# Contents

## Public Cloud as a New Backup Target
- Pay-As-You-Go Pricing 3
- No Media Management 3
- Instant Data Access 3

## Challenges with Public Cloud Infrastructure
- Challenge 1: Infrastructure Complexity 3
- Challenge 2: Minimizing Cost 4
- Challenge 3: Recovery Times (RTO) 4
- Challenge 4: Security 4

## Introducing Cloud DVX
- Automated Infrastructure Management 5
- Network Infrastructure 5
- Compute Infrastructure 6
- Monitoring Infrastructure 6
- Infrastructure Cost Optimization 6
  - Global Deduplication and Compression 6
  - Forever-Incremental Backup 6
  - Built-in VPN 6
  - Continuous Cloud Infrastructure Cost Optimization 7
- Fast Restore Time 7
  - Dedupe-aware Restore 7
  - Granular Restore 7
  - Direct to Host 7
- Security 7
  - AWS Best Practice 7
  - Minimum On-prem Network Requirements 8
  - End-to-End Encryption 8

## Summary 8
Public Cloud as a New Backup Target
Dedicated tape or disk-based backup and archival systems have traditionally been a key part of enterprise data protection strategies. However, many companies have found the cost and effort around system setup, purchasing, and managing backup media and software to be too burdensome.

Recently, systems built on public cloud object storage services have become an attractive alternative for long-term, offsite data retention use cases. There are three key advantages that public cloud-based systems offer over traditional tape or disk-based backup and archive products.

Pay-As-You-Go Pricing
Unlike disk or tape systems that need long-term sizing forecasts and upfront CAPEX, public clouds offer pay-per-use pricing and enabling scaling to massive levels on demand.

No Media Management
Unlike disk or tape systems, where the media has to be refreshed every few years due to support expiry or media degradation, public clouds free up end-users from risky, costly, and time-consuming media management.

Instant Data Access
Unlike alternative media options, especially tapes, which can take days to make data accessible, data in the public cloud is accessible within a few minutes to hours, greatly accelerating data recovery time. This enhanced data accessibility also enables new use cases where companies can run analytics on large amounts of data in the public cloud for business profit.

However, using public cloud brings its own set of challenges around the expertise required to operate public cloud resources, cost, and security. We will review these challenges in more detail next.

Challenges with Public Cloud Infrastructure
There are numerous backup and archive solutions that leverage public cloud infrastructure. Most of these offerings write directly to object storage services, while a few have ported their software to run on public cloud infrastructure. However, none of these solutions comprehensively address the challenges that come with using public cloud infrastructure.

Let’s review each of these challenges one by one.

Challenge 1: Infrastructure Complexity
Public clouds offer a wide variety of infrastructure services around compute, security, storage, and networking. Operating these infrastructure services at an enterprise-grade level requires deep expertise. Public cloud vendors such as Amazon offer certification programs for developing such expertise; these programs require a significant investment in time and effort. Existing cloud-based backup and archive solutions require customers to develop this expertise to some degree. They leave cloud infrastructure monitoring, availability, and recovery to end-users. These solutions create new problems specific to operating in public cloud environments and ultimately don’t simplify the management burden for customers. Customers expect a service-based consumption model for public cloud-based offerings, and existing solutions don’t meet this requirement.
Challenge 2: Minimizing Cost

In the public cloud, nothing is free. Every cloud infrastructure usage needs to be scrutinized to ensure that service usage is cost-optimized; failure to do so inevitably leads to cost overruns and surprises. For example, we found that some HCI vendors’ solutions recommend setting up VPN connection/gateway to the public cloud. Such a requirement has enormous consequences on the total cost of ownership because charges for VPN cloud infrastructure services typically apply to both ingress and egress bandwidth consumed. Besides storage costs for backup data, customers will end up paying for ingress bandwidth consumed. Also, none of the legacy HCI or backup-only vendors offer end-to-end global data reduction in transit from on premises to the cloud and at-rest in the public cloud. That’s extremely important because backup economics depend heavily on reducing the large amount of backup data in the cloud to the absolute minimum. As data sizes approach typical backup and archival capacities, the cost of public cloud storage heavily outweighs other associated costs. Cost is more of an issue with HCI Backup vendors because they add another appliance to the cost footprint of on-premises infrastructure. Also, because they write to S3 directly without a process in cloud coordinating the backup data, they require regular full backups of data for every few incremental backups. That increases the total capacity required and significantly increases cloud costs. Customers expect backup solutions to minimize the cost of operating in the public cloud.

Challenge 3: Recovery Times (RTO)

One of the primary reasons for backup and archival is to ensure timely data recoverability in an unexpected event. However, the lack of global data reduction and forever-incremental backups to public cloud leads to long data copy times back from the public cloud, and the RTO suffers. Most primary storage and HCI systems have datastore or LUN level recoverability, which is a lot of data to transfer when a VM or virtual disk recovery would suffice. HCI backup vendors do a nice job of enabling in-guest file recoverability. But, recovery requires a full copy of data from cloud to HCI backup system, and then to the primary system. Combined with the need for regular full backups, synthesizing full backups from incremental backups, and hydrated copy to primary, the RTO can be very high.

Challenge 4: Security

In the public cloud, security is a shared responsibility between the service provider and customers. The service provider’s responsibility is to secure compute, storage, and network infrastructure services from their physical data center facilities to endpoints that serve as interfaces for operating these services. When using these infrastructure services directly, customers are responsible for securing their applications, operating systems, network, firewall, user identity, and access management. Public cloud vendors publish detailed best practices documents to guide customers. Applying these recommendations and keeping all configurations and patches up to date is a full-time job on its own. Customers expect cloud backup solutions to implement a service provider’s security best practices and keep all the infrastructure, application, and operating systems updated and secure.
Introducing Cloud DVX

Datrium Cloud DVX delivers the same unmatched, always-on data reduction (global dedupe and compression) efficiencies and scaling flexibility of on-prem DVX. At the same time, we’ve designed the service from the ground up to fully address challenges around cloud infrastructure operation complexity, cost, and security.

The following will review each of these challenges in more detail.

Automated Infrastructure Management

Setting up Cloud DVX in AWS is as simple as pairing another on-prem DVX replication target. Just select the AWS region, and click finish. Within a few minutes, Cloud DVX is provisioned automatically, and customers can start replicating backups to AWS immediately. Once deployed, the automated Cloud DVX management software continuously monitors relevant AWS infrastructure and automatically detects & repairs any failure (e.g. EC2 instance termination due to hardware fault or maintenance).

Next, let’s have a behind-the-scenes look at how we’ve automated provisioning, monitoring, self-healing, and upgrade functions. The automation software responsible for provisioning, monitoring, self-healing, and upgrades manages the following AWS infrastructure components used by Cloud DVX.

Network Infrastructure

- **Virtual Private Cloud (VPC):** Logically isolated section of AWS where Cloud DVX is hosted. We create a dedicated VPC instance to avoid any potential configuration conflicts from other services running in the customer’s AWS account. That makes problem detection, isolation, and repairs much more reliable because the automation software doesn’t need to account for conflicting configuration changes intended for other use cases. Any AWS component failure or deviation from target settings within this VPC are automatically repaired.
- **Subnet:** Subnet within VPC where Cloud DVX instance is deployed. This subnet is configured with a route table specifically tailored for Cloud DVX network access requirements. Unintentional changes or removal of this subnet are automatically detected and repaired.
- **Route Table:** A set of routing rules for the subnet where Cloud DVX is running. We configure this route table to ensure that backup data traffic to AWS S3 object service stays within AWS’s internal network. The automation software continuously monitors this route table and corrects any misconfiguration.
- **Endpoints:** Traffic to AWS services (such as S3) from within VPC are not automatically routed through Amazon’s internal network. Endpoints for specific services (such as S3) must be created and added to the route table to avoid egress to WAN. If any required endpoint is removed or misconfigured, the automation software corrects the problem automatically.
- **Internet Gateway:** Performs NAT for Cloud DVX and routes traffic from/to on-prem DVX system. Failure or removal of internet gateway is automatically detected and repaired.
- **Security Group:** Firewall rules tailored for Cloud DVX. We’ve locked down all ports except for a few inbound ports required for backup data replication and snapshot management. These rules are continuously monitored, and any misconfiguration is automatically repaired.
Compute Infrastructure

- **Cloud DVX EC2 Instance**: EC2 compute instance where Cloud DVX data path software runs. If the instance terminates due to hardware fault or scheduled maintenance by Amazon, the automation software detects the issue and automatically provisions a new instance with all the required configurations. The replication pairing with the on-prem system is automatically reestablished after the instance is repaired, and any previously running replication tasks are resumed.

- **Upgrades/AMI**: When a new version of Cloud DVX software becomes available, the automation software automatically detects and upgrades Cloud DVX. The timing of upgrades is managed by Datrium support staff on a per-customer basis. Usually, upgrades will be released during regularly scheduled maintenance windows, as published by Datrium Support.

Monitoring Infrastructure

- The **management automation software** runs as AWS Lambda functions independently from Cloud DVX AWS resources; failure or misconfiguration of Cloud DVX VPC components doesn’t affect the Cloud DVX monitoring and repair functions. AWS Lambda is a serverless infrastructure monitored and maintained by Amazon; it is designed to use replication and redundancy to provide high availability, and there are no maintenance windows or scheduled downtimes.

- Furthermore, **Datrium can update this automation software independently**. Enhancements to self-healing functions can be rolled out without any downtime for Cloud DVX. It also enables us to release software changes that optimize AWS infrastructure cost further as new AWS services become available.

- Also, **Datrium has a monitor running within the EC2 instance for further hardening**. Configuration changes can be quickly detected, and any AWS outage situations addressed.

Infrastructure Cost Optimization

On-premises and Cloud DVXs combine to deliver unmatched data efficiency with global deduplication and compression on-wire and at-rest. Only unique data is replicated from on-prem systems to Cloud DVX and back, optimizing bandwidth, storage capacity, and IO usage in AWS. Also, Cloud DVX software implements an enterprise-grade SSL VPN stack. That removes the need for a separate AWS VPN gateway service, significantly saving AWS cloud infrastructure costs and management burden.

Below is a review of each of these innovations in more detail.

**Global Deduplication and Compression**

Before sending the actual backup data to Cloud DVX, on-prem DVX prepares fingerprints of compressed backup data. Cloud DVX uses these fingerprints to determine what data has not been backed up already. On-prem systems send only the data that Cloud DVX has marked as new; old data is never sent again. So Cloud DVX never stores the same data twice in the S3 object store, even when they are from different on-prem DVX systems. Cost savings from global deduplication multiplies as more on-prem systems are backed up to a Cloud DVX instance. Backup data retrieval from Cloud DVX works the same way in reverse. Before retrieving any backup data, the on-prem system is first queried for missing data; only the missing data is actually retrieved from Cloud DVX, significantly reducing the cost of egress from AWS.

**Forever-Incremental Backup**

On-prem systems send only the incremental changes since the last backup. And these incremental changes are further deduplicated against existing data in Cloud DVX, as explained in the previous section. On-prem systems never send full copies of existing backup data again; only the incremental changes are transferred, minimizing the bandwidth and storage usage.

**Built-in VPN**

AWS cost for egress out to WAN is significant. For the backup use case, this cost is incurred only when restoring backup data from AWS. Data restoration is an infrequent operation, and Cloud DVX optimizes restoration by retrieving only the missing data. On the other hand, there is no AWS charge for ingress backup traffic. That is ideal for backup use cases because customers want to have policies that back up to Cloud DVX regularly at daily or even hourly frequency. However, if the backup data traffic is secured
through the use of AWS VPN gateway service, customers will be charged for both ingress and egress bandwidth consumption. Furthermore, setting up VPN gateways is another management burden customers don’t want. To address these issues, Cloud DVX implements an enterprise-grade SSL VPN in its software. The transport between on-prem systems and Cloud DVX is secured against man-in-the-middle attacks and uses the best cipher suite available.

**Continuous Cloud Infrastructure Cost Optimization**

Amazon regularly releases new services along with enhancements to existing services. Some of these updates may provide opportunities for cost optimizations when used effectively. Datrium engineering actively works on minimizing cloud infrastructure costs for customers while improving the availability and performance of Cloud DVX. Updates containing such optimizations are automatically applied to customers’ Cloud DVX systems. Datrium customers will see lower AWS infrastructure bills as Datrium engineering continues to optimize for cost as well as availability and performance.

**Fast Restore Time**

Cloud DVX reduces the amount of data that must be retrieved during restore by only pulling missing data from the cloud. Furthermore, because there is no intermediate backup system between Cloud DVX and on-prem DVX, retrieved data can be immediately used instead of having to go through a rehydration process. These optimizations result in recovery times that are many times faster compared to typical backup systems where backup data must traverse through a backup system before it lands on the primary storage system.

Let's review these advantages in detail.

**Dedupe-aware Restore**

The on-premise system is first queried for any existing data before backup data is retrieved from Cloud DVX. Only the missing data is retrieved from cloud DVX resulting in faster restore time. That also reduces the cost of retrieving backup data from the cloud, as described in the previous section.

**Granular Restore**

Cloud DVX further reduces the amount of data transferred by allowing end-customers to recover not just virtual machines (versus LUNs or Datastores) but also individual virtual disks, datastore-files (OVAs, ISOs), persistent container volumes and in-guest files (DVX Software v4.1). Customers can manage backup policies at the same object granularity. The metadata for these objects is persisted and indexed in a highly scalable search catalog. Users can quickly and easily search these catalogs for both on-prem and Cloud DVX systems from the same user interface.

**Direct to Host**

With a two-tier on-prem-to-cloud model enabled by on-premises DVX and Cloud DVX, data is recovered from the cloud straight to the host where it can be instantly used on the primary infrastructure. Unlike HCI backup vendors, they don’t need to wait for incremental backups to be applied first. That enables customers to start using the data as soon as retrieval from Cloud DVX finishes.

**Security**

Security is a major concern when using public clouds. Public cloud resources must be secured to prevent any unauthorized access. At the same time, customers must eliminate any possibility of security breach into on-prem data centers as a result of connecting to public cloud resources. Cloud DVX implements AWS’s best practices to secure its public cloud resources while eliminating any risky networking requirements for an on-prem data center.

**AWS Best Practice**

Cloud DVX is deployed in a logically isolated virtual private cloud in a private subnet with proper firewall rules to prevent any unauthorized access to its services. Backup services running in EC2 instances use regularly rotating credentials associated with an IAM profile created for Cloud DVX during setup; no user credentials are persisted anywhere in AWS. At the same time, all communications with AWS services are secured with SSL. Backup data is also encrypted at rest in S3.
Minimum On-prem Network Requirements
Cloud DVX doesn't require any inbound firewall ports to be opened for an on-prem data center. That minimizes the surface area that attackers can probe for vulnerabilities.

End-to-End Encryption
Cloud DVX implements an enterprise-grade SSL VPN. It’s secured against man-in-the-middle attack and allows only authorized on-prem DVX systems to connect to its backup services. Any unauthorized connection attempts are refused during the SSL handshake phase.

Summary
With Cloud DVX, using public cloud resources for long-term, off site retention of backup data is easier than ever before. With fully automated cloud infrastructure management, cost optimizations, fast restores, and end-to-end security in a single converged system, customers can realize dramatic total cost of ownership savings while meeting their RTO SLAs.