THALES

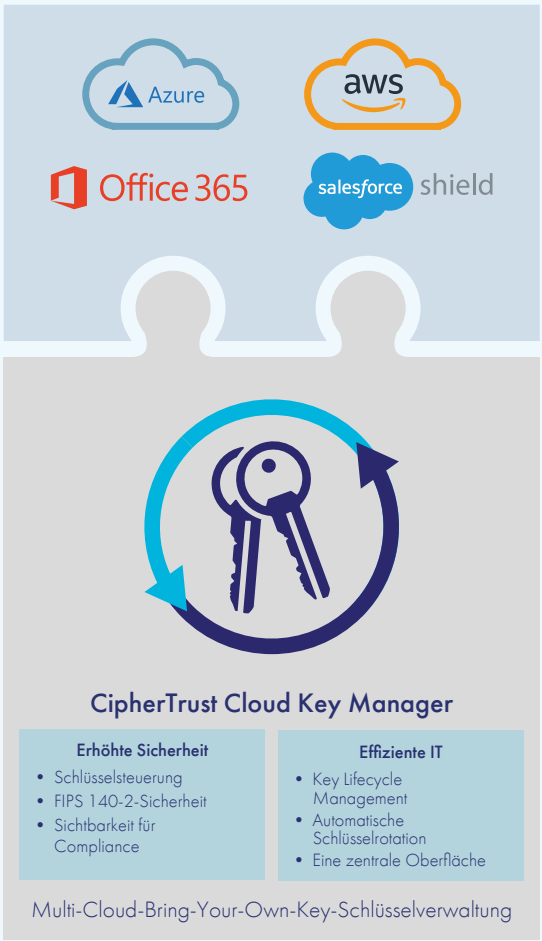
www.thalesesecurity.com

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.
- Wählen Sie zwischen Bereitstellung „as-a-Service" oder „vor Ort".

‹Thales eSecurity›

CIPHERTRUST CLOUD KEY MANAGER VON THALES



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 bzw. von Nutzergeheimnissen, die zur Erstellung dieser Schlüssel verwendet werden.

CipherTrust Cloud Key Manager nutzt APIs (Application Programming Interfaces – Anwendungsprogrammier-Schnittstellen) 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.

CIPHERTRUST CLOUD KEY MANAGER

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 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 Anmeldung, die sich in verschiedenen Clouds befinden. 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 in verschiedenen Clouds. Zu den unterstützten Clouds gehören:

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

HOHE SICHERHEIT FÜR KRYPTOGRAPHISCHE SCHLÜSSEL

Schlüsselsteuerung durch den Kunden fordert eine sichere Schlüsselerstellung und -speicherung. CipherTrust Cloud Key Manager nutzt die Sicherheit von **Vormetric Data Security Manager**- oder **Thales nShield Connect**-Hardware-Sicherheitsmodulen, um Schlüssel mittels fortschrittlicher Zufallszahlengenerierung 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 Treuhanddienst 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 Anmeldungen hinweg.
- Automatisierte Schlüsselrotation bietet IT-Effizienz und erhöhte Datensicherheit
- Federated Login bietet einfache Mechanismen 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 Schlüsselerstellung beim Cloud-Anbieter beantragen und ein vollständiges Lifecycle-Management dafür anbieten
- 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 (Verwaltung von Sicherheitsdaten und -ereignissen) gerichtet werden.

SOFTWARE-AS-A-SERVICE

CipherTrust Cloud Key Manager as-a-Service ist eine einfache Cloud-basierte Lösung, die gleichzeitig die Kontrolle bietet, die für die Erfüllung sowohl interner als auch branchenspezifischer Compliance-Anforderungen erforderlich ist. Mit dem „as-a-Service"-Modell ist es nicht länger erforderlich, eine hochverfügbare Cloud-Schlüsselverwaltung vor Ort zu entwerfen, bereitzustellen und zu pflegen. Schlüssel werden stattdessen in einer virtuellen Anwendung mit FIPS 140-2 Level-1-Zertifizierung gespeichert.

OPTIONEN FÜR DIE BEREITSTELLUNG VOR ORT

CipherTrust Cloud Key Manager ist überdies in Formfaktoren erhältlich, die für eine Reihe von Vor-Ort-Bereitstellungsoptionen mit einer Schlüsselsicherheit bis FIPS 140-2 Level 3 geeignet sind. Außerdem sind virtuelle Anwendungen im Azure Marketplace und für Amazon Web Services sowie VMware verfügbar.

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 eSecurity 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.

WEITERE INFORMATIONEN

Besuchen Sie uns auf **www.thalesesecurity.com** und erfahren Sie, wie unsere erweiterten Datensicherheitslösungen 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