THALES

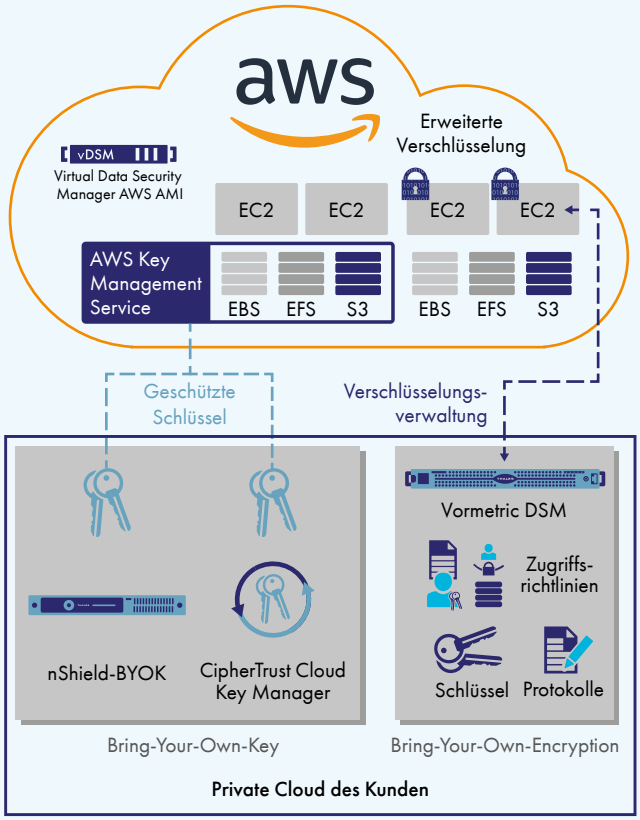
www.thalesesecurity.com

ERWEITERTE VERSCHLÜSSELUNG MIT UMFANGREICHER SCHLÜSSELVERWALTUNG

- Vermeiden Sie anbieterabhängige 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 mit Cloud-übergreifenden Lösungen für die zentrale Schlüsselverwaltung.
- Erkennen Sie Angriffe schneller durch Datenzugriffs-Protokollierung zu branchenführenden SIEM-Anwendungen.
- Reduzieren oder beseitigen Sie Risiken im Zusammenhang mit kompromittierten Zugangsdaten durch erweiterte Verschlüsselung einschließlich Kontrollen von privilegierten Benutzerzugriffen.

‹Thales eSecurity›

THALES eSECURITY LÖSUNGEN FÜR AMAZON WEB SERVICES



Sichern Sie Workloads in Hybrid Clouds wie Amazon Web Services

IT-Workloads in Amazon Web Services (AWS) bieten Vorteile und Kosteneinsparungen. Sie müssen jedoch 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. Die Thales eSecurity Lösungen helfen Ihnen, diesen Anforderungen gerecht zu werden. Mithilfe von Bring-Your-Own-Encryption (BYOE) mit erweiterten Funktionen und zentraler Schlüsselverwaltung können Sie die vor Ort, in Amazon Web Services oder bei anderen Cloud-Anbietern gespeicherten Daten schützen und kontrollieren.

Kunden, die den Schlüsselverwaltungsdienst von AWS nutzen, können mehrere Optionen zur Schlüsselverwaltung von Thales eSecurity einsetzen, die allesamt sicherstellen, dass die Best Practices der Industrie sowie die gängigen Compliance-Anforderungen hinsichtlich der Datensicherheit erfüllt werden.

‹Thales eSecurity›

THALES eSECURITY LÖSUNGEN FÜR AMAZON WEB SERVICES

ERWEITERTE VERSCHLÜSSELUNG FÜR AMAZON WEB SERVICES UND DARÜBER HINAUS

Wenn 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, benötigen Sie 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 Microsoft Azure Marketplace erhältlich.

VERWALTUNG KRYPTOGRAPHISCHER SCHLÜSSEL IN AWS

Unternehmen, die keine eigene Verschlüsselung mitbringen können, können dennoch den Best Practices der Industrie folgen, indem sie Schlüssel mit dem **CipherTrust Cloud Key Manager** oder Thales **nShield Bring Your Own Key (BYOK)** extern verwalten.

- Der CipherTrust Cloud Key Manager nutzt APIs (Application Programming Interfaces – Anwendungsprogrammierschnittstellen) von Cloud-Anbietern zur Schlüsselsteuerung. Dies reduziert die Komplexität der Schlüsselverwaltung sowie die Betriebskosten, da der Kunde die kryptographischen Schlüssel über den gesamten Lebenszyklus zentral und transparent verwaltet. CipherTrust Cloud Key Manager kann „as-a-Service" bereitgestellt werden und ist nahezu sofort einsetzbar. Aber auch eine Bereitstellung vor Ort ist möglich, um strengere Compliance-Vorgaben zu erfüllen.
- Thales nShield Hardware-Sicherheitsmodule (HSM) ermöglichen es Ihnen, Ihre eigenen Schlüssel in AWS zu verwenden, und sind in drei Formfaktoren erhältlich: Dem Netzwerk beigefügt, als PCIe-Karte und über USB angeschlossen. Je nach den Anforderungen Ihrer Anwendungen und Ihrem Bedarf in Bezug auf die Leistung können Sie den für Sie optimalen Formfaktor wählen.

Sowohl CipherTrust Cloud Key Manager als auch nShield BYOK bringen folgende 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!
- Einheitliche lokale Schlüsselverwaltung für führende Anbieter von Public Clouds.

ERFÜLLEN SIE IHRE DATENSCHUTZANFORDERUNGEN

Thales eSecurity vereinfacht den Schutz Ihrer Workloads in Amazon Web Services und hilft Ihnen dabei, die Datensicherheits-bestimmungen 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 Schlüsselverwaltungslösungen für die Cloud von Thales eSecurity befolgen Sie Best Practices und halten Datenschutzanforderungen ein.

WEITERE INFORMATIONEN

Besuchen Sie uns unter **www.thalesesecurity.com** und erfahren Sie, wie unsere erweiterten Datensicherheitslösungen und -dienste überall dort Vertrauen schaffen, wo Informationen erstellt, geteilt oder gespeichert werden.

Folgen Sie uns auf:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel.:+1 888 744 4976 oder +1 954 888 6200 • Fax:+1 954 888 6211 • E-Mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, 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
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