Pathfinder Paper

March 2023

Hybrid and Multicloud Deployments Bring New Backup Challenges

Commissioned by

VEEAM

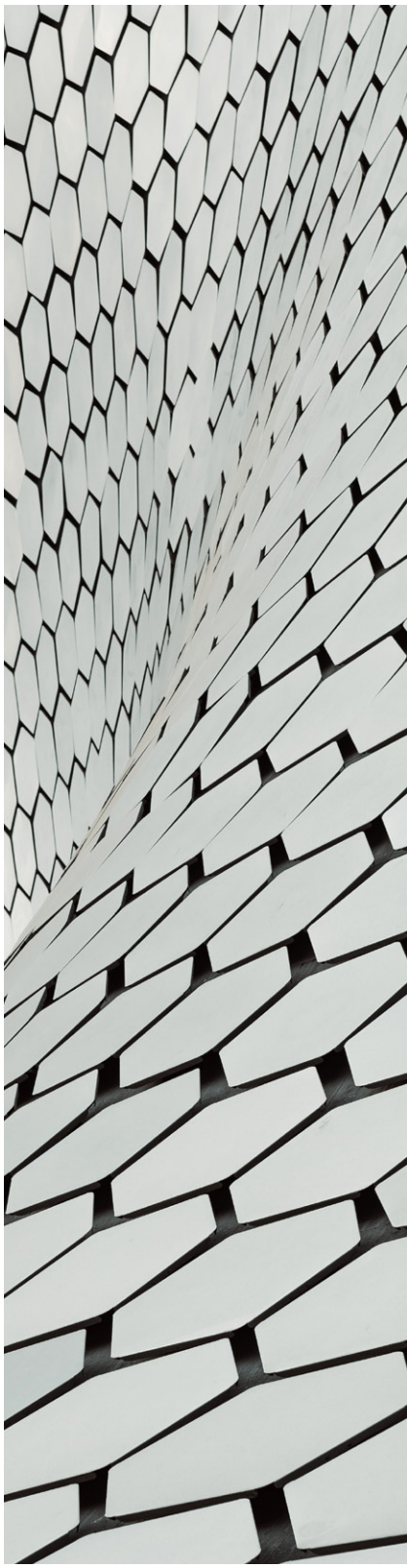
S&P Global
Market Intelligence

Executive summary

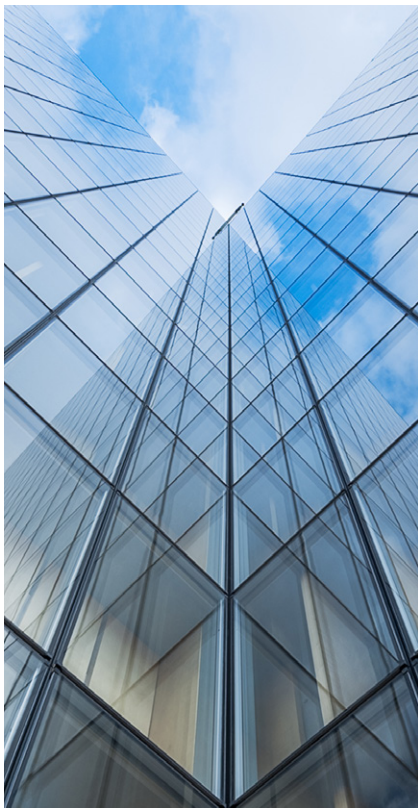
Hybrid cloud and multicloud deployments provide organizations with key benefits such as workload mobility, the ability to expand or contract resource consumption based on workload needs, and rapid access to new technology innovations delivered as cloud services. With customer expectations for resiliency increasing rapidly, hybrid and multicloud environments require enhanced tools that not only provide data protection, but also address the nuances of cloud-native elements such as Kubernetes and modern applications to ensure recovery operations run smoothly and consistently when a disaster strikes. With many organizations struggling to meet recovery expectations, many are turning to managed and professional services to enhance the resiliency of their workloads.

Key findings

1. In a recent 451 end-user survey, 56% of organizations that are using or planning to use public cloud services said they will use multicloud and hybrid cloud together as their preferred cloud operating model.
2. A third of survey respondents have experienced an outage in the past two years, and 30% of these incidents led to losses of more than $1 million.
3. Of these recent outages, 28% were caused by public cloud or SaaS failures.
4. Security, cost and skills gaps were cited by surveyed organizations as top challenges in executing their cloud strategies.
5. Among survey respondents, 83% said they are likely to leverage managed and professional services providers to support their cloud strategies.



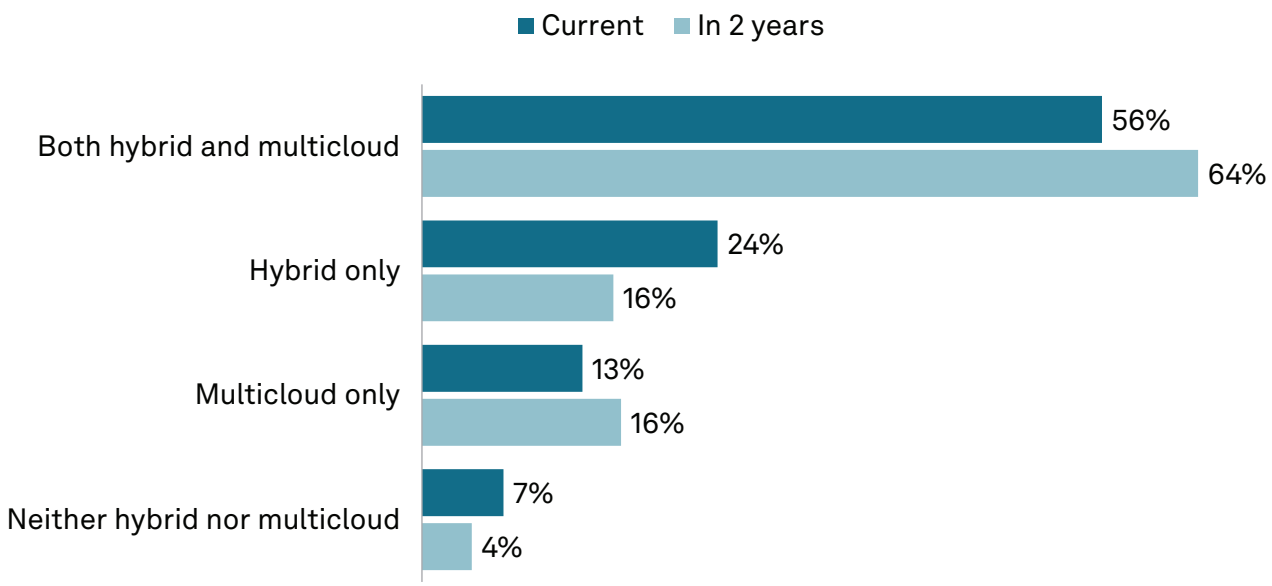
Multicloud and hybrid cloud are both essential for cloud operating models



In 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022 study, we found that most respondents (56%) are looking to leverage both hybrid and multicloud in their cloud operating models (see Figure 1). Organizations that favor hybrid-only cloud operating models increased to 24% of respondents, up from 16% a year ago, which shows that even if an organization decides to work with a single cloud provider, some still want to have the option to bring data and workloads back to on-premises infrastructure.

To meet persistent storage requirements for containers, 51% of survey respondents prefer to leverage public cloud storage services, while 48% prefer either on-premises storage resources or purpose-built software-defined storage offerings. Given this even distribution of persistent data across public cloud and on-premises venues, it is clear that organizations should be prepared to provide their stakeholders with a variety of storage options, especially if these organizations want to facilitate workload mobility.

Figure 1: Hybrid and multicloud together is the preferred operating model



Q. Which best describes your organization's cloud operating model, now and in two years?
Base: Organizations that use public cloud, or plan to use public cloud in the next year. Now (n=494); In two years (n=464).
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022.

Factors driving multicloud architectures

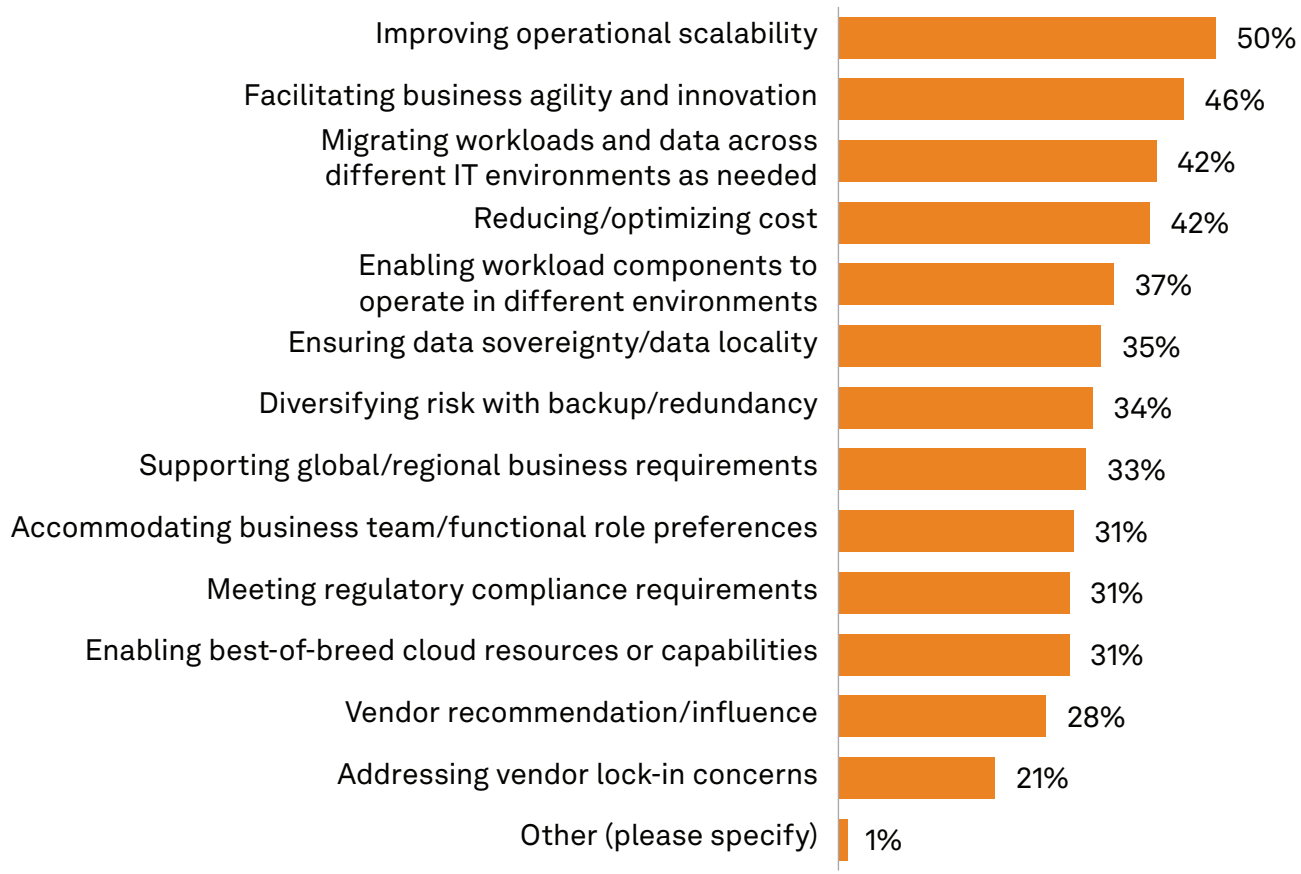
Organizations are seeking to attain several key infrastructure and data management benefits by adopting hybrid and multicloud environments for their cloud operating models. Infrastructure transformation enhancements for scalability, agility and cost reduction are major goals among respondents in the Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022 study, including:

- **Improved operational scalability:** 50% of respondents cited this as a major factor driving their multicloud strategy. Through the use of elastic storage, compute and microservices, companies are able to rapidly add new workloads, or resize resources to match the needs of a workload without requiring the disruptive "forklift upgrade" commonly seen in physical IT infrastructures.
- **Business agility and innovation:** 46% of respondents felt the adoption of multicloud would give their business improved access to new innovations from cloud providers such as microservices, AI/ML algorithms and analytics services.
- **Workload and data migration** was a desired improvement for 43% of survey respondents. Migration capabilities can be helpful for load management purposes when a site or cloud region becomes overburdened, and they are also needed to facilitate failover operations when an availability zone or site goes down.
- **Workload interoperability across different environments** was a factor for 37% of respondents. This is essential for bouncing workloads between on-premises and public cloud venues for hybrid cloud customers. Likewise, organizations using multiple public cloud vendors want the ability to move a workload between hyperscaler environments without requiring significant application coding, in order to get workloads up and running in a new cloud when necessary.
- **Reduced/optimized costs:** Cost-related benefits were targeted by 42% of survey respondents. The wide range of cloud compute, storage and service classes offer customers multiple choices to match the needs of specific workloads to appropriate price bands.

There are other factors also underpinning the adoption of multicloud architectures. Data management improvements were in high demand among our survey respondents, driven by requirements around resiliency, security, governance and risk management:

- **Ensuring data sovereignty/data locality** was a factor for 35% of survey respondents, and it continues to be a requirement for organizations in countries that do not allow sensitive data to be processed or stored outside of their borders. According to the United Nations Conference on Trade and Development (UNCTAD), 137 out of 194 countries have put in place legislation to secure the protection of data and privacy.
- **Diversifying risk with backup and redundancy** was required by 34% of respondents, which highlights the ability for cloud environments to create backup repositories and recovery sites on demand, as an alternative to building and running secondary failover datacenters.
- **Meeting regulatory compliance requirements:** 31% of survey respondents were looking to deploy clouds to meet various compliance requirements such as those around data retention, and also for resiliency (discussed further in the next section).

Figure 2: Operational scalability, agility and cost reduction drive cloud transformation



Q. Which of the following are the most significant factors driving your organization's hybrid/multicloud strategy? Please select all that apply.
Base: Organizations with hybrid or multicloud as their current or future cloud operating model, abbreviated fielding (n=353).
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022.

Resiliency is a key concern

Workload resiliency is important for every organization, regardless of size and industry. In 451 research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2022 study, nearly a third of organizations said they suffered a significant outage that either led to data loss or a loss of worker productivity within the last two years (see Figure 3). The negative business impact of outages also leads to lost revenue from missed business opportunities (which 26% of respondents experienced), damaged reputation (18%), lost customer loyalty (13%), penalties related to compliance (13%), and even employee termination (13%). For 30% of survey respondents, their most recent outage led to over $1 million in losses, with 11% losing over $5 million.

Complicating matters is the fact that there are many causes behind these outages. In the study, public cloud or SaaS failures were responsible for 28% of the most recent outages among respondents, which highlights the need to add data and workload protection, even though customers are not responsible for maintaining the software and hardware that runs a cloud service. Network failures were the cause of 34% of the outages, which highlights the need for customers to have secondary failover sites to handle production workloads should a primary datacenter lose its connectivity.

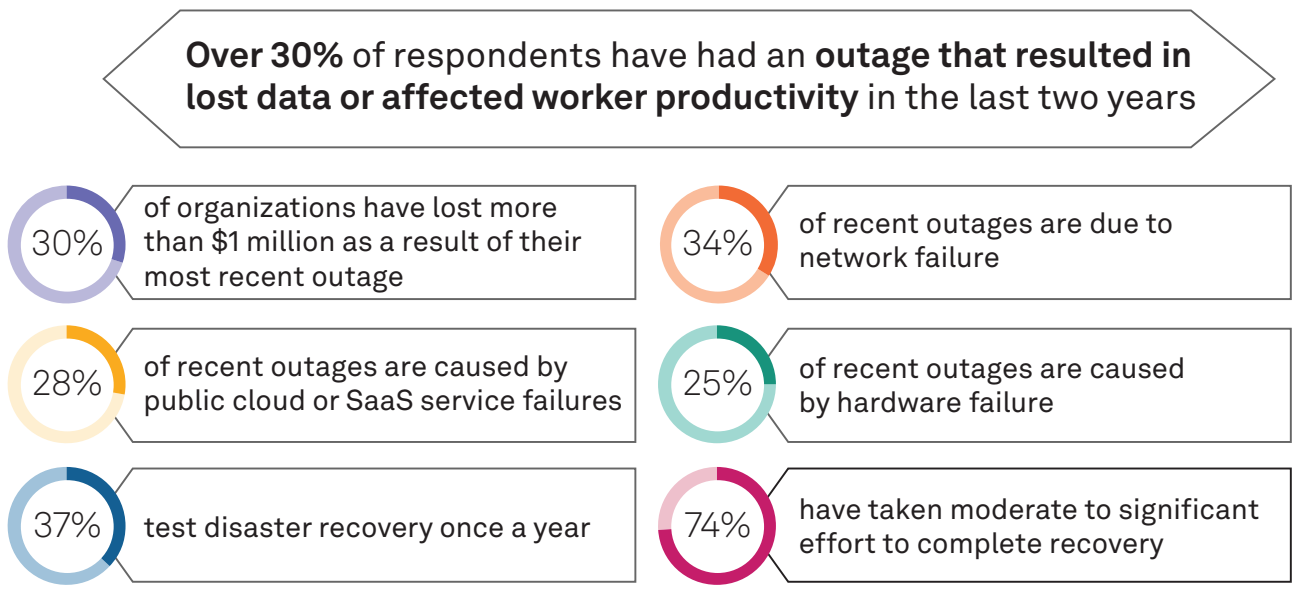
To best match the resiliency requirements of hybrid and multicloud environments, which could stretch across multiple clouds and geographies, modern data protection tools must be able to support all the execution venues where workloads can run, while also facilitating data replication and migration between the various sites.

Just as the evolution of IT infrastructure from physical servers to virtual machines created opportunities for emerging players to take market share away from legacy vendors that did not rearchitect their offerings to match the needs of virtualization, the emergence of cloud-native technologies such as Kubernetes is creating a similar market disruption. In the study, 58% of respondents said they preferred to use data protection tools and services that were designed for containers, as opposed to just 29% that favored sticking with their legacy backup tools to protect cloud-native workloads.

Another concern for organizations is the difficulty associated with recovery operations, as 74% of respondents to the Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2022 study claimed it took moderate to significant levels of effort to recover from their most recent outages. While disaster recovery tests can help organizations ensure that recovery operations run smoothly, many still need to improve their testing frequency. In the study, 37% of respondents claimed they tested DR once a year, while 30% tested twice a year. Just 21% claimed they were running tests more than twice a year. This frequent level of testing must become more common going forward, given that cloud-native infrastructure and modern applications are highly dynamic, with frequent changes and updates to applications or cloud services that could lead to complications when recovery operations are initiated.

Another finding of the Data Management and Disaster Recovery study was that 59% of respondents claimed they were increasing their spending on backup services and backup storage because of the growing threat of ransomware. With attackers now taking aim at the backup repository safety net, customers must now invest in immutable cloud storage or immutable storage systems to prevent attackers from modifying or deleting backups, in order to ensure that recovery operations can occur and avoid having to pay a ransom to recover data and workloads. In the study, 47% of respondents were storing their golden backup copies in public cloud storage, while 61% favored on-premises backup targets such as object storage systems and virtual tape libraries. Meanwhile, 27% were still clinging to off-premises tape for backup storage, which highlights the need for broad backup target support for next-generation data protection platforms.

Figure 3: Costly and common outages are driving resiliency improvements



Q. When was the last time your organization experienced an outage that resulted in lost data or affected worker productivity? Base: All respondents (n=372).
Q. Please estimate the total cost of your most recent cloud outage or downtime (from outage to full recovery, including direct costs, opportunity costs, etc.). Base: Organizations with recent service outages/incidents and have estimated costs (n=192).
Q. What was the cause of your most recent outage that resulted in lost data or affected worker productivity? Please select all that apply. Base: Organizations with an outage that resulted in lost data or lost worker productivity (n=256).
Q. How much effort is required to resume normal operations after a failure (i.e., a failback)? Base: All respondents (n=367).
Q. How frequently does your organization test your disaster recovery plan? Base: All respondents (n=372).
Source: 451 Research's Voice of the Enterprise: Storage, Data Management & Disaster Recovery 2022.

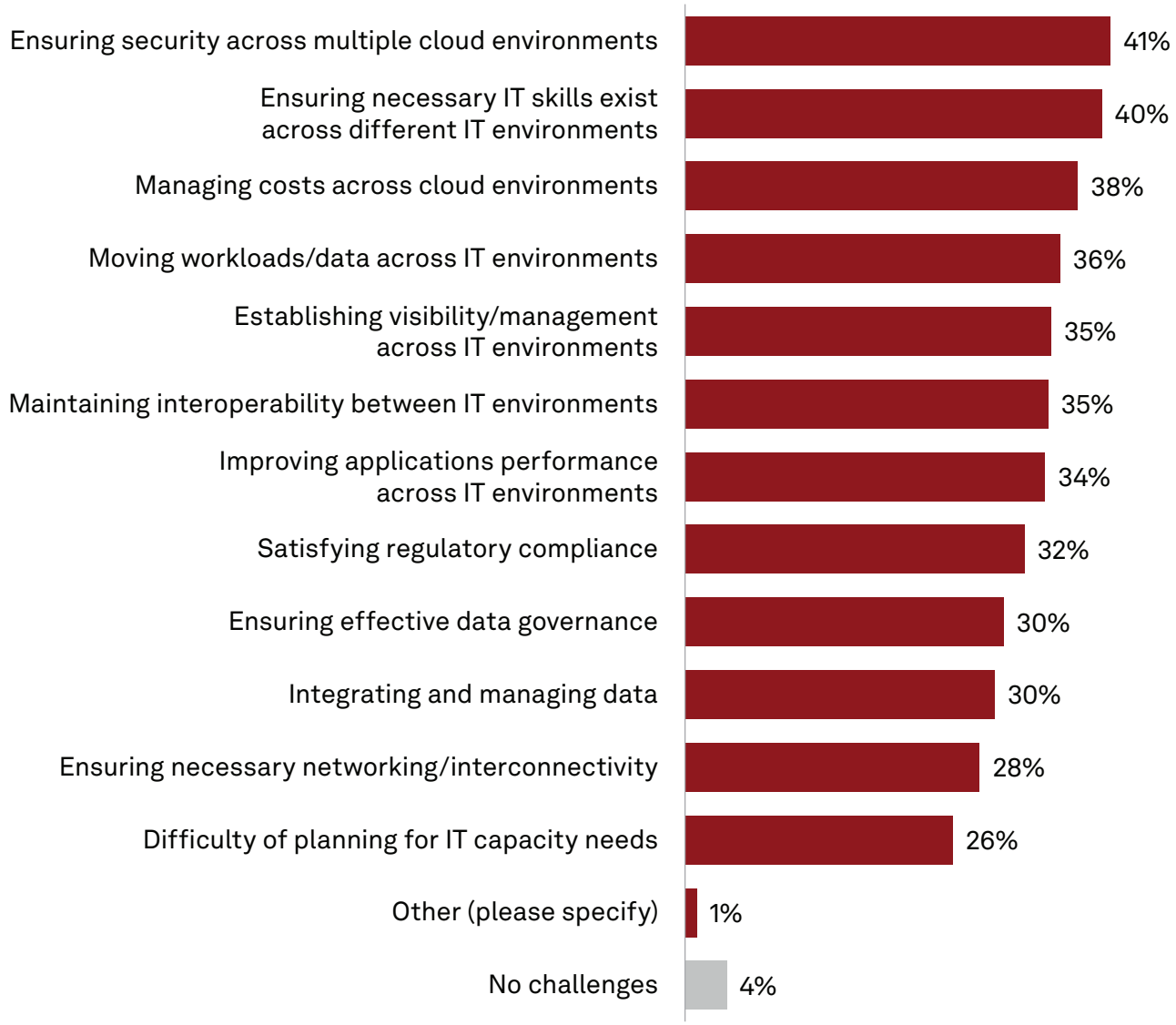
Multicloud challenges

Companies that have made, or are now making, the transition to multicloud environments say this evolution creates challenges. For 41% of respondents to the Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022 study, the enforcement of security across multiple cloud environments was a significant challenge (see Figure 4). For 40% of respondents, the transition to multicloud revealed that their current IT staff did not have adequate skills to manage the various cloud environments, which increased the need to invest in education for their employees or recruit new employees such as DevOps and site reliability engineers who have experience managing multicloud environments.

While the dynamic, on-demand scalability of cloud services is a tremendous benefit for customers, 38% of survey respondents claimed they are concerned with the prospect of managing costs across multiple environments, and they often fear that a rapid spike in consumption could blow past an organization's budget. Likewise, as cloud environments expand rapidly, 35% are concerned with getting adequate visibility and management capacities across the growing cloud estate. Meanwhile, workload and data migration are a challenge for 36% of survey respondents, and this is a key area where the replication and orchestration capabilities of data protection tools could help.

Data management is another area with multiple challenges, such as difficulties around satisfying regulatory compliance (cited by 33% of respondents), ensuring effective data governance (31%), and integration and management of data (30%). Proper data management requires tools to enforce retention and deletion policies, including the management of immutable storage to prevent the unauthorized modification or deletion of sensitive data. These are also capabilities that organizations should look for when evaluating data protection and archiving tools.

Figure 4: Security, cost and skills gaps are main multicloud challenges



Q. Which of the following are the most significant challenges related to your organization's hybrid/multicloud strategy? Please select all that apply.
Base: Organizations with hybrid or multicloud as their current or future cloud operating model, abbreviated fielding (n=351)
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022

Conclusions

While there are many benefits an organization can realize from implementing a cloud operating model with hybrid and multicloud elements, some of the expected benefits from this transition will not be realized without an adequate investment in data protection capabilities. In many cases, organizations are seeking the help of knowledgeable service providers to ensure that their significant cloud investments will deliver on the desired implementation goals. As organizations progress on their cloud transformation journeys, they should keep the following issues in mind:

1. **Most surveyed organizations (83%) are planning to use managed and professional services to reduce operational burdens**. In our Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022 survey, 50% of respondents said they were "very likely" to use external managed services or professional services to support their hybrid and multicloud efforts, while an additional 33% claimed they were "somewhat likely" to use such services (see Figure 5). Besides the key time-to-value benefit that comes with relying on an experienced service provider, these services can also help organizations that are struggling with the cloud skills gaps highlighted earlier.

2. **Choose managed services and data protection platforms designed for cloud-native environments**. When evaluating managed service providers, it's wise to seek vendors that are not only certified for industry-leading backup and disaster recovery platforms, but also have expertise with major cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud. In addition, data protection for key SaaS offerings such as Microsoft 365 and Salesforce, as well as containerized workloads managed by Kubernetes, should be considered.

3. **Leverage intelligent data protection tools and automation**. Proactive data protection and automation tools can help identify issues before they lead to data loss, while also making recovery operations more consistent and reliable. Modern data protection tools should also have secure and isolated labs capabilities to test recovery operations, without exposing the production environment to ransomware or viruses. Given the importance of automation and frictionless operations in cloud-native environments, modern tools must have self-service capabilities to allow users to easily apply approved data protection policies to workloads, and also to initiate recovery operations without the aid of a backup administrator.

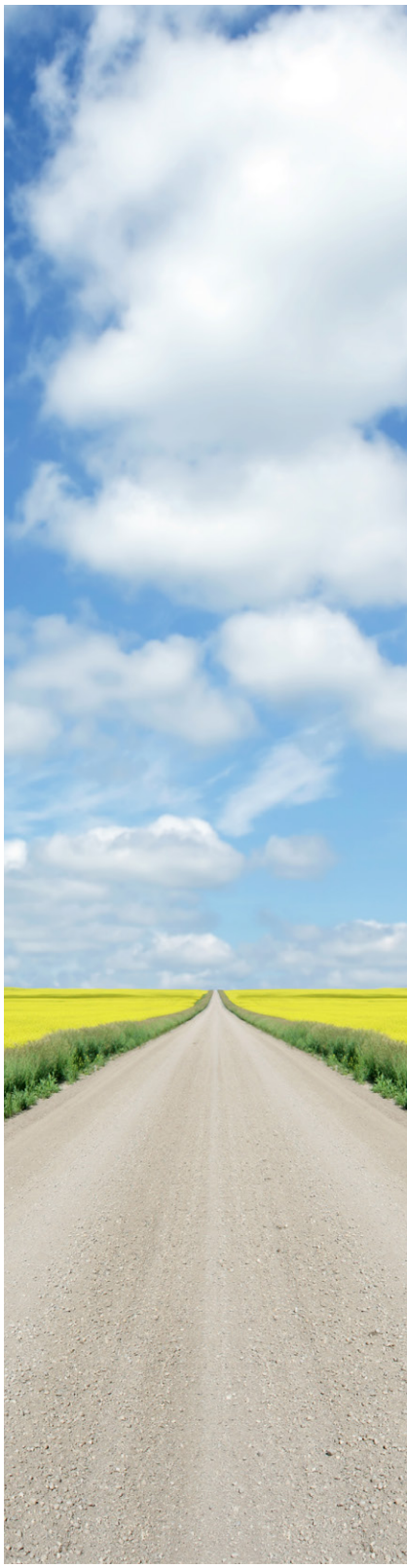
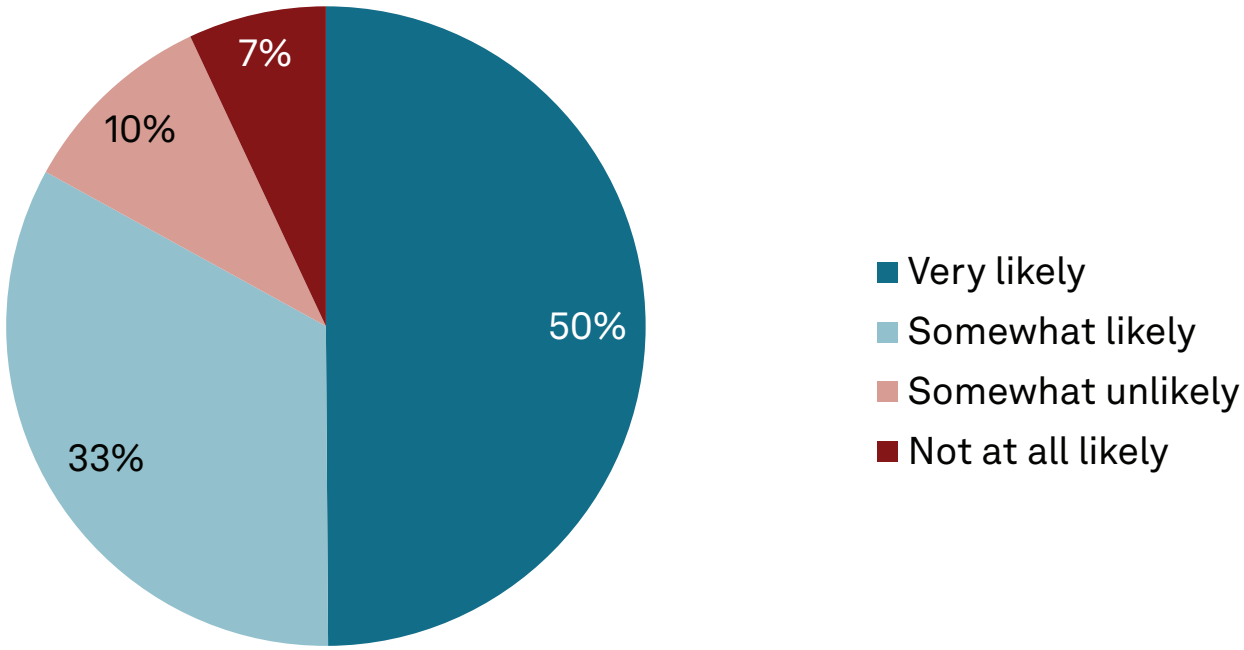


Figure 5: Many organizations are likely to use external managed and professional services



Q. Over the next two years, how likely is your organization to use external managed services or professional services to support your hybrid/multicloud efforts?
Base: Organizations with hybrid or multicloud as their current or future cloud operating model (n=459)
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Hybrid/Multicloud 2022

Content provided by

With 56% of survey respondents planning to adopt a multicloud or hybrid cloud model in the near future, data protection aims to become more complex, costly and resource-intensive. Of recent outages, 28% were caused by public cloud service failure — not including other data loss risks, such as ransomware, accidental deletion, or internal and external security threats.

It's no wonder that 83% of surveyed organizations are looking to leverage managed services to support their cloud strategies. With 74% of survey respondents claiming significant difficulty in recovering from data loss, leveraging managed backup and disaster recovery experts is in the best interest of any organization looking to ensure their cloud data is not only protected, but quickly recoverable.

Veeam® powers a global network of cloud and managed service providers who understand the complexities of protecting your data in any environment — virtual, physical, cloud, SaaS and Kubernetes. Veeam helps you stay resilient to data loss, so that you can focus time and resources towards initiatives that grow your business. Have confidence that your data will be there when you need it by leaving public cloud data protection to the experts. Click here to learn more.

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.

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 S&P Global Market Intelligence

S&P Global Market Intelligence's Technology, Media and Telecommunications (TMT) Research provides essential insight into the pace and extent of digital transformation across the global TMT landscape. Through the 451 Research and Kagan products, TMT Research offers differentiated insight and data on adoption, innovation and disruption across the telecom, media and technology markets, backed by a global team of industry experts, and delivered via a range of syndicated research, advisory and go-to-market services, and live events.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence

www.spglobal.com/en/enterprise/about/contact-us.html