druva

The definitive guide to enterprise data backup and recovery architectures

Comparing on-premises, hybrid, hosted, and cloud-native solutions

druva

From legacy to cloud data protection

The evolution of modern data protection strategies

The all-encompassing data center is a thing of the past. Modern data environments are distributed and include remote and branch offices, mobile devices, and the Internet of Things (IoT) as well as cloud solutions such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). There is more critical data to back up than ever before. Plus, data silos and fragmented management mean poor visibility, which can make it difficult to comply with regional data residency and security rules as well as service-level agreements (SLAs).

On-premises data protection has not kept pace. According to a survey by Fujitsu, 45 percent of IT managers said they had lost data or productivity related to data protection inefficiency within the previous year.[1] Often, this is because on-premises backups are cumbersome and do not always happen on time.

[1] https://go.druva.com/rs/307-ANG-704/images/451_DisasterRecovery_DataBackup_RM.pdf

druva

Businesses are moving data protection to the cloud

A growing number of businesses are thinking about moving data protection to the cloud, because it promises to be:

- **Less expensive.** With cloud services, you eliminate hardware installation and maintenance costs. You don't have to build and manage a data center. When you back up all of your data to the cloud, you only pay for the capacity you use, thereby minimizing storage costs and overall total cost of ownership (TCO).
- **More scalable.** You can add or subtract capacity to support large and rapidly changing workloads virtually instantaneously.
- **Easier to manage and maintain.** Data unification—storing all of your backup data in the cloud—makes it easier to know exactly what data you have and manage it from a single control panel rather than multiple, incompatible tools. Plus, IT often doesn't have to manage routine software patches and updates for data protection infrastructure.
- **Highly flexible.** Cloud providers are increasingly adopting open standards, which means greater flexibility and more applications to choose from.
- **More reliable (and less risky).** Cloud providers are more likely to meet their SLAs for recovery time and recovery point objectives (RTO and RPO) when restoring business-critical data, and therefore ensure business continuity.

Today, there are many data protection architectures to choose from. This paper will compare on-premises data protection with hybrid, hosted, and cloud-native options and help you determine which one is right for you.

The problem with on-premises data protection

Although a growing number of businesses are adopting or considering data protection in the cloud, most still depend on on-premises backup and recovery. In an ESG survey, 49 percent of businesses said they still rely on tape as their primary form of direct backup.[2] Why is this a problem? Downsides of on-premises backup and recovery include:

High costs

Maintaining and upgrading traditional backup solutions can be very expensive. Tape backups in particular can absorb significant IT resources and generate escalating maintenance costs.

Poor scalability

On-premises data protection is difficult to scale as your business grows. When data growth outstrips the capabilities of your data protection system, backups may be late or simply not happen. An ESG survey of almost 400 IT and storage managers at midmarket companies revealed that only 70 percent of backup jobs are completed on time.[3]

Data loss

When backups are late or incomplete—which is often the case with on-premises data protection during periods of rapid business growth—recovery from events such as outages or ransomware attacks can be compromised.

Non-compliance

Traditional backup solutions that store regional data in centralized hubs may not comply with evolving data privacy regulations and can present significant legal risks.

[2] https://www.lto.org/wp-content/uploads/2014/06/ESG-WP-LTO-EVV-Feb_2016.pdf
[3] https://go.druva.com/rs/307-ANG-704/images/ESG-Solution-Showcase-Druva-April-2017.pdf

druva

Is the cloud secure enough for data protection?

Just a couple of years ago, the public cloud was considered too dangerous and unreliable for storing sensitive company data. A lot has changed since then, including:

Improved physical security

Maintaining and upgrading traditional backup solutions can be very expensive. Tape backups in particular can absorb significant IT resources and generate escalating maintenance costs.

Continuous monitoring

Automated, 24/7 security monitoring allows cloud service providers to identify potential issues long before they impact customer data. Through 2020, Gartner predicts public cloud IaaS workloads will suffer at least 60 percent fewer security incidents than those in traditional data centers.[4]

Frequent security audits

Cloud service providers conduct frequent security audits to ensure they're using the latest best practices.

New compliance measures

Cloud service providers have introduced local archiving and thoughtful storage policies for full compliance with regional data privacy and security rules.

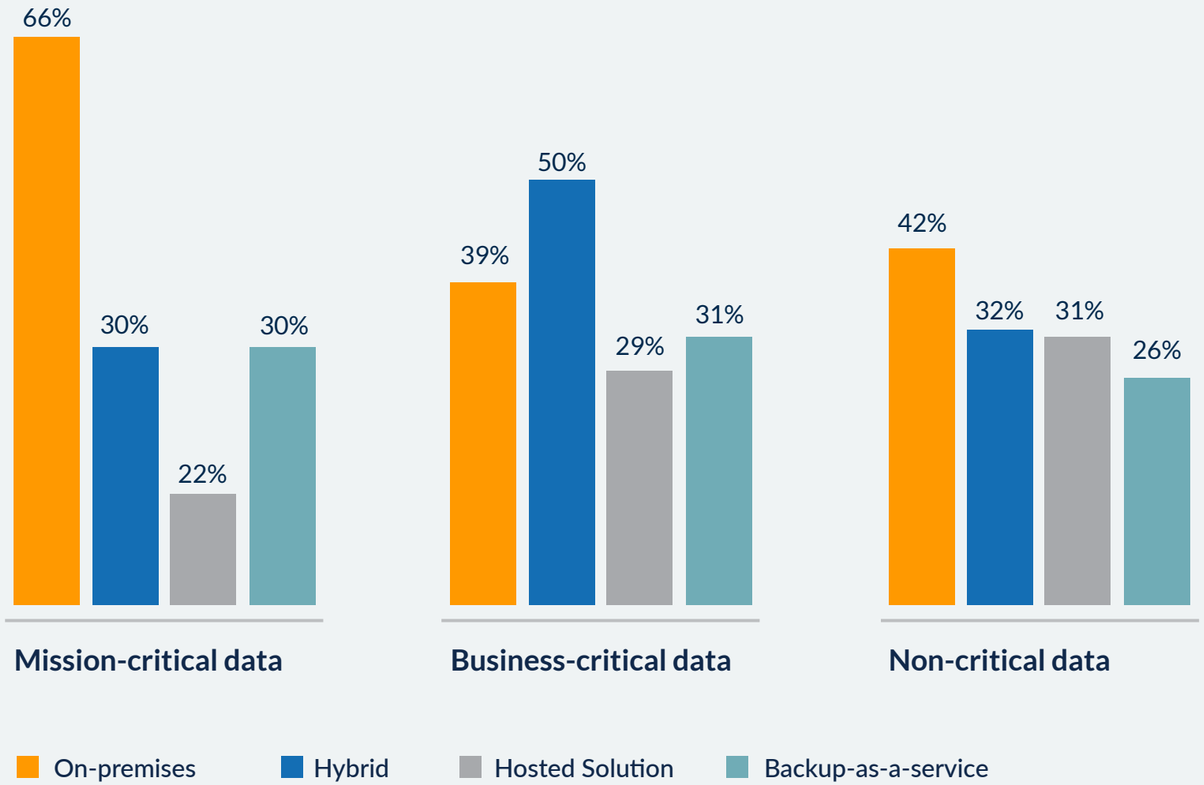
[4] http://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf

Popular data protection architectures

On-premises architectures are still commonly used for data protection.

While enterprises are moving some of their data to the cloud and actively considering the cloud for data protection, most still rely on some form of on-premises architecture, especially for mission-critical data. According to a study commissioned by Forrester, most businesses use multiple approaches to data protection, including on-premises architectures as well as hybrid, hosted, and native cloud.[5]

What approach(es) are you using to backup your data?



[5] Base: variable; IT professionals at organizations in the US and Canada
Source: a commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

druva

A brief overview of the most popular solutions for enterprise data protection

On-premises

On-premises data protection architectures are deeply entrenched in many organizations. Although this model lacks scalability, some IT teams may believe on-premises data protection gives them more control over critical data and minimizes security risks.

Hybrid cloud

A hybrid cloud data protection strategy relies on on-premises infrastructure and software for recent backups and uses the cloud for long-term archiving. Hybrid solutions may include data replication and tape backups. TCO may be better than traditional, on-premises data protection, but it is hard to scale, may take months to build, and can be complex in a way that makes achieving visibility into global data more difficult. This kind of cloud offers IT more control, but also requires active IT involvement at all phases of development.

Hosted cloud

Hosted cloud is traditional on-premises backup software running in the cloud and using warm storage. It offers greater availability than hybrid cloud, but it isn't necessarily optimized for a cloud environment; it doesn't fully deliver the economies of scale the cloud has to offer. TCO is similar to or slightly better than hybrid cloud, and it still requires considerable IT oversight.

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 than hybrid and hosted solutions. It also scales quickly. IT has much less day-to-day involvement than with hybrid and hosted models.

druva

Comparing data protection architectures

Cloud-native data protection offers much lower TCO, greater resiliency, and more features than competing architectures.

	On-premises	Hybrid	Hosted	Cloud-native
Resilience/Durability	99%	99.5%	99.99%	99.99999%
Availability	99%	99%	99.5%	99.95%
Time to market	Months	Months	Days	Days
Total cost of ownership	High	Mid	Mid	Low
Offsite options	Replication/tapes	Replication/tapes	Limited replication	3-way replication
Retention options	Disk/tapes	Disk/cold storage	Disk/cold storage	Object/cold storage
Network throughput	LAN	LAN + WAN	WAN (Restricted bandwidth)	WAN (Unrestricted bandwidth)
Scalability	On-request	On-request	On-request	Scale-out (unlimited)
RTO/RPO	High	High	Low	High (cache/disaster recovery)
Global reach (new data centers)	On-request	On-request	On-request	On-demand

druva

How fast is fast enough?

Can cloud data protection meet your RTOs?

When an event happens that takes your business offline, time is money. You want to recover your data as quickly as possible and if the problem system can't be recovered, data must be restored from backup. A recovery time objective (RTO) is how long you have to restore data from backup without incurring business consequences. Your ideal RTOs may be different for different applications and lines of business.

The ABCs of RTOs in the cloud

RTO is a common metric in data protection SLAs, both internal and external. Yet recovery jobs often fail to meet RTO SLAs. In many cases, cloud data protection—especially hosted and cloud-native solutions—can offer greater reliability as well as significantly better RTOs than on-premises solutions for:

- **Active-system recovery.** Most backup and recovery architectures can support active-system recovery, but hybrid, hosted and cloud-native solutions offer coverage for both on-premises and cloud applications. Hosted and cloud-native models also offer extremely fast RTO for endpoints and remote offices.
- **Archive recovery (cold data > 1 year).** On-premises and hybrid cloud solutions that rely on tape backups are significantly slower than hosted and cloud-native solutions that use cold storage.

RTO comparison for active-system recovery

	On-premises	Hybrid	Hosted	Cloud-native
Endpoints	20 minutes	20 minutes	5 minutes	5 minutes
Remote offices	30 minutes	30 minutes	20 minutes	20 minutes
Small DC (100TB+)	30 minutes	30 minutes	1 hour	1 hour
Large DC (100TB+)	30 minutes	30 minutes	1 hour	1 hour
Cloud applications	N/A	N/A	1 hour	1 hour

RTO comparison for archive recovery

	On-premises	Hybrid	Hosted	Cloud-native
Remote offices	Days	Days	4-8 hours	4-8 hours
Small DC (100TB+)	Days	Days	4-8 hours	4-8 hours
Large DC (100TB+)	Days	Days	4-8 hours	4-8 hours
Cloud applications	Days	Days	4-8 hours	4-8 hours

druva

Hosted cloud vs. cloud-native

What's the difference ?

Both hosted and cloud-native data protection services are typically delivered as SaaS. Unfortunately, it can be difficult to tell the difference between the two because buzzwords like "cloud-enabled" are often used to describe a broad spectrum of cloud frameworks.

Generally speaking, hosted cloud solutions repurpose traditional data protection software by running it in the cloud. Cloud-native solutions rely on software designed specifically for the cloud.

Hosted

A hosted solution is limited by the on-premises software it uses.

- Uses traditional software in the cloud
- Doesn't completely leverage cloud-native technologies for scale and efficiency
- Expensive to build and manage
- Limited search or disaster recovery capabilities
- Single-tenant, manual updates

Cloud-native

A cloud-native solution utilizes the full capability of the cloud.

- Uses software designed to take full advantage of the cloud
- Leverages cloud-native technologies for scale and efficiency
- Lower cost and effort
- Higher value of data with integrated disaster recovery, archival, search, and analytics
- Multi-tenant, automatic updates

druva

Find the right cloud data protection strategy

Ultimately, the best data protection for your business is the one that meets your requirements.

The first step to moving some or all of your data protection to the cloud is understanding your RTO and RPO needs for mission-critical, business-critical, and non-critical data. Once you've defined your requirements, it's time to research cloud data protection and management solution providers.

When you're talking to solution providers, these questions can help you see beyond the "cloud" buzzwords and identify which solutions will work best for you:

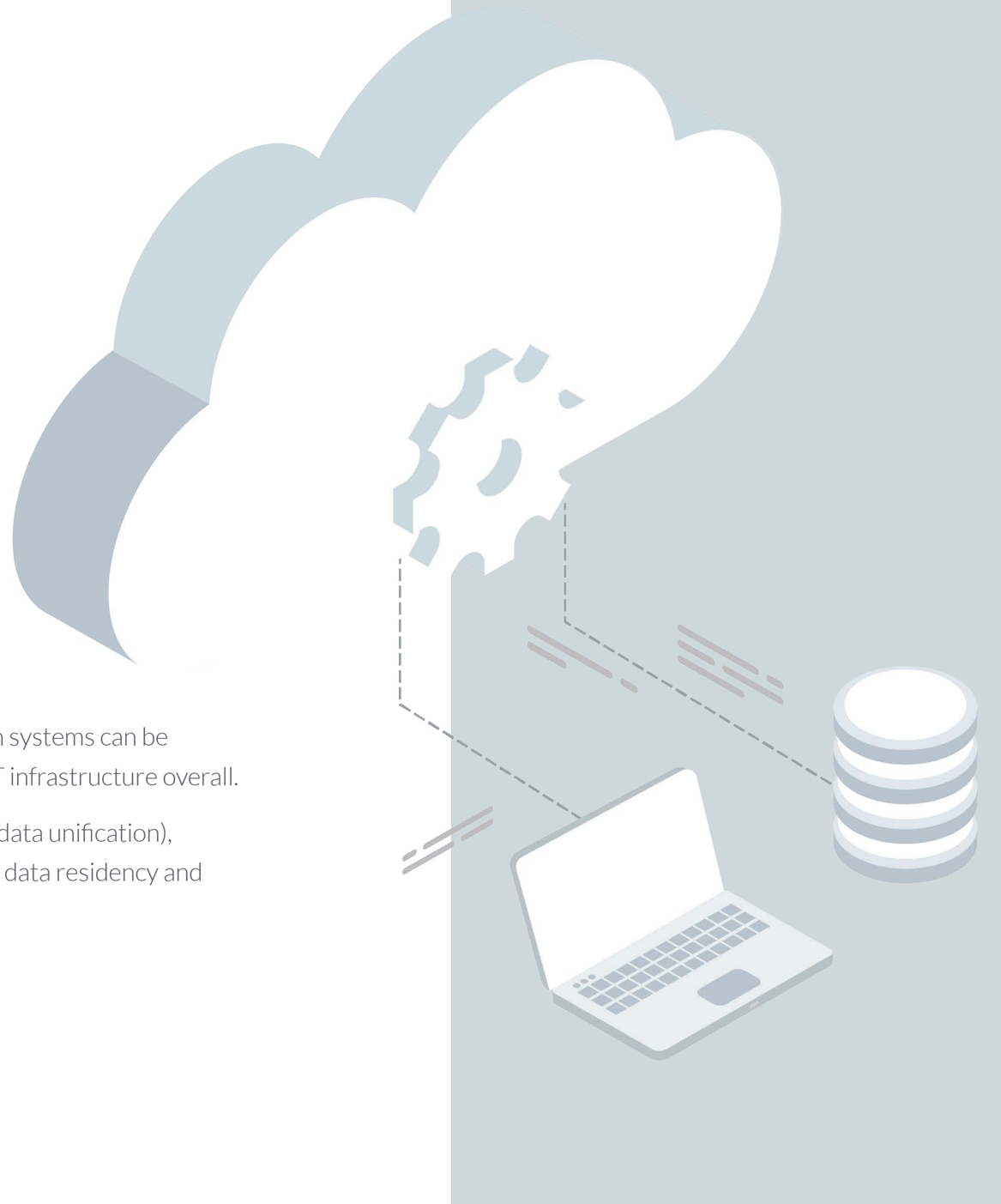
- How much data will be stored given your current data protection footprint, and how much will it cost?
- How much more will you pay if you need to support more data? How do costs go down when data is purged?
- What is the archiving model? How is data moved from warm to cold storage? What are the associated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

druva

It’s better in the cloud

The value of cloud-native data protection

- **Improved reliability and recoverability of backups.** This is no surprise, as most cloud data protection models—and cloud-native in particular—are built to meet aggressive SLAs.
- **Increased security.** A growing number of businesses are recognizing that data protection in the cloud is actually more secure than on-premises data protection.
- **Reduced IT personnel costs.** Cloud data protection—especially hosted and cloud-native—requires much less IT involvement than on-premises protection.
- **Reduced or eliminated on-site data protection hardware infrastructure costs.** For midmarket and larger companies, this savings can be substantial, freeing up resources for innovation.
- **Reduced complexity within an IT environment.** Legacy, on-premises data protection systems can be complex and time-consuming to maintain. Cloud data protection can help streamline IT infrastructure overall.
- **Greater manageability and compliance.** If all backup data is stored in the cloud (e.g., data unification), businesses can manage that data from a single dashboard and more easily comply with data residency and other rules as well as SLAs.



druva

Druva: cloud-native data protection and management

Enterprise cloud backup with integrated disaster recovery and archival

Druva solutions, built on AWS, deliver data protection and governance for all enterprise infrastructures from mobile endpoints to VMs and cloud workloads. Druva offers high-performance, scalable backup, DR, archival, and analytics to simplify data protection, improve visibility, and dramatically reduce the risk, cost, and effort of managing today's complex information environments.

Key features include:

- **Offsite infrastructure.** It automatically protects data without the need for expensive on-site hardware and administrative overhead.
- **Improved business agility.** Response times for failover are nearly instantaneous with RTOs measured in minutes. Likewise, it can seamlessly replicate and move VMs across regions.
- **Workload mobility.** It supports workload mobility, which brings data protection to local applications and addresses their testing and development requirements.
- **Simplified management.** It provides a single dashboard for managing all of your server backup and DR policies, so you don't have to rely on multiple storage, compute, and network management tools.
- **Low TCO.** Its pay-per-use model means you pay only for what you consume. Because it performs backups, DR, archiving, and analytics on a single, unified data set, you also avoid the costs associated with managing multiple data silos.

Discover how Druva delivers a SaaS-based platform to protect and manage enterprise data across endpoint, data center, and cloud workloads.

druva

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 and follow us @druvainc.

Q120–20023