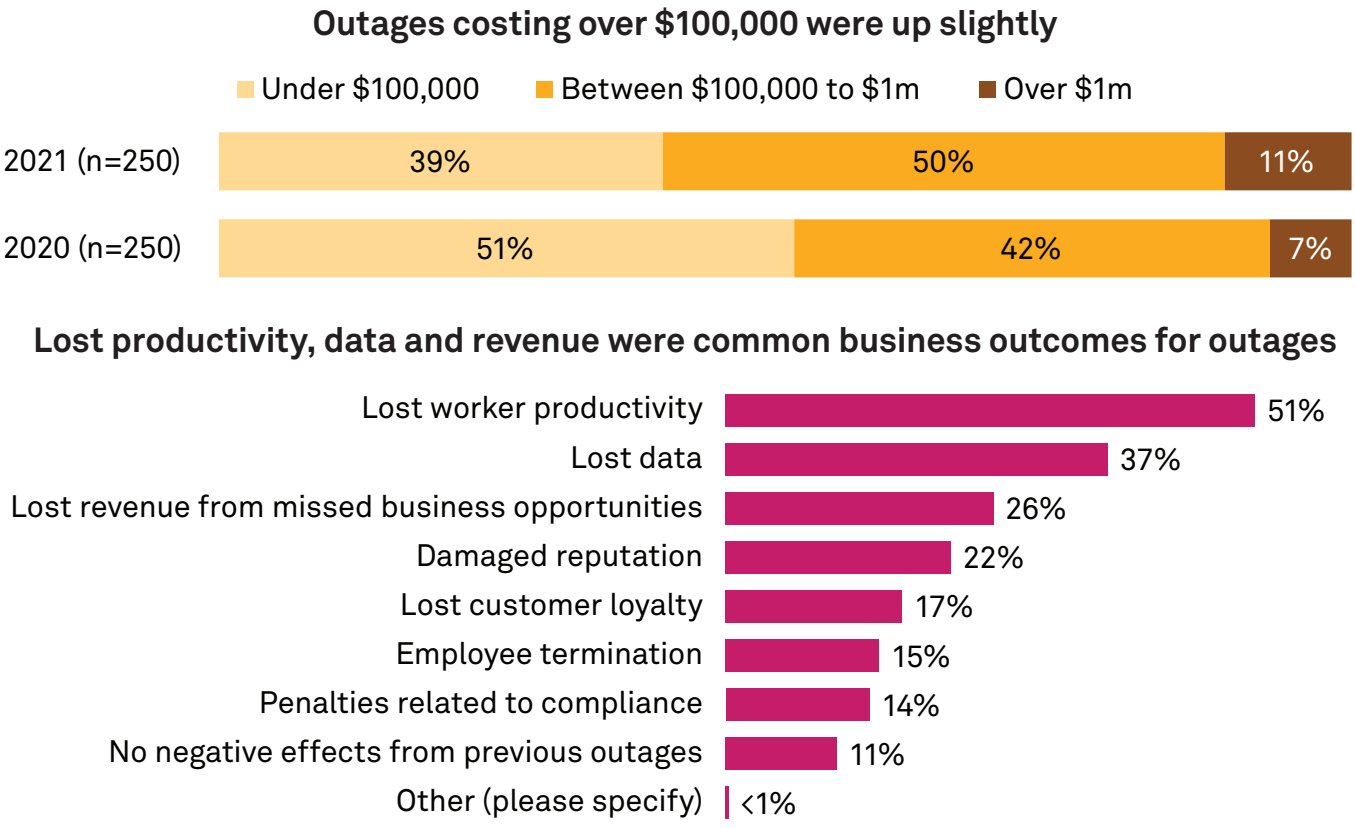
"When there's an outage, it means people cannot work. It's not their fault, whether they're contractors or whether they're full-time members of staff, whatever. If there's an outage, they simply can't work, and you still have to pay them… They just go back to the coffee room and start drinking coffee all day, whatever, and go home."

IT/engineering manager/staff

10,000-49,999 employees, $10bn+ revenue, financial services

According to the Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021 survey, meeting disaster recovery and business continuity requirements is the second most important pain point organizations have to face. In the study, nearly 30% of respondents said they were impacted by an outage within the last two years. Of all the respondents who said they have had an outage that resulted in lost data or productivity, 11% said that the outage cost their organization over $1m, which was up slightly from 7% in the previous study, and 50% said their outages cost $100,000-$1m, up from 42% a year ago.

Figure 2: Outages Are Costly – in Terms of Lost Productivity and Revenue



Q: What was the estimated total cost of your organization's most recent downtime incident (from outage to full recovery)?
Base: Had outage that resulted in data or productivity loss
Q: Which of the following effects did your organization experience as a result of your previous outages? Please select all that apply.
Base: Had outage that resulted in data or productivity loss (n=317)
Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021

Loss of worker productivity, highlighted in the quote from a large financial services company, was the most common business outcome from outages (according to the 51% of respondents who experienced an outage), followed by lost data (37%). The impact of these two consequences is driving many organizations to increase their investments in improving their data protection capabilities to avoid future outages. Given the rising importance of customer experience for companies, damaged reputation, loss of customer loyalty and the loss of business revenue are all key factors that show upper management teams, which are sometimes hesitant to make the required investments, the need for improved resiliency. Outages could also lead to substantial penalty fees for organizations if deliverables aren't produced in a timely manner.

Technology Discussion

Cloud-Based Data Protection Is Already the Norm

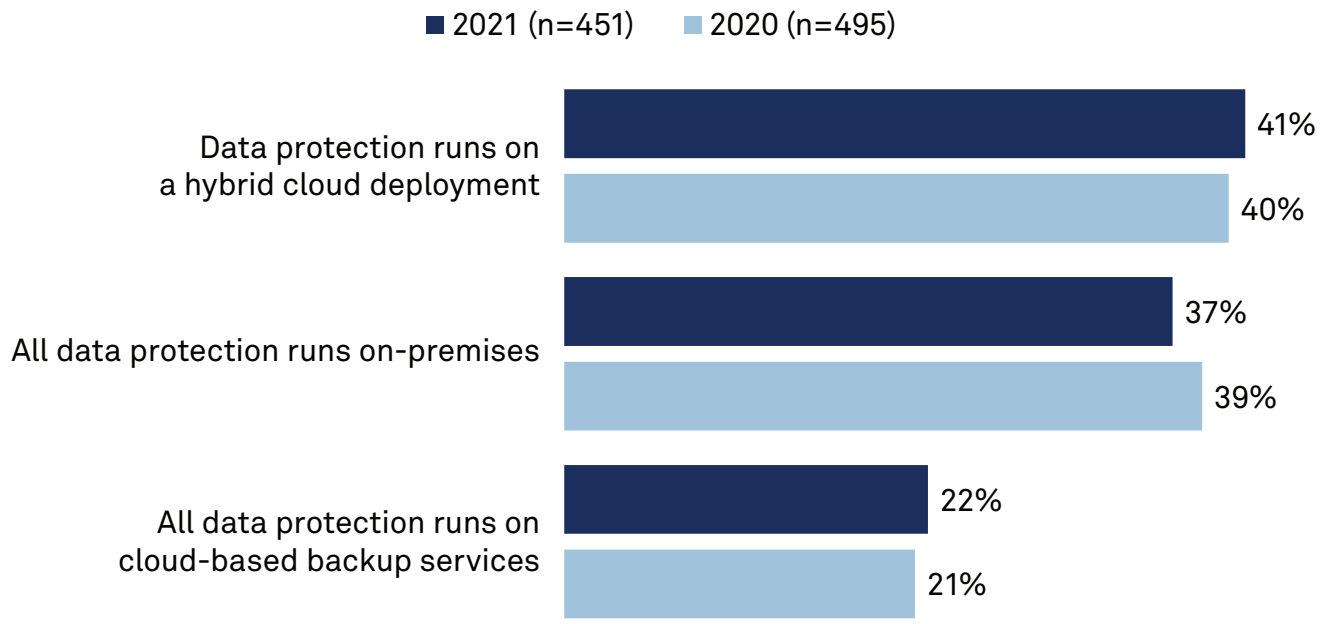
"On the cloud, we're looking for resiliency, we're looking for scalability…and we're looking for cost per terabyte…[For data management] there's a point that we take advantage of our cloud providers' tools and third-party tools to help us carry that out."

IT/engineering manager/staff

10,000-49,999 employees, $10bn+ revenue, financial services

As the quote above suggests, cloud storage can provide a variety of benefits, such as resiliency, scalability and cost reduction. *Cloud-based data protection such as hybrid backups, online backup and DRaaS have become more commonplace in recent years, and often represent a company's first steps into cloud. In the study, the majority of respondents are already leveraging cloud storage resources and services to protect their data and workloads.* Just 37% of respondents reported that they are running all their data protection on-premises, compared with 41% who are running hybrid backup deployments –running backups locally and storing long-term backup data in a cloud.

Figure 3: Most Organizations Are Using Cloud-Based Data Protection, But Some Are Not Budging



Q: Which of the following best describes your organization's current use of data protection (e.g., backup, disaster recovery)?
Base: All respondents
Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021

Cloud-only data protection services such as online backup and DRaaS are preferred by 22% of respondents. These offerings can be easily adopted by newer and smaller companies that need enhanced IT resiliency but may not have an existing investment in on-premises backup and disaster-recovery tools. The drive to reduce and, if possible, eliminate downtime has also increased the popularity of DRaaS offerings, which can rapidly failover workloads to a cloud environment in the event of an outage. Another benefit of DRaaS offerings is that they take advantage of the elasticity of cloud so that resources are only consumed when required. In contrast, traditional disaster-recovery implementations can be extremely costly since they require companies to set up or lease secondary datacenters with standby equipment to handle the workload in the event of a disaster.

Organizations that only have one site are leveraging the cloud to act as a secure repository in a different geographic region for recovery or long-term data storage, which is necessary for rapidly restoring operations in the event of a major disaster such as a fire, flood or earthquake. Even established companies that already have multiple sites to facilitate failovers are looking to leverage cloud, since a cloud-based recovery service would not require on-premises IT staff members to manage and run them, which is another key driver for switching to cloud storage over on-premises storage assets such as arrays and virtual tape libraries.

Cost continues to be a concern for cloud storage customers, and this extends well beyond the standard per-GB, per-month charges associated with file, block and object storage services. Charges for API access and egress, which would be incurred when a hybrid cloud backup customer downloads backup data from a cloud repository, impact the overall cost for recovery and should be factored into a customer's cost considerations.

Egress and API Access Fees Are Making an Impact

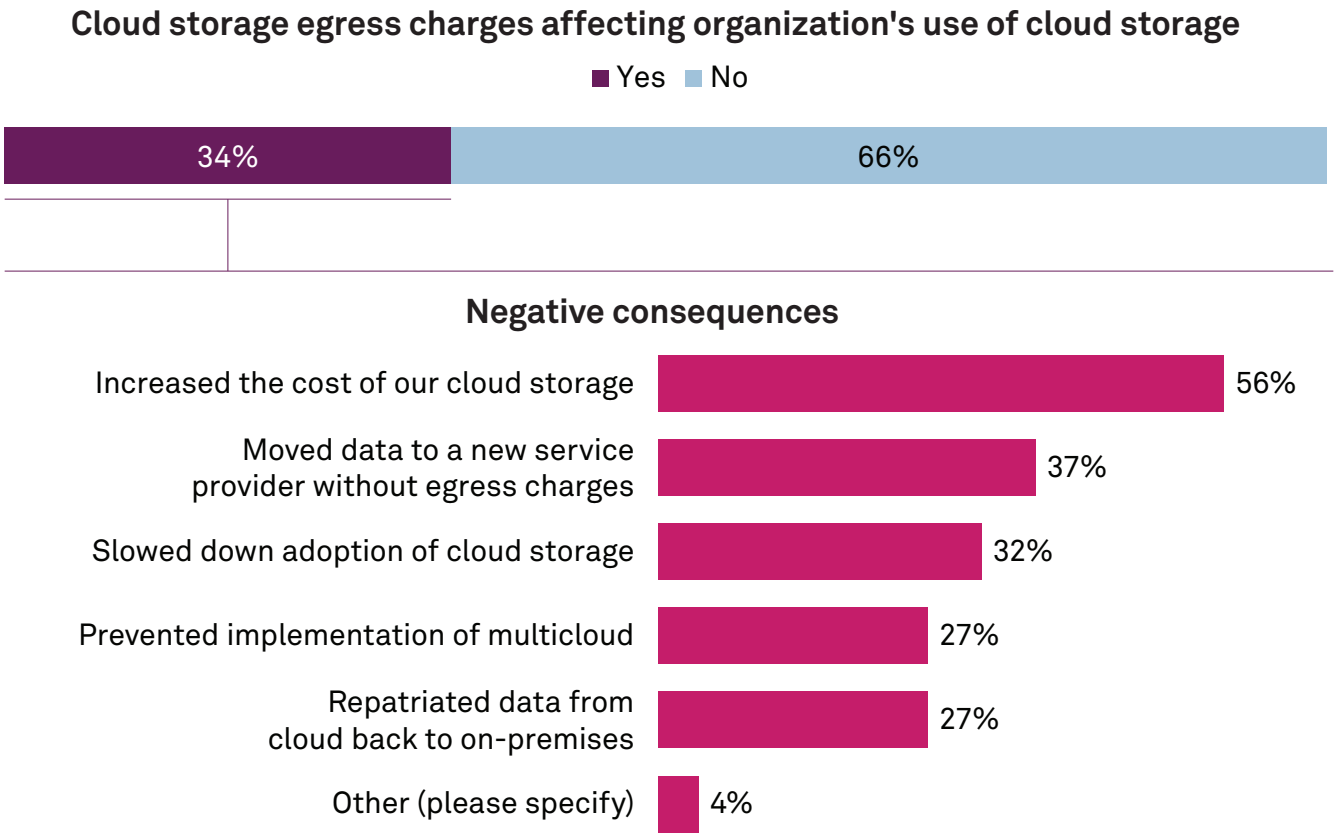
"The egress costs and the data movement costs involved in doing [data migration], and just the sheer amount of time of moving hundreds of terabytes of data into and out of the cloud, it just makes it impractical [for us]."

Mid-level management

5,000-9,999 employees, $1bn-$2.49bn, financial services

Though many of the major cloud storage service providers do not charge their customers ingress fees for the data they import into their clouds, these vendors typically charge customers egress fees for downloading data over the internet or migrating their data out of the provider's cloud. In our study, 34% of respondents said they have been impacted by egress charges, and the top consequence of these charges are increased costs for cloud storage (56%).

Figure 4: Consequences of Egress Charges



Q: Have cloud storage egress charges affected your organization's use of cloud storage? Base: Uses public cloud storage (n=222)

Q: Which negative consequences have occurred? Please select all that apply. Base: Cloud storage egress charges affected use of cloud storage (n=75)

Source: 451 Research's Voice of the Enterprise: Storage, Transformation 2021

In recent years, new service provider competitors have started offering cloud storage services with either no or reduced egress fees to entice customers to their cloud, and 37% of the survey respondents said they migrated their data to these providers. Given that 32% of respondents slowed down their adoption of cloud storage as a result of egress charges, some of these organizations may eventually switch to services with no or reduced egress fees. Twenty-seven percent of respondents reported that egress charges prevented their organization from implementing their multicloud strategy, which is another reason why this issue could impede the transition to cloud. In the quote above, the financial services organization slowed down its migration to cloud due to cost fears associated with egress charges, in addition to fears it would not be able to move large amounts of data in the hundreds-of-terabyte scale from the cloud in a timely manner. Some cloud storage providers are now offering physical transport and shuttle services to rapidly move data when migration over existing network connections would be too slow to meet business requirements.

Beyond egress charges, organizations are being financially impacted by API access fees based on the number of API requests sent to the cloud provider. Like the egress charges, API access fees are often an unwelcome surprise to customers that did not factor these fees when designing and budgeting their cloud solutions.

Ransomware Recovery Is Centered On Golden Copies

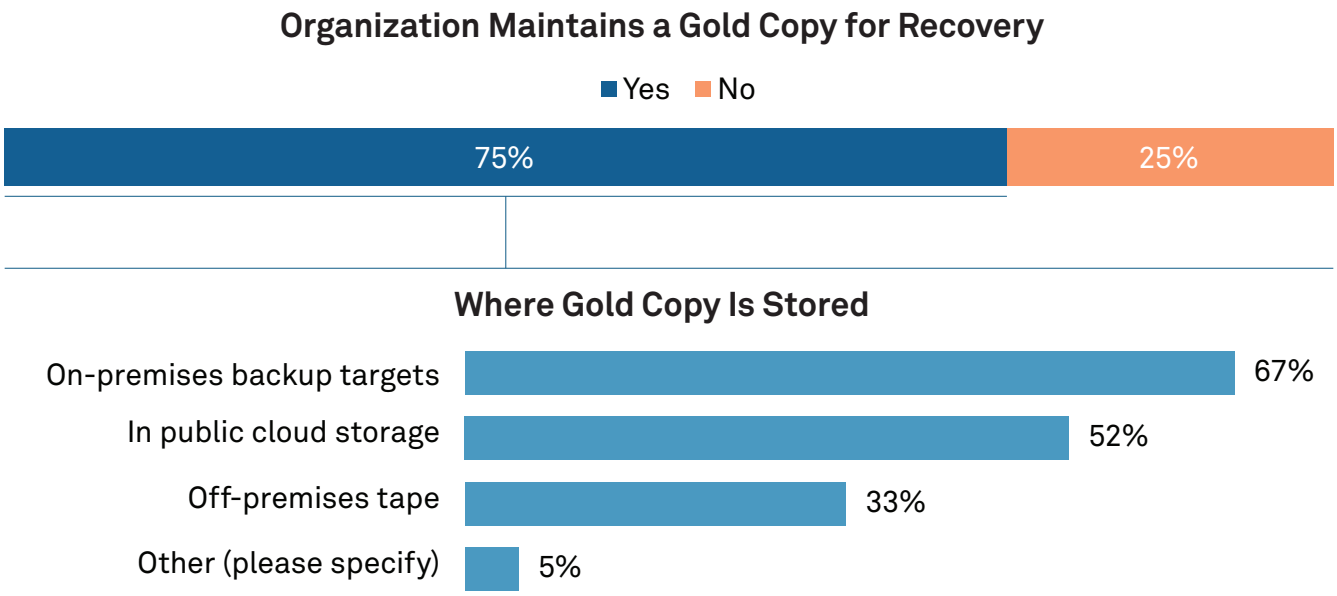
"It's definitely a concern to be able to recover from ransomware, how would we be able to take advantage of our DR tools, our backup tools…the replication tools, VMware, stuff like that… We're looking for disaster recovery tools for their capability to help us cope from ransomware."

IT/engineering manager/staff

100-249 employees, $10m-$24.9m, media & communications

The rising impact of ransomware attacks, which are becoming more frequent and costly for organizations, is another major factor pushing organizations to leverage cloud-based data protection. The media & communications organization quoted above highlighted the need to improve backup and disaster-recovery capabilities as a result of the growing ransomware threat. The 3-2-1 backup guidelines call for customers to have a minimum of three copies of data (the production data and two backup copies) on two media types (disk, tape, cloud) with one copy off-site for disaster recovery. Cloud storage is an attractive choice in this scenario since it not only acts as alternative media format, but it also covers the off-site disaster recovery requirement. In the study, 67% said they store their golden copies for data restoration in on-premises backup targets, and 52% are already leveraging cloud storage. A third of respondents are still using off-site tape, though we note that it could take a while to recover due to the time it takes to transport and restore data from that format.

Figure 5: Golden Copies Provide a Safety Net Against Ransomware



Q: Does your organization maintain a 'gold copy' of data to recover after a ransomware incident? Base: All respondents (n=411)
Q: Where does your organization store its gold copy of data? Please select all that apply. Base: Organization has a 'gold copy' (n=300)
Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021

Given that backup repositories are the final safety net for organizations and are now being targeted by hackers, immutable or air-gapped storage – which prevents backup data from being deleted or corrupted – is a key requirement for ransomware recovery. While tape has been a popular air-gapped storage solution for years because it can be physically detached from networks, many cloud storage providers now have the ability to make their object storage services immutable to satisfy this requirement while still keeping data available for read access in a timely manner.

The existence of a golden copy alone isn't sufficient to ensure protection against ransomware or other disasters. Organizations need to test backup and disaster-recovery processes regularly and leverage automation, when possible, to both reduce the burden of testing and to ensure consistency in the recovery operation. Slow recovery operations only prolong outages and can lead to additional lost revenue and consequences. Without testing, matters could get worse if the data recovered is corrupted on incomplete. Beyond site-recovery benefits, cloud-based backup and disaster recovery can also take advantage of elastic cloud resources to facilitate testing.

Implications

"[A significant business outage] was what compelled this current migration into a move to the cloud... Aging equipment. Aging infrastructure. Aging legacy systems. A lack of visibility into this aging system. That was the two factors I could easily identify as being the cause for the outage."

IT/engineering manager/staff

Other, $500m-$999.99m, 2,000-4,999 employees

The need for enhanced resiliency has driven many organizations to rethink how they fulfill their data protection and recovery requirements. As illustrated in the quote above, cloud storage services have emerged as an alternative to legacy on-premises data protection equipment and software.

As organizations look to enhance their IT resiliency, it's important that they keep the following points in mind:

- Cloud storage is already mainstream, and data protection is a good place to start.
- Be aware of egress and API charges and consider alternative services to reduce costs.
- Ransomware recovery volumes should be kept at multiple sites and should be immutable.
- Consider using a cloud storage provider that offers physical transports for moving large datasets to/from cloud.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence