THALES

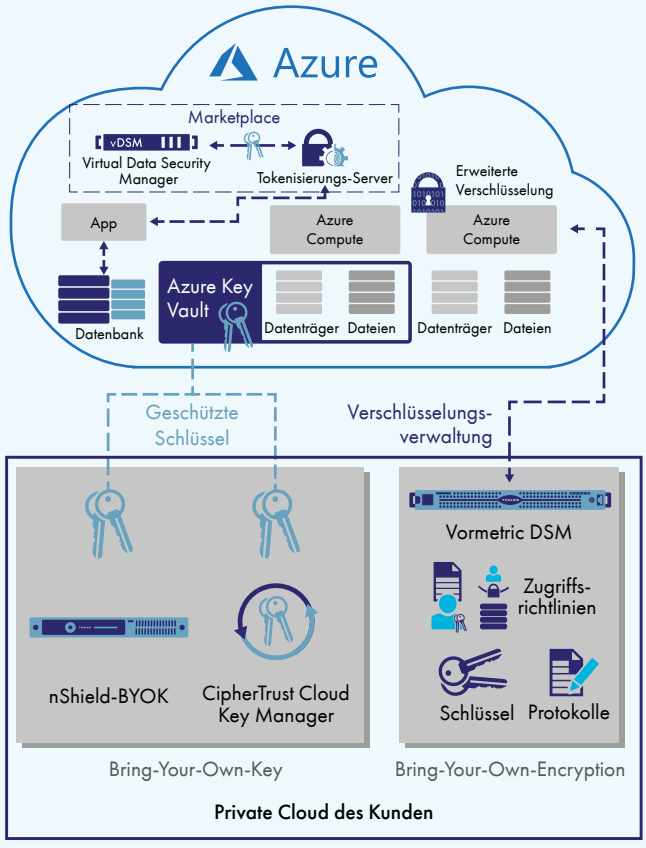
www.thalesesecurity.com

ERWEITERTE VERSCHLÜSSELUNG MIT UMFANGREICHER SCHLÜSSELVERWALTUNG

- Vermeiden Sie vom Anbieter abhängige Verschlüsselung und gewährleisten Sie die erforderliche Datenmobilität, während Sie gleichzeitig Workloads und Daten effizient und sicher auf verschiedene Cloud-Anbieter wie Microsoft Azure auslagern – durch zentrale, unabhängige Verschlüsselungsverwaltung.
- Nutzen Sie auf sichere Weise die Vorteile von Azure Key Vault mit zentralisierten Schlüsselverwaltungs-Lösungen über mehrer Clouds hinweg.
- Erkennen Sie Angriffe schneller mit 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

‹Thales eSecurity›

THALES eSECURITY LÖSUNGEN FÜR MICROSOFT AZURE



SICHERN SIE WORKLOADS IN HYBRID-CLOUDS WIE MICROSOFT AZURE

IT-Workloads in Microsoft Azure bieten Komfort und Kosteneinsparungen. Sie müssen jedoch dennoch 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 proprietäre Verschlüsselungslösungen von Cloud-Anbietern beeinträchtigt werden kann. Thales eSecurity Lösungen helfen Ihnen mit erweiterter Verschlüsselung und zentraler Schlüsselverwaltung, diese Anforderungen zu erfüllen und bieten Ihnen Schutz und Kontrolle Ihrer bei Ihnen vor Ort und bei Microsoft Azure und anderen Cloud-Anbietern gespeicherten Daten.

Kunden, die Azure Storage-Verschlüsselung 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 MICROSOFT AZURE

ERWEITERTE VERSCHLÜSSELUNG FÜR MICROSOFT AZURE UND DARÜBER HINAUS

Ob Sie mit strikten Datensicherheitskontrollen zu 100 % in Microsoft Azure arbeiten oder Hybrid-Clouds betreiben und Ihre Daten auf die private Cloud vor Ort, verschiedene Cloud-Anbieter und Microsoft Azure verteilt haben, Sie benötigen eine erweiterte Lösung für die Datenverschlüsselung. Vormetric Transparent Encryption schützt Ihre Dateien und Datenbanken unabhängig vom Speicherort, wie etwa Microsoft Azure, ohne dass Sie Ihre Anwendungen, Datenbanken, Infrastruktur oder Geschäftsprozesse ändern müssen. Verwenden Sie Ihre eigene Verschlüsselung (Bring Your Own Encryption) für Microsoft Azure und andere Anbieter von Infrastructure-as-a-Service! Vormetric Transparent Encryption:

- Stärkt die Datensicherheit mit Kontrollen 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 schnell bezahlt dank einer flexiblen Implementierung, die nicht in die bestehende Infrastruktur eingreift. Verschlüsselungsagenten werden auf Azure-Recheninstanzen oder anderen auf Server zugreifenden Speicherorten betrieben, schützen Azure Disk und Azure Files und sind für zahlreiche Windows-Versionen und Linux-Distributionen verfügbar

ZENTRALE, SICHERE SCHLÜSSELVERWALTUNG

Der Vormetric Data Security Manager (DSM) zentralisiert die Verwaltung von Schlüsseln, Richtlinien und Protokollen für die Vormetric Transparent Encryption, verfügbar als FIPS 140-2 Level 2- oder 3-Anwendung für die Bereitstellung vor Ort oder als virtuelle FIPS 140-2 Level 1-Anwendung, etwa auf dem Azure Marketplace.

BESCHLEUNIGTE PCI-DSS-COMPLIANCE

Vormetric Tokenization 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 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 virtuelle Anwendung auf dem Microsoft Azure Marketplace verfügbar.

Folgen Sie uns auf:

VERWALTUNG KRYPTOGRAPHISCHER SCHLÜSSEL IN AZURE

Unternehmen, die keine eigene Verschlüsselung einbringen 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 – 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. Der CipherTrust Cloud Key Manager kann „as-a-Service" bereitgestellt werden und ist damit rasch einsetzbar. Er ist auf dem Microsoft Azure Marketplace verfügbar, kann aber auch vor Ort oder in einer privaten Cloud bereitgestellt werden, um strengere Compliance-Vorgaben zu erfüllen.
- Thales nShield Hardware-Sicherheitsmodule (HSM) ermöglichen es Ihnen, Ihre eigenen Schlüssel in Azure 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 Microsoft Azure, AWS KMS 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 Microsoft Azure und hilft Ihnen dabei, die Datensicherheitsbestimmungen zu erfüllen. Vormetric Transparent Encryption und Tokenisierung funktionieren nahtlos mit Workloads in Microsoft Azure und bei Ihnen vor Ort und bieten Ihnen zentrale Richtlinien- und Schlüsselverwaltung. Und die Schlüsselverwaltungslösungen für die Cloud von Thales eSecurity ermöglichen es Ihnen, den Best Practices und Vorgaben in Bezug auf den Datenschutz zu entsprechen.

WEITERE INFORMATIONEN

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

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