VARONIS

AWS BEST PRACTICES

The ultimate playbook to understanding AWS and securing your cloud environment

NAVIGATING CLOUD DATA SECURITY IN AWS

If you've just created an Amazon Web Services (AWS) account and are worried about your cloud data security, you're not alone. Unknown organization-wide settings or simple misconfigurations could put your data at risk.

Fortunately, you can adopt several best practices to improve your security posture significantly.

In this guide, we'll review the AWS Well-Architected Framework, an architecture aligned to AWS best practices. We'll focus on the security pillar and cover the importance of the shared responsibility model, AWS permissions and accounts, and more.

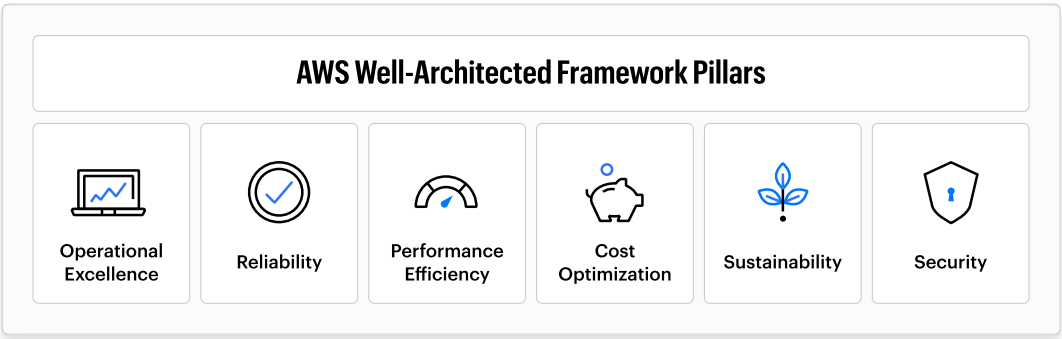
By adopting these best practices, you can build architectures that secure your cloud data and prevent security incidents.

The AWS Well-Architected Framework

The AWS Well-Architected Framework helps you weigh the pros and cons of your actions when building systems, incorporating best practices to enhance your cloud environment.

The AWS Well-Architected Framework is built on six pillars:

1. Operational excellence
2. Reliability
3. Performance efficiency
4. Cost optimization
5. Sustainability
6. Security



For this guide's purposes, we'll highlight the security pillar, which provides a way to consistently measure architectures against best practices and identify areas for improvement (see more on page 5).

Before we dive into the principles of the security pillar, let's review some AWS basics: the shared responsibility model and AWS accounts.

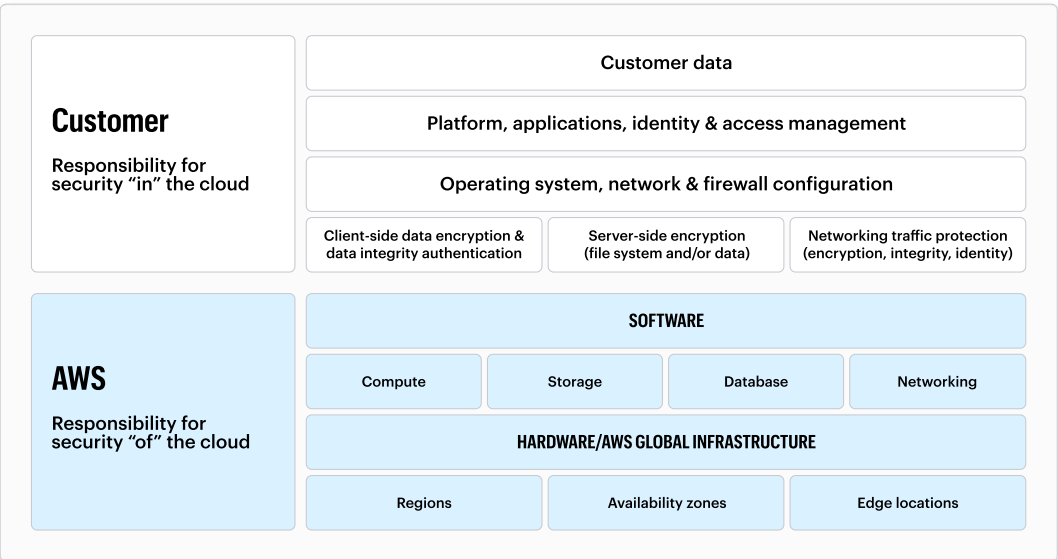
Shared responsiblity model

Understanding which security aspects an organization is responsible for versus which fall under the cloud application's domain is known as the shared responsibility model.

For example, Amazon provides you with tools and services to help secure your environment, you are responsible for configuring these services correctly and routinely monitoring for gaps or issues so your data stays protected.

While AWS provides security *of* the cloud, including the physical security of its datacenters, hardware and software infrastructure, and network infrastructure, customers are responsible for security *in* the cloud including identity and access management, network security, and data security of their environment.

AWS manages access permissions using IAM, allowing you to create policies that define what actions users or services can perform on specific resources. These policies are attached to users, groups, or roles, and AWS verifies them to decide if a request should be allowed or denied. This model controls who can do what in your AWS environment. Security teams must understand this model to protect sensitive information and mitigate risks from today's top cloud threats.



AWS accounts

Unlike typical user accounts, AWS accounts are a collection of your AWS identities, resources, and services. Grouping these assets into distinct collections helps segregate business areas, separating duties, billing management, or maintaining geographic dissemination.

For example, you could have an account for your North American team, your finance team, or for your developers. Decentralizing sections of your organization allows you to create unique security environments, which aid in blocking users from accessing inappropriate data. Every account is associated with a root user who possesses unrestricted access and permissions for the entire account, and this user cannot be deleted.

AWS Organizations helps you manage multiple AWS accounts from a single place. It allows you to group accounts, apply policies for security and compliance, and consolidate billing. This makes controlling access, sharing resources, and monitoring costs easier across all your accounts.

AWS security pillar design principles

Security teams must understand how security is applied in every aspect of the public cloud to mitigate risks from today's top cyber threats and protect their sensitive information.

AWS' security pillar has seven design principles that strengthen your data security.

1. Implementing a strong identity foundation

The first principle is to implement a strong identity foundation. This includes the following actions:

- Implement the least privilege model. This principle limits users' access to only what is necessary for their job. For example, giving users read and write access to an S3 bucket when only read access is needed violates this principle.

- Avoid using the root account for daily tasks. Root user credentials provide unlimited access to an account and all its resources, which introduces many risks if used for routine daily tasks. Instead, IAM users and roles should be used with restricted permissions. Ensure MFA is enabled on the root account and securely store root user credentials.

- Enforce segregation of duties with proper authorization for each interaction with AWS resources and limit privileged access. These steps significantly reduce your blast radius.

- Centralize identity management and aim to eliminate reliance on long-term static credentials. Using temporary or ephemeral credentials reduces risk to your environment immensely.

- Perform regular audits of access permissions.

2. Enable transparency

The second principle is to enable and maintain traceability.
Implement comprehensive logging and monitoring and set up real-time alerts to stay on top of actions and changes in your environment. Integrate log and metric collection with systems to automatically investigate and act.

3. Apply security at all layers

Apply a defense-in-depth approach with multiple security controls. A defense-in-depth approach is a security strategy that layers multiple protective measures to safeguard systems and data. This approach ensures that if one layer fails, others will still provide protection, enhancing overall security and reducing the risk of breaches. It includes implementing protective measures at the network edge, VPC, load balancers, instances, the operating system, applications, and code.

4. Automate security best practices

Use infrastructure as code (IaC), implement security controls programmatically, and automate security processes and responses that you can with the use of software-based security mechanisms. Create secure architectures, including implementing controls defined and managed as code in version-controlled templates.

Varonis can improve your ability to scale rapidly and cost-effectively securely by providing automated data security solutions that continuously discover, classify, and protect sensitive data across your cloud and on-premises environments.
This proactive approach ensures that sensitive data is not inadvertently exposed, enhancing the security of your IaC deployments.

5. Protect data in transit and at rest

Encrypt data in motion and at rest to implement proper access controls and classify it appropriately. With data classified correctly by sensitivity, you can apply the appropriate protection measures as needed.

6. Keep people away from data

Use mechanisms and tools to reduce or eliminate the need for direct access or manual data processing. This reduces the risk of mishandling or modification and human error when handling sensitive data.

The best way to keep people away from data is to reduce or eliminate direct human access to production data using the tools available. Also use these tools to minimize manual data handling.

This reduces the risk of mishandling, modification, and human error when handling sensitive data.

7. Prepare for security events

In today's threat landscape, it's important to be prepared for security events because they are more likely to happen than not.

To prepare for incidents at your organization, implement policies and processes aligning with your organizational requirements. Conduct regular security drills and simulations to ensure your employees understand their role in minimizing the likelihood of a breach.

With Varonis, you can increase your speed to detection with our Managed Data Detection and Response (MDDR) service.

Varonis MDDR provides 24x7x365 threat detection and response focused on protecting sensitive data. It combines Varonis' advanced threat detection technology with a global team of security experts to monitor, investigate, and respond to threats in real time. This service helps organizations prevent data breaches by identifying and mitigating risks to their most valuable asset: data.

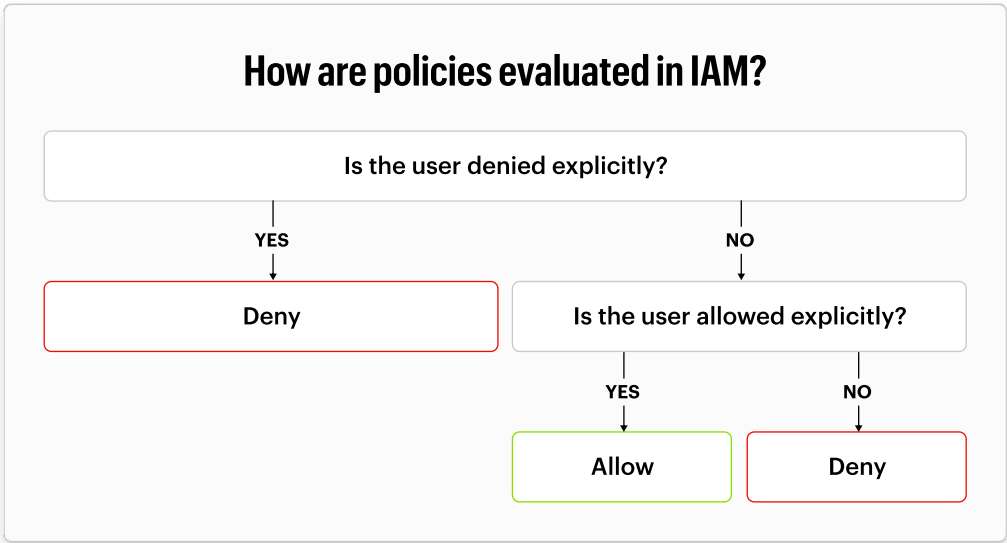
AWS permissions

IAM manages AWS permissions. IAM is a key part of an information security program, ensuring that only approved users and components can access your resources how you intend them to be accessed.

Security principles of AWS permissions include users, groups, roles, and resources that can perform actions in your account.

Build and apply access policies that are attached to these security principles, with the initial level of access starting at zero permissions. If a user is denied explicitly, they are always denied, invalidating any other permission.

If a user is explicitly allowed, they can be granted permission to use the specific resources needed. If your evaluation proves they are neither denied nor allowed explicitly, deny them.



AWS roles

IAM roles are also an important element of security in the AWS ecosystem. These roles are entities you create and assign specific permissions to that allow trusted identities to perform actions in AWS, like a disguise that a user or resource puts on to assume a role.

Roles will invalidate any other permissions and are temporary, making it a security best practice because they don't need to be rotated.

Trust and access policies help AWS teams understand who can assume certain roles and what access a role can have. These are primarily used for external identities like Active Directory, Entra ID, or Okta.

How Varonis helps

At Varonis, we use a different approach than other vendors to protect what matters most: your data.

Improving your data security posture in AWS can be easy. The hard part is understanding and analyzing permissions risks, remediating those risks, mapping identities, fixing misconfigurations, alerting on suspicious behavior, and more.

Varonis provides a comprehensive solution to protect AWS, including IAM, storage (S3), database (RDS), and compute (EC2) from insider threats, cyberattacks, and data exposure.

YOUR DATA. OUR MISSION.

We hope this guide helps you in your AWS journey and drives the cloud data security outcomes you're looking for! If you have questions, don't hesitate to contact us.

Partner with the leader in data security.

Gartner

#1 DSPM vendor on Gartner Insights

FORRESTER®

Leader in Forrester Wave™: Data Security Platforms, Q1 2023

GIGAOM

Leader in GigaOm Radar for Data Security Platforms (DSPs)

Reduce your risk without taking any.

Our free Data Risk Assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a risk-based view of the data that matters most and a clear path to automated data security.

Get a demo at www.varonis.com/demo.

About Varonis

Varonis (Nasdaq: VRNS) is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.