Data Protection on AWS

Jura Berg, Amazon Web Services

2023-01-23

Why use Data Protection on AWS?

Protect intellectual property and trade secrets

Protect customer information and build a trusted brand

Automate tasks to save time and reduce risk

Scale with visibility and control as your business grows

Ease of use - integration with hundreds of AWS services

Inherit global security and compliance controls

How are customers using Data Protection?

Migrate workloads securely from on-premise to the cloud

Encrypt cloud storage and databases

Protect data lakes and analytics pipelines

Authenticate container deployments

Authenticate IoT device networks

Eliminate high-risk hardcoded secrets

Discover and classify sensitive data for privacy regulations

Create robust DevSecOps pipelines

Data Protection on AWS

A suite of services designed to automate and simplify many security tasks ranging from key management and storage to sensitive data discovery

Amazon Macie

Discover and protect your sensitive data at scale

AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data

AWS Certificate Services

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS CloudHSM

Managed FIPS 140-2 Level 3 hardware security module (HSM) on the AWS Cloud

Customer Data Protection Journey

Foundational

1 Implement server-side **encryption for data at-rest** in AWS storage and database services

2 Store and manage encryption keys with **AWS Key Management Service**

3 Enable HTTPS (TLS) to **encrypt data in-transit**

4 Manage TLS certificates at scale with **AWS Certificate Manager**

Customer Data Protection Journey

Intermediate

1 Use **KMS and ACM on all accounts** in an organization for broad security coverage

2 Leverage features like S3 **bucket keys to optimize cost structure** while maintaining security

3 Replicate **encryption keys and secrets for disaster recovery** and business continuity

4 Use **Amazon Macie to evaluate data footprint** and determine any data compliance requirements

Customer Data Protection Journey

Advanced

1 Use **AWS Secrets Manager to reduce risk** by protecting database access credentials

2 Activate **AWS Private CA** to secure Kubernetes pods and manage certificates at scale

3 Leverage service integrations and technology partners for hybrid and multi cloud security

4 Build or enhance a **DevSecOps pipeline** with data protection and privacy integration

AWS Key Management Service

What is AWS Key Management Service?

AWS Key Management Service (KMS) makes it easy to create, manage, and securely store cryptographic keys

KMS is incorporated in over 90 AWS services to encrypt sensitive data and create digital signatures.

AWS Key Management Service

How Can I Use KMS?

- Enable data encryption in AWS services using symmetric or asymmetric keys
- Encrypt data on-premises or in AWS using AWS Encryption SDK
- Digitally sign and verify data using asymmetric key pairs
- Random number generation suitable for cryptographic applications

Fully Managed Key Service

- You control access to encrypted data with IAM policy and KMS key policy

- AWS manages the underlying infrastructure - hardware security modules, key management APIs, and service integrations

- KMS enforces the permissions you define in key policy and handles the durability and physical security of KMS keys

Secure, Centralized Key Management

- As usage grows, KMS scales automatically to meet your needs, from a few KMS keys to thousands of keys in an account
- KMS is a highly-available service, with a stated service commitment of a 99.999% monthly uptime percentage
- KMS is designed to provide 99.999999999% durability of keys
- Encrypted data can be protected with Multi-Region KMS Keys, to facilitate disaster recovery, multi-region HA, or encrypted Global DynamoDB tables

Encrypt Data in Your Applications

- Customers use separate KMS keys to partition access to data
- KMS key policy defines access
- KMS key authorization separates key administrators from encryption key users
- KMS keys cannot leave the HSMs in which they are stored, and plaintext keys are never written to durable storage

Native Integrations with AWS Services

- Encryption is available in every AWS service where you can store data
- Full list of KMS service integrations:
  - KMS Service Integrations
- AWS services, such as S3 and EBS, utilize KMS to generate, retrieve, and protect data keys that are used to encrypt your sensitive data
- Many services support data key caching or features like S3 Bucket Keys to help reduce your KMS costs

S3 Bucket Key: A bucket-level key that is used for a time-limited period within Amazon S3. This reduces the need for S3 to make requests to KMS, allowing you to access AWS KMS-encrypted objects in S3 at a fraction of the previous cost.

Monitor encryption key usage with KMS

- AWS KMS encryption context can be used to correlate events in AWS CloudTrail
- Detective controls & an audit record prove access and ensure non-repudiation
- Use AWS Config to track changes to KMS key policy

AWS CloudTrail

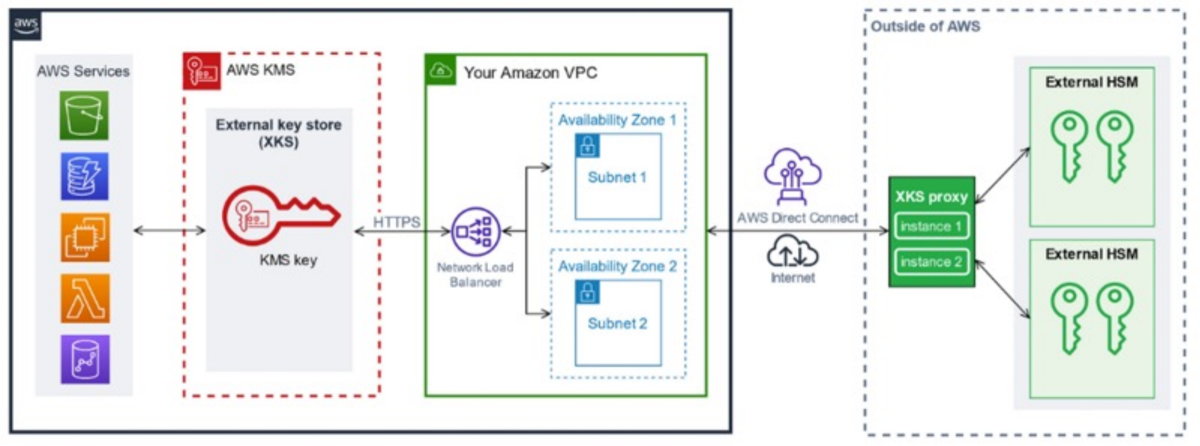
AWS Config

Encryption context: Non-secret additional information that is included verbatim in CloudTrail logs and can be used in IAM policies

AWS KMS External Key Store (XKS)

CUSTOMER OPERATED EXTERNAL HSM SUPPORT FOR REGULATED WORKLOADS

- Replace KMS key hierarchy with customer managed root of trust
- Root keys generated and stored in external HSM
- KMS XKS proxy transforms KMS requests to native HSM format
- Allows an additional layer of authorization control



Unblock migrations for workloads that have regulatory requirements for external encryption keys

AWS Certificate Services

AWS Certificate Services

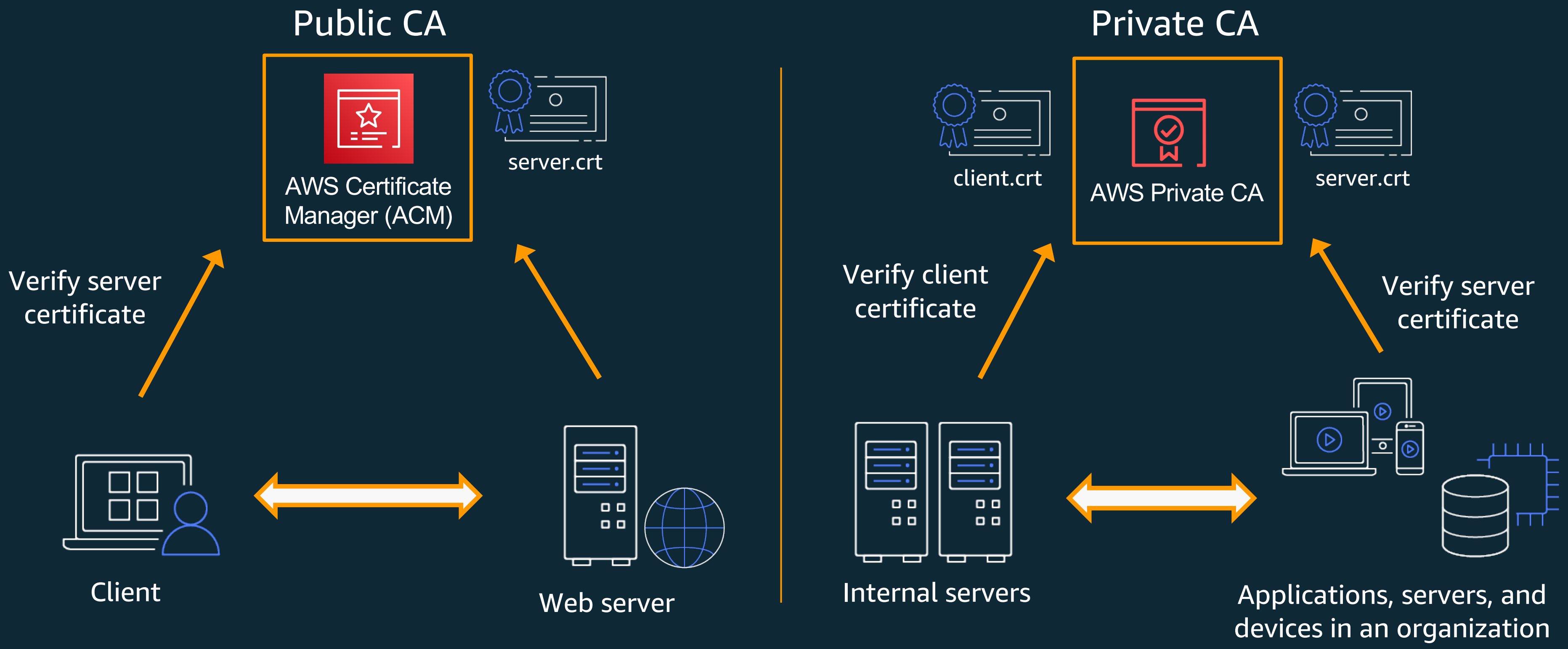
AWS Certificate Manager (ACM)

Easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources

AWS Private Certificate Authority (CA)

Highly-available private certificate authority service without the upfront investment and ongoing maintenance costs of operating your own private CA

Public vs. Private Certificate Authority



Public CA
AWS Certificate Manager (ACM)
server.crt
Verify server certificate
Client
Web server
Private CA
client.crt
AWS Private CA
server.crt
Verify client certificate
Verify server certificate
Internal servers
Applications, servers, and devices in an organization

ACM & PCA - Differentiators

	AWS Certificate Manager (ACM)	AWS Private CA
Certificate private keys	ACM generates and manages the private key	Customer generates and manages the private key
Certificate subject/SANs	Valid DNS names only	Any valid X.509 subject/SANs
Validity period	13 months	Any validity period
Key and signature algorithm	RSA 2048 with SHA-256 hashing	ECDSA or RSA keys SHA-256, SHA-384, SHA-512 hashing
Export	Available for private certificates	n/a – Customer manages the private keys and certs
Renewals	Automatic after association or export	Customer-managed
Deployment	ACM-managed for ACM-integrated services Customer-managed for on-premises, EC2, IoT	Customer-managed
Benefits	Central management	Flexibility, Greater level of customer control

AWS Certificate Manager

AWS Certificate Manager

AWS Certificate Manager

- Public Certificate Authority
  - Public certificates are trusted by browsers in the wild
- Provides TLS certificates
- Automated renewal of provisioned certificates
- Cannot export private key
- Natively integrated with AWS services:
  - API Gateway
  - CloudFront
  - Elastic Load Balancer

ACM Compliance for Data Privacy and Protection

- **HIPAA Eligible** - The standard for sensitive patient data protection
- **AICPA SOC 1, 2, and 3** – Provides deep insight into ACM's security processes and controls
- **PCI DSS** – The technical and operational requirements for protection of cardholder data
- **ISO 9001, 27001, 27017, and 27018** – Among the most recognized global security standards

ACM Pricing

Public SSL/TLS certificates provisioned through AWS Certificate Manager are free.

ACM Private CA

Securely Manage Private Certificates

Certificate Authority keys are secured with AWS-managed hardware security modules (HSMs) which adhere to FIPS 140-2 security standards

Private CA administrators can control access to the service using AWS Identity and Access Management (IAM) policies

Customers can audit private CA activity using AWS CloudTrail, as well as PCA-generated reporting

Private CA publishes and updates certificate revocation lists (CRLs) to Amazon S3 to help prevent the use of revoked certificates

ACM Private CA Use cases

ACM Private CA

Server certificates

- Private certificates to identify internal servers
- EC2, ECS, EKS, or on-premises servers: e.g. Apache, Tomcat, NGINX

Client certificates

- Second factor for API access
- TLS mutual authentication for server-server communication

Replacement for self-signed certificates

IoT device certificates

AWS Secrets Manager

AWS Secrets Manager

AWS Secrets Manager enables customers to manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycle

- Prevent devs from viewing or sharing secrets
- Stop secret sprawl
- Visibility into who use which secrets and when?
- Enable flexibility without waiting on other teams to provision secrets
- Roll-out secrets safely
- Rotate secrets safely with no downtime

Securely store and manage secrets

- Stored centrally and retrieved programmatically
- Secrets are encrypted by default using AWS Key Management Service (KMS)
- Customers can choose to own and manage their encryption keys, or allow AWS to manage keys for them
- Encryption keys are secured with hardware security modules (HSMs) which adhere to FIPS 140-2 security standards
- Create and store secrets so that developers don’t view or handle secrets

Rotate Secrets Safely

When you enable rotation for a supported secret, Secrets Manager provides a Lambda rotation function for you and populates the function automatically with the ARN in the secret. **Update Dec 2022:** *Amazon RDS announces integration with AWS Secrets Manager.*

Supported Secrets

- RDS Maria DB
- RDS MySQL
- RDS Oracle
- RDS PostgreSQL
- RDS Microsoft SQLServer
- Redshift
- DocumentDB

Fine-grained access control policies

- Use AWS IAM policies to manage access to your secrets for IAM users, roles, and groups to control access to individual secrets
- Use resource-based policies to access secrets across AWS accounts
- Assign tag-based policies for more granular access to your secrets with attribute-based access control (ABAC)

Audit and monitoring features

- Provides a central point of control for securing and auditing secrets
- Encrypts secrets by default with customer managed encryption keys using AWS KMS
- Access secrets securely through VPC-end points
- Audit and monitor secrets via integrations with CloudTrail, CloudWatch, and SNS
- Service supports compliance with PCI DSS, SOC, HIPAA, BAA, HITRUST CSF, ISO, FedRAMP-High and FedRAMP-Moderate

AWS CloudHSM

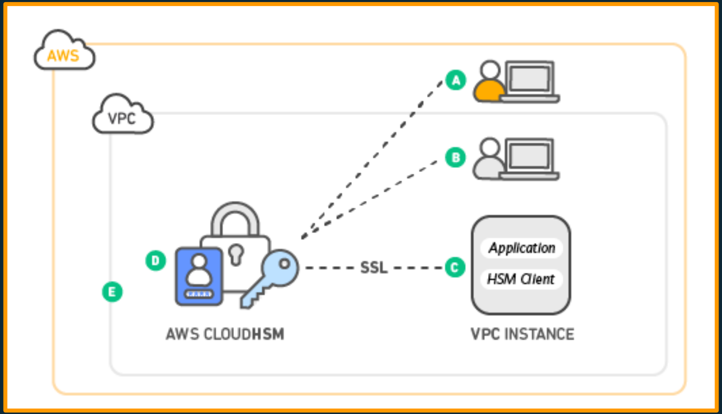
AWS CloudHSM

For customers with elevated regulatory or compliance requirements, CloudHSM offers flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.

- Cloud based Hardware Security Module (HSM)
- FIPS 140-2 level 3 validated
- Single tenant
- Actual hardware appliance in an AWS datacenter
- Integrates with KMS – Custom Key Store
- Highly available through clusters
- Enables export of keys to most other commercially available HSMs

AWS CloudHSM Use Cases

- SSL/TLS Offload
- Store master data encryption keys
- Sign certificates
- Sign documents and code
- Secure key exchange
- Blockchain



- Build your own application (C, Java, OpenSSL, Scripted, CNG/KSP)
- Drop-in CloudHSM SDKs with popular applications
- Use commercial solutions pre-integrated with CloudHSM

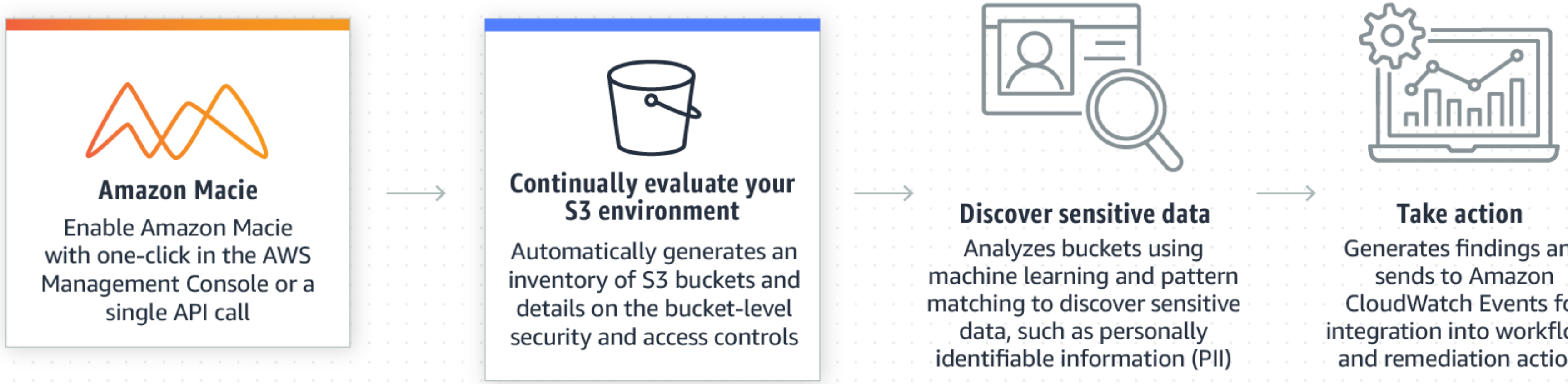
Amazon Macie

What is Amazon Macie?

Amazon Macie enables you to discover and protect your sensitive data at scale.

Amazon Macie

Amazon Macie – How it works



Amazon Macie

Enable Amazon Macie with one-click in the AWS Management Console or a single API call

Continually evaluate your S3 environment

Automatically generates an inventory of S3 buckets and details on the bucket-level security and access controls

Discover sensitive data

Analyzes buckets using machine learning and pattern matching to discover sensitive data, such as personally identifiable information (PII)

Take action

Generates findings and sends to Amazon CloudWatch Events for integration into workflows and remediation actions

Amazon Macie

Gain visibility and evaluate

- Bucket inventory
- Bucket policies

Discover sensitive data

- Inspection jobs
- Flexible scope

Centrally manage at scale

- AWS Organizations
- Managed & custom data detections

Automate and take actions

- Detailed findings
- Management APIs

Gain visibility and evaluate

Provides customers visibility into S3 bucket inventory

- Number of buckets
- Storage size
- Object count

Monitors changes to S3 bucket policies

- Publicly accessible
- Unencrypted
- Shared outside of the account
- Replicated to external accounts

Works across multiple accounts and automatically includes new buckets

Discover sensitive data

Ongoing evaluation of your Amazon S3 environment and data

- Select target for data discovery
- Create and schedule jobs

- Define the scope
- Scheduled frequency (one-time, daily, weekly, monthly)
- Object criteria (Tags, modified time, extension type, size)

- Review status (complete, cancelled, idle)
- Take actions (Cancel, copy)

Centrally manage at scale

Master/Member setup

- Multi-account with up to 1,000 member accounts
- AWS Organizations support up to 5,000 accounts

Macie master can create jobs on behalf of members

- One-click deployment with no upfront data source integration

With a few clicks in the AWS console, you can enable Macie across multiple accounts. Once enabled, Macie generates an ongoing Amazon S3 resource summary across accounts that includes bucket and object counts as well as the bucket-level security and access controls.

Centrally Manage at Scale – Managed Data Types

Fully managed sensitive data types

Amazon Macie maintains a growing list of sensitive data types that include common personally identifiable information (PII) and other sensitive data types as defined by data privacy regulations, such as GDPR, PCI-DSS, and HIPAA.

File formats

.txt .json .xml Avro
.csv .tsv
.doc .docx .xls .xlsx
.pdf
.tar .zip .gzip
Parquet

Data types

- *Financial (card, bank account numbers…)*
- *Personal (names, address, contact…)*
- *National (passport, ID, driver license…)*
- *Medical (healthcare, drug agency …)*
- *Credentials & secrets*

Centrally Manage at Scale – Custom Data Types

Custom-defined sensitive data types

Amazon Macie provides you the ability to add custom-defined data types using regular expressions to enable Macie to discover proprietary or unique sensitive data for your business.

- *Regular expression that defines a pattern to match*
- *Keywords that define specific text to match*
- *Ignore words that define specific text to exclude*

Automate and Take Actions – Finding Types

Finding types

- Bucket policy findings
- Sensitive data discovery findings

Findings categorized by

- By bucket
- By type
- By job

Detailed and actionable security and sensitive data discovery findings

- Findings sent to CloudWatch Events
- Bucket policy findings sent to Security Hub

Automate and Take Actions – Manage and Automate

Export findings to S3 bucket

- Show classifications

Automated actions on alerts

- Simplify with Lambda

Management APIs

- Integrate with additional services
- CloudTrail captures all API calls for Macie as events

Questions?

Thank you

https://aws.amazon.com/security/
https://aws.amazon.com/compliance/
https://aws.amazon.com/products/security

@AWSSecurityInfo
@AWSIdentity