thalesgroup.com

THALES

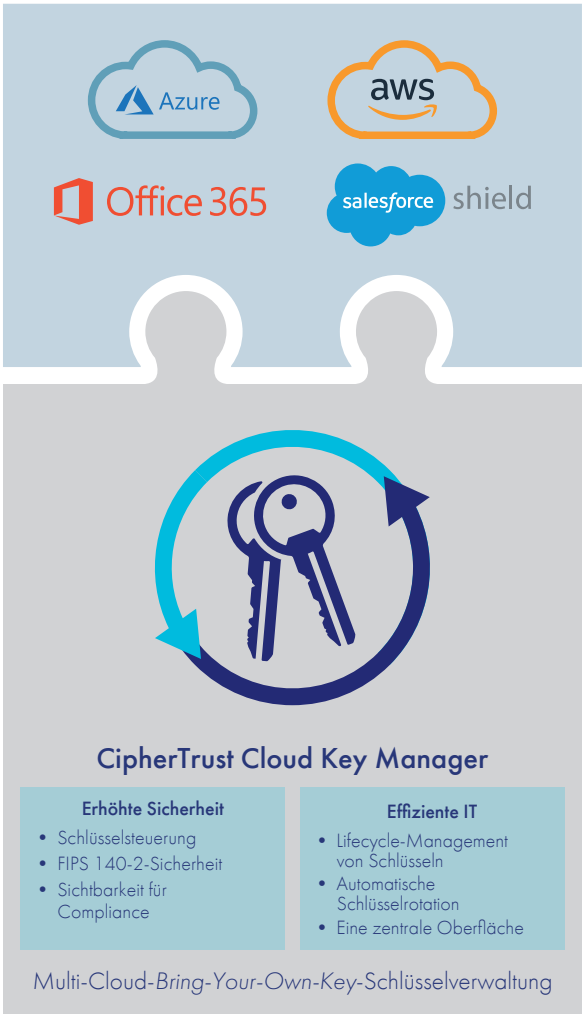
CipherTrust Cloud Key Manager

Viele Anbieter von Infrastructure-, Platform- und Software-as-a-Service stellen Data-at-Rest-Verschlüsselung zur Verfügung, bei der die kryptographischen Schlüssel vom Anbieter verwaltet werden. Allerdings fordern viele branchenspezifische oder interne Datenschutzvorschriften sowie die durch die Cloud Security Alliance definierten Best Practices der Branche, dass Schlüssel separat vom Anbieter von Cloud-Diensten sowie den dazugehörigen Verschlüsselungsverfahren gespeichert und verwaltet werden sollten. Anbieter können diese Anforderungen erfüllen, indem sie „Bring-your-own-Key" (BYOK) anbieten. Damit kann der Kunde die Schlüssel, die er zur Verschlüsselung seiner Daten verwendet, selbst verwalten. Die Schlüsselverwaltung durch den Kunden ermöglicht die Trennung, Erstellung, den Besitz und die Steuerung – inklusive Sperrung – von kryptographischen Schlüsseln oder von Nutzergeheimnissen, die zur Erstellung dieser Schlüssel verwendet wurden.

Der CipherTrust Cloud Key Manager nutzt Bring Your Own Key (BYOK) API's 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.

Übernehmen Sie die Kontrolle über Ihre kryptographischen Schlüssel für die Cloud

- Steigern Sie den Nutzen Ihrer „Bring-your-own-Key"-Dienste durch Verwaltung Ihrer kryptographischen Schlüssel für die Cloud über den gesamten Lebenszyklus.
- Erfüllen Sie die strengsten Datenschutzvorschriften dank zertifizierter Schlüsselprogrammierung und -speicherung von bis zu FIPS-140-2-Level 3.
- Erhöhen Sie die Effizienz Ihrer IT durch zentrale Schlüsselverwaltung über mehrere Cloud-Umgebungen hinweg, automatisierte Schlüsselrotation und Verwaltung der Ablaufdaten von Schlüsseln.



Das Schlüsselsteuerungsgebot

Die Anforderung, sensible Daten in Umgebungen wie Infrastructure-, Platform- und Software-as-a-Service (IaaS, PaaS, SaaS) zu schützen, hat zu einem breiteren Verschlüsselungsangebot von Cloud Anbietern geführt. Allerdings empfehlen die Cloud Security Alliance und Branchenanalysten, dass kryptographische Schlüssel vom Kunden verwaltet werden sollten. Die Herausforderungen der Schlüsselverwaltung steigen mit der hundertfachen Anzahl von Masterschlüsseln pro Abonnement, die gesichert und über verschiedene Clouds verwaltet werden müssen. Außerdem ist es unerlässlich, zu wissen, wie, wann und von wem kryptographische Schlüssel genutzt werden. CipherTrust Cloud Key Manager erfüllt die Anforderungen einer sicheren, umfangreichen Schlüsselverwaltung über verschiedene Clouds hinweg.

Zu den unterstützten Clouds gehören:

- Microsoft Azure
- Microsoft Office365
- Microsoft Azure Stack
- Azure China und Azure Deutschland Nationale Clouds
- Amazon Web Services
- Salesforce.com
- Salesforce Sandbox

Hohe Sicherheit für kryptographische Schlüssel

Schlüsselsteuerung durch den Kunden fordert eine sichere Schlüsselerstellung und -speicherung. CipherTrust Cloud Key Manager nutzt die Sicherheit des Vormetric Data Security Manager, SafeNet KeySecure oder unterstützter Hardware-Sicherheitsmodule (HSM), um Schlüssel zu erzeugen und mit FIPS-140-2-Sicherheit zu speichern. Aufgrund der Notwendigkeit von Schlüsselsicherheitsmechanismen, beispielsweise der sicheren Speicherung von Cloud-Backup-Schlüsseln, agiert CipherTrust Cloud Key Manager als Schlüsselhinterlegung für unterstützte Clouds und ermöglicht vollständige Kontrolle über Schlüssel-Metadaten sowohl während des Uploads als auch für Schlüssel in Verwendung.

Effizientere IT

CipherTrust Cloud Key Manager bietet verschiedene Möglichkeiten an, die IT-Effizienz zu steigern:

- Zentrale Schlüsselverwaltung gibt Ihnen Zugang zu jedem Cloud-Anbieter von einem einzigen Browserfenster aus, auch über mehrere Konten und Abonnements hinweg
- Automatisierte Schlüsselrotation bietet IT-Effizienz und erhöhte Datensicherheit
- Federated Login bietet einen einfachen Mechanismus für die Gewährung des Zugangs zu Schlüsseldaten. Anmeldungen bei einem Cloud-Dienst werden vom Anbieter authentifiziert und autorisiert – es ist keine Login-Datenbank oder AD- bzw. LDAP-Konfiguration notwendig
- Für Workloads, die dies erfordern, kann CipherTrust Cloud Key Manager die Erstellung nativer Schlüssel beim Cloud-Anbieter beantragen und ein vollständiges Lifecycle-Management dafür bieten
- Bei Vorhandensein unterschiedlicher Schlüsseltechnologien und -terminologien präsentiert CipherTrust Cloud Key Manager die Schlüsselvorgänge in der Semantik des Cloud-Anbieters
- Sie haben bereits tausende Schlüssel bei Ihrem Cloud-Anbieter erstellt? Der CipherTrust Cloud Key Manager synchronisiert seine Datenbank mit den beim Cloud-Anbieter erstellten Schlüsseln

Die Compliance-Tools, die Sie benötigen

Cloud-spezifische CipherTrust-Cloud-Key-Manager-Protokolle und vorkonfigurierte Berichte bieten schnelle Compliance-Berichterstattung. Protokolle können auch an einen syslog-Server oder SIEM gerichtet werden.

Optionen für die Implementierung, die Ihren Anforderungen entsprechen

CipherTrust Cloud Key Manager bietet verschiedene zweckmäßige Optionen der Implementierung um Ihre Sicherheits- und Bereitstellungsanforderungen zu erfüllen:

- Die gesamte Software ist mit FIPS 140-2 Level 1 zertifizierter Schlüsselsicherheit erhältlich. Die CipherTrust Cloud Key Manager Virtual Appliances und entweder die Data Security Manager oder KeySecure Virtual Appliances können in Amazon Web Services oder Microsoft Azure instanziiert werden, oder in jeder Public oder Private Cloud, die VMware einsetzt, bereitgestellt werden.
- Kunden, die FIPS 140-2 Level 3 oder 2 benötigen, können entweder bestehende Vormetric Data Security Manager nutzen oder bereitstellen oder unterstütze HSMs in on-premises oder gehosteteten Datenzentren verwenden.

Multi-Cloud-Datensicherheitslösungen

CipherTrust Cloud Key Manager vereinfacht die notwendige Verwahrung und Verwaltung von kryptographischen Schlüsseln für Cloud-Dienste und bietet so eine entscheidende Lösung, mit der Sie branchenspezifische und unternehmensinterne Datenschutzvorgaben erfüllen können. Die Multi-Cloud-Sicherheitsprodukte von Thales wie Bring-Your-Own-Advanced-Encryption in Kombination mit zentraler FIPS-zertifizierter Schlüsselverwaltung ermöglichen es Ihnen, Ihre Cloud-Speicherung zu verschlüsseln und steuern. So reduzieren Sie die Gefahr, dass sensible Daten offengelegt werden.

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.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • 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, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 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