Solution Brief

Advanced Data Protection for AWS Infrastructure

Secure workloads across hybrid clouds including Amazon Web Services.

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Amazon Web Services (AWS) provides cutting edge cloud services with benefits including scalability and high performance, reliability, cost-effectiveness, flexibility, ease of use, etc. Due to the nature of the cloud (outsourced, international services), cloud customers need to take their share of responsibility when processing workload and data in the cloud. To do so, analysts, certification schemes, and growing regulation frameworks state that cloud customers must define their own policies and enforce them using third-party tools to achieve better visibility, data security, threat protection, and compliance.

To that effect, cloud user-controlled data security is essential to mitigate cyberthreats on data, enforce data management and governance, or address key cyber resilience and compliance mandates. This document explores how cloud customers can maximize the benefits of AWS cloud services, while remaining in control using Thales solutions integrated and based on capabilities offered by AWS.

Overview - Comprehensive 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 solutions give you protection and control of data stored on your premises, on AWS, and with other cloud providers. Thales technology enables you to:

- Take full benefit from AWS cloud infrastructure, platform and software services while keeping control by combining Amazon Key Management Services (AWS KMS) and external key store (AWS XKS) with your own centralized key management solution.
- Increase the confidentiality of sensitive data with role/attribute-based encryption, managed centrally outside the cloud.
- Extra benefits include end-to-end encryption for secure data transfer from/to on-premises infrastructure and storage, from one subscription to another, or across multiple clouds.
- Identify attacks faster with data activity monitoring and AI-based data risk analytics, feeding into 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 data security using Vaultless Tokenization with Dynamic Data Masking, or API data protection gateway. Apply application security such as DDoS, Web Application Firewall, and Bot protection.

Advanced Encryption for AWS 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 and HYOK Management

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using CipherTrust Cloud Key Management. CipherTrust Cloud Key Management leverages cloud provider Bring Your Own Key (BYOK) APIs 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. AWS External Key Store (XKS) in AWS Key Management Service (KMS) that allows customers to protect their data in AWS using encryption keys held inside CipherTrust Manager or Luna Network HSMs external to AWS. The benefits include the ability to move critical workloads to the cloud, maintain sovereign control of sensitive data, and gain strong key control and security.

CipherTrust Secrets Management

CipherTrust Secrets Management is a state-of-the-art Secrets Management solution, powered by the Akeyless, which protects and automates access to secrets across DevOps tools and cloud workloads including credentials, certificates, API keys, and tokens.

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.

High Speed Encryption

Thales Network Encryption solutions provide customers with a single platform to encrypt everywhere — from network traffic between data centers and the headquarters to backup and disaster recovery sites, whether on premises or in the cloud. Rigorously tested and certified, our Network Encryption solutions have been vetted by such organizations as the Defense Information Systems Agency (DISA UC APL) and NATO.

payshield Cloud HSM

payShield Cloud HSM, an IaaS offering from Thales, is an alternative way to fulfill your payment security needs, offering your organization a more agile and faster rollout solution for payment security compared to the traditional on-prem ownership model – it shifts the risk of running a payment HSM infrastructure from you to Thales.

Identity and Access Management

OneWelcome Identity Platform provides a variety of capabilities from identity verification, single sign-on, passwordless and multi-factor authentication to fraud management, adaptive access, dynamic authorization and consent & preference management for the highest levels of assurance. More than 30,000 organizations trust us with their IAM and data security needs, enabling them to deliver secure digital services to their users.

Imperva Data Security Fabric

Imperva Data Security Fabric (DSF) enables security and compliance teams to quickly and easily secure sensitive data no matter where it resides with an integrated, proactive approach to visibility and predictive analytics. Imperva DSF hybrid cloud, data-centric solution is designed to secure all data types, protect the data estate from data breaches, and drastically reduce time spent managing compliance and privacy.

Imperva Application Security

Imperva Application Security mitigates risk for your business with full-function defense-in-depth, providing protection wherever you choose to deploy - in the cloud, on-premises, or via a hybrid model. Imperva offers advanced analytics to quickly identify the application threats that matter, DDoS protection with a 3-second mitigation SLA, a developer-friendly Content Delivery Network (CDN) for the utmost performance, Web Application Firewall (WAF) solutions, bot protection, Runtime Application Self-Protection (RASP) for security embedded into the application itself, and more.

Fulfill 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

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.