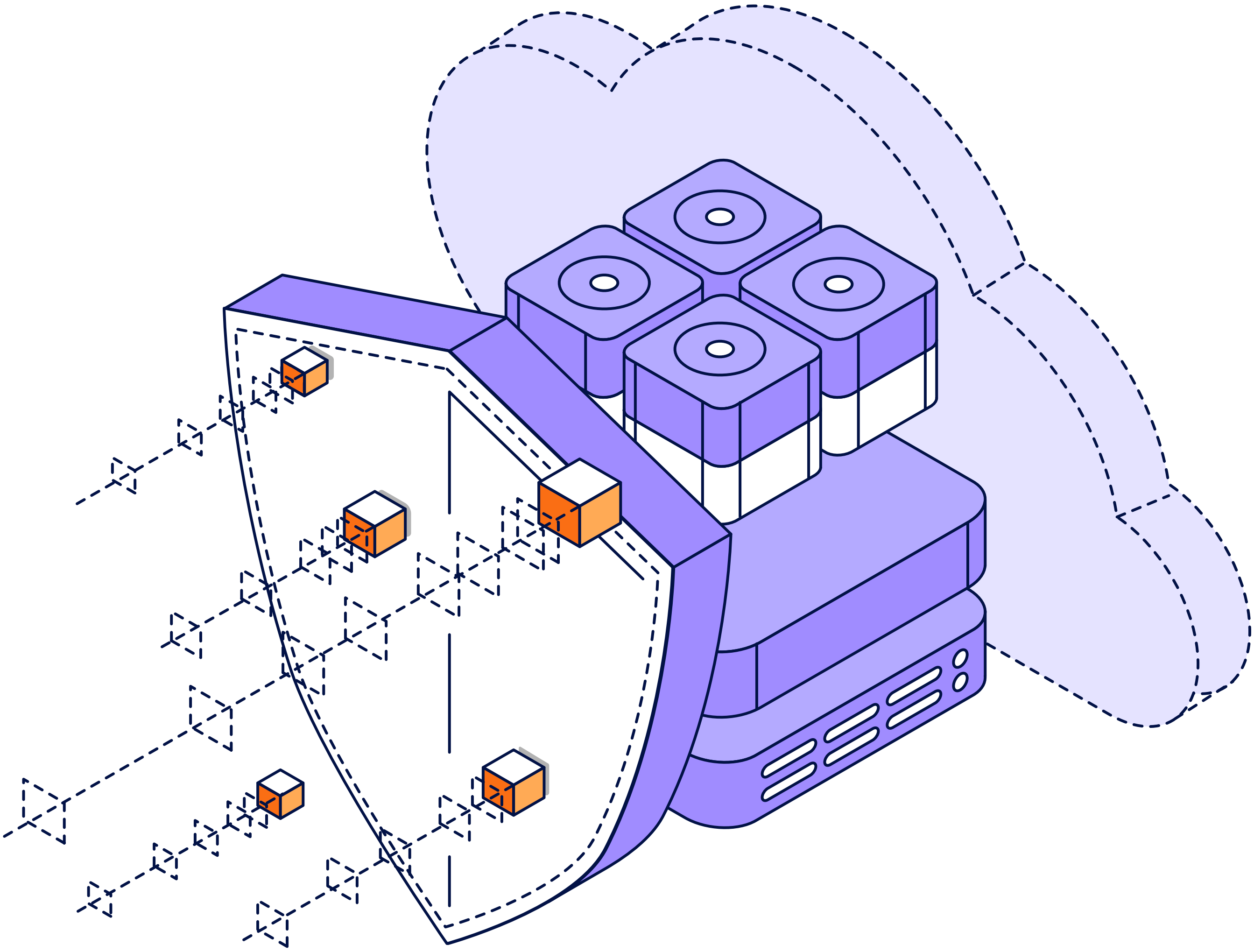
EXECUTIVE BRIEF

Cloud Protection Trends for 2023



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 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. The full report is located at http://vee.am/CPT23.

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 data center. That said, the "journey to the cloud" is not one direction, as most organizations have brought workloads back from the cloud at some point.

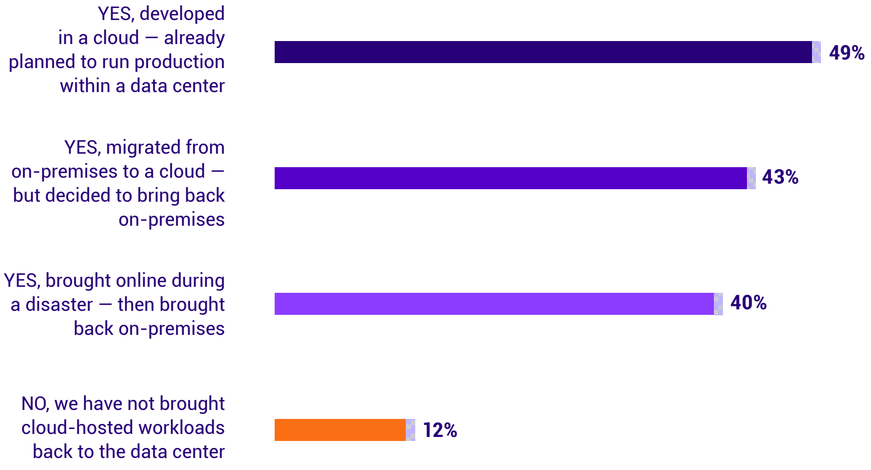


Figure 1.2

Has your organization brought any workloads BACK from a public cloud-host to on-premises?

It is notable that the fluidity of workloads returning on-premises varies somewhat by region:

	GLOBAL	Americas	EMEA	APJ
NO, we have not brought cloud-hosted workloads back on premises	12%	1%	26%	9%
YES (one or more reasons)	88%	99%	74%	91%
YES, after a disaster recovery	40%	45%	31%	45%
YES, migrated from on-premises, decided to bring back from cloud	43%	46%	35%	51%
YES, developed in a cloud — planned to run within a data center	49%	52%	40%	59%

88%

of organizations brought workloads back to their data centers for one of a few reasons, including disaster recovery failback, staging versus production, or reconciliation that the cloud was not optimum for that workload

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Considering the diverse mix as to where cloud-hosted workloads originate, as well as the myriad reasons that workloads are then brought back on-premises, data protection strategies in 2023 need 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 data center, or cloud to alternative cloud, based on business requirements.

Cloud-hosted file shares and databases

Cloud-hosted infrastructures offer a variety of **file sharing** capabilities, including:

- **76%** run file shares running within hosted server instances (e.g., Windows Server shares or Cloud ONTAP)
- **56%** run file share (SMB or NFS) services from the hyperscale cloud provider itself

With similar momentum of the cloud-hosted file shares as a primary means of "unstructured data" moving into cloud services, "structured data" **(databases)** are on a similar adoption rate:

- **78%** run databases running within hosted server instances (e.g., Windows or Linux servers)
- **56%** run managed database services from the hyperscale cloud provider itself

Running foundational services like file shares and databases is "universal" in appeal to IT organizations of all sizes, but there is some variation in usage of these cloud-services, presumably based accessibility to bandwidth and cloud infrastructure.

	GLOBAL	Americas	EMEA	APJ
File Shares in server instances	76%	86%	67%	75%
File Shares via managed services	56%	59%	48%	62%
Databases in server instances	78%	85%	71%	76%
Databases via managed services	65%	74%	53%	68%

In fact, **91%** of the global organizations surveyed run file services and/or databases from one or more cloud providers. So 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 shares and databases that are now running from cloud services. Surprisingly, some organizations underestimate how important previous versions and long-term retention are for cloud-hosted data, when the PaaS services are natively durable. In fact, 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.

91%

of organizations are running production File Shares and/or Databases from a cloud, using some combination of server instances and managed services.

As the offerings mature and organizations become more comfortable, it is likely that the mix of server-instances will gradually reduce and managed services will more significantly increase.

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

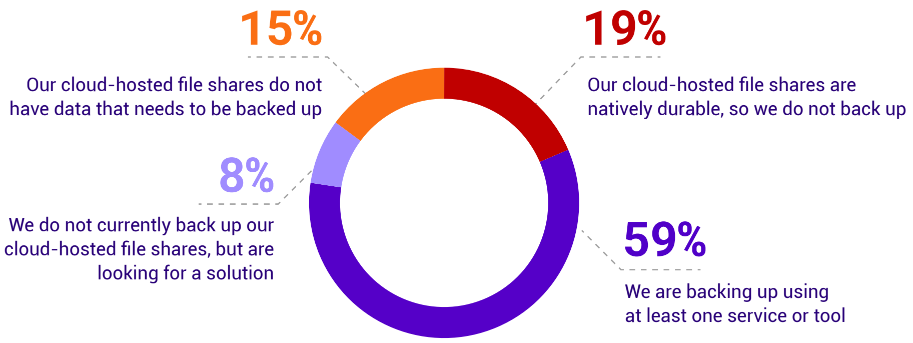


Figure 2.5

How are you backing up data within your file shares in Amazon or Azure?

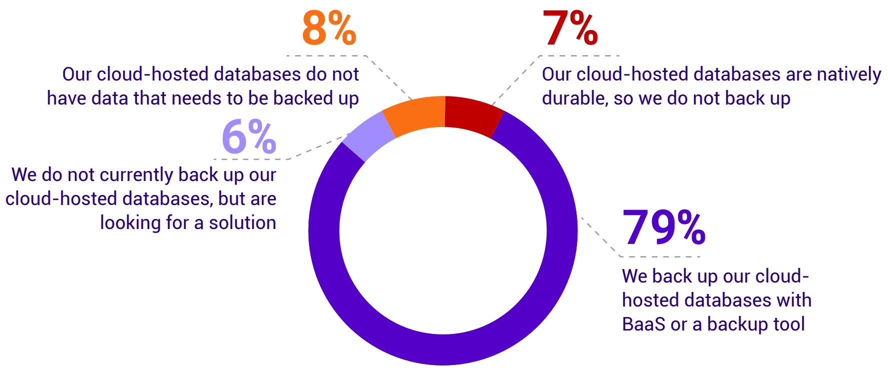


Figure 2.6

How are you backing up your databases running in Amazon or Azure?

Several teams affect data protection strategy, but backups are backups

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 data center 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 maintain a **2:1** ratio of the self-managed jobs, proportionally.

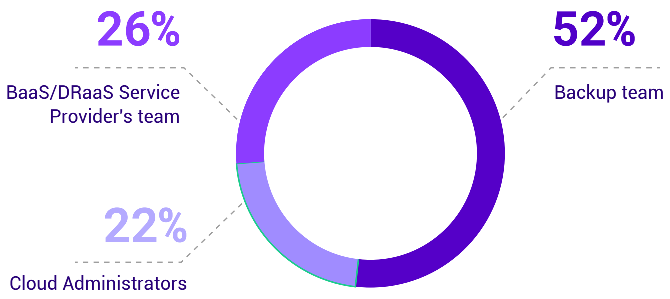


Figure 1.4

In general, who manages the backups/data protection of cloud-hosted servers in your organization?

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Debunking the myths of backing up M365 services

There are two common assumptions when it comes to SaaS and data protection:

- The built-in recycle-bin/undo/hold is good enough for backup
- Application admins do not understand that backups are important

Both assumptions are wrong. Early in most production "as a Service" journeys, many 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 BaaS 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.

Another 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. The chart below is good news in that both M365 administrators and backup specialists do mostly agree on the most important reasons to back up M365 data.

It wasn't that long ago that the built-in recycle bin was "good enough" for the majority of organizations who did not yet recognize the need for actual backups of M365.

In 2021, **47%** relied solely on the recycle bin, compared to **4%** today. Meanwhile, **78%** now use a third-party backup, compared with **45%** in 2021.

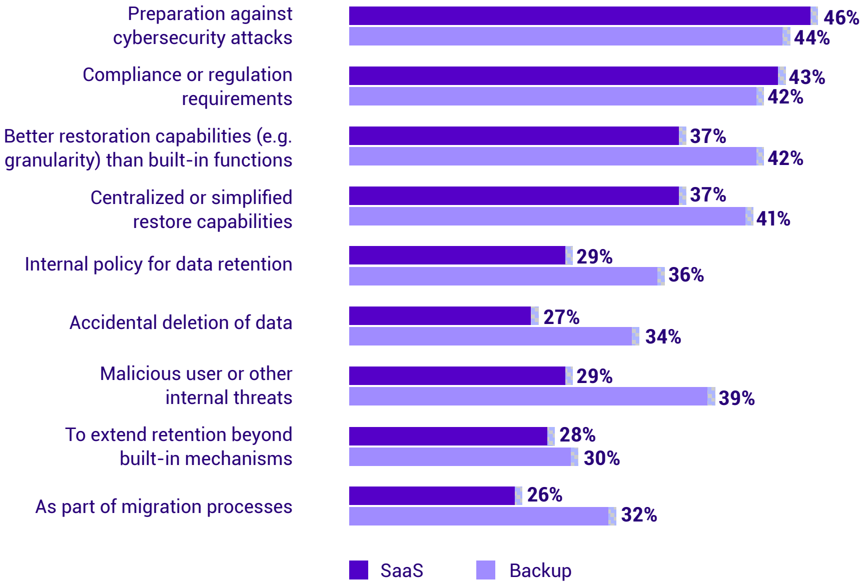


Figure 3.4

What are your organization's primary reasons for backing up your data within Microsoft 365?

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

Why BaaS or DRaaS?

When considering cloud-powered data protection services, it's important to be clear about which:

- Backup as-a-Service (BaaS), focused on protecting and restoring data via a cloud repository and service
- Disaster Recovery as-a-Service (DRaaS), focused on resuming functionality by utilizing cloud-hosted infrastructure in lieu of a secondary "failover" site

Start by asking the most fundamental question of any cloud service is, *"What are the benefits of (BaaS or DRaaS) versus managing my own solution?"*

- **For BaaS,** the answer is *Operational Efficiency*. Other than data survivability and agility (i.e., ability to access backups anywhere), the top five most common reasons come down to operational efficiency.
- **For DRaaS,** respondents recognized 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 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.

81%

of organizations anticipate utilizing cloud-based data protection (BaaS or DRaaS) by 2023.

http://vee.am/DPR22

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 interesting insight from this figure.

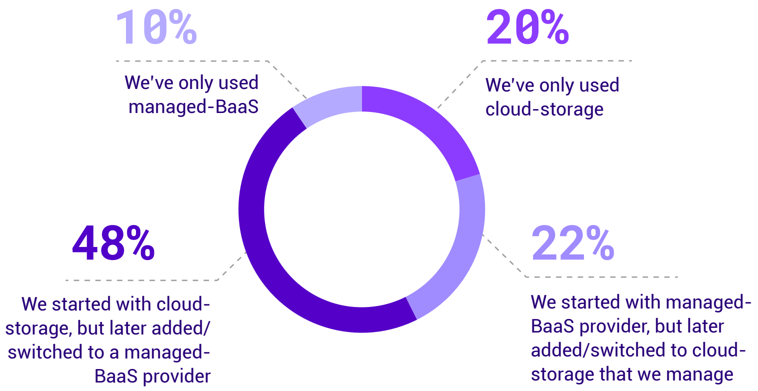


Figure 5.1

How would you describe your organization's use of and journey with cloud-backup storage/services?

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

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 FROM Cloud-storage (instead of from BaaS to cloud storage) — 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 cloud repositories, nearly half of respondents **(48%)** started with simple cloud storage and later chose to utilize BaaS instead.

It is worth noting that these statistics do vary by region:

	Global	Americas	EMEA	APJ
Only used cloud-storage	**20%**	26%	15%	19%
Started with managed-BaaS, but later switched to cloud-storage	**22%**	38%	58%	47%
Started with cloud-storage, later switched to managed-BaaS	**48%**	21%	20%	27%
Only used managed-BaaS	**10%**	14%	7%	7%

There is almost no wrong answer regarding which kind of cloud or who is managing it:

- 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.

And as usual, there is some variance by region:

	Global	Americas	EMEA	APJ
Mostly IT-managed	**46%**	45%	50%	41%
Balance of IT & MSP	**23%**	18%	24%	28%
Mostly MSP-managed	**31%**	36%	26%	31%

The shifts from cloud-storage to managed BaaS can best be seen when looking at the increased interest in "turn-key" or "white-glove" BaaS services.

In 2021, only **13%** want their service provider to do the majority of management, but that is now **31%**. Meanwhile, **46%** currently want to manage their own services, which is down from **63%** in 2021.

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.

The Veeam perspective

Veeam's Backup and Data Management Platform

Now more than ever, it's critical for businesses to remain confident their data is protected and always available, whether it's on premises, at the edge or in the cloud. Veeam provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Our customers are confident their apps and data are protected from ransomware, disaster and harmful actors, and are always available with the most simple, flexible, reliable and powerful platform in the industry.

Veeam gives clients the confidence to accelerate Digital Transformation, protect against cybercrime and drive business resiliency, ensuring that your data is always protected and always available. Reduce cost and complexity, and achieve your business objectives with Veeam: the #1 Backup and Recovery.

To learn more, visit **https://www.veeam.com**.

Click here to view
the Global complete
research report

Questions related to this research
data and insights can be directed
to StrategicResearch@veeam.com

© 2023 Veeam Software. All rights reserved. All trademarks are the property of their respective owners.