VEEAM

5 Veeam on AWS: Secure Backup Best Practices

aws PARTNER

- Public Sector
- Storage Software Competency

Contents

The proliferation of ransomware

The growth and evolution of ransomware is one of the most destructive trends of the last decade. This explosion has moved ransomware from an economic crime to one with immense global security implications. NATO, the U.S. federal government and military, and the G7 have all recently acknowledged the severity of the ransomware threat and the need for large-scale coordinated response from government and industry.

Coordinated government and industry response takes time. In the meantime, organizations of all sizes need to protect themselves and their customers and constituents today. Fortunately, concrete steps using readily available tools and security frameworks can assist.

The sophistication and adaptability of ransomware and other cyberthreats today require an agile, layered defense.

Yet many organizations still maintain standalone security products that are focused on a single attack vector, which can be bypassed.

Compounding the technology issues is a lack of security expertise on staff. The staffing issues go beyond technical skills to knowing how to apply policies that create consistency and provide a way to measure your organization's overall effectiveness. These gaps in people, process and technology make attacking your data easier than ever for sophisticated cybercriminals.

Bad actors have the opportunity of infinite attempts to get into your infrastructure and only be right once. Good actors – you – have just one shot to block attacks, and you must be right 100% of the time.

!!! IMPORTANT INFORMATION !!!
All of your files are encrypted
with RSA-2048 and AES-128 ciphers.
More information about the RSA
and AES can be found here:

Building a framework for resilient recovery

Effective security programs require structure to understand what should be protected and the value of the asset to the organization to determine how protection should be implemented. No matter the methodology companies choose, the framework needs to define measurable outcomes that allow IT teams to defend against attacks and recover quickly if an attack is successful. As an example, the NIST Cybersecurity Framework (CSF) is widely adopted, constantly updated, and is designed to create a common language across different stakeholders. The NIST CSF has become the foundation on which cybersecurity practitioners have built their programs to define best practices and create a unified lexicon for understanding and managing the risks associated with the modern infrastructure.

Without a structured way to manage cybersecurity risk, it would be easy to focus all your efforts into detection-based defenses such as firewalls and anti-virus while neglecting the processes and tools that are mandatory to effectively respond to, and recover from, a successful attack. Put another way, the best offense is a solid defense, including having a robust strategy for backing up and protecting your data and workloads. Successful backups are the last line of defense for cyberattacks and can be the deciding factor to prevent considerable downtime, data loss and paying a costly ransom.

Cloud security at AWS is the highest priority, with a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Security in the cloud is much like security in your on-premises data centers — only without the costs of maintaining facilities and hardware. In the cloud, you don't have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and out of your cloud resources.

Security benefits of AWS

Keep Your Data Safe:

AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.

Meet Compliance Requirements:

AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.

Save Money:

Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility

Scale Quickly:

Security scales with your AWS Cloud usage. No matter the size of your business, AWS infrastructure is designed to keep your data safe.

However, Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. This differentiation of responsibility is commonly referred to as "Security 'of' the Cloud" versus "Security 'in' the Cloud."

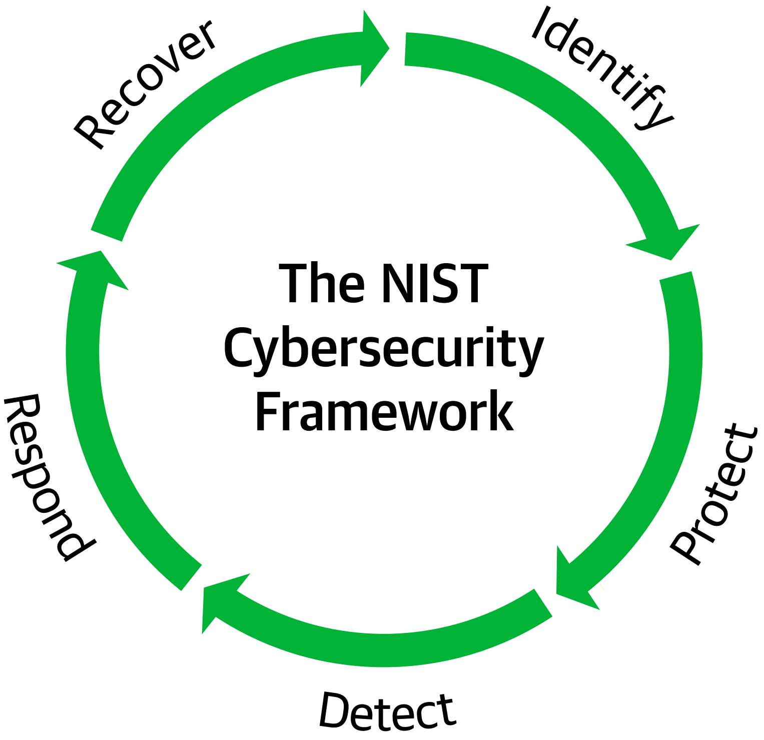
To that end, we've put together these best practices guide to provide real-world advice on securing your data.

1. Secure backup is your last line of defense

The data protection solution deployed should be capable of securely protecting the breadth of all mission-critical workloads, whether they're traditional workloads in the data center like physical and virtual machines, or cloud-native and containerized workloads in AWS. Regardless of if workloads are deployed on-premises or in the cloud, the data must be portable to account for uncertainties and future requirements. This portability takes many forms, but is critical in your defense. For example, utilizing secure AWS storage as a target for on-premises backups, migrating workloads to AWS in the event of a successful attack, recovering workloads in one AWS account to another, etc.).

The protection solution should also be capable of dynamically scaling up or down depending on requirements and workloads being protected, eliminating the potential of retention gaps that may hinder a successful recovery in the event of an attack.

The backup solution should be capable of capturing data via a multitude of methods, for example native snapshots, image-based backup, replication, etc. Furthermore, utilization of AWS security technologies and services like Amazon Simple Storage Service (Amazon S3) Object Lock and AWS Key Management Service (KMS) are critical to ensure backup data remains untouched in the event of an attack for an assured, clean recovery.



2. Follow the 3-2-1-1-0 Rule

The 3-2-1-1-0 Rule is the golden rule of data protection and at the core of any secure backup strategy, helping organizations navigate the risk of ransomware and other security incidents and keeping service levels high. Many organizations are familiar with the 3-2-1 Rule, however there are two distinct and necessary additions that help thwart ransomware.

3: Maintain at least three copies of your data

In addition to production data, there should also be at least two more backups. The potential for something to go wrong with three data sets at the same time is significantly smaller than with a single backup device, especially when the primary backup is often situated close to the primary data.

2: Store backups on two different media

It is not recommended to store the two copies of your backup on the same type of storage media. In the case of on-premises data, a better approach is to store one of the copies on disk in the data center, and another copy in cloud storage like Amazon S3. Conversely for cloud-native workloads, options for storing protection data include snapshots on Amazon Elastic Block Storage (Amazon EBS) and backups on Amazon S3, different regions or accounts, or even backup copies on-premises.

1: Store at least one of the copies at an off-site location

It is highly recommended to keep at least one copy of the backups away from the physical location where the primary data and primary backup is located. As discussed above, AWS offers many storage types and regions across the globe to ensure geographic separation of production, primary and secondary backups. It's also recommended to protect those backups with encryption.

1: One copy is offline, air-gapped, or immutable

Once a hacker has access to your environment, everything with an online connection can be impacted. While truly offline or air-gapped media is difficult to achieve with the cloud due to constant connection, immutability with Amazon S3 Object Lock offers write once read many (WORM) functionality so that once backups are committed to storage, they cannot be changed or deleted until a policy-based predetermined time passes.

0: Be sure to have verified backups without errors

Backups must be consistently monitored and verified. Monitoring alleviates the potential for any errors as they can be remediated quickly and effectively, minimizing the risk of retention gaps that may hinder recovery point objective (RPO) attainment. Verification involves frequent testing to verify not only the success of a recovery, but also the cleanliness of the data within it before it is placed into production in a real-world scenario.

3. Utilize Amazon S3 Object Lock

For anyone looking to store backup data in AWS, being able to target Amazon S3 object storage provides an incredibly durable, scalable and cost-effective repository. However, one of the key features and benefits of using Amazon S3 is leveraging S3 Object Lock and its immutability capabilities. Immutability is an effective way to not only protect against cybersecurity events like ransomware or rogue administrators, but also more benign incidents that can destroy the integrity of backup data like accidental deletion, changes, etc. It may even be required for compliance with regulatory mandates.

S3 Object Lock achieves immutable functionality through a WORM model. Objects within configured Amazon S3 buckets are unable to be changed, deleted or overwritten for a pre-determined period of time, often defined by policies set in the AWS console based on retention.

Third-party data protection solutions are also capable of leveraging S3 Object Lock via APIs. By defining policies in the backup solution and configuring immutability capabilities, you ensure that any backup stored in the configured repository remains secure and untouched. This is critical when recovering from successful ransomware attacks and other cybersecurity events as the data is assured to be clean, restoring business operation without having to pay the ransom.

4. Isolate data in separate accounts

A recommended best practice when protecting data on AWS is to leverage multiple AWS accounts. An AWS account is a security boundary that has its own privileges, user accounts and IP subnets, among other things. By having separate AWS accounts for workloads like production, dev/test and backup, you create multiple secure environments that protect against an attack on an individual workload.

Imagine a scenario where a production environment is compromised by a brute force attack. If the production data and backup data are in the same AWS account, then the attacker has access to not only that mission-critical production data, but also the backup data. Any compromise of that data will result in restores of the backup data incredibly challenging, if not impossible. Conversely, when backup data is kept separate to the production data by using a different AWS account, you in effect have a completely different environment where that data is stored. In the event that a restore has to be performed, the data can be copied from the backup account and recovered to the production account, safe in the knowledge that the data has not been compromised by the attack.

5. Least privilege access permissions

When implementing a backup solution in any environment, whether on-premises or on AWS, it is always a best practice to implement the least amount of access privileges. You should always start with a minimum set necessary to perform the task, and when requirements change, add the new necessary permissions. By implementing this best practice, you are ensuring that tasks using those access permissions can perform minimal tasks and reduce the attack surface that someone can use this account for.

Access permissions should be continuously audited, including the removal of any unnecessary credentials when no longer required, as well as the rotation of credentials periodically.

IAM Roles

As a best practice, use AWS Identity and Access Management (IAM) roles to temporary create credentials to access only the resources you need to do your job (granting least privilege). Configure AWS Single Sign-On to allow users from your external identity source to access AWS resources in your accounts. For IAM users, create separate roles for specific job tasks and assume those roles for those tasks. Don't use your IAM admin user for your everyday work.

AWS IAM provides methods to help you understand which access is needed

- Understand access level groupings – You can use access level groupings to understand the level of access that a policy grants.
- Validate your policies – You can perform policy validation using IAM Access Analyzer when you create and edit JSON policies.
- Generate a policy based on access activity – To help you refine the permissions that you grant, you can generate an IAM policy that is based on the access activity for an IAM entity (user or role).
- Use last accessed information – Another feature that can help with least privilege is last accessed information. View this information on the Access Advisor tab on the IAM console details page for an IAM user, group, role or policy. Last accessed information also includes information about the actions that were last accessed for some services, such as Amazon EC2, IAM, AWS Lambda and Amazon S3.
- Review account events in AWS CloudTrail – To further reduce permissions, you can view your account's events in the AWS CloudTrail Event history.

Other considerations

Multi Factor Authentication

Multi Factor Authentication (MFA) or Two Factor Authentication (2FA) adds an extra layer of security to the login process, ensuring that the user who is attempting access can only log in by providing adequate username and password credentials, as well as a secure code generated by an authentication algorithm solution. This is especially critical in defending against brute force attacks.

Role Based Access Control

Role Based Access Control (RBAC) is another essential consideration for data protection. By only providing specific data protection functions access to individual tasks, or by creating roles for users, you can protect backup data by having different roles for individuals. For example, an administrator role may have access to backup policies, restore capabilities and the data itself, whereas an operator may only be able to perform backups. This ensures there is no access to perform restores and overwrite existing production data sets.

AWS KMS

Data encryption is another critical feature and comes in many forms, either from the data protection vendor themselves, or by leveraging services like AWS KMS. AWS KMS delivers a simple and scalable way to centrally create and manage cryptographic keys for backup data in object storage repositories. This helps secure protection data against theft and unauthorized access, as well as help meet compliance regulations. AWS KMS also integrates with other services like AWS CloudTrail, delivering logs of key usage to further manage risk and report on compliance.

aws PARTNER

- Public Sector
- Storage Software Competency

Accelerate to Modern Data Protection with Veeam and AWS

A five-time Gartner Magic Quadrant leader, 400K+ customers — from 82% of the Fortune 500 to the SMB — trust Veeam with their data, including:

AWS-Native Backup & Recovery

Hybrid Cloud and VMware Cloud on AWS

Kubernetes Backup & Recovery

Backup and Archive to AWS

Modernize and Migrate to AWS

Whether you're all in with AWS today or you're just getting started, Veeam® can help you protect, manage and secure it all with ease, from cloud-native apps and services on AWS to traditional on-prem workloads in hybrid cloud environments.

Learn more at veeam.com