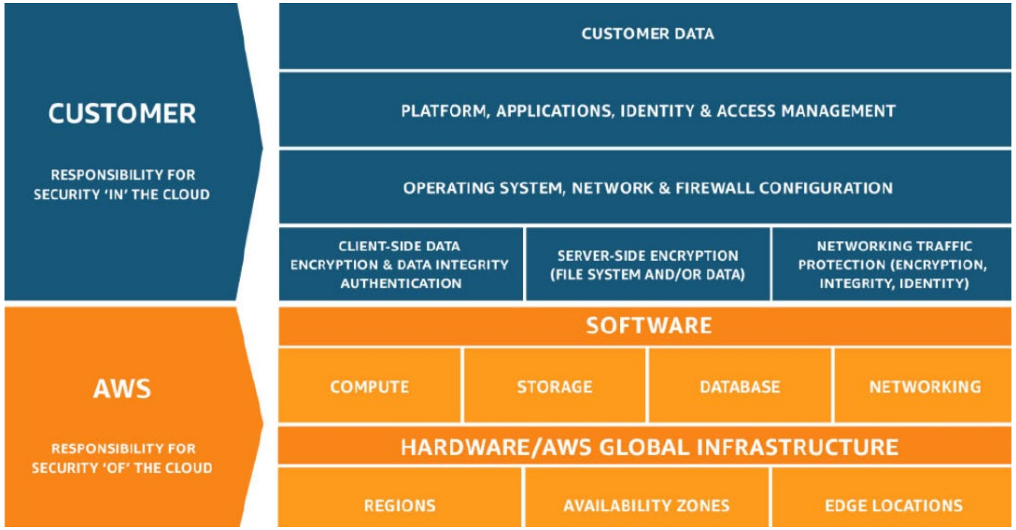
VEEAM

Choosing the Best **AWS Backup and Recovery** Solution

Contents

The need to back up AWS data

If you're like most organizations who run workloads on public cloud platforms like Amazon Web Services (AWS), you know that protecting these workloads matter. However, your data in AWS doesn't protect itself. To quote AWS, "AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud" however "customers are responsible for managing their data." But what does "managing" mean?


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

AWS Shared Responsibility Model

We need look no further than AWS' Shared Responsibility Model, which demonstrates perfectly what your responsibilities are and what AWS responsibilities as a provider are. Irrespective of the level of service(s) you utilize, you always retain responsibility for your data, meaning it is always your responsibility to protect and secure that data.

AWS provides a robust infrastructure to ensure that your applications continue to work in case something happens, such as AWS Regions each having multiple Availability Zones (AZs) which are made up of either one or several data centers. When this infrastructure is leveraged properly, your data should be replicated across AZs and regions to guarantee the best experience possible. This is to make sure that normal operations continue in the event there is a localized hardware or software failure, natural disaster, etc.

Despite the remarkable resiliency and availability that can be architected within AWS, it still comes with the limitations of replication. Data that becomes compromised by a security incident like ransomware, corrupted, accidentally deleted, etc. is simply replicated to the target destination, leaving no way to recover. This is why a solid backup strategy is always needed to complement even the most resilient of AWS environments.

Options for AWS backup and recovery

So, if data doesn't protect itself and backup is required just like with all data hosted on-premises or in the cloud, what options are available to help achieve this?

Snapshots

A simple built-in data protection option in AWS is the snapshot because nothing needs to be deployed. Amazon Elastic Block Store (Amazon EBS) snapshots are automatically stored on long-term Amazon Simple Storage Service (Amazon S3) object storage media.

Snapshots are an easy option, but they are not a true backup. Since the snapshots are not stored independently from the original data, you could lose data if your account were compromised, representing a single point-of-failure. Additionally, snapshots are one of the more expensive storage options in AWS.

AWS Backup

AWS Backup is a first party offering from AWS, built to backup and recover AWS data in a centralized, automated solution. AWS Backup builds on some of the limitations of native snapshots with capabilities like policy-based automation, cross-region backup, lifecycle management and more, all of which can be set up when your account is created.

While AWS Backup is a significantly more robust option than snapshots alone, it still has its limitations.

Veeam Backup *for AWS*

Veeam® Backup *for AWS* utilizes AWS-native snapshot, storage and security technologies to provide a flexible, robust and purpose-built AWS backup and recovery solution. Policy-based automation, cost calculation and stringent security measures deliver a powerful yet easy to manage solution that ensures optimal data protection and security while controlling costs.

Veeam Backup *for AWS* can seamlessly integrate with Veeam Backup & Replication™, allowing users to centrally manage the entirety of their environment — cloud, virtual, physical, Software as a Service (SaaS) and Kubernetes — not just data in AWS. This is a critical capability for the majority of organizations that are hybrid/multi-cloud in nature, utilizing AWS alongside an on-premises data center and/or one or more cloud vendors.

Choose what's best for your business

As you review the options available for your organization, make sure to prioritize protection and security. Take time to assess your organization's requirements and objectives when it comes to backup to ensure that the solution fits the needs of your business and your budget.

This next part of this document takes a deeper dive into the features of the above options, broken down into five capability categories to help you assess your needs and choose the solution that's right for you.

Ease of deployment and management

— Not supported ✓ Partially supported ✔ Fully supported

	AWS snapshots	AWS Backup	Veeam Backup *for AWS*
Simple setup: Easy deployment and configuration directly within AWS Management Console or AWS Marketplace[1].	✓	✔	✔
Breadth of supported workloads: Protect multiple AWS services that can host your workloads and data, including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Elastic File System (Amazon EFS), Amazon Aurora and Amazon Virtual Private Cloud (Amazon VPC)[2].	✓	✓	✔
Automated, policy-based protection: Create snapshot- and image-based backup policies that automatically protect workloads based on account, region and tags.	—	✓	✔
Support multiple accounts: Schedule, manage and monitor data protection for multiple accounts and regions from one interface.	—	✔	✔
Unified management: Increase visibility of data protection compliance and operations through a unified console that supports multiple clouds, virtual machine platforms and physical systems[3].	—	✓	✔

[1] In addition to AWS Marketplace, Veeam Backup *for AWS* can also be deployed directly through Veeam Backup & Replication™.

[2] When combined with Veeam Backup & Replication, you can also protect VMware Cloud on AWS.

[3] Veeam Backup & Replication offers versatile data protection options for any environment through a single, wizard-driven interface. Switch to a web-based console if you'd like to protect workloads only within AWS.

Meeting SLAs

	AWS snapshots	AWS Backup	Veeam Backup *for AWS*
Flexible scheduling: Align backup schedules with service level agreements (SLAs), including workloads that need backups throughout the day[4].	–	✓	✔
Application consistency: Create application consistent snapshots and backups for zero data loss backup and recovery.	–	✓	✔
Multiple recovery options: Recover entire instances, volumes, databases, file systems as well as individual files and folders. This includes the ability to restore a resource to its original or different location[5].	–	✓	✔
Effortless scalability: Effortlessly protect environments of all sizes while scaling backup operations up or down.	–	✔	✔
Intelligent retention: Store backup data in multiple storage tiers to balance retention requirements, recovery speed and storage costs.	–	✔	✔

[4] Veeam Backup *for AWS* can create multiple snapshots per hour for fine-grained scheduling.

[5] Veeam Backup & Replication can be used to restore Amazon EC2 instances to locations outside of AWS (e.g., On-premises VMs, Microsoft Azure, and Google Cloud).

Optimizing spend

	AWS snapshots	AWS Backup	Veeam Backup *for AWS*
Transparent pricing: Built-in cost calculation to forecast monthly expense of resources like compute, networking and storage that are associated with data protection.	–	–	✔
Minimize backup costs: Optimize backup infrastructure and operations costs (e.g., dynamic compute, network traffic, etc.) without negatively impacting the performance of backup and restore processes.	–	–	✔
Compression: Compresses backup data when targeting repositories to minimize storage consumption and reduce costs.	–	✓	✔
Storage options: Use multiple storage access tiers like Amazon Simple Storage Service (Amazon S3), S3 Glacier and S3 Glacier Deep Archive to reduce costs in longer-term retention scenarios.	–	✓	✔

Security and compliance

	AWS snapshots	AWS Backup	Veeam Backup *for AWS*
Encryption: Leverage advanced 256-bit AES encryption to encrypt data blocks in backup files.	–	✓	✔
AWS Key Management Service (AWS KMS): Use AWS KMS to encrypt, manage and provide access to secure backup data, which improves security and control over keys and passwords that are used by backup policies.	–	✔	✔
Granular permissions: Delegate roles and access permissions to specific users to ensure greater security with least-privileged access required.	–	✔	✔
Advanced reporting: Automatically generate and deliver reports on your protection status, including protected and unprotected workloads and policy execution results (e.g., success warning or failure).	–	–	✔

Hybrid-/multi-cloud support

	AWS snapshots	AWS Backup	Veeam Backup *for AWS*
Single console: Centrally manage AWS backup and recovery with other workloads like virtual, physical, SaaS, Kubernetes and other cloud workloads.	–	✓	✔
Data portability: Use backup data to assist in platform migration and meet data compliance requirements to hold a copy of backups in a different platform. Avoid platform lock-in with the ability to back up, recover and migrate all data across any environment as business requirements change (e. g., on-premises to cloud, cloud to cloud, cloud to on-premises).	–	–	✔
Flexible licensing: Portable licensing that can be reused for different solutions that protect different workloads as business requirements change.	–	–	✔
Centralized monitoring: Monitor the entirety of a hybrid-/multi-cloud environment from a single dashboard, including custom views, report generation for audits, etc.	–	–	✔

Summary

In this ever-changing, hybrid cloud world, it's critical that you retain ownership and control of your data. There are multiple data protection options available for AWS, and they all have their own capabilities. Make sure you properly assess your organization's requirements and choose the right solution for your needs as you anticipate how those needs might change in the future.

About the Authors

Kelsey Teske,

Cloud Specialist,
Product Marketing

Sam Nicholls,

Director of
Public Cloud,
Product Marketing

Dustin Albertson

Manager of Cloud and
Application Alliances,
Product Management

About Veeam Software

Veeam® is the leader in Modern Data Protection. The company provides backup, recovery and data management solutions through a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected from ransomware, disaster and harmful actors and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects 450,000 customers worldwide, including 81% of the Fortune 500 and 70% of the Global 2,000. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers and alliance partners. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeamsoftware and Twitter @veeam.