**SEC 1. How do you securely operate your workload?**

To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations.

[Security Best Practices the Well-Architected Way](https://youtu.be/u6BCVkXkPnM?ref=wellarchitected)  
 [Managing Multi-Account AWS Environments Using AWS Organizations](https://youtu.be/fxo67UeeN1A?ref=wellarchitected)  
 [Enable AWS adoption at scale with automation and governance](https://youtu.be/GUMSgdB-l6s?ref=wellarchitected)  
 [AWS Security Hub: Manage Security Alerts and Automate Compliance](https://youtu.be/HsWtPG_rTak?ref=wellarchitected)  
 [Using AWS Control Tower to Govern Multi-Account AWS Environments](https://youtu.be/2t-VkWt0rKk?ref=wellarchitected)  
 [IAM Best Practices](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?ref=wellarchitected)  
 [Getting started with AWS Organizations](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started.html?ref=wellarchitected)  
 [AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html?ref=wellarchitected)  
 [Security Bulletins](https://aws.amazon.com/security/security-bulletins/?ref=wellarchitected)  
 [AWS Security Audit Guidelines](https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html?ref=wellarchitected)  
 [How to use service control policies to set permission guardrails across accounts in your AWS Organization](https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-aws-organization/?ref=wellarchitected)

Afbeelding met tekst, computer, computer, schermafbeelding

Automatisch gegenereerde beschrijving

#### Separate workloads using accounts Organize [workloads](https://wa.aws.amazon.com/wat.concept.workload.en.html) in separate accounts and group accounts based on function or a common set of controls rather than mirroring your company’s reporting structure. Start with [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) and infrastructure in mind to enable your organization to set common guardrails as your [workloads](https://wa.aws.amazon.com/wat.concept.workload.en.html) grow.

#### Secure AWS account Secure access to your accounts, for example by enabling [MFA](https://wa.aws.amazon.com/wat.concept.mfa.en.html) and restrict use of the [root user](https://wa.aws.amazon.com/wat.concept.root-user.en.html), and configure account contacts.

#### Identify and validate control objectives Based on your compliance requirements and risks identified from your threat model, derive and validate the control objectives and controls that you need to apply to your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html). Ongoing validation of control objectives and controls help you measure the effectiveness of risk mitigation.

#### Keep up to date with security threats Recognize attack vectors by staying up to date with the latest [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) threats to help you define and implement appropriate controls.

#### Keep up to date with security recommendations Stay up to date with both AWS and industry [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) recommendations to evolve the [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) posture of your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html).

#### Automate testing and validation of security controls in pipelines Establish secure baselines and templates for [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) mechanisms that are tested and validated as part of your build, pipelines, and processes. Use tools and automation to test and validate all [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) controls continuously. For example, scan items such as machine images and infrastructure as code templates for [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) vulnerabilities, irregularities, and drift from an established baseline at each stage.

#### Identify and prioritize risks using a threat model Use a threat model to identify and maintain an up-to-date register of potential threats. Prioritize your threats and adapt your [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) controls to prevent, detect, and respond. Revisit and maintain this in the context of the evolving [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) landscape.

#### Evaluate and implement new security services and features regularly AWS and [APN](https://wa.aws.amazon.com/wat.concept.apn.en.html) Partners constantly release new features and services that allow you to evolve the [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) posture of your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html).

**SEC 2. How do you manage identities for people and machines?**

There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right conditions. **Human Identities:** Your administrators, developers, operators, and end users require an identity to access your AWS environments and applications. These are members of your organization, or external users with whom you collaborate, and who interact with your AWS resources via a web browser, client application, or interactive command-line tools. **Machine Identities:** Your service applications, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identities include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions. You may also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment.

[Mastering identity at every layer of the cake](https://www.youtube.com/watch?v=vbjFjMNVEpc&ref=wellarchitected)  
 [Managing user permissions at scale with AWS SSO](https://youtu.be/aEIqeFCcK7E?ref=wellarchitected)  
 [Best Practices for Managing, Retrieving, and Rotating Secrets at Scale](https://youtu.be/qoxxRlwJKZ4?ref=wellarchitected)  
 [IAM Best Practices](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?ref=wellarchitected)  
 [The AWS Account Root User](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html?ref=wellarchitected)  
 [Getting Started with AWS Secrets Manager](https://docs.aws.amazon.com/secretsmanager/latest/userguide/getting-started.html?ref=wellarchitected)  
 [Temporary Security Credentials](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html?ref=wellarchitected)  
 [Identity Providers and Federation](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html?ref=wellarchitected)  
 [Security Partner Solutions: Access and Access Control](https://aws.amazon.com/security/partner-solutions/?ref=wellarchitected#access-control)

Afbeelding met tekst

Automatisch gegenereerde beschrijving

#### Use strong sign-in mechanisms Enforce minimum password length, and educate users to avoid common or re-used passwords. Enforce [multi-factor authentication](https://wa.aws.amazon.com/wat.concept.mfa.en.html) ([MFA](https://wa.aws.amazon.com/wat.concept.mfa.en.html)) with software or hardware mechanisms to provide an additional layer.

#### Use temporary credentials Require identities to dynamically acquire temporary credentials. For workforce identities, use [AWS Single Sign-On](https://wa.aws.amazon.com/wat.concept.aws-sso.en.html), or federation with [IAM](https://wa.aws.amazon.com/wat.concept.iam.en.html) roles to access AWS accounts. For machine identities, require the use of [IAM](https://wa.aws.amazon.com/wat.concept.iam.en.html) roles instead of long term access keys.

#### Store and use secrets securely For workforce and machine identities that require secrets such as passwords to third party applications, store them with automatic rotation using the latest industry standards in a specialized service.

#### Rely on a centralized identity provider For workforce identities, rely on an identity provider that enables you to manage identities in a centralized place. This enables you to create, manage, and revoke access from a single location making it easier to manage access. This reduces the requirement for multiple credentials and provides an opportunity to integrate with HR processes.

#### Audit and rotate credentials periodically When you cannot rely on temporary credentials and require long term credentials, audit credentials to ensure that the defined controls (for example, [MFA](https://wa.aws.amazon.com/wat.concept.mfa.en.html)) are enforced, rotated regularly, and have appropriate access level.

#### Leverage user groups and attributes Place users with common [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) requirements in groups defined by your identity provider, and put mechanisms in place to ensure that user attributes that may be used for access control (e.g., department or location) are correct and updated. Use these groups and attributes, rather than individual users, to control access. This allows you to manage access centrally by changing a user’s group membership or attributes once, rather than updating many individual policies when a user’s access needs change.

**SEC 3. How do you manage permissions for people and machines?**

Manage permissions to control access to people and machine identities that require access to AWS and your workload. Permissions control who can access what, and under what conditions.

[Become an IAM Policy Master in 60 Minutes or Less](https://youtu.be/YQsK4MtsELU?ref=wellarchitected)  
 [Separation of Duties, Least Privilege, Delegation, and CI/CD](https://youtu.be/3H0i7VyTu70?ref=wellarchitected)  
 [Grant least privilege](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?ref=wellarchitected#grant-least-privilege)  
 [Working with Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html?ref=wellarchitected)  
 [IAM Access Analyzer](https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html?ref=wellarchitected)  
 [Remove unnecessary credentials](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?ref=wellarchitected#remove-credentials)  
 [Attribute-based access control (ABAC)](https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Define access requirements Each [component](https://wa.aws.amazon.com/wat.concept.component.en.html) or resource of your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html) needs to be accessed by administrators, end users, or other [components](https://wa.aws.amazon.com/wat.concept.component.en.html). Have a clear definition of who or what should have access to each [component](https://wa.aws.amazon.com/wat.concept.component.en.html), choose the appropriate identity type and method of authentication and authorization.

#### Grant least privilege access Grant only the access that identities require by allowing access to specific actions on specific AWS resources under specific conditions. Rely on groups and identity attributes to dynamically set permissions at scale, rather than defining permissions for individual users. For example, you can allow a group of developers access to manage only resources for their project. This way, when a developer is removed from the group, access for the developer is revoked everywhere that group was used for access control, without requiring any changes to the access policies.

#### Establish emergency access process A process that allows emergency access to your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html) in the unlikely [event](https://wa.aws.amazon.com/wat.concept.event.en.html) of an automated process or pipeline issue. This will help you rely on least privilege access, but ensure users can obtain the right level of access when they require it. For example, establish a process for administrators to verify and approve their request.

#### Reduce permissions continuously As teams and [workloads](https://wa.aws.amazon.com/wat.concept.workload.en.html) determine what access they need, remove permissions they no longer use and establish review processes to achieve least privilege permissions. Continuously monitor and reduce unused identities and permissions.

#### Define permission guardrails for your organization Establish common controls that restrict access to all identities in your organization. For example, you can restrict access to specific [AWS Regions](https://wa.aws.amazon.com/wat.concept.region.en.html), or prevent your operators from deleting common resources, such as an [IAM](https://wa.aws.amazon.com/wat.concept.iam.en.html) role used for your central [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) team.

#### Manage access based on life cycle Integrate access controls with operator and application life cycle and your centralized federation provider. For example, remove a user’s access when they leave the organization or change roles.

#### Analyze public and cross account access Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access.

#### Share resources securely Govern the consumption of shared resources across accounts or within your AWS Organization. Monitor shared resources and review shared resource access.

**SEC 4. How do you detect and investigate security events?**

Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.

[Threat management in the cloud: Amazon GuardDuty and AWS Security Hub](https://youtu.be/vhYsm5gq9jE?ref=wellarchitected)  
 [Remediating Amazon GuardDuty and AWS Security Hub Findings](https://youtu.be/nyh4imv8zuk?ref=wellarchitected)  
 [Centrally Monitoring Resource Configuration and Compliance](https://youtu.be/kErRv4YB_T4?ref=wellarchitected)  
 [Setting up Amazon GuardDuty](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_settingup.html?ref=wellarchitected)  
 [AWS Security Hub](https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html?ref=wellarchitected)  
 [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/?ref=wellarchitected)  
 [Getting started: Amazon CloudWatch Logs](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html?ref=wellarchitected)  
 [Amazon EventBridge](https://aws.amazon.com/eventbridge?ref=wellarchitected)  
 [AWS Config](https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html?ref=wellarchitected)  
 [AWS Answers: Centralized Logging](https://aws.amazon.com/answers/logging/centralized-logging/?ref=wellarchitected)  
 [Security Partner Solutions: Logging and Monitoring](https://aws.amazon.com/security/partner-solutions/?ref=wellarchitected#logging-monitoring)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Configure service and application logging Configure logging throughout the [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html), including application logs, resource logs, and AWS service logs. For example, ensure that [AWS CloudTrail](https://wa.aws.amazon.com/wat.concept.cloudtrail.en.html), [Amazon CloudWatch](https://wa.aws.amazon.com/wat.concept.amazoncw.en.html) Logs, [Amazon GuardDuty](https://wa.aws.amazon.com/wat.concept.guardduty.en.html) and AWS [Security](https://wa.aws.amazon.com/wat.pillar.security.en.html) Hub are enabled for all accounts within your organization.

#### Analyze logs, findings, and metrics centrally All logs, metrics, and telemetry should be collected centrally, and automatically analyzed to detect anomalies and indicators of unauthorized activity. A dashboard can provide you easy to access insight into real-time health. For example, ensure that [Amazon GuardDuty](https://wa.aws.amazon.com/wat.concept.guardduty.en.html) and [Security](https://wa.aws.amazon.com/wat.pillar.security.en.html) Hub logs are sent to a central location for alerting and analysis.

#### Automate response to events Using automation to investigate and remediate [events](https://wa.aws.amazon.com/wat.concept.event.en.html) reduces human effort and error, and enables you to scale investigation capabilities. Regular reviews will help you tune automation tools, and continuously iterate. For example, automate responses to [Amazon GuardDuty](https://wa.aws.amazon.com/wat.concept.guardduty.en.html) [events](https://wa.aws.amazon.com/wat.concept.event.en.html) by automating the first investigation step, then iterate to gradually remove human effort.

#### Implement actionable security events Create alerts that are sent to and can be actioned by your team. Ensure that alerts include relevant information for the team to take action. For example, ensure that [Amazon GuardDuty](https://wa.aws.amazon.com/wat.concept.guardduty.en.html) and AWS [Security](https://wa.aws.amazon.com/wat.pillar.security.en.html) Hub alerts are sent to the team to action, or sent to response automation tooling with the team remaining informed by messaging from the automation framework.

**SEC 5. How do you protect your network resources?**

Any workload that has some form of network connectivity, whether it’s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.

[Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield](https://youtu.be/0xlwLEccRe0?ref=wellarchitected)  
 [AWS Transit Gateway reference architectures for many VPCs"](https://youtu.be/9Nikqn_02Oc?ref=wellarchitected)  
 [Amazon VPC Security](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html?ref=wellarchitected)  
 [Getting started with AWS WAF](https://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html?ref=wellarchitected)  
 [AWS Firewall Manager](https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html?ref=wellarchitected)  
 [Amazon Inspector](https://aws.amazon.com/inspector?ref=wellarchitected)  
 [Lab: Automated Deployment of VPC](https://www.wellarchitectedlabs.com/Security/200_Automated_Deployment_of_VPC/README.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Create network layers Group [components](https://wa.aws.amazon.com/wat.concept.component.en.html) that share reachability requirements into layers. For example, a database cluster in a VPC with no need for internet access should be placed in subnets with no route to or from the internet. In a serverless [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html) operating without a VPC, similar layering and segmentation with microservices can achieve the same goal.

#### Control traffic at all layers Apply controls with a defense in depth approach for both inbound and outbound traffic. For example, for [Amazon Virtual Private Cloud](https://wa.aws.amazon.com/wat.concept.amazonvirtualprivatecloud.en.html) (VPC) this includes [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) groups, [Network ACLs](https://wa.aws.amazon.com/wat.concept.network-acl.en.html), and subnets. For [AWS Lambda](https://wa.aws.amazon.com/wat.concept.lambda.en.html), consider running in your private VPC with VPC-based controls.

#### Automate network protection Automate protection mechanisms to provide a self-defending network based on threat intelligence and anomaly detection. For example, intrusion detection and prevention tools that can pro-actively adapt to current threats and reduce their impact.

#### Implement inspection and protection Inspect and filter your traffic at each layer. For example, use a web application firewall to help protect against inadvertent access at the application network layer. For Lambda functions, third-party tools can add application-layer firewalling to your runtime environment.

**SEC 6. How do you protect your compute resources?**

Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.

[Securing Serverless and Container Services](https://youtu.be/kmSdyN9qiXY?ref=wellarchitected)  
 [Running high-security workloads on Amazon EKS](https://youtu.be/OWRWDXszR-4?ref=wellarchitected)  
 [Security best practices for the Amazon EC2 instance metadata service](https://youtu.be/2B5bhZzayjI?ref=wellarchitected)  
 [AWS Systems Manager](https://aws.amazon.com/systems-manager/?ref=wellarchitected)  
 [Replacing a Bastion Host with Amazon EC2 Systems Manager](https://aws.amazon.com/blogs/mt/replacing-a-bastion-host-with-amazon-ec2-systems-manager/?ref=wellarchitected)  
 [Security Overview of AWS Lambda](https://pages.awscloud.com/rs/112-TZM-766/images/Overview-AWS-Lambda-Security.pdf?ref=wellarchitected)  
 [Lab: Automated Deployment of Web Application Firewall](https://wellarchitectedlabs.com/Security/200_Automated_Deployment_of_Web_Application_Firewall/README.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Perform vulnerability management Frequently scan and patch for vulnerabilities in your code, dependencies, and in your infrastructure to help protect against new threats.

#### Reduce attack surface Reduce your attack surface by hardening operating systems, minimizing [components](https://wa.aws.amazon.com/wat.concept.component.en.html), libraries, and externally consumable services in use.

#### Implement managed services Implement services that manage resources, such as [Amazon RDS](https://wa.aws.amazon.com/wat.concept.amazonrelationaldatabaseservice.en.html), [AWS Lambda](https://wa.aws.amazon.com/wat.concept.lambda.en.html), and [Amazon ECS](https://wa.aws.amazon.com/wat.concept.ecs.en.html), to reduce your [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) maintenance tasks as part of the shared responsibility model.

#### Automate compute protection Automate your protective compute mechanisms including vulnerability management, reduction in attack surface, and management of resources.

#### Enable people to perform actions at a distance Removing the ability for interactive access reduces the risk of human error, and the potential for manual configuration or management. For example, use a change management workflow to deploy [EC2 instances](https://wa.aws.amazon.com/wat.concept.ec2-instance.en.html) using infrastructure as code, then manage [EC2 instances](https://wa.aws.amazon.com/wat.concept.ec2-instance.en.html) using tools instead of allowing direct access or a bastion host.

#### Validate software integrity Implement mechanisms (for example, code signing) to validate that the software, code, and libraries used in the [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html) are from trusted sources and have not been tampered with.

**SEC 7. How do you classify your data?**

Classification provides a way to categorize data, based on criticality and sensitivity in order to help you determine appropriate protection and retention controls.

[Introducing the New Amazon Macie](https://youtu.be/I-ewoQekdXE?ref=wellarchitected)  
 [Data Classification Whitepaper](https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf?ref=wellarchitected)  
 [Getting started with Amazon Macie](https://docs.aws.amazon.com/macie/latest/user/getting-started.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Identify the data within your workload This includes the type and classification of data, the associated business processes. data owner, applicable legal and compliance requirements, where it’s stored, and the resulting controls that are needed to be enforced. This may include classifications to indicate if the data is intended to be publicly available, if the data is internal use only such as customer personally identifiable information (PII), or if the data is for more restricted access such as intellectual property, legally privileged or marked sensititve, and more.

#### Define data protection controls Protect data according to its classification level. For example, secure data classified as public by using relevant recommendations while protecting sensitive data with additional controls.

#### Automate identification and classification Automate identification and classification of data to reduce the risk of human error from manual interactions.

#### Define data lifecycle management Your defined lifecycle strategy should be based on sensitivity level, as well as legal and organization requirements. Aspects including the duration you retain data for, data destruction, data access management, data transformation, and data sharing should be considered.

**SEC 8. How do you protect your data at rest?**

Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.

[How Encryption Works in AWS](https://youtu.be/plv7PQZICCM?ref=wellarchitected)  
 [Securing Your Block Storage on AWS](https://youtu.be/Y1hE1Nkcxs8?ref=wellarchitected)  
 [AWS Key Management Service](https://aws.amazon.com/kms?ref=wellarchitected)  
 [Protecting Amazon S3 Data Using Encryption](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html?ref=wellarchitected)  
 [Amazon EBS Encryption](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html?ref=wellarchitected)  
 [Encrypting Amazon RDS Resources](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html?ref=wellarchitected)  
 [AWS KMS Cryptographic Details Whitepaper](https://d1.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf?ref=wellarchitected)  
 [AWS Encryption SDK](https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html?ref=wellarchitected)  
 [AWS Crypto Tools](https://docs.aws.amazon.com/aws-crypto-tools?ref=wellarchitected)  
 [AWS cryptographic services and tools](https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-overview.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Implement secure key management Encryption keys must be stored securely, with strict access control, for example, by using a key management service such as AWS KMS. Consider using different keys, and access control to the keys, combined with the AWS [IAM](https://wa.aws.amazon.com/wat.concept.iam.en.html) and resource policies, to align with data classification levels and segregation requirements.

#### Enforce encryption at rest Enforce your encryption requirements based on the latest standards and recommendations to help protect your data at rest.

#### Automate data at rest protection Use automated tools to validate and enforce data at rest protection continuously, for example, verify that there are only encrypted storage resources.

#### Enforce access control Enforce access control with least privileges and mechanisms, including backups, isolation, and versioning, to help protect your data at rest. Prevent operators from granting public access to your data.

#### Use mechanisms to keep people away from data Keep all users away from directly accessing sensitive data and systems under normal operational circumstances. For example, provide a dashboard instead of direct access to a data store to run queries. Where CI/CD pipelines are not used, determine which controls and processes are required to adequately provide a normally disabled break-glass access mechanism.

**SEC 9. How do you protect your data in transit?**

Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.

[AWS Certificate Manager](https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html?ref=wellarchitected)  
 [Services Integrated with AWS Certificate Manager](https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html?ref=wellarchitected)  
 [HTTPS Listeners for Your Application Load Balancer](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html?ref=wellarchitected)  
 [AWS VPN](https://docs.aws.amazon.com/vpn/?id=docs_gateway&ref=wellarchitected)  
 [API Gateway Edge-Optimized](https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-edge-optimized-custom-domain-name.html?ref=wellarchitected)

Afbeelding met tekst, computer, computer, schermafbeelding

Automatisch gegenereerde beschrijving

#### Implement secure key and certificate management Store encryption keys and certificates securely and rotate them at appropriate time intervals while applying strict access control; for example, by using a certificate management service, such as [AWS Certificate Manager](https://wa.aws.amazon.com/wat.concept.acm.en.html) ([ACM](https://wa.aws.amazon.com/wat.concept.acm.en.html)).

#### Enforce encryption in transit Enforce your defined encryption requirements based on appropriate standards and recommendations to help you meet your organizational, legal, and compliance requirements.

#### Automate detection of unintended data access Use tools such as GuardDuty to automatically detect attempts to move data outside of defined boundaries based on data classification level, for example, to detect a trojan that is copying data to an unknown or untrusted network using the DNS protocol.

#### Authenticate network communications Verify the identity of communications by using protocols that support authentication, such as Transport Layer [Security](https://wa.aws.amazon.com/wat.pillar.security.en.html) (TLS) or IPsec.

**SEC 10. How do you anticipate, respond to, and recover from incidents?**

Preparation is critical to timely and effective investigation, response to, and recovery from security incidents to help minimize disruption to your organization.

[Prepare for and respond to security incidents in your AWS environment](https://youtu.be/8uiO0Z5meCs?ref=wellarchitected)  
 [Automating Incident Response and Forensics in AWS](https://youtu.be/f_EcwmmXkXk?ref=wellarchitected)  
 [DIY guide to runbooks, incident reports, and incident response](https://youtu.be/E1NaYN_fJUo?ref=wellarchitected)  
 [CloudEndure Disaster Recovery](https://aws.amazon.com/cloudendure-disaster-recovery/?ref=wellarchitected)  
 [AWS Incident Response Guide](https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf?ref=wellarchitected)  
 [Lab: Incident Response Playbook with Jupyter - AWS IAM](https://www.wellarchitectedlabs.com/Security/300_Incident_Response_Playbook_with_Jupyter-AWS_IAM/README.html?ref=wellarchitected)  
 [Lab: Incident Response with AWS Console and CLI](https://wellarchitectedlabs.com/Security/300_Incident_Response_with_AWS_Console_and_CLI/README.html?ref=wellarchitected)

Afbeelding met tekst, schermafbeelding, computer, computer

Automatisch gegenereerde beschrijving

#### Identify key personnel and external resources Identify internal and external personnel, resources, and legal obligations that would help your organization respond to an [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html).

#### Develop incident management plans Create plans to help you respond to, communicate during, and recover from an [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html). For example, you can start an [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html) response plan with the most likely scenarios for your [workload](https://wa.aws.amazon.com/wat.concept.workload.en.html) and organization. Include how you would communicate and escalate both internally and externally.

#### Prepare forensic capabilities Identify and prepare forensic investigation capabilities that are suitable, including external specialists, tools, and automation.

#### Automate containment capability Automate containment and recovery of an [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html) to reduce response times and organizational impact.

#### Pre-provision access Ensure that [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html) responders have the correct access pre-provisioned into AWS to reduce the time for investigation through to recovery.

#### Pre-deploy tools Ensure that [security](https://wa.aws.amazon.com/wat.pillar.security.en.html) personnel have the right tools pre-deployed into AWS to reduce the time for investigation through to recovery.

#### Run game days Practice [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html) response [game days](https://wa.aws.amazon.com/wat.concept.gameday.en.html) (simulations) regularly, incorporate lessons learned into your [incident](https://wa.aws.amazon.com/wat.concept.incident.en.html) management plans, and continuously improve.