Fundamentals of Data Protection on AWS

How can I keep my data confidential?

How do I know my data and resources are trustworthy?

How do I keep control of my personal data?

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**

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 Enable **KMS multi-Region keys for disaster recovery** and expansion to global AWS Regions

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

Data Protection Journey

ADVANCED

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

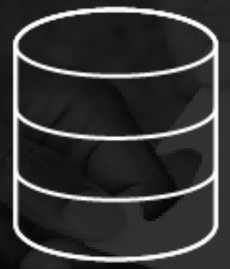
2 Activate **AWS Private CA** to secure Kubernetes pods and manage certificates at scale

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

How are customers using Data Protection?

Migrate workloads securely from on-premise to the cloud



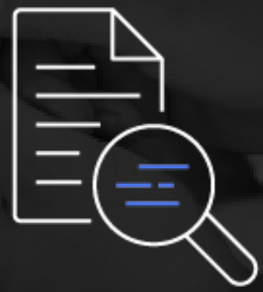
Encrypt cloud storage and databases

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