

CIO's guide to **cloud-first** **data protection**

Strategies for moving on-premises data protection
and disaster recovery to the cloud



From here to the cloud

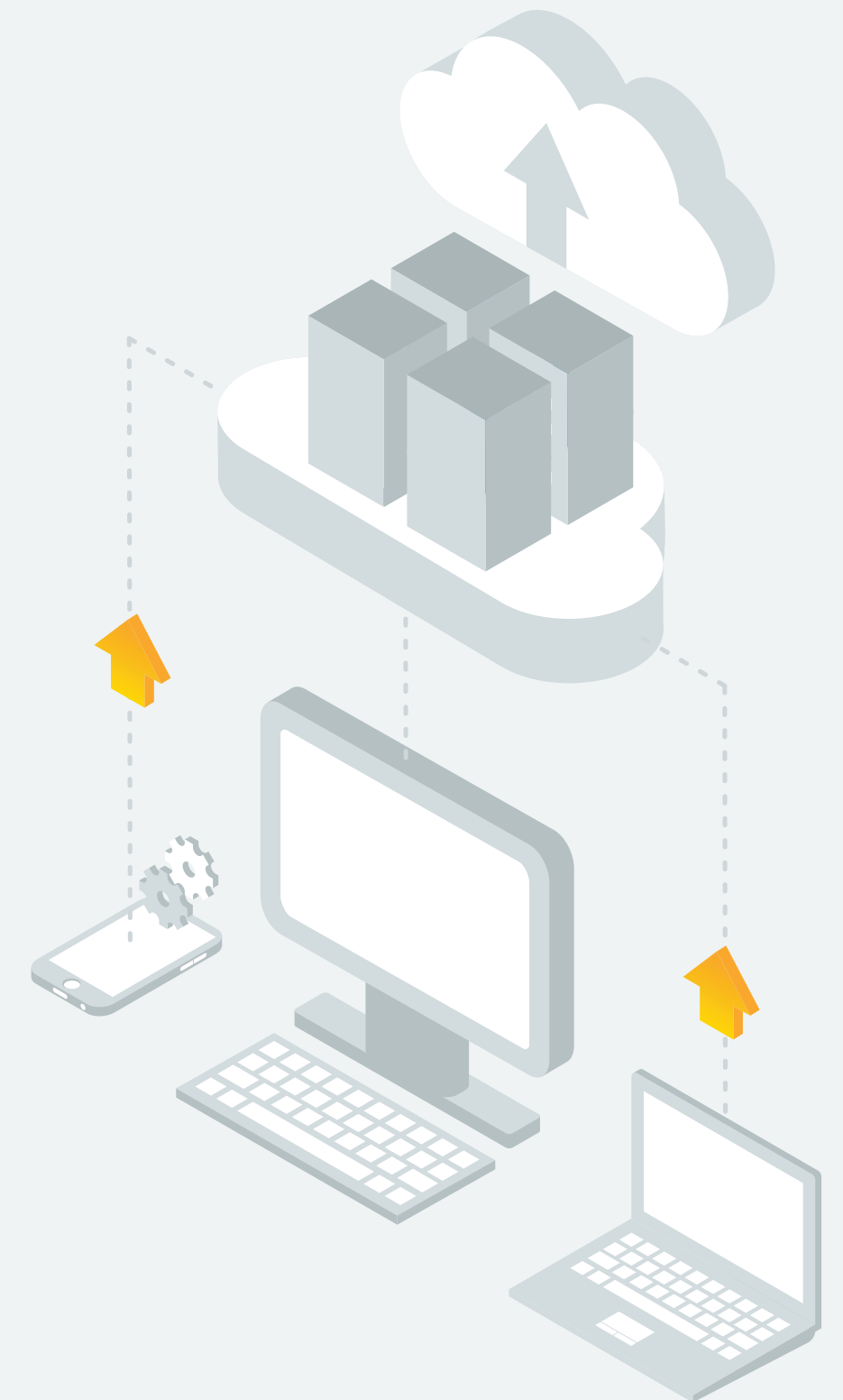
Why move data protection to the cloud (and why it isn't easy)

A growing number of businesses are adopting a cloud-first strategy, in which they look for cloud solutions before they even think about on-premises hardware or software. According to a survey of 2,000 IT managers from Intel Security, 80 percent of enterprises have a cloud-first policy in place.¹ They may define cloud-first as adding new cloud-native solutions, migrating on-premises solutions to the cloud, or a little of both.

At the same time, businesses are looking for a better way to handle data protection. Many organizations are struggling to scale outdated tape-based backups and redundant capacity as the amount of data that needs to be protected skyrockets. For cloud-first organizations, moving data protection to the cloud can seem like a no-brainer; it is often one of the first IT functions to migrate to the cloud.

But transitioning data protection to the cloud isn't easy. Simply relocating legacy backup solutions can lead to unexpected costs, incomplete data, and compromised performance. It can also make it difficult to comply with regional data privacy rules that limit how data can be copied and stored. Businesses get best results from a thoughtful cloud strategy that considers how data is stored, secured, and kept resilient.

This guide provides key strategies for CIOs to consider—and pitfalls to avoid—when transitioning backups and disaster recovery to the cloud.



¹ <https://www.mcafee.com/us/solutions/lp/cloud-security-report.html>

The steady move to the cloud

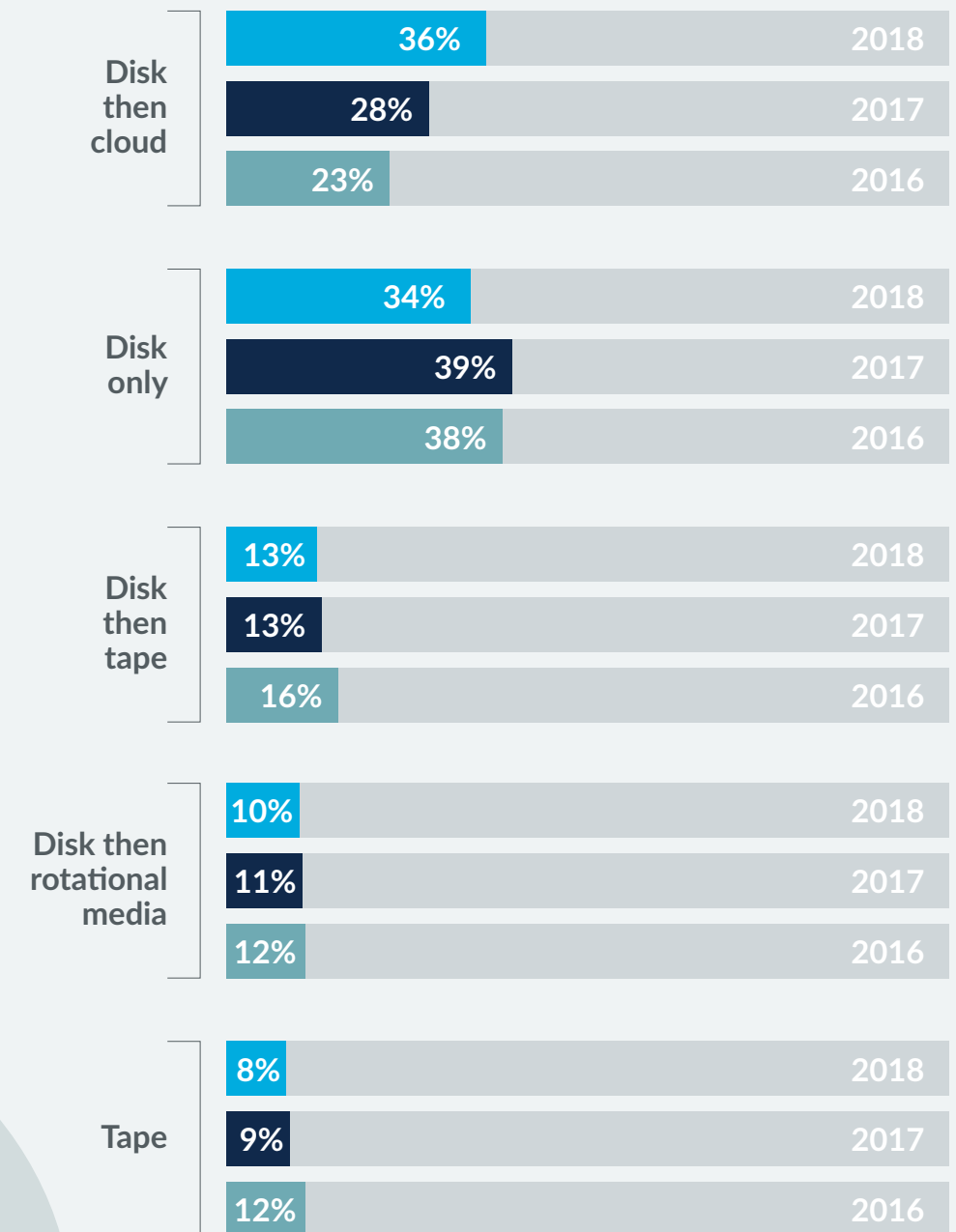
Cloud backup adoption rates vary significantly, depending on the use case

Most companies have a cloud-first policy, and migration to the cloud is increasing, with over 36 percent of businesses surveyed in a 2018 Unitrends study² indicating they store backups in the cloud rather than physical media. However, this leaves a significant number of enterprises still relying on physical media as their primary form of direct backup.

Companies that already leverage SaaS apps widely, startups, and those expanding their IT groups are naturally more likely to adopt the latest cloud data protection solutions. Long-standing IT departments with significant investments in reasonably reliable, legacy infrastructure will tend to defer. However, to the extent that an enterprise depends on uninterrupted access to critical data, is minimizing capital expenditures for infrastructure, and requires the fastest possible RTO/RPO, a cloud solution as the primary backup method is likely.



What primary method of backup do you use?
2016, 2017, 2018



²https://www.unitrends.com/wp-content/uploads/Cloud_SurveyResults_A.pdf

Is cloud-first **right for my business?**

Five reasons why businesses are going cloud-first

A cloud-first strategy is extremely appealing to both business and IT leaders. In fact, many startups are adopting a “cloud only” strategy that allows them to avoid upfront investments in hardware and software altogether. Cloud-first and cloud-only strategies can be applied to almost any technology challenge, including backups and disaster recovery.

Here are five reasons the vast majority of businesses have adopted a cloud-first policy, even if it's only on paper:

- **Lower IT costs.** With cloud services, you can avoid hardware, development, installation, and maintenance costs as well as the need to build and manage a data center.
- **Rapid scalability.** Cloud services are extremely scalable. You can add or subtract capacity and applications in response to business needs. You also avoid the hassle of managing software licenses.
- **Effortless provisioning.** Software patches and updates happen instantly without any user intervention.
- **Open standards.** Cloud providers are increasingly adopting open standards, which means greater flexibility and more applications to choose from.
- **Greater security.** Contrary to myth, cloud services are more secure than on-premises systems. Through 2020, Gartner predicts public cloud infrastructure-as-a-service (IaaS) workloads will suffer at least 60 percent fewer security incidents than those in traditional data centers.³

1-2-3 cloud

Three ways to bring data protection to the cloud

Hybrid cloud: A hybrid cloud data protection strategy relies on traditional, on-premises infrastructure and software that uses the cloud as a storage target. It's typically expensive to install and maintain, and it may present compliance challenges. However, it does give you complete control over your environment.

Cloud enabled: Cloud-enabled data protection is traditional on-premises software offered as-a-service (SaaS). Compared with hybrid cloud, you generally pay less up front and significantly more for maintenance, because your vendor will spend considerable time managing infrastructure and technology that isn't optimized for the cloud. It's also important to remember that cloud-enabled solutions are occasionally marketed using deceptive, “cloud washing” language that can make it hard to distinguish cloud enabled from cloud native.

Cloud native: Cloud-native data protection is optimized for performance and scalability over the public cloud. It offers centralized management of backup and recovery processes, consistent performance even with petabytes of data, and lower TCO compared to hybrid and cloud-enabled solutions. Of course, your cloud-native solution is only as reliable as your service provider, so extra diligence is required when choosing a data-protection partner.

³http://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf

Benefits of cloud-native backup and recovery

Organizations are quickly adopting cloud-native solutions. According to a recent survey by Cap Gemini, 32 percent of new enterprise applications will be cloud native by 2020.⁴ Why is cloud native becoming so popular? Cloud-native solutions can take advantage of scale-out technologies, like object storage, that can be inefficient to deploy on-premises. This means they can deliver superior performance and flexibility, even with very large volumes of data.

When used for data protection, cloud-native solutions offer higher performance and lower TCO compared to traditional architectures using block storage.

Five benefits of using cloud-native services for data protection include:



Scalability and elasticity

A true cloud-native service can allocate capacity on demand as well as expand and contract capacity to ensure performance. This is essential for data protection, since data volume and performance requirements will continue to increase as businesses capture data from the Internet of Things (IoT).



Predictable cloud costs

Cloud-native services can offer a transparent cost structure and pricing model, in which fees are tied directly to consumed resources. As an added benefit, this model provides immediate visibility into utilization. Hosted software models in the public cloud are much less transparent.



Instant failover and data access

Cloud-native data protection can offer immediate disaster recovery failover and data access in case of on-premises system failure, minimizing business downtime.



Higher performance

Cloud-native services typically come with an all-inclusive SLA for all your infrastructure and data. You get higher, guaranteed performance and data durability without the hassle of dealing with multiple third-party vendors and software providers.



Tighter security

Working with infrastructure providers like AWS and Azure, cloud-native providers can deliver higher security through continual monitoring, thorough testing, and security updates that are applied quickly and consistently.


⁴ <https://www.capgemini.com/service/cloud-native/>

How to tell the difference between cloud-enabled and cloud-native data protection services

Both cloud-enabled and cloud-native data protection are typically delivered as SaaS. Unfortunately, it can be difficult to tell the difference between the two because of cloud-washing—the aggressive use of cloud-related buzzwords applied to traditional architectures retrofitted to operate in the cloud.

Here are some questions to ask your provider to help you determine if their solution is cloud enabled or truly cloud native:

- How much data will be stored given your current data-protection footprint and how much will it cost? How much more will you pay if you need to support more data? How do costs go down when data is purged?
- Can your provider explain how fees are calculated?
- What is the archiving model? How is data moved from warm to cold storage? What are the associated costs?
- How quickly does the system scale when you need more capacity?
- What about management across multiple regions?
- Does the provider utilize block or object-based storage? If block, how do they provide replication/resiliency and scale as capacity increases?



Generally speaking, cloud-native solutions are less expensive than cloud-enabled options while offering more predictable costs, rapid failover, and the flexibility to quickly scale up or down.

Your journey to data protection in the cloud

Six steps for a smooth transition to cloud backup and recovery

Moving from traditional, tape-based backup and recovery to cloud backup and recovery can deliver significant cost reductions and performance benefits—but it also requires careful planning. The following six steps can help you establish a game plan as you transition your data protection operations to the cloud.

Step 1:

Inventory your workloads

First, you'll need a thorough understanding of all the data you will need to back up and where it resides, whether it's in data centers, regional or branch offices, or somewhere in the cloud.

If you are already using SaaS applications, be sure to include those as well, since most SaaS providers recommend third-party solutions to backup business data. Lastly, don't forget to include end-user data, especially on mobile devices.

Step 2:

Check your requirements

Next you'll need to identify your data protection requirements. Questions to consider include:

- How fast do backups need to be?
- How much of your data is mission critical?
- What kinds of data sovereignty and data privacy regulations do you need to comply with?
- What are your current SLAs for recovery point and recovery time objectives (RPO and RTO)? Are they good enough? What would you like your RPO and RTO targets to be?
- Do you need disaster recovery? How about workload mobility and testing/development?
- What are your requirements for long-term archiving?
- What do you want your total cost of ownership (TCO) to look like?

Step 3: Decide how much cloud you need

Once you've identified your requirements and the scope of the data you need to protect, it's time to determine where cloud will offer the most value for you.

For example, many businesses choose to start at the "edge" first, transitioning piecemeal backup and recovery efforts of remote and satellite offices to the cloud. Others may wish to fully replace an expensive legacy backup and recovery system with something that can address modern cloud workloads.

Depending on your needs, you may move some or all of your data protection into the cloud. You can opt for a hybrid cloud, a cloud-enabled, or a cloud-native solution, each with different pros and cons. A hybrid cloud solution may offer the peace-of-mind of a physical backup component, but it's likely to be the most expensive option due to on-premises hardware costs. Cloud-enabled products may be more clunky and difficult to

manage since they weren't designed for the cloud, but costs may be lowered by leveraging existing on-premises infrastructure. Cloud-native solutions can offer lower costs with the greater scalability of the cloud, but may not meet everyone's RTO/RPO requirements.

You may choose a blended solution, with elements of all three. For example, if you have limited bandwidth, you may want to mix cloud-native with an onsite appliance/caching system to improve performance and work around low-bandwidth sites.

When you know how much cloud you'll need for data protection, you can develop a RFI and begin evaluating service providers.

Step 4: Figure out what it's going to cost

If you have determined your architecture and identified one or more service providers, you probably have enough information to figure out what your new cloud data protection model is going to cost.

Many cloud services offer subscription-based models, and cloud-native services can provide pricing based on consumption. Your service providers should be able to provide a cost calculator to help you estimate your payments under different pricing models.

Step 5: Try cloud data protection for yourself

The only way to truly feel right about a solution is to see it in action in your own unique environment.

With any approach, you want your IT group's enthusiastic buy-in, and a trial is the fastest and easiest way to get it.

If you've chosen a hybrid cloud or cloud-enabled solution, most likely this will require some trial hardware from the data protection vendor, so you'll need to plan for shipping and installation. Cloud-native solutions have no hardware, so you'll be able to set up a trial in less than 30 minutes in most cases.

During the trial period, you'll want to assess several areas:

- **Ease of use:** Was the installation simple? Is the management console intuitive?
- **Scalability:** Will it scale as my business grows?
- **Security:** What kind of admin controls exist? Is the data secure?
- **Coverage:** Does the solution cover all of my backup needs?

Step 6: When it's time to decide

Choosing to trust your enterprise data with a particular cloud-native data protection and management solution isn't that complicated.

- Does the product do the job you need it to do?
- Has the provider proven its character and corporate strength over time with sustained, growing customer relationships and partnerships with industry leaders?
- Can you make the numbers work? Does the solution fit into your IT financial model?

Adding up the appropriateness and quality of the feature set, the strength and reliability of your vendor, and the viability of the business model will ensure you make the best decision for keeping all of your enterprise data safe.

The rewards from migrating to the cloud

Comprehensive benefits enterprise-wide

While the idea for cloud data protection typically comes from the CIO's office, it also has major benefits for the CFO and CEO. Cloud data protection is an important business strategy for the whole company:

- **Lower IT budgets.** Complex, large-scale backups requiring local storage drives and tapes can be enormously expensive to maintain. Cloud data protection, especially when implemented through cloud-native solutions, can cut costs dramatically.
- **Refocus IT on innovation.** Cloud data protection with policy-based automation takes significantly less time to maintain than on-premises solutions. This means IT can spend less time on routine backups and more time applying technology to business challenges.
- **Quickly respond to business needs.** Cloud data protection, especially when delivered as a cloud-native service, can quickly scale to handle larger volumes of data. Because it provides global visibility and access, data can quickly be identified and made available for compliance, legal, and other department requirements.
- **Reduce the risk of a security incident.** Most high-profile security breaches involve on-premises IT, not cloud services. With the right service provider, cloud data protection can be more secure than those onsite.

At Druva, we specialize in cloud-native data protection and management solutions, and we've seen all of our customers benefit from using cloud-native services for backups and disaster recovery. Discover more about cloud-native data protection and management by visiting druva.com.



About Druva

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital and Nexus Partners. Visit [Druva](https://druva.com) and follow us [@druvainc](https://twitter.com/druvainc).