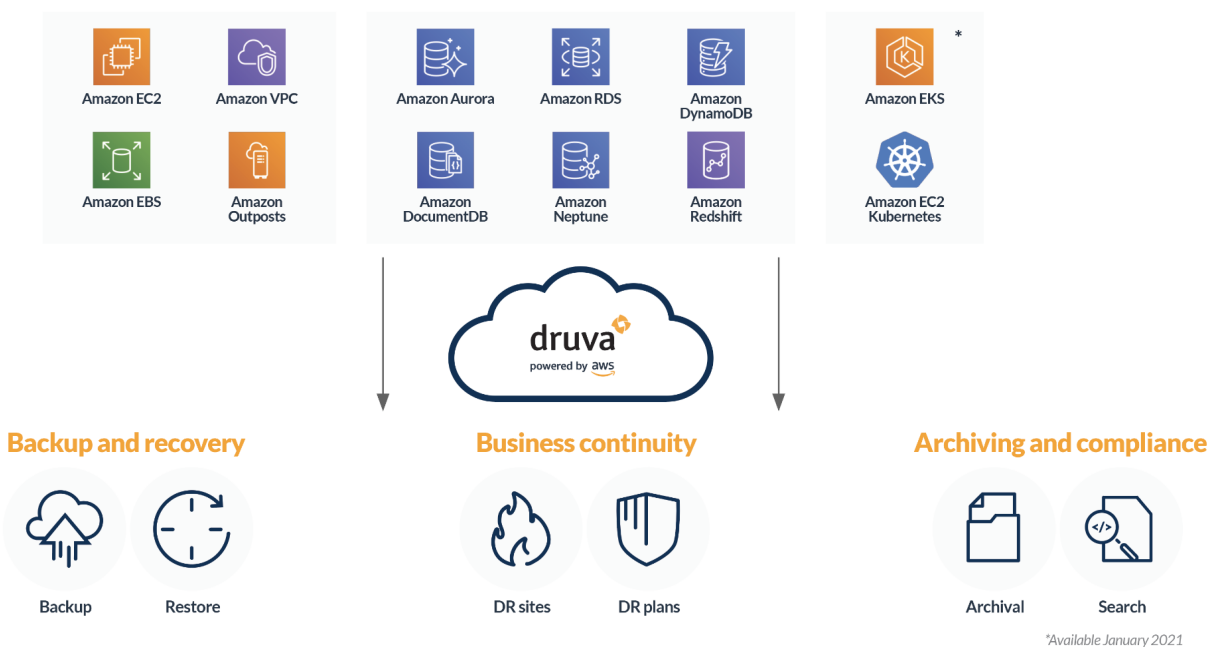# Druva CloudRanger

Protect your Amazon Web Services (AWS) data at scale with Druva CloudRanger — Druva delivers data protection and management for the cloud era. Built on AWS, Druva's cloud-native SaaS solution delivers globally accessible, infinitely scalable, and autonomous enterprise data resiliency.

Druva CloudRanger is an easy-to-use data protection and disaster recovery solution built for AWS workloads. Get enterprise-ready data protection for your AWS infrastructure with full data agility across AWS regions and accounts to ensure business continuity.

Enterprise-ready data protection for native AWS workloads

Amazon EC2	**Amazon VPC**
Amazon EBS	**Amazon Outposts**

Amazon Aurora	**Amazon RDS**	**Amazon DynamoDB**
Amazon DocumentDB	**Amazon Neptune**	**Amazon Redshift**

Amazon EKS *
Amazon EC2 Kubernetes

druva
powered by aws

Backup and recovery

Backup Restore

Business continuity

DR sites DR plans

Archiving and compliance

Archival Search

Available January 2021

Why Druva CloudRanger?

Globally accessible backup and disaster recovery

Get enterprise-ready backup and disaster recovery for your AWS infrastructure with global backup policies for data flexibility across AWS regions, accounts, and storage tiers to ensure business continuity and compliance.

Delivered "as-a-Service," built on AWS

Self-managed, SaaS data protection solution for AWS workloads, designed for infinite scale, security, and flexibility.

Optimize your AWS costs

Reduce storage costs by automatically archiving Amazon EBS snapshots to lower-cost Amazon S3 storage tiers. You can also implement resource scheduling for non-critical AWS workloads to reduce costs by up to 70 percent.

Supported AWS resources

AWS IaaS — Amazon EC2 | Amazon EBS | Amazon EKS

Simplify the day-to-day data protection of your cloud native AWS workloads and containerised applications running on AWS, to mitigate risk of your business critical infrastructure.

AWS databases — Amazon RDS | Amazon Aurora | Amazon DynamoDB | Amazon Redshift | Amazon Document DB | Amazon Neptune

Protect your data across a variety of AWS database services to keep your business information secure and readily available.

Cloud hosted databases — MySQL | PostgreSQL | Oracle | MS SQL Server | MariaDB | NoSQL

The most comprehensive backup and disaster recovery support for databases running on AWS cloud services.

Key features

AWS backup and recovery

- Global backup policies across AWS accounts
- Transition EBS snapshots to lower-cost S3 storage
- Cross-region and cross-account backup
- Instant, granular recovery at a file-level
- Full app protection of Kubernetes on AWS

AWS disaster recovery

- One-click disaster recovery
- Clone AWS environments with VPC mappings
- Automate DR plan testing
- DR compliance reporting
- Validate RTO and RPO requirements

Metadata-based file search

- Index snapshots for search
- Granular recovery of specific files
- Search file systems of snapshots
- Search across multiple AWS regions
- Find files within a specific time frame

Governance and compliance

- Data lifecycle management
- Data never leaves your cloud
- Role based access control (IAM)
- All AWS GovCloud regions supported
- Automated compliance reporting

Administration

- Multi-AWS account support
- RESTful API integration
- Integrates with 1,600+ applications
- SSO and MFA authentication

Use cases

AWS cloud backup and recovery

100% SaaS solution that leverages AWS snapshot technology to utilize native APIs and microservices for scalability, efficiency, and flexibility.

AWS cloud disaster recovery

One-click disaster recovery function, which allows organizations to clone VPCs along with associated configurations across AWS regions and AWS accounts to ensure successful failover.

Archiving and compliance

Transition EBS snapshots to S3 storage tiers for long term retention and schedule automated reports as part of monitoring and compliance with a fully available audit trail.

Risk management and ransomware

For extra protection against ransomware, copy your snapshots to another region or AWS account and schedule regular automated tests of disaster recovery plans.