Cloud Data Protection (CDP) Blog Series

#1

Why Enterprises are Turning to the Cloud for Data Protection and Management

This is the first in a six-part series of Druva blogs that discuss how a cloud-native approach to data protection and management enables less complexity, greater capabilities, and lower overall costs. Upcoming blogs will cover the basics of cloud data protection architectures, how the cloud minimizes data risks and malware, as well as specific ways the cloud enables lower infrastructure and operating expenses.

Many organizations are struggling to scale outdated tape-based backups and redundant capacity as the amount of data that needs to be protected skyrockets.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 data protection and management as well as virtually all modern enterprise business processes, they're turning to the cloud.

According to a recent survey by Cap Gemini, 15% of new enterprise applications are cloud-native today and this will jump to 32% by 2020.[1] If you add hybrid and cloud-enabled applications, the number is much greater, and according to a survey of 2,000 IT managers from Intel Security, 80% of enterprises have a cloud-first policy in place[2]. Why is the cloud so attractive? What makes a cloud-native app such an improvement over on-premises solutions for data protection and management?

Using cloud computing to protect and manage data makes sense on many levels. With software as a service (SaaS), a data protection app runs on the SaaS application's platform rather than on an enterprise's on-premises infrastructure. A SaaS data protection and management solution like Druva leverages all the inherent strengths of cloud computing:

- Savings — It can reduce operational costs up to 90% and deliver up to 50%+ TCO savings while reducing data center footprint.
- Scalability — With virtually infinite storage resources, the solution can scale on demand into the multi-petabyte range.
- Security — Cloud-native storage architecture and encryption design isolates data and complies with the strictest certifications such as HIPAA, SOC-2, FIPS, and FedRAMP.

[1] https://www.capgemini.com/service/cloud-native/

[2] https://www.mcafee.com/us/solutions/lp/cloud-security-report.html

- Simplicity — Automated policy management and a unified data model breaks silos and makes administration easy with no hardware, software, or patching/upgrading overhead.

With these kinds of benefits, it’s easy to see why the cloud is the first place to look for powerful and cost-efficient solutions.

Druva is the only SaaS data protection app built on AWS. It offers unique, consumption-based pricing as it protects enterprise data across endpoints and cloud workloads including virtualized/hybrid data centers deploying VMware, Hyper-V, and VMware on AWS.

Unique Druva global deduplication capabilities can reduce storage footprints by 60%, and Druva transforms backup data into an asset, enabling enhanced data governance for compliance, archival, and eDiscovery as well as business intelligence apps for insights and machine learning.

Watch for the next blog in this series!

For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.

#2

Deployment Options for Your Cloud Data Protection

In the first installment of this six-part series of Druva blogs, we discussed "Why Enterprises are Turning to the Cloud for Data Protection and Management" and the savings, scalability, security, and simplicity inherent to cloud-native solutions. Here, in our second blog of the Cloud Data Protection series, we review the different architectures you may encounter as you look at data protection offerings.

Moving essential business processes like data protection to the cloud is, according to Gartner, inevitable. Indeed, they assert that "By 2020, anything other than a cloud-only strategy for new IT initiatives will require justification at more than 30% of large-enterprise organizations.[3]" And because the cloud is so flexible, in addition to an all-in, cloud-only strategy, you can configure cloud data protection in a number of ways to meet your enterprise's unique needs.

The most popular setups for enterprise data protection are:

- **Hybrid cloud —** This configuration uses on-premises infrastructure and software for recent backups and the cloud for long-term archiving. The typical difference between this and a fully on-premises approach is that instead of generating tape or disk archives and storing them in on- or offsite facilities, backup data is replicated in the cloud. The internal IT group is responsible for managing and performing all data protection tasks. The group is also responsible for setting up disaster recovery and data management (in terms of enabling analytics/eDiscovery) systems.

  This approach offers greater internal control over configuring and executing the data protection workload. And for any company, there's an advantage from the convenience and cost-savings of cloud archives. The downsides are increased IT overhead and the physical and security risks inherent to on-premises backup infrastructure.

- **Cloud enabled —** This approach simply moves traditional on-premises apps and storage to the cloud. Companies gain the security and availability benefits of eliminating some on-premises infrastructure. IT overhead costs and whatever features are offered by the backup app are the same as with an on-premises or hybrid solution.

- **Cloud-native —** A cloud-native approach is built from the ground up to leverage the full benefits of cloud computing. Technically, this means the app is a microservice packaged in containers and managed on cloud infrastructure. In practical terms, cloud data protection is optimized for performance and scalability. With this approach, data can be

[3] Gartner, Cloud Strategy Leadership

unified from all enterprise data sources so that beyond enabling backups, it is available for analytics, eDiscovery, and other uses.

However you choose to deploy your data protection solution, Druva is a flexible, cloud-native solution that works with both hybrid and cloud-only architectures. Druva offers cloud backup and disaster recovery across endpoints, data center, and cloud workloads — without requiring any dedicated hardware, software, or skilled resources. And Druva Cloud Platform is built on AWS, making it secure, infinitely scalable, and globally accessible.

If you missed our previous blog, check out Why Enterprises are Turning to the Cloud for Data Protection and Management. Stay tuned for the next installment in our series!

For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.

#3

How Metadata Minimizes Your Data Risks in the Cloud

Previous blogs in this six-part series covered the savings, scalability, security, and simplicity inherent to cloud-native solutions and different data-protection architectures commonly found in today's fast-changing cloud environment. This blog looks at how rich metadata can make cloud-native data protection apps particularly effective.

With cloud data protection and management, a SaaS provider can collect and consolidate data from all an enterprise's sources. These typically include file servers, virtual machines, mobile endpoints, and cloud workloads from SaaS apps like Office 365 and PaaS apps like Oracle. But it's not just about the data. In addition to native file metadata, the app can create its own metadata, such as time-indexing, for each file, and maintain a "master" metadata database in the cloud.

On the other hand, the lack of metadata equals unstructured data, possibly quite valuable but difficult to manage. And according to Forbes, "Nearly 80% of enterprises have very little visibility into what's happening across their unstructured data."

Rich metadata enables a number of significant capabilities that enhance your data protection solution.

- Ransom- and other malware is a major risk to enterprise data. Cloud data centers are air-gapped to prevent infection from enterprise networks, and with pristine backups that include time-indexed metadata, a data protection app can make recovery fast and easy — eliminating any temptation to pay a ransom.
- Backups may need to be stored in different cloud data centers. For example, government data may need to reside in a FedRamp-authorized facility and other data may have residency restrictions to meet GDPR and eDiscovery requirements. Metadata can help guide where data is stored.
- Time-indexing also enables leveraging tiered storage pricing. Recent data can be stored in the highest-availability tier, and as it ages, it can automatically move to less-expensive lower-availability tiers.
- Rich metadata unlocks the value of enterprise data. It enables faster and more comprehensive analytics to gain critical insights, uncover opportunities, and expedite decision making.
- Corporate users typically keep identical copies of the same data, with the same files duplicated on hundreds and sometimes thousands of endpoints worldwide. Using rich metadata for global deduplication ensures that only one copy is backed up, reducing

data volume up to 80%. An added benefit is significantly reducing bandwidth usage during backups, lessening any impact on users.

Apart from extending metadata, a data protection app such as Druva can also automatically perform full-text indexing to speed eDiscovery and improve compliance and governance. Druva is a flexible, cloud-native solution that offers cloud backup and disaster recovery across endpoints, data center, and cloud workloads — without requiring any dedicated hardware, software, or skilled resources. And Druva Cloud Platform is built on AWS, making it secure, infinitely scalable, and globally accessible.

Check out blogs #1 and #2 in this series: Why Enterprises are Turning to the Cloud for Data Protection and Management and Deployment Options for Your Cloud Data Protection. Our next one will post soon.

For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.

#4

Stay a Step Ahead of Malware with Cloud Data Protection

Our six-part Cloud Data Protection blog series goes over some of the inherent benefits of the cloud in general and cloud-native data protection and management specifically. One not-so-obvious benefit for CIOs and IT managers like you is that with dialed-in cloud backups and rich metadata (our last blog was How Metadata Minimizes Your Data Risks in the Cloud), there's built-in insurance against ransomware and other threats.

Firewalls, physical security, software, and educated end-users all help you protect your enterprise network from malware. This layered, "defense-in-depth" approach, when done right, reduces vulnerability to the never-ending stream of ransomware, viruses, bots, and other threats lurking in email messages and the web. But sooner or later, hackers will compromise some of your data. In fact, according to Symantec's 2019 Internet Security Threat Report, enterprise infections were up by 12 percent in 2018.

That's why your IT group is so focused on backups. Backups hosted by a cloud service provider (CSP) are virtually impervious to any infection that's in your enterprise network. If you can identify and restore a pristine (before malware) version of your data from the CSP, you've minimized a tremendous amount of risk. However, the identification and restoration part is important, and how a SaaS data protection solution time-indexes its metadata is what can make the difference between a devastating attack and an annoying delay.

Shared security responsibilities

The reason you can worry less about a CSP is because they undergo significant security audits and generally must meet far more stringent requirements than the average business data center. They typically invoke a shared security model that splits responsibilities logically. For example, AWS takes responsibility for protecting the hardware, software, networking, and facilities that run AWS Cloud Services. They automatically encrypt all traffic on the AWS global and regional networks between AWS secured facilities. The SaaS vendor deals with what's between them and AWS, and you are then responsible for configuring the solution for your internal security controls such as who at your company has access to it.

A built-in early warning system

A malware attack typically starts to rename, delete, or encrypt files en masse. Constantly monitoring the company's data systems manually for such threats is not cost-effective. Yet in the process of backing up data to the cloud, a SaaS data protection solution automatically monitors file status and can detect odd changes (anomalies). It can then alert IT to help minimize losses. Not all cloud solutions do this, but those that do add tremendous value.

Druva is a SaaS data protection solution built on AWS that ensures all proper security controls are handled with regard to its interaction with the AWS cloud. In addition, it detects subtle data anomalies, the first warning signs of malware. Druva is a flexible, cloud-native app that offers cloud backup and disaster recovery across endpoints, data center, and cloud workloads — without requiring any dedicated hardware, software, or skilled resources.

Check out our previous blogs in this series:

- Why Enterprises are Turning to the Cloud for Data Protection and Management
- Deployment Options for Your Cloud Data Protection.
- How Metadata Minimizes Your Data Risks in the Cloud

And look for our next one, coming soon!

For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.

#5

How the Cloud Can Lower Your Data Protection Costs

Our most recent Cloud Data Protection blogs covered some of the functional benefits of moving to the cloud, particularly concerning data risks and malware threats. Combining the security capabilities of first-tier cloud service providers with a sophisticated cloud-native SaaS app minimizes attack vectors as well as speeds recovery times. But there's another benefit everyone will understand: lower costs. This blog shows how.

It's fairly simple: cloud data protection can save your enterprise a lot of money. Here are a few of the ways:

Eliminating on-premises infrastructure and IT overhead is big. Really big.

To accurately calculate the costs of using and maintaining an IT investment over time (TCO), you have to combine both direct and indirect expenses. Hardware, software, operations, and administration costs are usually easier to quantify, you know exactly how much you paid for infrastructure and you can track IT time spent on various tasks. But figuring out indirect costs is trickier. Research suggests that initial hardware investments typically represent a fraction of their TCO. To see why, visit a TCO calculator if only to see all the costs you may not have thought of. The missing percentage is all the technical support, maintenance, and other labor costs over time.

Mitigating ransomware with cloud-native backups can save millions

Every year, enterprises worldwide lose billions of dollars worth of data and lost productivity to ransomware. According to a recent report by Aberdeen Research, a company with 1,000 workers, each with a laptop, handling collectively 10TB of data, is likely to lose nearly $500K from a successful ransomware attack. And there's a 10% chance it'll lose more than $2.5M.

However, after setting up a cloud backup and restore solution, the likely loss goes down to about $54K. And the loss from a 10% worst-case attack goes down to $200K. That means a solution that lets you easily back-up all your enterprise data in the cloud, and restore it quickly, can reduce the impact of a ransomware attack by more than 90%.

There's also a hidden benefit to automatically backing up data to the cloud. A comprehensive process requires monitoring virtually all of an enterprise's data files. This means a solution can detect odd changes (anomalies) such as mass renaming, deleting, and encrypting that are warning signs of a malware attack. It can then alert IT to help minimize losses.

Not all your data needs four-nines availability

You have enterprise data that you simply can't do without and if it's lost for any reason, you need it restored immediately. You also have data, such as archived legal content for eDiscovery, that you must have access to but not necessarily right away. Because cloud storage offers different pricing for different availability, there's no reason to store both types of data in the same place. Furthermore, you frequently access some data and you infrequently access other content. Again, cloud storage offers different pricing for different access rates and you can store your data appropriately.

A SaaS data protection solution can automatically sort hot (frequently accessed requiring high availability), warm (less-frequently accessed data), and cold (rarely accessed data requiring low availability) data and store it where it belongs, significantly reducing costs.

Druva maximizes your savings in several ways, including pay-as-you-go pricing, anomaly detection to minimize ransomware losses, and automatic storage tiering to optimize service-provider fees. It is a flexible, cloud-native solution that offers cloud backup and disaster recovery across endpoints, data center, and cloud workloads — without requiring any dedicated hardware, software, or skilled resources. And Druva Cloud Platform is built on AWS, making it secure, infinitely scalable, and globally accessible.

Our previous blogs in this series include:

- Why Enterprises are Turning to the Cloud for Data Protection and Management
- Deployment Options for Your Cloud Data Protection.
- How Metadata Minimizes Your Data Risks in the Cloud
- Stay a Step Ahead of Malware with Cloud Data Protection

The last one will be up soon, it will discuss how a cloud data protection platform can enable big data analytics and enhance eDiscovery and compliance.

For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.

#6

How Your Cloud Data Protection Can Enable Big Data Analytics and Enhance Compliance

Our Cloud Data Protection blog series has ranged from the scalability, security, and simplicity inherent to cloud-native solutions to malware protection and lowering costs. We also discussed the power of rich metadata applied to otherwise unstructured content. This power is particularly beneficial when it comes to leveraging a data protection solution for something seemingly unrelated: big data analytics. That, and improving eDiscovery and compliance, are the subjects of this last blog in our series.

Without question, data is at the core of digital transformation. It's the raw material for analytics that provide critical insights to uncover opportunities and expedite decision making. Indeed, ZDnet reported that digital transformation spending will approach $2 trillion by 2022. This is often overlooked as one of the prime benefits of cloud data protection — its potential to simultaneously transform your backup information into a rich store of big data for analytics and other applications.

How does an effective, cloud-native data protection application do this? First, it accesses all of your enterprise data across endpoint, data center, and cloud workloads. Second, it collects it into one copy using a unified data model. Third, it provides immediate accessibility for any authorized user. The only difference between restoring lost data and providing raw data for analytics software is who or what program receives it. For that matter, there's no reason a sophisticated cloud data protection app can't add customized metadata to better enable analytics software.

Legal holds, eDiscovery, and compliance

When an enterprise gets involved in legal action, they have to keep any and all data connected to the legal action safe and accessible. That's much easier said than done. It means using a policy-based approach to categorizing and tagging all electronic communications — including e-mail, instant messages, and web transactions. Adding to the challenge, this data can live anywhere in the enterprise network or cloud, on an employee smartphone or hosted by a SaaS app. If an enterprise can't produce needed data, spoliation sanctions can be harsh.

The essence of the legal hold challenge is ensuring that all relevant data is identified, safe, and accessible for eDiscovery. Cloud data protection is uniquely appropriate. The right app can add metadata to identify all enterprise files, indicating not only time data but legal hold applicability.

Cloud storage is virtually always more secure than on-premises infrastructure, with all major cloud service providers offering at least 10-nines durability. Legal hold data must often reside in specific geographic regions. However, for eDiscovery in the public cloud, if there's an internet connection and secure credentials, there's access.

The exact same capabilities that make the cloud appropriate for legal hold and eDiscovery challenges apply for compliance requirements as well. With secure cloud data that is readily searchable and always accessible, governance and regulatory compliance is far simpler.

In the process of providing optimized data protection, cloud-native Druva adds rich metadata to enterprise data. This make data more quickly accessible for backups, eDiscovery, and compliance, and also prepares it for faster processing by big data analytics apps. Druva is a flexible, cloud-native solution that offers cloud backup and disaster recovery across endpoints, data center, and cloud workloads — without requiring any dedicated hardware, software, or skilled resources. And Druva Cloud Platform is built on AWS, making it secure, infinitely scalable, and globally accessible.

This six-part Cloud Data Protection blog series includes:

- Why Enterprises are Turning to the Cloud for Data Protection and Management
- Deployment Options for Your Cloud Data Protection.
- How Metadata Minimizes Your Data Risks in the Cloud
- Stay a Step Ahead of Malware with Cloud Data Protection
- How the Cloud Can Lower Your Data Protection Costs

We hope you've enjoyed them! For more detail about why the cloud is the place for enterprise data protection and management, download the Cloud Data Protection for Dummies book and our CIO's Guide to Cloud-first Data Protection.