druva

Top 10 principles of a cloud backup service

Key considerations for a cloud data protection and management solution

Introduction

New cloud offerings are coming to market everyday, and there are a number of fundamental principles that you should use to evaluate their appropriateness for your particular enterprise and applications. However, not all services are built to the same standards, nor will they necessarily meet your needs.

This eBook will help you understand the top ten principles of a cloud backup service, so you can make an informed decision by applying the following cloud-first principles:

Reduce the cost and complexity of data protection

Increase cyber resilience

Maintain compliance

Accelerate and protect cloud projects

#1 | Reliability and availability

Ensuring that a cloud data protection solution performs the services you need when you need them depends on the two most important attributes of a modern cloud service: the system works consistently and, if it does fail, there's immediate backup. Your business processes can't be interrupted.

- **A reliable cloud backup service** is virtually always up and running without interruptions or downtime. Interactions with the service are secure, and you can access the service from any credentialed endpoint anywhere in the world. A service with high availability has redundant systems that automatically engage when service levels spike or resources shift.
  A good provider also ensures reliability by consistently testing its vulnerability and always monitoring security.
- **Reliability** is about how long a system can carry on before something goes haywire. Availability is about how quickly and comprehensively functionality can be restored, so customers are least affected by an outage. All systems eventually have issues, even AWS servers have outages.
  But when they do, another resource or availability zone immediately kicks in, and customers are almost instantaneously back in business.

Cloud data protection ensures availability with a high level of system redundancy. Different types of data are maintained in different resources, such as storing configuration data in a relational database service, storing deduped metadata in Apache Cassandra nodes, and storing data itself in basic storage resources. A strong cloud data protection provider is consistently testing and re-evaluating storage resources — so customers don't have to. Look for well-defined uptime SLAs for every configuration of a provider's service.

KATZ MEDIA GROUP

> **"We wanted to get out of the business of managing hardware, simplify our backup and recovery implementation, and move towards a subscription-based model that would scale when needed.**

Read case study

#2 | Zero trust security

Many are surprised to learn that cloud storage platforms can be just as vulnerable to cyberthreats as on-premises backup appliances and data centers. It's not unusual for cloud customers to make configuration mistakes and enable inappropriate sharing, making backup data a rich target for malware. Once lodged inside a data store, ransomware can wait months before manifesting, quietly encrypting data, obscuring its roots, and frustrating remediation.

Cloud service providers (CSPs) are responsible for the security of their hardware, software, networking, and facilities, but not the stored data itself. That said, most CSPs like AWS do their best to look out for their customers, in any way they can, when it comes to cyberthreats.

The zero trust model — never trust, always verify — is a primary tenet of cloud security. So is the 3-2-1 rule: three copies of data (production and two backups) on two different media and one copy offsite, completely separate from the production environment. Of course, all data is encrypted in transit and at rest. In particular, a comprehensive cloud data protection solution, also incorporates:

- **Single sign-on, multi-factor authentication** and role-based access to isolate and control data access.
- **Anomaly detection** and alerts to identify and isolate infections of historical and current backups.
- **Easy identification** of last good-known-copies with audit trails and the ability to automatically block downloads of infected content.

expel

> **"From a third-party vendor risk perspective, Druva knocked it out of the park. As a security company that's our top priority, and Druva exceeded our security expectations.**

Read case study

#3 | Compliance and privacy

Yes, making life easy is the overarching benefit of using a cloud-based data protection solution. You don't have to worry about hardware, and the service automatically updates the application in the cloud without taxing your enterprise IT. But nobody can relax when it comes to compliance. Fines and lawsuits are too costly, and compliance policies need to be governed accurately over time. That's why when you're evaluating a cloud data protection provider, you have to be especially careful to ensure they take compliance as seriously as you do.

A huge threat to maintaining compliance is the proliferation of shadow IT. This is when people are accessing and using data and applications without adequate credentials or IT department approvals. The problem has been significantly aggravated with cloud-based applications, perhaps because again, cloud services tend to make things easy, and IT may let their guard down. But the risks of data leaks and compliance violations are too great to ignore.

Obtaining certifications such as those for the System of Operation Controls (SOC) 2, Federal Risk and Authorization Management Program (FedRAMP), and Health Insurance Portability and Accountability Act (HIPAA) isn't easy. For example, it can take a year and a half to complete SOC 2 reporting, but it's worth it. It ensures a provider has established and is following strict information security policies and procedures concerning the security, availability, processing, integrity, and confidentiality of customer data.

If you or the provider are doing any business with the federal government, FedRAMP compliance is mandatory. HIPAA certification isn't mandatory, but the regulations are exacting. In any case, having these and other certifications shows that the service provider takes security and best practices seriously.

NIH NATIONAL CANCER INSTITUTE

> **"Cloud-first is a no-brainer, and the Druva platform aligned with our goals for digital transformation.**

Read case study

#4 | Data localization and multi-regional support

Shipping products overseas has always involved customs regulations, trade agreements, and with some commodities, government inspections. Now, data has arguably become one of the most valuable international products, and with the cloud, it can cross borders faster than the blink of an eye.

Data localization/residency concerns the physical location of data storage and how agencies and companies control access to the data. Typically, governments extensively regulate any data that may include personal, governmental, or legal information, and a cloud data protection provider has to be 100 percent aware of very complex state, country, and regional laws.

The EU's General Data Protection Regulation (GDPR), Brazil's Lei Geral de Proteção de Dados (LGPD), the UK's Data Protection Act (DPA), and California's California Consumer Protection Act (CCPA) are the most highlighted regulations. Additionally, however, every corner of the world has unique, local restrictions on how data is stored and shared. Data is just too valuable a commodity.

And it's not just about keeping data storage physically localized. Regulations often require that processing or analyzing certain types of data take place locally as well, requiring investments in local compute infrastructure. A cloud-based data protection provider has to know and comply with these regulations as predictably as they maintain uptime.

This means multi-regional resources, having access to data centers strategically located close to wherever a customer conducts business. The cloud data protection provider's performance can significantly affect a company's success, particularly as the company expands multinationally.

GULFMARK

> **"The restore times were faster than we expected. By storing the data in a region in AWS, we don't have to send a backup across the globe.**

Read case study

#5 | Radical simplicity

Cloud-native SaaS does away with a score of management tasks typical of traditional enterprise apps. In fact, ease of management is a sure way of telling if an app was designed from the start for the cloud. Adding cloud-connectivity features to a legacy application or service and rebranding it as "cloud-ready" is called cloud washing — it's an obsolescent product and it's not going to give you real cloud performance.

Cloud services eliminate work. They're easy to deploy, run, and scale so you can enjoy their benefits rather than keep them running on time. Look for these characteristics of strong cloud data protection solution:

- **Feature upgrades**, patches, and other changes occur transparently without any service disruption. A good indicator of continuous improvement is regular updates.
- **Pricing is consumption based** and customer oriented — it lets you realistically test the product, scale your deployment to changing conditions, and otherwise flexibly manage your costs.
- **It is as easy to manage** one site as it is to manage thousands.
- **Capacity management**, system management, and software upgrades are not part of your workload.
- **Scaling up and down** to your day-to-day organizational requirements is automatic.
- And particularly for a data protection service, make sure your organization is getting a cloud data protection solution that includes **core security and regulatory certifications.**

BUILDGROUP

"My favorite thing about the Druva solution is the simplicity. I love the single pane of glass approach; it's easy to get what you need.

Read case study

#6 | Simplified pricing and lower costs

There was a time when only an electrician knew how to properly wire even a simple circuit. And only the electrician would get the hefty discount at the electrical supply wholesaler. Today, the switch itself is simplified for DIYers and the cost is a fraction of what you'd pay a contractor.

Modern cloud apps are no different. Old architectures have been replaced with comparatively simple solutions. Deployment involves little more than connecting to the internet. And the price? Again, a fraction of what you'd pay for a legacy app that didn't work half as well.

When you're shopping for a cloud data protection solution, follow these guidelines:

- **Buy it from a marketplace** (such as Amazon Marketplace). If you want to buy it from a traditional seller, just make sure you're being charged a competitive price.
- **Know exactly what you're paying for,** ideally a single price based on simple metrics: data stored, users protected, etc.
- **Look for a history of price reductions.** If the cost of cloud resources drops, you should reap some of the benefits.
- **Understand your licensing:** per user, per site, per volume.
- **Bottom line, times have changed,** and you don't have to put up with either retrofitted apps or retrofitted purchase processes.

NORTHGATE MARKET

"When I added up initial and ongoing costs, I discovered that we saved over 60%. Druva was a bargain. On top of being the best-performing, all-in-one, cloud-native solution by far.

Read case study

#7 | Linear and infinite scalability

With a well-architected cloud application, linear scalability nearly always means, in practical terms, infinite scalability. Linear scalability simply means that the same application can provide the same benefits regardless of how demand fluctuates. With a cloud application built on a cloud service provider's virtually infinite capacity, both processing and storage resources can be automatically added and subtracted. Need more GPUs to process an AI model? Additional VMs can be allocated in seconds. Need more backup capacity? The sky's the limit.

Bottom line, the time and effort of managing N amount of business is the same as managing 100N the amount of business. You simply pay more when the need increases and less when it decreases.

On the other hand, a traditional non-linear application that works within the confines of on-premises infrastructure requires exacting capacity planning. If you're subject to infrequent load bursts in business, you have to provision accordingly. If resources aren't used to capacity, there's wasted infrastructure. If resources are taxed beyond capacity, you lose business.

A true cloud-native data protection solution automatically scales up and down to meet your needs. It is easy to deploy, run, and scale, so you can focus on delivering value to the business.

SG360°

> **"Druva grows with you. We no longer have to worry about making room for more data. We'll always have the space we need.**

Read case study

#8 | Network optimization

Data sprawl is a simple fact of life for modern enterprise networks. Critically important enterprise data is stored in the cloud, on endpoints, and in data centers. Thanks to the cloud, it's all connected. But to function efficiently, cloud resources need to be managed in terms of deduplication and bandwidth management.

- **Data deduplication** changes the economics of data storage and management and is a critical component for any organization's cloud strategy. However, just how much efficiency is achieved depends on the type of deduplication implemented. Global deduplication delivers network efficiencies with a single dedupe index that ensures one copy of data is stored across all global backups. Source deduplication is completed at the very beginning of the backup process. The advantage of source dedupe is that it reduces network traffic as well as storage requirements.
- **Bandwidth management** entails routing traffic to and from the cloud while maintaining high performance and protection simultaneously — for all users wherever they're located, whether they're IT staff in the server room or salespeople doing business from a coffee shop. With a good SaaS application, this occurs transparently to the user. The application uses the bandwidth it needs until a higher priority needs it.

"Before Druva, we had always paid for more backup capacity than we used. Now, we get billed on what we're actually using, and we don't have to manage any hardware. Druva's built-in global deduplication, which is delivering a 10.5X reduction in storage for our hybrid cloud data, helps us reduce TCO.

Read case study

#9 | Data portability and disaster recovery

Any number of natural and man-made events can threaten business-critical data, from floods and earthquakes to cyberattacks and terrorist acts. To cope, most enterprises have implemented elaborate disaster recovery (DR) infrastructure and strategies to ensure that their organization's data is untouched and their processes are back online quickly.

However, cloud applications have completely changed the context of efficient DR. Enterprise-owned bunkers full of NAS servers are obsolete, as are most pre-cloud methods for protecting business-critical data.

The cloud also greatly enables data portability. When personal data was confined to a company's local server, perhaps processed with a local, proprietary program, consumers had no knowledge or control over it. With the cloud, that data can now be stored exactly where it belongs and be accessible only by those who are properly authorized. And the software that's processing the data is likely a customized, open-source solution hosted in a regional data center or wherever regulations dictate.

The enormous impact of cloud applications on data portability and DR include:

- **Elimination of infrastructure** capital expenditures (CapEx) and management overhead.
- **Adherence** to the strictest security protocols.
- **Worldwide geographical reach** with elastic scaling.
- **Merging data protection**, management, and analytics with DR.
- **Consumption-based pricing.**

LANGDALE INDUSTRIES, INC.

"We implemented Druva inSync and not only did we enable a robust DR plan and backup strategy for all endpoints, but it also gave us ransomware protection all in one.

Read case study

#10 | APIs that enable a healthy partner ecosystem

The cloud was enabled by standardized communication protocols, from the 1822 protocol used for ARPANET to IP/TCP and HTTP. This standardization in protocols and the development of REST APIs means that an enormous number of services can integrate with each other. In other words, it's the nature of the cloud to let multiple vendors work together and complement each other to provide enormously productive partner ecosystems.

For example, a legacy on-premises backup tool automatically moves data from servers and endpoints to storage appliances. That's what it was bought to do, that's what it does, and that's all it does. It's not designed to let other companies penetrate your firewall to interact with it. On the other hand, a cloud data protection solution can use the cloud for the express purpose of securely interacting with partners. It stores data using one or more cloud service providers. It works with identity and access management (IAM) services to apply policies and technologies that make sure only the right, credentialed people are interacting with enterprise data and other resources.

By its very design, cloud data protection can provide the backbone of a company's disaster recovery (DR) strategy. Litigation support software is another critically important component of the data protection partner ecosystem. eDiscovery requires preserving content and metadata, author and recipient information, and other important file properties. It's hard work, but it's infinitely easier when it can use a pre-built integration to access an enterprise's cloud data protection solution.

MANCHESTER 1824
The University of Manchester

> **"Druva Phoenix facilitated our migration to VMware Cloud on AWS, and it allows us to use more AWS services so that our IT department can expand the services it delivers to our customers. Druva also does all the hard work on the backend, like migrating our data to different tiers of storage, which we don't have to worry about. We simply copy our data to Druva and know it's protected.**

Read case study

Next steps

We've listed what we think are the most important considerations when evaluating a cloud data protection solution. If you're looking for data protection and management, Druva is a premier example of how a cloud-native data protection solution can help your organization reduce cost and complexity, increase cyber resilience, maintain compliance, and accelerate and protect cloud projects:

- **Reliability and availability** — Committed to well defined SLAs for resiliency and availability of your data without any compromise.
- **Zero trust security** — All data is encrypted in transit and at rest. Enables identity and access management, RBAC, and audit trails.
- **Compliance and privacy** — More than a decade of FedRAMP, HIPAA, and SOC 2 certifications.
- **Data localization and multi-regional support** — Thorough understanding of, and strict adherence to, all local and country data protection regulations.
- **Radical simplicity** — Eliminates capacity management, system management, and software upgrades.
- **Linear and infinite scaling** — Managing 100 TB of data is no different than managing 1 PB.
- **Simplified pricing and lower costs** — Ease of purchase, license transparency, and predictability of costs.
- **Network optimization** — Well architected for global deduplication and active bandwidth management.
- **Data portability and disaster recovery** — Recovers data anywhere when a regional disaster occurs; supports failing over to other regions without any manual steps.
- **APIs that enable a healthy partner ecosystem** — Easily integrates with other SaaS solutions and enables on-demand disaster recovery.

To get started, visit druva.com

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

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 by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.

Q421-20208