druva

Fill the Gaps in Your AWS Data Protection Strategy

10 Must-Have Capabilities to Protect Against Data Loss and Cyber Threats

Introduction

Public cloud delivers many benefits – but when it comes to data protection, public cloud solutions are one-size-fits-all and can leave gaps. Public cloud is a great solution for many businesses. However, these cloud providers might not provide a comprehensive data protection solution to meet the needs of your organization. If you're using Amazon Web Services (AWS), keep in mind that the company adheres to the Shared Responsibility Model, which means that AWS handles infrastructure security and uptime, while you are responsible for protecting your data.

You can use the native AWS backup tool to make copies of your data with snapshots, but for business continuity, you should also create copies in additional different accounts or regions. For many organizations using this method, creating and managing backups can quickly become unmanageable and costly – that's why they look at third-party alternatives to help.

Snapshots will always be the foundation of any operational and disaster recovery plan for AWS resources, but they are far from a complete solution. **This eBook will help you address 10 gaps in your AWS data protection strategy, to minimize the risk of data loss.**

AWS recommends that multiple copies of backups should exist and they should be stored in isolated, offline locations.

druva

1. Simplified backup management at scale

Challenge

When you have multiple AWS accounts operating across different regions, it can be difficult to enforce consistent data protection policies across all of the accounts or monitor their backups. In addition, some applications, databases, and tools such as Kubernetes require more sophisticated data protection. While snapshots may be part of the overall backup system design, relying solely on snapshots might not allow you to meet your data recovery objectives.

Solution

Your data protection solution should provide a single management and reporting console to configure policies and monitor all AWS backups across your entire environment. With a single, comprehensive view into your backups, you are able to:

- **Allow data backup and restore** in seconds — across regions and accounts
- **View and manage** all snapshots and backup jobs in one place
- **Readily gain reporting information,** changes, and access to data

druva

2. Support for both cloud-native and lift-and-shift workloads

Challenge

Organizations moving to the cloud may have both cloud-native as well as lift-and-shift workloads that need protection. Many IT leaders find themselves using multiple tools and storage platforms to protect their lift-and-shift workloads and their cloud-native applications. Using multiple tools escalates costs, creates security challenges, and slows the pace of business innovation.

Solution

The ideal solution is easy to use and helps protect, store, and recover business-critical lift-and-shift workloads (like Oracle on EC2 and SQL on EC2) as well as cloud-native applications running on Amazon EC2, Amazon RDS, Amazon DynamoDB, and many more. **With the ability to manage both lift-and-shift and cloud-native workloads you gain a holistic view of your environment without having to use multiple applications.**

druva

3. Air-gapped backups to protect against ransomware

Challenge

The first line of defense against ransomware is to have a clean backup copy of your data. After creating backup copies, you need to protect your backup environment. Some organizations create cross-region or cross-account backup copies for data protection. But these backup copies are still not completely protected. If cyber criminals gain access to your AWS accounts, they can encrypt or delete your backup copies.

Solution

To protect against malware, backup data should be air-gapped (separated) from the original data set. For increased security, all copies of your stored data should be air-gapped from the original AWS production environment. Air-gapped backups ensure that ransomware attacking your primary environment will find no route between your protected resources and the encrypted, protected data copy.

druva

4. A single, integrated console for comprehensive visibility and reporting

Challenge

As enterprises scale up their AWS workloads across hundreds (sometime thousands) of AWS accounts, they are looking to centrally manage, and monitor, backups across multi-account AWS environments.

Organization-level view of data protection across AWS services is difficult to automate and consistently apply across all AWS accounts. Although it is possible to protect data using native AWS tools, it's not easy and requires a lot of manual effort.

Solution

A single, integrated console provides a comprehensive view and significantly reduces the manual effort your IT teams need to expend to assess and monitor the snapshots and backups for all your AWS accounts. You should be able to generate logs, and other reports from this console such as reports on backup policies, schedules, and disaster recovery plans across all your AWS accounts. The console should also log user and administrator activities to comply with data governance and compliance requirements.

druva

5. File-level recovery

Challenge

Recovering a single file is a basic task for any data protection software. However, that's not the case if you want to recover a file from an AWS snapshot. Recovery is tedious and cumbersome as you need to complete a series of steps before receiving the desired file. The effort doubles if you have to recover files from multiple volumes.

Solution

Your solution should go beyond the basic snapshot or AMI level recovery that's common in many solutions. It is important to ensure that you can navigate to a folder within Amazon EBS snapshots and retrieve or download the necessary files. This allows admins to recover files that may have been deleted or confirm whether a file exists for governance purposes.

druva

6. File-level search

Challenge

One of the downsides to backing up data as EBS snapshots is the complexity of search and retrieval of individual files. The ability to recover a single image or database file rather than an entire volume or instance is important, especially when you're simply trying to confirm a volume contains the files you wish to restore.

Solution

File-level search isn't the same as file-level recovery. Ideally, your data protection solution has both capabilities. A granular search option can be invaluable when you're recovering files that have been accidentally deleted or lost due to migration errors. You can use this functionality to recover files that may have been deleted or confirm whether a file exists, (for instance, as part of compliance and governance activities).

druva

7. Integrated disaster recovery plans

Challenge

A typical disaster recovery (DR) plan tries to ensure that data backups are isolated from their primary production environment to ensure business continuity. One of the biggest challenges with DR planning is the lack of adequate testing and verification. In this situation, you will have no idea as to whether or not you'll actually be able to recover from a disaster and whether your recovery time objectives (RTOs) and recovery point objectives (RPOs) are valid. Infrequent testing of backup environments puts businesses at substantial risk when outages eventually occur.

Solution

Automation is an important part of any disaster recovery solution. Features such as auto-discovery ensure that a set of policies are automatically applied as soon as you add a data source to your environment. Other features such as creating cross-region or cross-account customized disaster recovery plans based on the business SLAs, easy cloning of VPCs and their dependents such as subnets and security groups, and the ability to route tables from your source site to the target site are important for any disaster recovery solution.

Having integrated testing capabilities to validate your organization's RTO and RPO objectives through real-time execution is another important part of any disaster recovery solution. Based on the results of testing, you can increase the resource capacity or select a lower activity destination to reduce RTO and increase backup frequency to reduce the RPO.

druva

8. Strict authentication before permanent deletion

Challenge

Ponemon Institute's 2022 Cost of Insider Threats Global Report found that credential thefts have almost doubled since 2020. The same report showed that **56%** of incidents experienced by organizations were due to negligence. These findings raise a key question: If a malicious insider has full access to your cloud and backup environments, or if there's just an accidental data issue, how will you recover the data? If someone has full access to your cloud and is able to circumvent or verify the full multi-factor authentication (MFA) policies you've put in place, all it takes is a deliberate or accidental deletion to ruin your chances of recovery.

Solution

You need a solution that requires multiple people to verify and authenticate before any backup data is permanently deleted or archived. This will ensure that even if one person's credentials are compromised, your data won't be permanently deleted.

Additionally, you should make sure that any changes to settings for data deletion should follow the same process of multiple verification and authorization. This deletion prevention mechanism should be applied to all AWS accounts that you back up.

druva

9. A data lock feature to protect against insider threats

Challenge

Insider threats are serious and can result in the loss of vital data. Insiders know how to get to the most important files, so they're motivated by financial gain or revenge. To protect yourself from insider attacks, you need to understand bad actors' personas and enhance ways to restrict them from abusing data access privileges which include tampering with snapshot retention rules or unauthorized deletion.

Solution

To protect your backup copies, your solution should provide immutability, meaning that retention on your backups are locked and cannot be changed. A data lock feature works in close conjunction with the deletion prevention feature. Look for an option in the backup policy to define the retention period of the backed up data. Once defined, the backup tool should prevent anyone from modifying or deleting these settings. To make changes in this policy should require multiple people to verify and authenticate their identity before changes are rolled out.

druva

10. Recovery for deleted files and folders

Challenge

EBS snapshots are a point-in-time copy of your data. As easy as it is to create an EBS snapshot, it is equally easy to delete a snapshot by accident or by malicious intent. Whatever the cause of the deletion, you need an easy way to recover deleted snapshots.

Solution

Your solution should have a local cache (something like a recycle bin) that allows for the recovery of any data intentionally or unintentionally deleted. Keep in mind:

- **Any data deleted in the error should end up in the cache** and stay there for a pre-defined number of days before being permanently removed.
- **The data should be auto-deleted permanently** only after the time limit expires.
- **Once the retention period is set,** it should not be possible to alter it.

In the case of credential misuse where a bad actor may maliciously delete backup snapshots, the administrator should be able to roll back actions made by an individual to quickly recover deleted data. This provides the administrator with the ability to revert malicious or unintended actions without data loss and enables rapid restoration of productivity.

druva

Fill the AWS data protection gaps with Druva

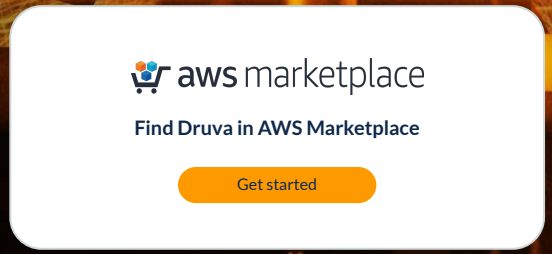
Druva's SaaS-based data protection solution gives you the enterprise-grade capabilities you need to protect your AWS data, and reduce risk. Druva harnesses and builds on the native technologies and global reach of AWS with these additional enterprise-scale benefits:

- **Complete protection —** Combine snapshot orchestration for fast, operational recovery and secure, air-gapped backups for ransomware protection
- **Secure, air-gapped data —** Secure, encrypted, and air-gapped backups, isolated from customers' production environments
- **Lower TCO —** Reduce TCO by up to 50% compared to native AWS backup by eliminating unnecessary cross-region or cross-account snapshot copies
- **Radical storage efficiency —** Built-in source-side global deduplication and automated cold-storage tiering for long-term retention
- **Easy to use —** Global visibility and control, with simplified AWS data protection and management for tens to thousands of AWS accounts
- **Fast recovery —** Perform fast, point-in-time restores across AWS regions and accounts in just minutes — as simple as restoring from a snapshot

druva

Next steps

Visit the Druva site to learn more about how we provide comprehensive data resilience for your AWS environments and schedule a free demo to experience Druva for yourself.



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: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.