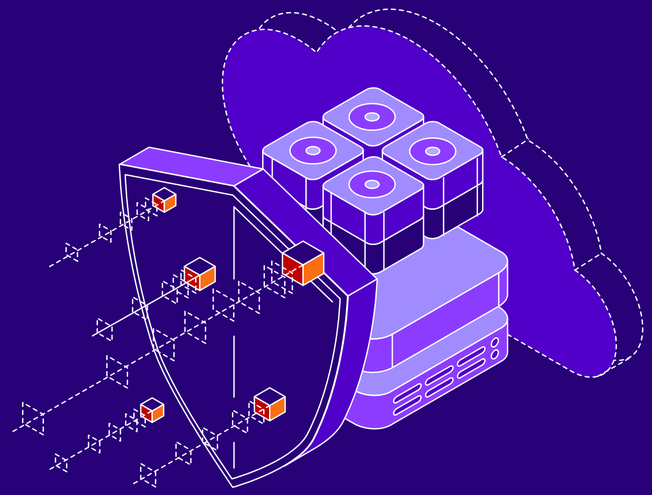
Cloud Protection Trends for 2023



Contents

Introduction

In the fall of 2022, an independent research firm completed their survey of 1,700 unbiased IT leaders regarding their use of cloud services in both production and protection scenarios, with representative personas for each scenario being asked so that the differences between personas' perspectives, as well as strategy drivers and backup methodologies, could all be gathered.

This was a broad-based market study on unbiased organizations running at least one production workload in a cloud (IaaS, PaaS or SaaS). The survey was conducted on Veeam's behalf in order to understand the various personas' perspectives, responsibilities and methodologies related to operating and protecting cloud-hosted workloads, as well as considerations when using cloud-powered data protection.

This report is presented in five sections:

1.0 IAAS – INFRASTRUCTURE AS-A-SERVICE

2.0 PAAS – PLATFORM AS-A-SERVICE INCLUDING CLOUD-HOSTED DATABASES & FILE SHARES

3.0 SAAS – SOFTWARE AS-A-SERVICE USING MICROSOFT 365 AS THE PRIMARY USE CASE

4.0 BAAS/DRAAS – BACKUP AS-A-SERVICE AND DISASTER RECOVERY AS-A-SERVICE PROTECTING BOTH ON-PREMISES AND CLOUD WORKLOADS

5.0 MSP – MANAGED SERVICE PROVIDER CONSIDERATIONS FOR BAAS & DRAAS

About the research

This research report summarizes the responses of five different IT roles that interact with cloud-powered production and/or protection solutions:

- 511 IaaS Administrators
- 251 PaaS database or file share administrators
- 255 SaaS Microsoft 365 administrators
- 255 IT Operations generalists
- 428 Backup administrators.

Questions about these research findings can be sent to StrategicResearch@veeam.com

Multi/Hybrid cloud strategies from 2020 to 2024

This entire research project was born from one of the most powerful charts from the Data Protection Trends Report for 2022, taking nearly 8,000 responses across three annual surveys to map out the gradual dilution of physical servers within hybrid environments, the relatively stable virtualization adoption, and the dramatic increases in cloud usage.

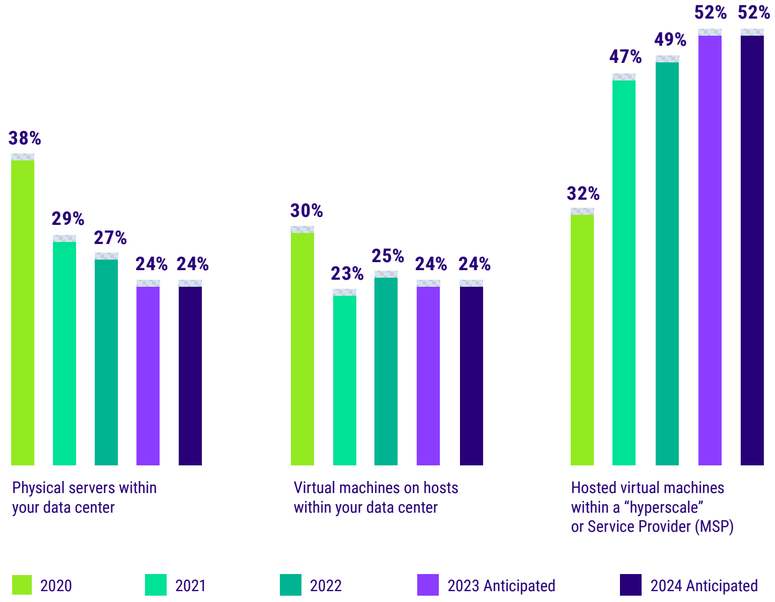
In 2020, 2021 and 2022, organizations were asked what % of their production servers ran as physical servers, virtual machines within the data center or cloud-hosted platforms. Each were also asked what they expected their mix to be two years later (2022, 2023 and 2024 respectively).

Interleaving these three datasets provides what is believed to be the largest single view as to the trajectory of hybrid strategies across the modern IT enterprise.

DPR22 Figure 1.2

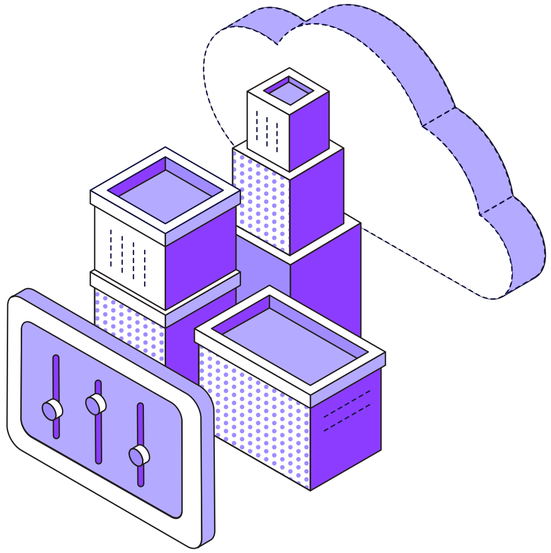
What do you estimate is your organization's percentage of servers in each format currently?

What do you anticipate the percentage will be in two years' time?



1.0

Infrastructure as-a-Service (IaaS)



If a key benefit of cloud-hosted infrastructures is "flexibility," then it makes sense that most organizations would presume to move workloads in to, out of and in between cloud platforms.

1.1

Hybrid IT = fluid movement to AND from cloud hosts

For most organizations with a "cloud first" strategy, new workloads that can run in a cloud will start there, with just less than 1/3 of cloud servers first launched in a cloud host, while 2/3 were migrated from the datacenter.

However, only 1 in 8 organizations have not repatriated cloud-hosted workloads back to their datacenter **(Figure 1.2)**. Most **(88%)** organizations brought workloads back to their datacenters for one of a few reasons, including disaster recovery failback, staging versus production, or reconciliation that the cloud was not optimum for that workload.

This means that a data protection strategy needs to not only back up cloud-hosted workloads after they are brought online in a cloud, but also ideally be able to assist in the migration from cloud to datacenter, or cloud to alternative cloud, based on business requirements.

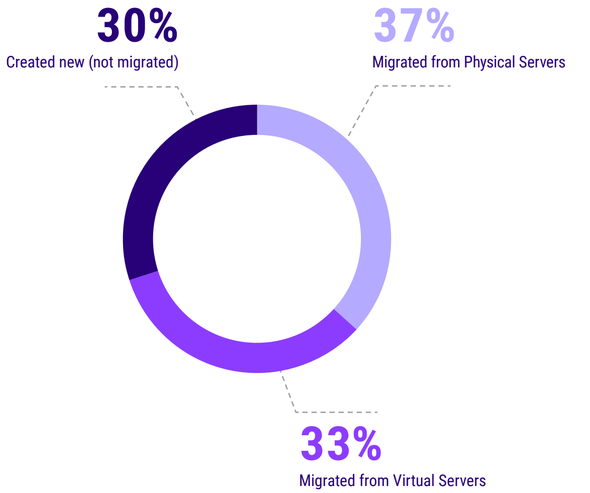


Figure 1.1

Thinking about the production worklads brought online within a cloud in the last year, what percentage came from each of the following? (n=1,272)

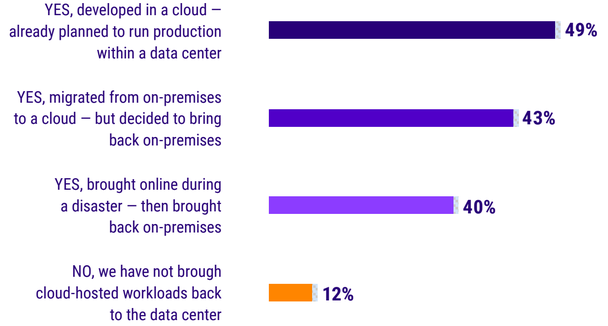


Figure 1.2

Has your organization brought any workloads BACK from a public cloud-host to on-premises? (n=1,272)

1.2

Several teams affect strategy, but backups are backups

Historically, good datacenter backup strategies including input from at least IT Operations AND backup specialists. Today's cloud-hosted environments are seeing an even better range of inputs that include cloud specialists and the application owners, even more so than the prior year.

After the strategy is established, most backups for cloud-hosted workloads are conducted by the same team that backs up datacenter workloads, by a 2:1 margin = backup admins (69%) versus cloud admins (31%).

For organizations that utilize Backup as-a-Service (BaaS) for their cloud-hosted workloads, BaaS team members manage the backup jobs a fourth of the time, with backup and cloud teams still maintaining a 2:1 ratio of the self-managed jobs, proportionally.

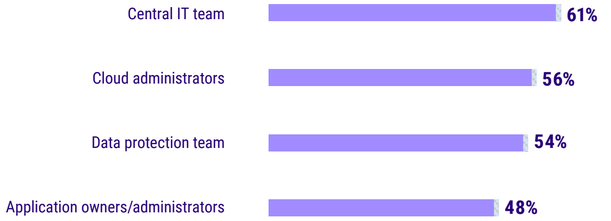


Figure 1.3

Which team(s) within your organization are involved in determining your data protection strategy and requirements for cloud-hosted servers? (n=1,700)

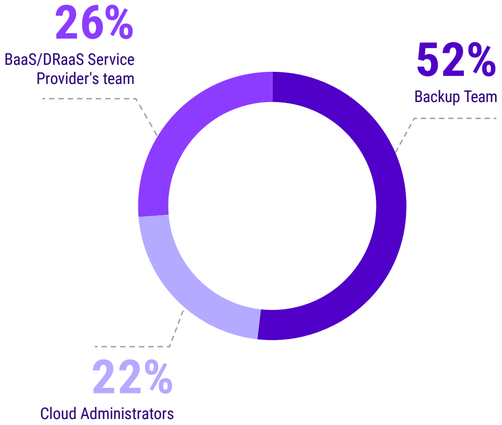


Figure 1.4

In general, who manages the backups/data protection of cloud-hosted servers in your organization? (n=1,700)

1.3

Long Term Retention still applies to cloud-hosted data

Most organizations have historically backed up their data for two reasons:

- To recover from outages/downtime
- To retain previous versions

While many assume that IaaS is more resilient (addressing reason #1), regulatory mandates, accidental overwrites/deletions/corruption, and remediation from ransomware all require previous versions to be retained.

It is notable, that half **(49%)** of organizations do not retain previous versions of their cloud-hosted data for even one year – regardless of the often 5-, 10-, or 20-year mandates that their datacenter data might be retained. For those that do retain data for longer than one year:

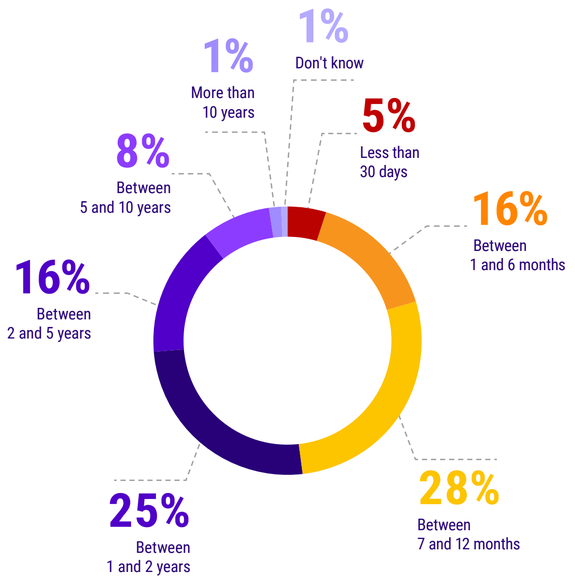
- **57%** use either cloud-based storage with an alternate provider (e.g. BaaS or another hyperscale cloud);
- **48%** within the same cloud as production;
- **38%** back up their cloud data to their datacenter;
- **28%** of organizations utilize tape as their long-term retention media for cloud-hosted production data.

Nearly every organization has long-term (> 1 year) retention mandates, and yet half of organizations aren't applying that to their cloud-hosted data.

This will inevitably change as compliance & legal teams become more aware of IT "cloud-first" strategies.

Figure 1.5

On average, how long is backup data from cloud-hosted sources retained? (n=1,700)



1.4

There are multiple cloud-powered data protection options

For most organizations, simply storing a copy of their backups within a cloud "tier" or repository is the start of their cloud-powered data protection journey.

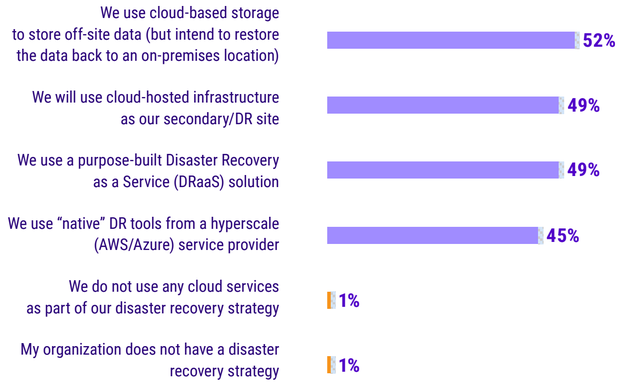
Eventually, most organizations aspire to recover workloads in the cloud instead of simply restoring data back from a cloud, leading to disaster recovery and other server failover scenarios.

As organizations become more comfortable with cloud-powered scenarios, many turn to DRaaS because they can gain BC/DR expertise and not just a cloud infrastructure.

Said another way, **98%** of organizations utilize at least one cloud-powered capability as part of their data protection strategy.

Figure 1.6

How do cloud services contribute to your organization's disaster recovery (DR) strategy? (n=1,194)



VEEAM CLOUD BACKUP

1.5

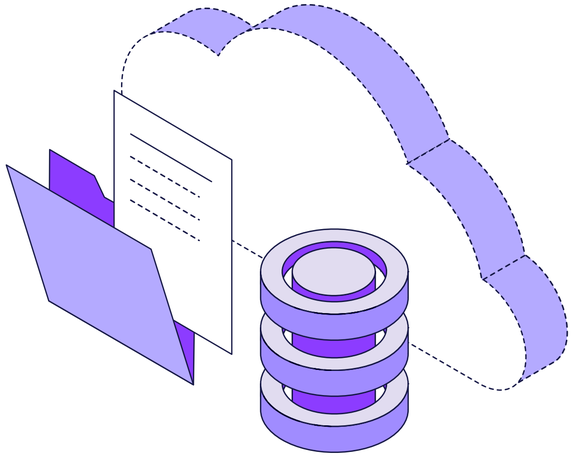
The Veeam Perspective

Cloud-hosted IaaS has quickly become the de facto standard for production workloads thanks to cloud-first initiatives being increasingly mainstream. Clear trends such as a desire for portability to the cloud for lift and shift and refactoring is almost obvious, however, less obvious is the need for portability from the cloud back to on premises. Other significant factors include cost-optimized, long-term retention, as well as a more holistic input across the organization in data protection solution selection and operation.

- Veeam delivers AWS, Azure and Google Cloud-native backup and recovery for not only IaaS-hosted workloads, but also PaaS. In line with the above trends and requirements, Veeam solutions deliver:
- Cloud Mobility capabilities that allow users to make data portable across infrastructures, including to, from and across different clouds
- Policy-defined automated tiering of backup data across cloud storage – including archive tier object storage – to help organizations meet retention requirements while effectively optimizing spend
- A single platform to centrally manage cloud, virtual, physical, SaaS and Kubernetes backup and recovery, standardizing protection across the hybrid cloud for operational consistency
- Role-Based Access Control (RBAC) and least privileged access permissions to securely delegate backup and recovery tasks to central IT, cloud administrators, application owners and more

2.0

Platform as-a-Service (PaaS)



2.1

Cloud-hosted file shares

For as long as there have been LAN-based servers (1980s), unstructured file shares has been a mainstay workload. And just like the NetWare, Windows Server, and Network-Attached Storage (NAS) platforms before them, cloud-hosted infrastructure offers a variety of file sharing services, including:

- File shares running within hosted server instances (e.g., Windows Server shares or Cloud ONTAP);
- File share (SMB or NFS) services from the hyperscale cloud provider itself.

While lifted+shifted server instances are still the majority, the diverse mix suggests that data protection strategies in 2023 and beyond for cloud-hosted environments MUST protect the range of file share services being offered.

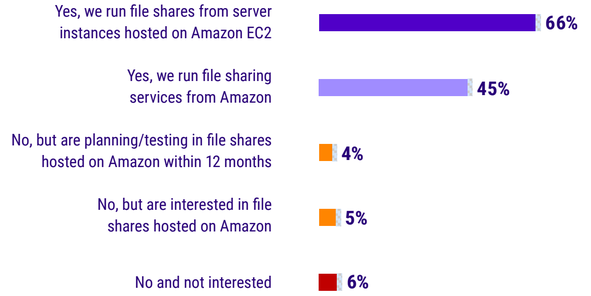


Figure 2.1

Does your organization run file shares on Amazon? (n=1,017)

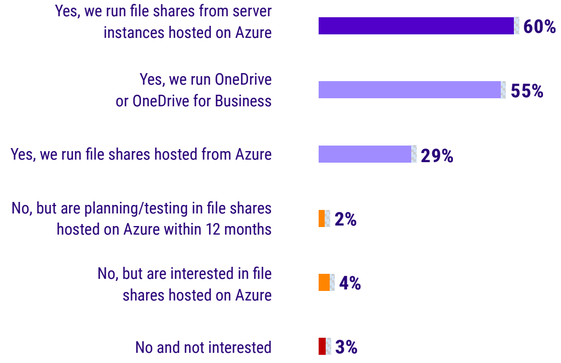


Figure 2.2

Does your organization run file shares on Microsoft Azure? (n=1,017)

2.2

Cloud-hosted databases

Similar to the cloud-hosted file shares described in **Figures 2.1** and **2.2**, as the primary means of "unstructured data" moves into cloud services, "structured data" (databases) are on a similar evolution, including:

- Databases running within hosted server instances (e.g., Windows or Linux servers);
- Managed database services from the hyperscale cloud provider itself.

Verbatim to the guidance for cloud-hosted file shares, while lifted+shifted server instances are still the majority, the diverse mix suggests that data protection strategies in 2023 and beyond for cloud-hosted environments MUST protect the range of databases now running from cloud services.

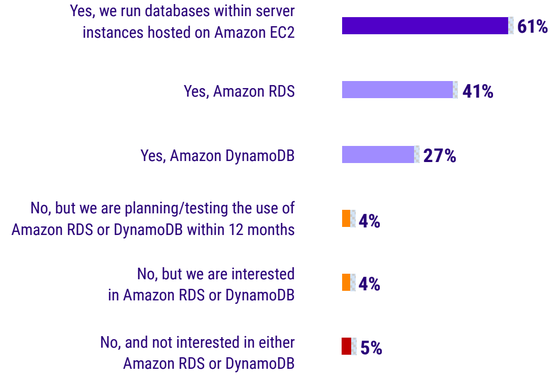


Figure 2.3

Does your organization run databases in AWS? (n=1,017)

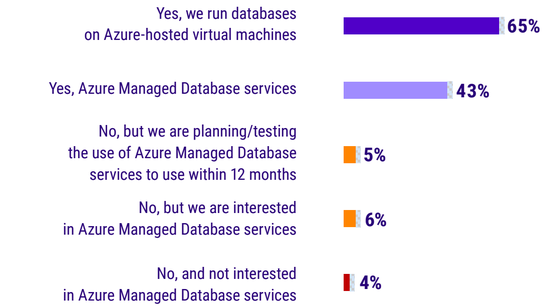


Figure 2.4

Does your organization run databases in the Azure cloud? (n=1,017)

2.3

Service resiliency does not absolve the need to back up

As shown in **Figure 2.5** resiliency of cloud services can sometimes incorrectly lead organizations to not back up their cloud-hosted workloads:

- **34%** believe that their cloud-hosted file shares are durable or do not need to be backed up;
- **15%** believe that their cloud-hosted databases are durable or do not need to be backed up.

They are wrong.

When considering that cyberattacks and accidental overwrites/deletions/corruption are the most common causes of outages (see Data Protection Trends Report 2022, **Figure 2.2**), the need for previous versioning for weeks or months has never been more important. As such, **59%** of cloud-hosted file shares and **79%** of cloud-hosted databases are being backed up to a BaaS provider, with a third-party backup tool, or both.

It is hard to imagine that 1/3 of file shares and 1/6 of databases do not need to be backed up.

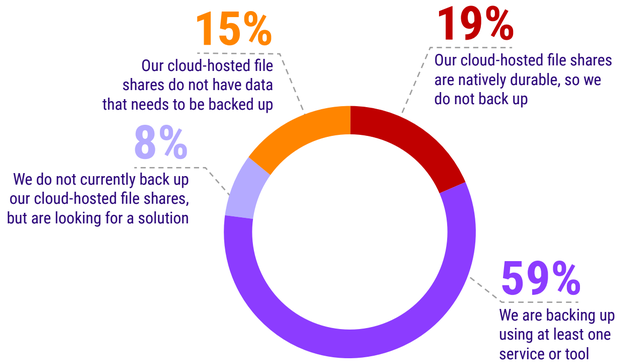


Figure 2.5

How are you backing up data within your file shares in Amazon or Azure? (n=1,019)

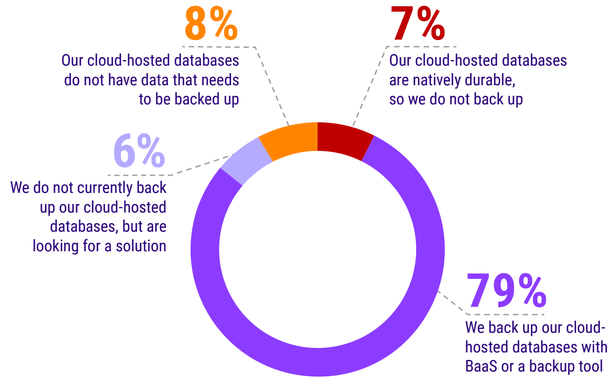


Figure 2.6

How are you backing up your databases running in Amazon or Azure? (n=1,019)

VEEAM CLOUD BACKUP

2.4

The Veeam Perspective

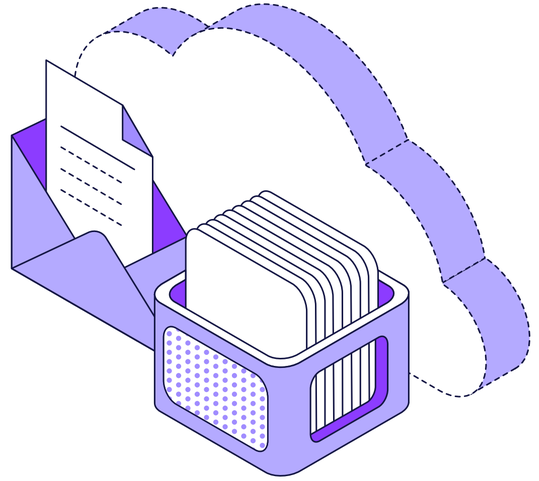
The prevalence of cloud-hosted databases and file shares continues to increase across both IaaS (likely lift and shift from on premises) and dedicated PaaS offerings. Irrespective of where or how these are run by the organization both today and in the future, protection of this data is critical. Shared Responsibility Models and Matrices clearly state security and protection of data is a responsibility of the user and not the provider. Well architected resilience does not account for the actions of bad actors (e.g., cyberattacks) or human error (e.g., accidental deletion).

Veeam delivers AWS, Azure and Google Cloud-native backup and recovery options for databases and file shares, whether they are hosted on IaaS or PaaS. Native backup and recovery for PaaS offerings include Amazon RDS, Amazon EFS, Azure SQL, Azure Files, Cloud SQL for MySQL, and more. Recovery options are extensive and wizard-driven for speed and ease, from entire databases to granular file and folder restore to the original location or to a new location.

Veeam does not compromise data protection comprehensiveness by using generic, one-size-fits-all tooling. Instead, protection is native to, and purpose built for each workload or dataset.

3.0

Software as-a-Service (SaaS) focusing on M365



3.1

Combine third-party data protection with enhanced M365 services

Early in most production "as a Service" journeys, organizations incorrectly assume that server resilience or built-in "undo" functions negate the need for backup. This confusion was certainly true in M365's early days; compounded by enhanced capabilities like "legal hold" in the premium offerings.

Today, only **4%** rely solely on the M365 recycle bin or similar undo capabilities and (thankfully) only **3%** incorrectly believe that M365's resilience negates the need for backup. For the other **93%** of M365 organizations:

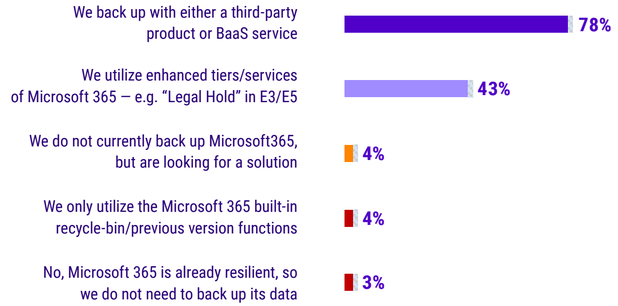
- Most of the **43%** that utilize the enhanced tiers of M365 understand that those capabilities are designed for scenarios other than "backup" or long-term retention;
- More than 3 out of 4 **(78%)** use a third-party backup product or a BaaS service to back up M365.

It is worth noting that the most common repository for long-term M365 data is Azure Storage, as used by **42%** of organizations, which can enable great recovery scenarios, if separate credentials are used to minimize cyber scenarios.

It is worth noting that Veeam's M365 solution can be utilized as part of a BaaS service, run within a cloud-VM, or even within the data center to bring cloud data "back" to the organization.

Figure 3.1

Does your organization back up the data from within Microsoft 365? (n=619)



3.2

Diverse strategy stakeholders, but consistent backup operators

The analysis of **Figures 3.2** and **3.3** resembles **Figures 1.3** and **1.4**, whereby a growing number of stakeholders are driving the strategy and requirements for protecting M365, but the team responsible for backing up the rest of IT is increasingly asked to back up M365 as well.

This is a common milestone in the maturation of any new platform into the mainstream, when tasks like data protection may no longer require the deep expertise of the application owners or platform specialists:

- For self-managed M365 organizations, **61%** of backups are done by backup specialists versus **39%** by M365 administrators;
- When BaaS is used to protect M365, backup admins still do most of the backups, but the BaaS team handles backups for 1 in 4 organizations.

The shift from "Admin-operated" backups to "being run by the central backup team" is a good indicator to the maturity of data protection technologies as well as a good understanding by the corporate teams that cloud data is still corporate data.

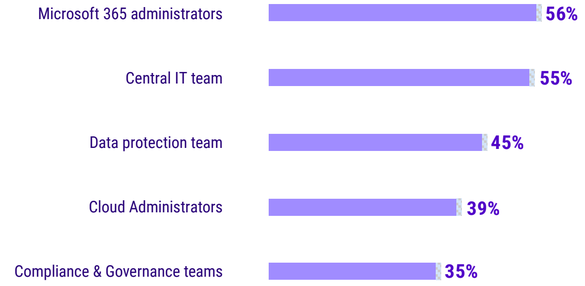


Figure 3.2

Which team(s) within your organization are involved in determining your data protection strategy and requirements for your data within Microsoft 365? (n=578)

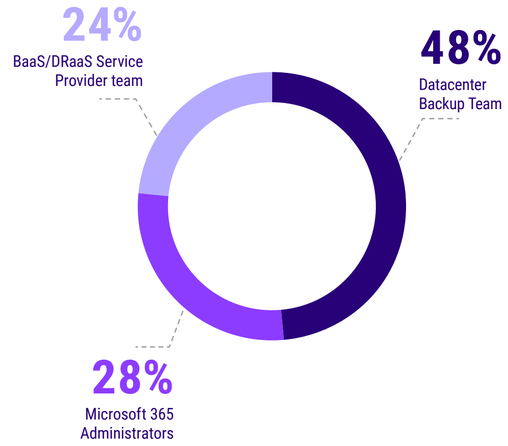


Figure 3.3

In general, who manages the backups/data protection of data within Microsoft 365 in your organization? (n=358)

3.3

There isn't just one reason to back up Microsoft 365

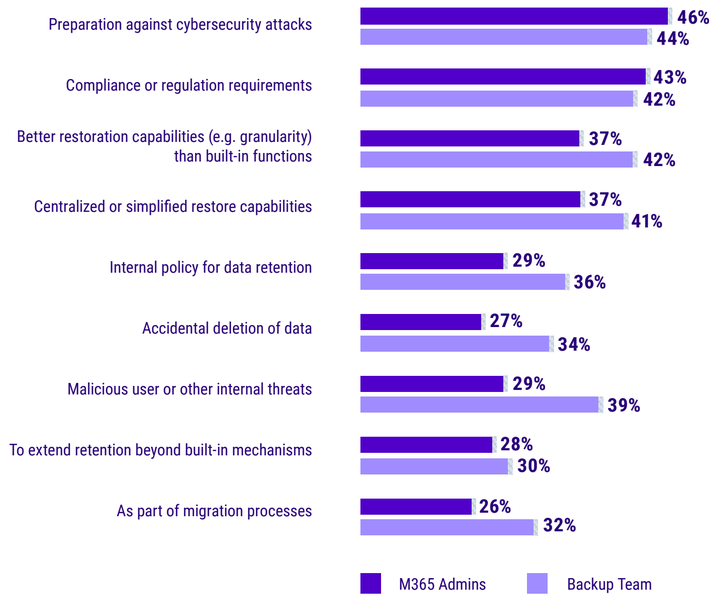
One of the more common misunderstandings between application owners and backup admins are the myriad reasons for doing data protection. While application owners may be primarily concerned with uptime and only relatively recent rollback, backup admins tend to focus on compliance mandates, cyber and other disasters.

Figure 3.4 is good news in that both the M365 administrators and the backup specialists are mostly in agreement on the most important reasons to back up; though backup admins do still have a higher concern for traditional data overwrite/deletion issues than SaaS admins.

It is worth noting that both groups did recognize that a backup tool (or BaaS) provided better capabilities than the built-in functions, which administrators of less mature platforms often do not.

Figure 3.4

What are your organization's primary reasons for backing up your data within Microsoft 365? (n=358)



VEEAM BACKUP FOR M365

3.4

The Veeam Perspective

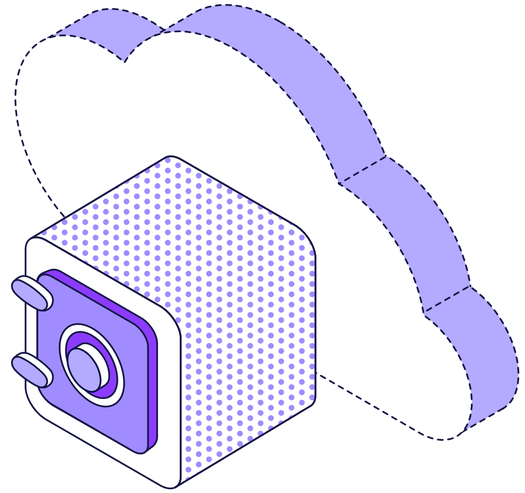
The growth in third-party backup adoption for Microsoft 365 is being driven by the demand for Backup as a Service (BaaS). Backing up and managing SaaS environments is complex, especially with talent and budget constraints. For this reason, companies unable to deploy their own backup solution for Microsoft 365 are now motivated to leverage a BaaS provider due to their expertise and ability to implement a solution quickly. Veeam is uniquely qualified to address this market shift with its large ecosystem of Veeam Cloud & Service Provider partners and the product, Veeam Backup *for Microsoft 365*. Service providers can leverage the Veeam platform to deliver a comprehensive BaaS and DRaaS offering fit to meet the needs of customers' ever-changing IT landscape.

With an increased number of Microsoft 365 data protection tasks no longer requiring app owners and specialists, third-party backup solutions require high levels of simplicity and flexibility to meet the demands of any team which deploy them. Veeam Backup for Microsoft 365 has a very low learning curve combined with intuitive, wizard-driven backup and recovery processes, so that even the least experienced admin can easily manage enterprise-grade data protection.

It's clear there are many reasons for protecting Microsoft 365 data, and with the wave of ransomware attacks aimed at SaaS apps in recent years, it comes as no surprise this is top of mind for organizations. Regardless of what the driver is, Veeam can address every Microsoft 365 data loss concern organizations have today — whether providing a multitude of recovery options, establishing separation of data and administrative access, or helping to meet compliance requirements in a timely manner.

4.0

Backup / Disaster Recovery as-a-Service (BaaS & DRaaS)



4.1

What does "Backup as-a-Service" mean?

There is not just one definition of BaaS.

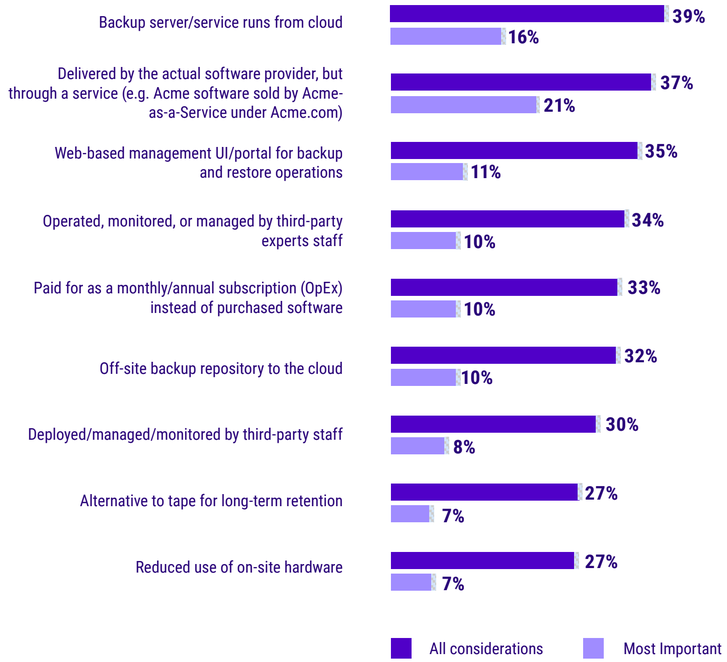
While the top two most common answers refer to the backup engine running from a cloud provider, several other facets also are notable:

- Original backup software offered under its own brand, presumably instead of white-labeled or "re-skinned" software strictly under the BaaS brand;
- Web-based management tools;
- Expert staffs performing monitoring and/or management, instead of the customer IT staff;
- Subscription pricing, instead of outright purchases of hardware and software.

It is interesting and somewhat myth-busting that BaaS negates the need for tape, and BaaS doesn't always result in less hardware; the latter being important if you are concerned about file/object level recovery speeds.

Figure 4.1

What does "Backup as a Service" mean to you? Which of these is most important to you in regard to "Backup as a Service"? (n=1,700)



4.2

Why BaaS?

The most fundamental question asked whenever considering any cloud service is, "What are the benefits versus managing my own solution?"

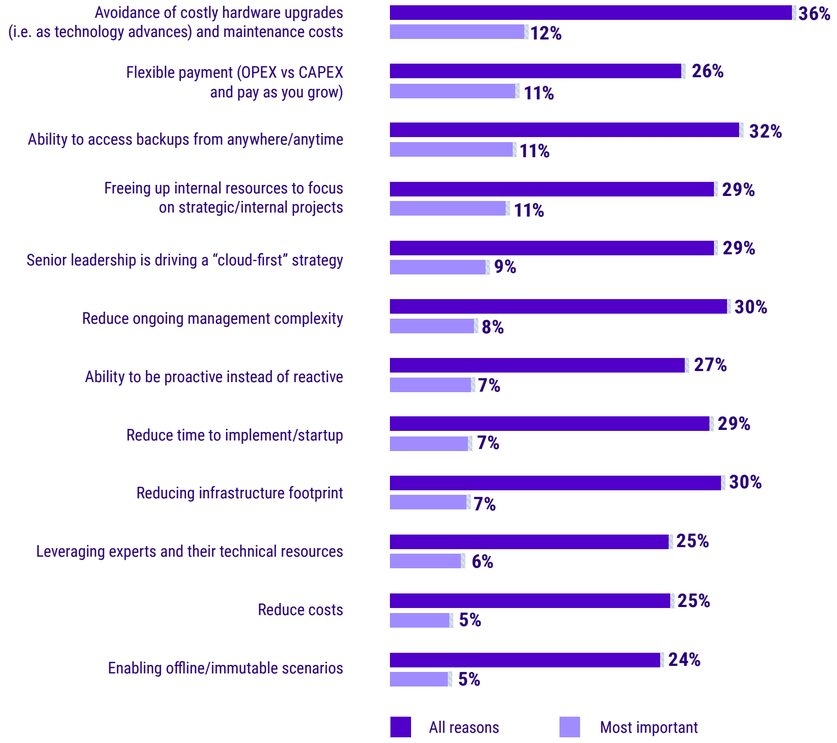
The answer, regarding BaaS, is Operational Efficiency. Other than data survivability and agility (i.e., ability to access backups anywhere), the top five most common reasons all come down to operational efficiency:

- Hardware/maintenance costs;
- Subscription payment instead of capital expenses;
- Reduced operational complexity;
- Reduced hardware footprint.

It is notable that "reduce costs" is near the bottom, meaning that BaaS may not be "unequivocally cheaper" – but the value gained and the changes in operating models provide a quantifiable and justified economic benefit.

Figure 4.2

Which best describes why your organization uses or would use Backup as a Service (BaaS), instead of traditional backup software/ hardware? What is the main reason? (n=663)



4.3

Why DRaaS?

While **BaaS** is predominantly seen as operational efficiency, **DRaaS** has a broader variety of justifications; with the three most important justifications being grounded in the expertise that a **DRaaS** provider offers in complement to IT staffs:

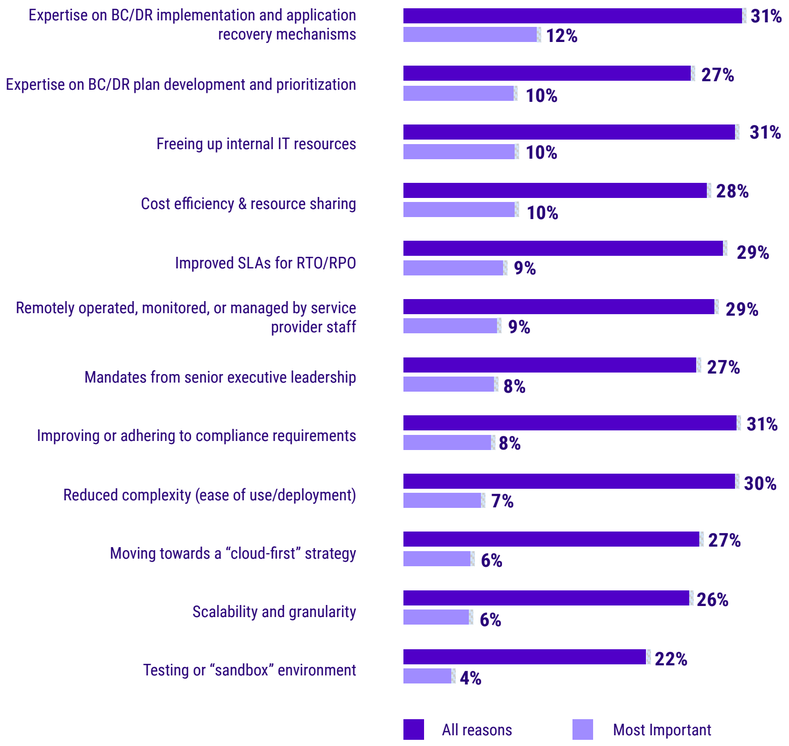
- Expertise in implementation;
- Expertise in planning;
- Freeing up the IT staff's internal experts for other tasks.

Only after the three expertise justifications do we see efficiencies, improved capabilities, and monitoring — i.e., the justifications for **BaaS**.

Said another way, while **BaaS** may be seen as delivering *tactical* improvements, **DRaaS** is justified for its *strategic* benefits to the organization.

Figure 4.3

Which best describes why your organization uses or would use Disaster Recovery as a Service (DRaaS), instead of managing your own secondary data center? What is the main reason? (n=663)



FIND A VEEAM BAAS PROVIDER

4.4

The Veeam Perspective

If companies are looking to modernize their data protection, why wouldn't they consider modernizing the way they consume it too? While the definition of BaaS isn't universal, there is commonality in the benefits organizations experience when leveraging an "as a Service" model.

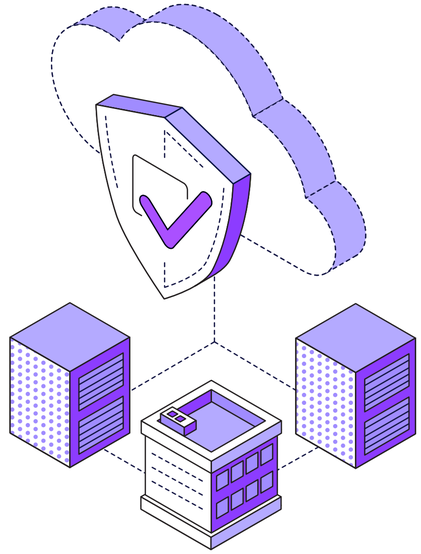
When partnering with a service provider, organizations are looking for more than just software delivery. They seek expertise in implementation, plan development, testing, documentation, and recovery mechanisms. These critical components of a BC/DR strategy, plus the economic benefits, are driving more organizations to modern delivery of IT.

Organizations of all sizes can experience Modern Data Protection from the Veeam Platform in an "as a Service" model. Veeam-powered BaaS and DRaaS is delivered by a global network of service providers that offer a variety of these capabilities based on what BaaS means to you. These partners are experts in BC/DR and the Veeam Platform, delivering you the business outcomes and SLAs that meet your needs.

Learn more at vee.am/BaaS

5.0

Service Provider Considerations for BaaS/DRaaS



5.1

The journey to cloud-powered protection?

Today, **42%** use cloud-storage within their data center backup solution, while **58%** use BaaS — but that is not the most important aspect of **Figure 5.1.**

Perhaps one of the most powerful new questions within this year’s Cloud Protection Trends report, was when respondents were asked how they first added cloud capabilities to their data protection strategy:

- First used cloud storage, as part of a traditional data protection solution
- First enrolled in a managed BaaS subscription

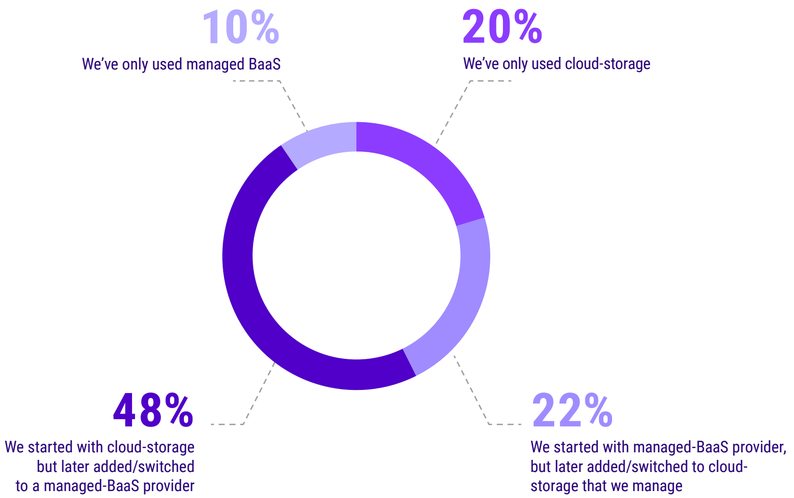
But then, where are they today?

- **30%** stayed as they started;
- **70%** switched from self-managed to BaaS, or vice versa.

Of those that switched, nearly 2:1 switched TO BaaS versus FROM BaaS – meaning that many started with self-managed backups that utilized cloud storage (e.g., hyperscale bucket/blob) but moved to embrace the rest of what service providers offer: expertise. While **22%** started with BaaS but later decided to run their own, nearly half of respondents **(48%)** started with simple cloud storage and then chose to utilize BaaS instead.

Figure 5.1

How would you describe your organization’s use of and journey with cloud-backup storage/services? (n=589)



5.2

“White glove” versus “self-managed”

There is no wrong answer:

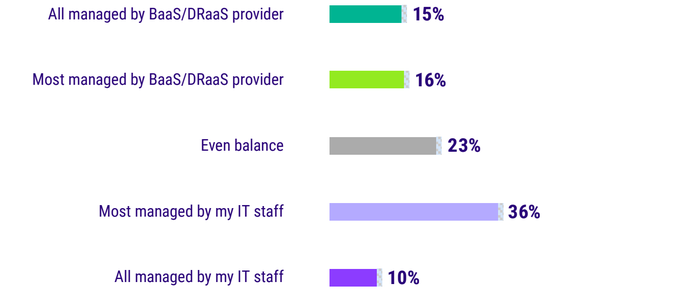
- Nearly half **(46%)** of organizations, choose to self-manage their backup jobs, but rely on a BaaS provider for maintaining the backup server/services this alone can significantly relieve IT teams by removing the “baby sitting” and management of backup servers, storage, software patches, etc;
- A third **(31%)** of organizations prefer to delegate most backup operations (e.g., backup job monitoring, capacity planning, alerts, and even restore tasks) to BaaS service desks.

This reveals a shift towards the desire for more “turnkey” service outcomes from the **63%** self-managed versus **13%** white glove that was reported in *Data Protection as-a-Service Trends 2021*.

That year over year increased interest in managed services likely also contributed to **Figure 5.2** shift from self-managed cloud storage to managed BaaS described earlier.

Figure 5.2

In your opinion, which of the following describes how you’d ideally like to utilize a BaaS or DRaaS service? (n=673)



5.3

The Veeam Perspective

Veeam BaaS and DRaaS providers give organizations of all sizes the power of choice when deciding what level of service is required for their data protection needs. From self-managed, off-site backup storage options to a fully-managed BaaS or DRaaS offering complete with implementation, management, monitoring, testing and recovery needs, the level of service can vary widely but one thing is certain: BaaS and DRaaS are on the rise.

Many companies are turning to BaaS providers to not only protect their on-premises infrastructure and endpoints but also to protect their workloads running in public clouds — including AWS, Microsoft Azure and Google Cloud — as well as Software as a Service applications like Microsoft 365. The Veeam platform gives cloud and managed service providers everything they need to deliver a comprehensive BaaS and DRaaS offering fit to meet the needs of their customers’ ever-changing IT landscape.

Learn more and find a partner at vee.am/BaaS

Service providers: Learn more at https://vee.am/BaaSSstrategicValue

To download additional materials from this research, click here.

For questions on this research or its usage: StrategicResearch@veeam.com

Summary

This analysis covers the opinions of 1,700 unbiased organizations on their use of cloud-based production and cloud-powered protection services. Specifically, Veeam contracted with an independent research firm to survey a broad range of IaaS, PaaS, SaaS, BaaS and DRaaS consumers for the purposes of understanding what organizations are doing today and what they want to do moving forward. The most interesting findings to Veeam include:

- **IaaS** & PaaS — The trend around fluid movement between multi-hybrid cloud storage strategies has escalated especially considering the growing adoption of cloud-powered tools and services. Based on this multi-faceted approach, organizations have reached a point where long-term retention is playing a larger role in IT strategy. It is an especially sensitive point involving data protection specific to data loss prevention.
- **SaaS** — There are multiple reasons why organizations are backing up their M365 data. Indicators show the broader market is more likely to use third-party data protection with enhanced M365 services and capabilities. More important, these use cases are reaching beyond the traditional backup and long-term retention scenarios.
- **BaaS & DRaaS** — While there are many notions around what Backup as a Service means to organizations, most consider it as running through the cloud or as a service with an MSP in order to improve operational efficiencies. For DRaaS, it is more so on gaining expertise. For a more concise interpretation, BaaS is noted as extending further on tactical improvements, and DRaaS is more purposeful to the business in generating strategic benefits.
- A special note to **managed service providers** delivering cloud-powered data protection solutions — many organizations started with self-managed backup using cloud storage. But, later, they switched to an MSP in order to further leverage expertise around capabilities. These shifts are seen as having a prolific impact due to increased optimism around hybrid, multi and the importance of a comprehensive data protection strategy.

About the authors

Jason Buffington
VP, Market Strategy

@JBuff

Dave Russell
VP, Enterprise Strategy

@BackupDave

Julie Webb

Director,
Market Research & Analysis