

AWS Advanced Data Protection



Secure workloads across hybrid clouds including Amazon Web Services

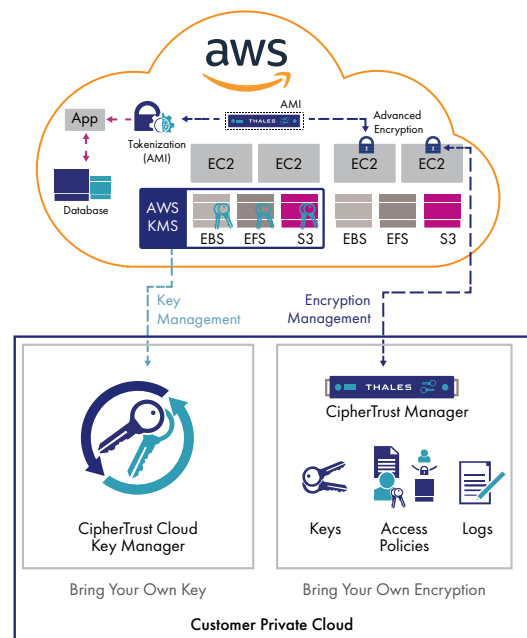
Amazon Web Services (AWS) can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices, for protecting data. Further, you need rapid data mobility across all clouds you currently use and those in your future, a need which can be compromised with cloud-vendor-specific encryption solutions.

- Identify attacks faster with data access logging to industry-leading SIEM applications
- Reduce or eliminate risks arising from compromised credentials with advanced encryption including privileged user access controls
- Architect applications for the cloud with built-in security using Vaultless Tokenization with Dynamic Data Masking

Advanced data protection for AWS

Effective, secure cloud use involves an increasing number of decisive moments, such as when you consider using sensitive data in any cloud. You can rely on Thales to secure your digital transformation. Thales Data Discovery and Classification, advanced encryption and centralized key management solutions give you protection and control of data stored on your premises, Amazon Web Services, and other cloud providers. Thales technology enables you to:

- Avoid cloud vendor encryption lock-in and ensure the data mobility you need while you efficiently and securely spread workloads and data across multiple cloud vendors, including AWS, with centralized, independent encryption management
- Take secure advantage of Amazon Key Management Services (AWS KMS) with a centralized key management solution that spans multiple clouds



Data Discovery and Classification

[CipherTrust Data Discovery and Classification](#) locates regulated data in AWS, other clouds and on-premises across many different types of data stores, include AWS block storage offerings and AWS S3. It offers a quick start with a full set of built-in classification templates with centralized operations on [CipherTrust Manager](#). The product enables informed decision making about what and how to protect data in AWS.

Advanced encryption for Amazon Web Services and beyond

If you're 100% Amazon Web Services-based with stringent data security controls, or if you're running hybrid clouds with data distributed across your on-premises private cloud, multiple cloud providers, and on AWS, you need an advanced data encryption solution. [CipherTrust Transparent Encryption](#) protects your files and databases on your premises and across multiple clouds including AWS, without any changes to applications, databases, infrastructure or business practices. You can [bring your own encryption](#) to AWS and other infrastructure- and platform-as a service providers!

CipherTrust Transparent Encryption:

- Protects data stored in AWS S3 buckets for any S3 data source, operating in AWS, another cloud, or on-premises, that is using S3 protocols and equipped with a Transparent Encryption agent
- Strengthens data security with operating system-level controls against unauthorized access based on granular access policies, including user identity (including for administrators with root privileges), and process, among many others
- Accelerates breach detection and satisfies compliance mandates with detailed file access logs, directed to your security information and event management (SIEM) system

Delivers a fast return on investment with a non-intrusive, flexible implementation. Encryption agents operate on AWS EC2 compute instances or any other server accessing storage, protect EBS, EFS and S3 storage, and are available for many Windows versions and Linux distributions, including Amazon Linux

Centralized, secure key management

CipherTrust Manager centralizes key, policy and log management for CipherTrust Transparent Encryption, and is available in various hardware models for on-premises deployment, or can be instantiated as a shared AWS AMI.

Accelerated PCI-DSS compliance

[CipherTrust Tokenization with Dynamic Data Masking](#) secures and anonymize sensitive assets in the data center, big data environments or the cloud for simplified PCI-DSS compliance. Format-preserving or random tokenization protects sensitive fields while maintaining database structure, for a non-disruptive implementation. Then, it's easy to add policy-based dynamic data masking to applications.

The CipherTrust Tokenization Server is available as a shared AWS AMI.

Multicloud BYOK management

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager.

The CipherTrust Cloud Key Manager leverages cloud provider Bring Your Own Key (BYOK) API's to reduce key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility. The solution is available as a shared AWS AMI, or can be deployed on premises or in any supported private cloud deployment to meet more stringent compliance requirements.

CipherTrust Cloud Key Manager offers the following advantages:

- Enhanced IT efficiency with multi-cloud key management from a single console that offers automated key rotation and comprehensive key life cycle management
- Safer key management practices combined with cloud benefits of scale, cost and convenience
- Greater control over keys—you can control key generation and storage of keys used in AWS KMS, Microsoft Azure the Google Cloud Platform Customer Managed Encryption Key (CMEK) Service and more!

Fulfill your data protection requirements

Thales simplifies securing Amazon Web Services workloads and helps achieve compliance with data security regulations. Ciphertrust Data Security Platform products operate seamlessly on workloads in AWS and on your premises delivering centralized policy and key management, and Thales multi-cloud key management brings you into compliance with best practices and data protection mandates.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.