

# Thales eSecurity Lösungen für Amazon Web Services



## Sichern Sie Workloads über Hybrid Clouds hinweg, inklusive Amazon Web Services

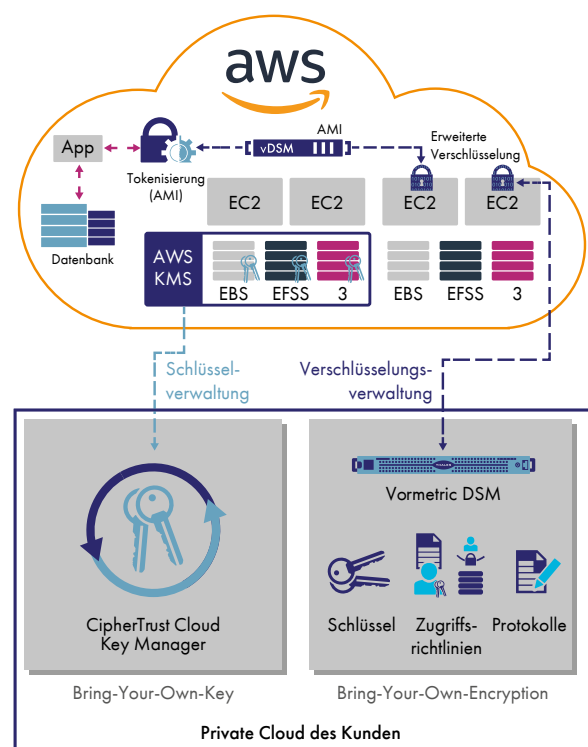
IT-Workloads in Amazon Web Services (AWS) können Vorteile und Kosteneinsparungen bieten. Dennoch müssen Sie auch weiterhin Regeln im Hinblick auf Sicherheit, Datenschutz und Compliance sowie Best Practices zum Schutz Ihrer Daten befolgen. Darüber hinaus benötigen Sie rasche Datenmobilität über alle Clouds hinweg, die Sie derzeit und in Zukunft nutzen. Eine Anforderung, die durch spezifische Verschlüsselungslösungen des Cloud-Anbieters eingeschränkt werden kann.

## Erweiterte Verschlüsselungslösungen mit umfangreicher Schlüsselverwaltung

Wenn Sie Cloud-Dienste effektiv und sicher einsetzen wollen, stehen Sie immer häufiger vor Entscheidungen, z. B. wenn Sie in Betracht ziehen, sensible Daten in einer beliebigen Cloud zu verwenden. Vertrauen Sie bei der Sicherung Ihrer digitalen Transformation auf Thales. Mit den Lösungen für erweiterte Verschlüsselung und Schlüsselverwaltung von Thales schützen und kontrollieren Sie Ihre on-premises sowie bei Amazon Web Services und anderen Cloud-Anbietern gespeicherten Daten. Mit der Technologie von Thales:

- Vermeiden Sie vom Cloudanbieter abhängige Verschlüsselung und gewährleisten Sie die erforderliche Datenmobilität, während Sie gleichzeitig Workloads und Daten durch zentrale, unabhängige Verschlüsselungsverwaltung effizient und sicher auf verschiedene Cloud-Anbieter wie Amazon Web Services verteilen
- Nutzen Sie auf sichere Weise die Vorteile des Schlüsselverwaltungs-Dienstes von Amazon (AWS KMS) mit einer Cloud-übergreifenden Lösung für die zentrale Schlüsselverwaltung

- Erkennen Sie Angriffe schneller dank Datenzugriffs-Protokollierung zu branchenführenden SIEM-Anwendungen.
- Reduzieren oder beseitigen Sie Risiken im Zusammenhang mit kompromittierten Zugangsdaten durch erweiterte Verschlüsselung, einschließlich Kontrollen von privilegierten Benutzerzugriffen.
- Erstellen Sie Anwendungen für die Cloud mit integrierter Sicherheit durch Vaultless Tokenization mit dynamischer Datenmaskierung



# Erweiterte Verschlüsselung für Amazon Web Services und darüber hinaus

Ob Sie mit strikten Datensicherheitskontrollen zu 100 % in Amazon Web Service arbeiten oder Hybrid-Clouds betreiben und Ihre Daten auf die private Cloud vor Ort, verschiedene Cloud-Anbieter und AWS verteilt haben – Sie benötigen eine erweiterte Lösung für die Datenverschlüsselung. Vormetric Transparent Encryption schützt Ihre Dateien und Datenbanken vor Ort und in einer Vielzahl von Clouds wie etwa AWS, ohne dass Sie Ihre Anwendungen, Datenbanken, Infrastruktur oder Geschäftsprozesse ändern müssen.

## Vormetric Transparent Encryption:

- Stärkt die Datensicherheit mit Kontrollen der operativen Systemebene zum Schutz vor nicht autorisierten Zugriffen, basierend auf granularen Zugriffsrichtlinien, darunter die Benutzeridentität (auch für Administratoren mit Root-Privilegien), Prozesse und viele weitere.
- Beschleunigt die Erkennung von Datenschutzverletzungen und erfüllt Compliance-Anforderungen mit detaillierter Dateizugriffsprotokollierung, die an Ihr SIEM-System (Security Information and Event Management) weitergeleitet wird.
- Ihre Investition macht sich dank einer flexiblen Implementierung, die nicht in die bestehende Infrastruktur eingreift, schnell bezahlt. Verschlüsselungsagenten werden auf AWS-EC2-Recheninstanzen oder anderen auf Server zugreifenden Speicherorten betrieben, schützen EBS-, EFS und S3-Speicherung und sind für zahlreiche Windows-Versionen und Linux-Distributionen verfügbar.

## Zentrale, sichere Schlüsselverwaltung

Der Vormetric Data Security Manager zentralisiert die Verwaltung von Schlüsseln, Richtlinien und Protokollen für Vormetric Transparent Encryption, verfügbar als FIPS-140-2-Level 2- oder 3-Anwendung oder als virtuelle FIPS-140-2-Level-1-Anwendung. Mit der physischen Anwendung können Ihre Standorte vor Ort Verschlüsselungsagenten weltweit über jeden beliebigen Cloud-Anbieter verwalten. Die virtuelle Anwendung ist in vielen Virtualisierungsformaten wie VMware und KVM sowie als Amazon Web Services AMI und auf dem Microsoft Azure Marketplace erhältlich.

## Beschleunigte PCI-DSS-Compliance

Vormetric Tokenisierung mit dynamischer Datenmaskierung schützt und anonymisiert sensible Assets im Rechenzentrum, in Big Data-Umgebungen oder in der Cloud und erleichtert so die PCI-DSS-Compliance. Formaterhaltende oder zufällige Tokenisierung schützt sensible Felder bei gleichzeitiger Beibehaltung der Datenbankstruktur und ermöglicht so eine reibungslose Umsetzung. Dann kann ganz einfach auf Richtlinien basierende dynamische Datenmaskierung zu Anwendungen hinzugefügt werden.

Der Vormetric Tokenization Server ist als gemeinsame AWS AMI erhältlich.

# Verwaltung kryptographischer Schlüssel in AWS

Unternehmen, die keine eigene Verschlüsselung mitbringen können, können dennoch den Best Practices der Branche folgen, indem sie Schlüssel mit dem CipherTrust Cloud Key Manager extern verwalten.

Der CipherTrust Cloud Key Manager nutzt Bring Your Own Key (BYOK) APIs von Cloud-Anbietern. Dies reduziert die Komplexität der Schlüsselverwaltung sowie die Betriebskosten, da der Kunde die kryptographischen Schlüssel über den gesamten Lebenszyklus zentral und transparent verwaltet. Der CipherTrust Cloud Key Manager kann „as-a-Service“ bereitgestellt werden und ist damit rasch einsetzbar. Er ist als geteilte AWS AMI verfügbar, kann aber auch on-premises oder in einer unterstützten privaten Cloud bereitgestellt werden, um strengere Compliance-Vorgaben zu erfüllen.

Der CipherTrust Cloud Key Manager bietet die folgenden Vorteile:

- Sicherere Verfahren zur Schlüsselverwaltung, kombiniert mit den Vorteilen der Cloud in Bezug auf Skalierbarkeit, Kosten und Komfort
- Mehr Kontrolle über Ihre Schlüssel – Sie kontrollieren die Erstellung und Speicherung von Schlüsseln, die für AWS KMS, Microsoft Azure und weitere Dienste genutzt werden!
- Verbesserte IT-Effizienz durch Multi-Cloud-Schlüsselverwaltung über eine einzige Konsole, die eine automatisierte Schlüsselrotation und ein umfassendes Life Cycle Management für die Schlüssel bietet

## Erfüllen Sie Ihre Datenschutzanforderungen

Thales eSecurity vereinfacht den Schutz Ihrer Workloads in Amazon Web Services und hilft Ihnen dabei, die Datensicherheitsbestimmungen zu erfüllen. Die Produkte der Vormetric Data Security Platform funktionieren nahtlos mit Workloads in AWS und an Ihren Standorten und ermöglichen die zentrale Verwaltung von Richtlinien und Schlüsseln. Mit den Multi-Cloud-Schlüsselverwaltungslösungen von Thales eSecurity befolgen Sie Best Practices und halten Datenschutzanforderungen ein.

## Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit werden Unternehmen immer häufiger mit entscheidenden Momenten konfrontiert. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.

> [thalesecurity.com](https://thalesecurity.com) <



**Americas** – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel.: +1 888 744 4976 oder +1 954 888 6200 • Fax: +1 954 888 6211 • E-Mail: [sales@thalessec.com](mailto:sales@thalessec.com)  
**Asia Pacific** – Thales Transport & Security (HK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hongkong • Tel.: +852 2815 8633 • Fax: +852 2815 8141 • E-Mail: [asia.sales@thales-esecurity.com](mailto:asia.sales@thales-esecurity.com)  
**Europa, Naher Osten, Afrika** – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel.: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-Mail: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)