THE CLOUD-FIRST DATA PROTECTION PLAYBOOK

Strategies for Moving On-Premises Backups and Disaster Recovery to the Cloud

START

druva

From Here to 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-based solutions before they even think about on-premises hardware or software. According to a survey of 2,000 IT managers from Intel Security, 80% of enterprises have a cloud-first policy in place.[1] They may achieve cloud first by adding new cloud-based 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 Many organizations are struggling to scale outdated tape-based backups and redundant capacity as the amount of data that needs to be protected explodes. **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 playbook 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

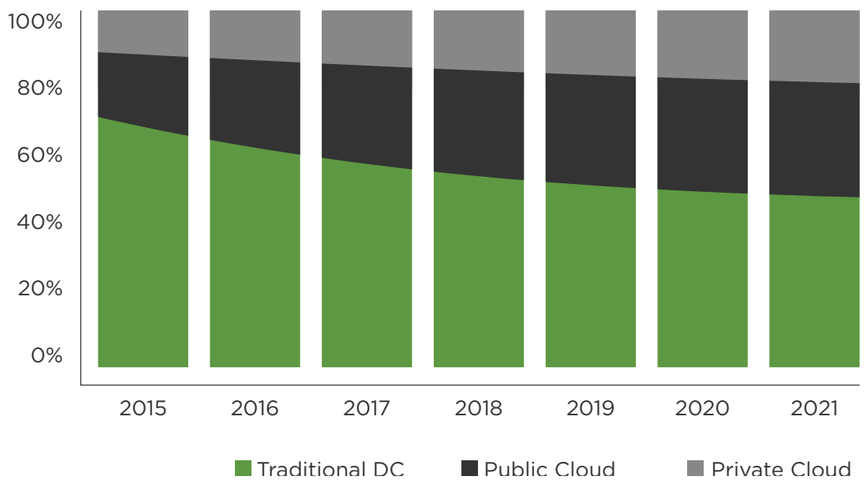
The Slow Rise of Cloud

Cloud Backup Adoption Rates Vary Significantly, Depending on the Use Case

Although most companies have a cloud-first policy, the movement to public cloud is slow and steady. This helps explain why 49% of businesses surveyed in an ESG study say they still rely on tape as their primary form of direct backup.

Worldwide Cloud IT Infrastructure Market Forecast by Deployment Type 2015–2021 (shares based on value)

Source: Worldwide Quarterly Cloud IT Infrastructure Tracker, Q4 2016



49% of businesses surveyed in an ESG study say they still rely on tape as their primary form of direct backup.[2]

[2]https://www.lto.org/wp-content/uploads/2014/06/ESG-WP-LTO-EVV-Feb_2016.pdf

Everyone is Doing It

5 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

1. **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.
2. **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.
3. **Effortless provisioning**. Software patches and updates happen instantly without any user intervention.
4. **Open standards**. Cloud providers are increasingly adopting open standards, which means greater flexibility and more applications to choose from.
5. **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% fewer security incidents than those in traditional data centers.[3]

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

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 software 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 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 due diligence is required when choosing a data protection partner.

5 Benefits of Cloud-Native Backup and Recovery

Organizations are quickly adopting cloud-native development. According to a recent survey by Cap Gemini, 15 percent of new enterprise applications are cloud native today with adoption set to increase rapidly in the next three years, jumping to 32 percent 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. That 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:

1. **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).

2. **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.

3. **Instant failover: 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.

4. **Higher performance:** Cloud-native services typically come with an all-inclusive SLA for your all your infrastructure and data. You get higher, guaranteed performance and data durability without the hassle of dealing with multiple vendors (e.g., AWS and software providers).

5. **Tighter security:** Working with infrastructure providers like AWS and Azure, cloud- native providers can deliver higher security through continual monitoring, thorough testing, and ensuring that security fixes and patches 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 services 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

7 Steps for A Smooth Transition to Cloud-Based Backup and Recovery

Moving from traditional, tape-based backup and recovery to cloud-based backup and recovery can deliver significant cost reductions and performance benefits—but it also requires careful planning. The following 7 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.

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, it's time to determine where cloud will offer the most value. 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 more modern and less expensive.

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. Or 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 an RFI and begin evaluating service providers.

STEP 4: TAKE A DEEPER DIVE

After you define the level of service you need, we recommend mapping out whatever backup and recovery architecture your IT team will be responsible for. If you're opting for a hybrid environment, you'll need to define how on-premises data will be stored in the cloud and how recovery will work.

STEP 5: 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-based 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 6: ADD POLICY-BASED AUTOMATION

Policy-based automation can help you dramatically reduce storage costs by moving backup data to inexpensive storage on a predetermined schedule.

STEP 7: DON'T FORGET THE FINANCIALS

If you sign up with one or more service providers, you'll need to integrate their fees into your IT financial model. If you have a cloud-native solution, you'll be able to easily track usage and bill it back to the correct business units.

Your Journey to Data Protection in the Cloud

7 Steps for A Smooth Transition to Cloud-Based Backup and Recovery

While the idea for cloud-based data protection typically comes from the CIO's office, it also has major benefits for the CFO and CEO. In fact, many companies see cloud-based data protection as a business strategy, because it allows them to:

- **Manage IT budgets.** Complex, large-scale backups requiring local storage drives and tapes can be enormously expensive to maintain. Cloud-based data protection, especially when implemented through cloud-native solutions, can cut costs dramatically.
- **Refocus IT on innovation.** Cloud-based 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-based data protection, especially when delivered as cloud-native services, can be quickly scaled 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 providers, cloud-based 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 our customers benefit from using cloud-native services for backups and disaster recovery.

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data- management-as-a-service solution that aggregates data from endpoints, servers, and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance, and intelligence—dramatically increasing the availability and visibility of business-critical information while reducing the risk, cost, and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data and unify backup, disaster recovery, archival, and governance capabilities onto a single, optimized data set. As the industry's fastest-growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 40 petabytes of data. Join the conversation at **twitter.com/druvainc**

For more information, visit **www.druva.com**

Druva, Inc.
Americas: +1 888 248 4976
Europe: +44 (0) 203-7509440
APJ: +919886120215
sales@druva.com
www.druva.com