Improving your security with AWS

Top areas of focus for your security team

Accurate account information

AWS Management Console

We use the contact information you provide in your AWS account profile, found in the AWS web console, when we need to reach you about a security concern.

Learn more

Email

Make sure all email addresses go to aliases that are not dependent on a single person. Your security contact email address should deliver to multiple people or a 24/7 security team who have been trained on how to respond. Watch for security notifications from Amazon emails such as abuse@amazon.com.

Use multi-factor authentication (MFA)

Always set up MFA on your root user and AWS Identity and Access Management (IAM) users to provide an extra layer of protection from inappropriate access.

If you use AWS Single Sign-On to control access to AWS or federate your corporate identity store, you can enforce MFA there.

Learn more

No hard-coding secrets

Use IAM roles to deliver temporary credentials for using AWS services. When you need longer-lived credentials, **don't** hard code these secrets in the application or store them in source code.

Instead, use AWS Secrets Manager to rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle.

Learn more

Limit AWS security groups

Learn more

What

You can use AWS security groups to limit communications between your AWS resources and with the Internet. This can be achieved by only allowing the minimally required ports, and with sources and destinations that you trust.

How

You can use services such as AWS Firewall Manager and AWS Config to implement and monitor AWS security group configurations.

You can also use AWS Firewall Manager to protect the Internet facing resources by automatically applying **AWS WAF** rules, and implementing AWS Shield Advanced.

Intentional data policies

Learn more

Developing Data Policies

Not all data are created equal, so classifying data properly is crucial to its security. Consider factors such as over-classification with additional costs, grouping of sensitive data that have the same technical requirements, and user accessibility when designing your data classification strategy to meet a broad range of requirements.

Implementing Data Policies

Organizational policies must have a means to be technically implemented or run the risk they will not be followed, enforced, or monitored for compliance. You can use AWS IAM policies, service control policies, and Amazon Config to implement organizational data policies.

Centralize AWS CloudTrail logs

Logging and monitoring are important parts of a robust security plan.

Being able to investigate unexpected changes in your environment or iterate on your security posture relies on having access to data.

We recommend that you write logs to an Amazon Simple Storage Service (Amazon S3) bucket in an AWS account designated for logging. The permissions on the bucket should prevent deletion of the logs, and these logs should be encrypted at rest.

Learn more

Validate IAM roles

Over time, you may discover that IAM users and roles are no longer needed, or that their permissions have expanded beyond what is needed.

Learn more

AWS IAM Access Analyzer

Review access to your internal AWS resources and determine where you have shared access outside your AWS accounts. Regularly reviewing roles and permissions will give you the visibility needed to validate compliance with your governance, risk, and compliance policies.

AWS Config

Continuously monitor, identify, and remove unused IAM users, roles, and groups.

Take action on findings

AWS Security Hub, Amazon GuardDuty, Amazon Macie, Amazon Inspector, and AWS IAM Access Analyzer provide you with actionable findings in your AWS accounts. Take action on these findings based on your incident response policy. And to better mitigate scope and impact of an event, you can automate responses to more quickly contain suspicious activity and notify humans for awareness.

Learn more

Rotate your keys

Avoid using long-term AWS access keys. Instead, use IAM roles and federation. If you need to use access keys rather than roles, rotate them regularly.

You can use AWS Security Hub to check for IAM users with long-lived access keys.

Learn more

Be involved in dev cycle

Raising the security culture of your organization can pay big dividends. Everyone in your organization should feel comfortable seeking help from the security team, as security is everyone's job.

Whether you use DevOps or another development methodology, make sure that security requirements, such as patch automation capabilities, are embedded in every phase of your organization's development lifecycle.

Learn more

Ready to learn more?

AWS Well Architected Framework – Security Pillar

Dive into the AWS Foundational Security Best Practices standard.

Learn more

AWS Training and Certification

Explore 30+ no-cost digital courses on cloud security.

Learn more