thalesgroup.com

THALES

Datensicherheit und -kontrolle in der Hybrid Cloud

Mit einer Hybrid-Cloud-Strategie können Unternehmen die Agilität, Kostenersparnisse und Skalierbarkeit der öffentlichen Cloud-Dienste nutzen und gleichzeitig eine private Cloud oder andere On-Premises-Infrastruktur beibehalten, um gesetzliche Vorschriften einzuhalten, Kosten zu sparen oder die IOPS-Leistung aufrechtzuerhalten.

Obwohl die meisten Cloud-Plattformen sehr sicher sind, ist es nicht immer einfach, mit den eigenen Tools und APIs wirksame Sicherheitskontrollen für Daten, die zwischen mehreren Clouds oder hybriden Systemen übertragen werden, zu gewährleisten. Das führt zu großen Lücken in Bezug auf Visibilität, Kontrolle und Kontinuität.

Wenn Ihr Unternehmen auf der Suche nach der optimalen Hybrid- oder Multi-Cloud-Strategie ist, sollten Sie sich vorab ein paar Fragen stellen:

- Haben Sie die Übersicht und Kontrolle über Ihre Cloud-Daten?
- Können Sie verhindern, dass die Cloud-Administratoren auf Ihre sensiblen Daten zugreifen?
- Wie schützen Sie Ihre Daten im Falle eines Verstoßes oder einer Vorladung?
- Können Sie die Einhaltung regulatorischer Vorschriften unabhängig überprüfen und nachweisen?

Unabhängig davon, welches Cloud-Modell und welchen Anbieter Sie nutzen – es liegt in IHRER Verantwortung, für die Sicherheit Ihrer Unternehmensdaten zu sorgen.

- Wie verwalten Sie Ihre über mehrere Anbieter und Umgebungen verteilten kryptographischen Schlüssel?
- Sind sie sich der versteckten Fallen bei der Verschlüsselung isolierter Daten bewusst?
- Erfordert die Nutzung verschiedener Cloud-Anbieter eine agnostische Einstellung zur Sicherheit?
- Haben Sie die Flexibilität, Ihre Anwendungen und Daten von einem Cloud-Dienst auf einen anderen oder von On-Premises auf die Cloud zu übertragen?

Da Cloud-Anbieter verschiedenste Dienste und Modelle anbieten, ist Ihr Unternehmen letztlich selbst dafür verantwortlich, Antworten auf diese Fragen zu finden und für die Sicherheit Ihrer Daten zu sorgen.

Treiber und Herausforderungen der Hybrid Cloud

Thales hat kürzlich untersucht, was hinter der zunehmenden Beliebtheit von Multi- und Hybrid-Cloud-Architekturen steckt. Sie bieten eine Reihe von Vorteilen, werfen aber auch Probleme auf.

Unsere Studien zeigen, dass 84 % der Unternehmen eine Multi-Cloud-Strategie übernehmen, weil Anwendungen nur mit bestimmten Clouds kompatibel sind, weil sie nicht von einem einzigen Cloud-Anbieter abhängig sein möchten, aufgrund unterschiedlicher Vorlieben verschiedener Teams (führt zum Risiko einer Schatten-IT) und natürlich auch, um Preise besser verhandeln zu können. Die Herausforderungen bei der Anwendung mehrerer Clouds sind somit klar: unterschiedliche Workflows und Verwaltungs-Tools, keine einheitliche Sicherheitsüberwachung der Anbieter, und die Risiken, die entstehen, wenn Daten mit mehreren Cloud-Anbietern geteilt werden.

Die häufigsten Gründe für einen Umstieg auf eine hybride Cloud sind erhöhte Sicherheit, Vereinfachung und Standardisierung, verbesserte IT-Agilität und die Möglichkeit, Ausgaben zu sparen und vollständig amortisierte On-Premises-IT-Ressourcen zu nutzen. Unabhängig von Cloud-Anbieter und -Modelle sind Sicherheit und Kontrolle die größten Herausforderungen im Zusammenhang mit Hybrid Cloud.

Wir sollten die Vor- und Nachteile von Multi- und Hybrid-Cloud als Gelegenheit sehen, gründlich und vorausschauend über Cloud-Sicherheit nachzudenken.

Die Sicherheit ist sowohl der wichtigste treibende Faktor als auch das größte Hindernis bei der Einführung einer Hybrid Cloud.

Lösungsansätze für Cloud-Sicherheit

Um das Potenzial der Cloud vollständig auszunutzen, müssen Sie in der Lage sein, selbstständig zu überprüfen und nachzuweisen, dass sowohl Ihre Daten als auch die Verschlüsselungscodes stets sicher sind und von Ihnen kontrolliert und überwacht werden.

Die folgenden Fragen helfen Ihnen, herauszufinden, ob die von Ihren Cloud-Diensten gebotene Sicherheit für Ihr Unternehmen ausreicht:

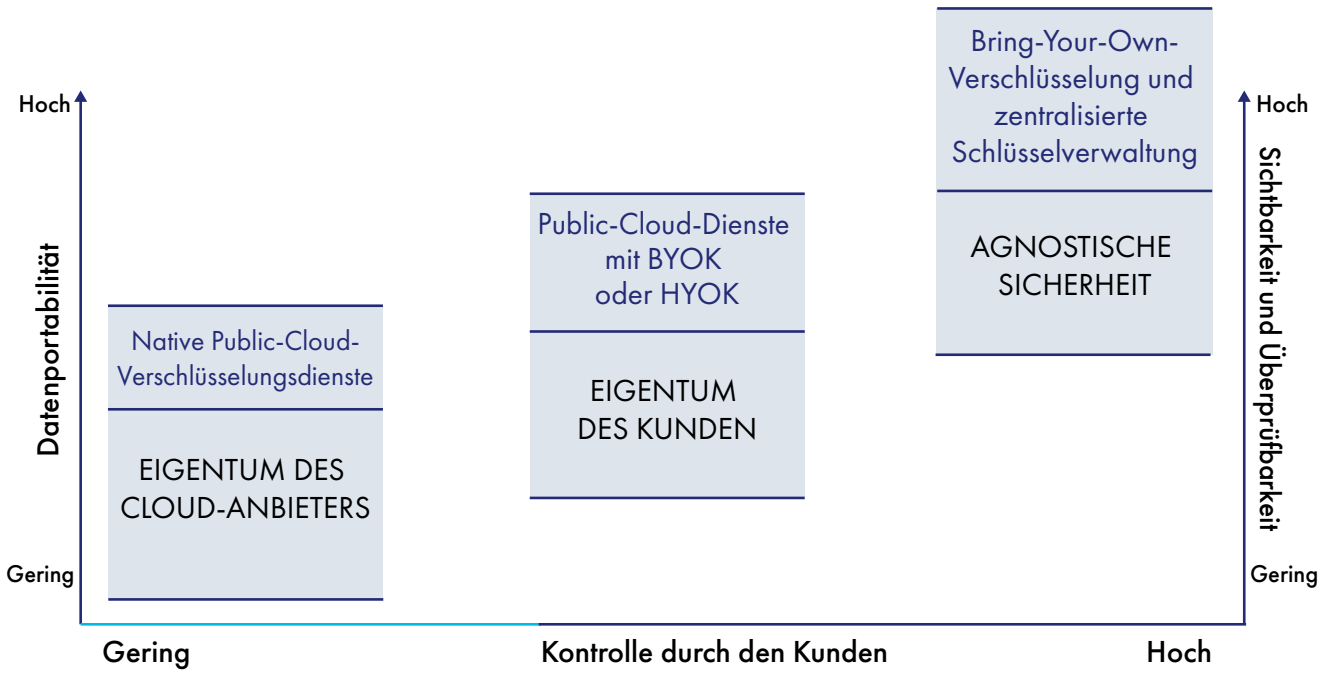
- Bietet der Cloud-Anbieter Verschlüsselung? Falls ja – Haben Sie die nötige Kontrolle und Einsicht, um die Verschlüsselungscodes zu sichern und Audits durchzuführen?
- Falls der Anbieter keine Verschlüsselung anbietet, können Sie die Daten in der Cloud selbst verschlüsseln und die Codes verwalten?

Zwischen den verschiedenen Anbietern und Anwendungsmodellen bestehen große Unterschiede in Bezug auf die Cloud-Sicherheit. Ganz allgemein gibt es folgende drei Möglichkeiten:

1. Sie nutzen Ihre eigene Verschlüsselung und Schlüsselverwaltung: So können Sie in der gesamten hybriden Umgebung selbst bestimmen, wie Sie Ihre sensiblen Daten schützen, und haben maximale Kontrolle, Visibilität und Portabilität. Dieses Modell ist unabhängig von Clouds, Anbietern und Standort, wodurch Sie die Sicherheit einheitlich und zentral verwalten, Betriebsabläufe vereinfachen und die Compliance verbessern können.

2. Cloud-Verschlüsselungsdienste mit Bring-Your-Own-Key (BYOK): Um die Best Practices der Schlüsselverwaltung einzuhalten, bieten die meisten IaaS-/PaaS-Anbieter Bring-Your-Own-Key (BYOK) Application Programming Interfaces (APIs), wobei manche Hold Your Own Key (HYOK) bieten. In einer Multi-Cloud-Umgebung mit mehreren BYOK-APIs benötigen Sie wahrscheinlich zusätzliche Tools zur Verwaltung der BYOK-Schlüssel.

3. Nutzung nativer Verschlüsselungsdienste: sind für jeden Cloud-Anbieter einzigartig und werden vollständig durch diesen verwaltet. Je nach Risikoprofil und Empfindlichkeit der Daten müssen Sie diese Dienste möglicherweise durch zusätzliche Visibilitäts-, Kontroll- und Portabilitätstools ergänzen.



Bring-Your-Own-Encryption

Thales bietet eine breite Auswahl an Verchlüsselungs- und Tokenisierungslösungen über die Vormetric Data Security Platform und den SafeNet High Speed Encryptor. Mit der Vormetric Platform können Sie alle Ihre Verschlüsselungsanwendungen zentral kontrollieren und verwalten, um für kontinuierliche Sicherheit und Compliance zu sorgen.

- **Vormetric Transparent Encryption** schützt On-Premises und in der Cloud gespeicherte Daten durch Verschlüsselung und Zugriffskontrolle auf Dateiebene.
- **Vormetric Application Encryption** verschlüsselt Ihre sensiblen Daten, sobald sie in einer Cloud- oder On-Premise-Anwendung erstellt oder verarbeitet werden.
- **Vormetric Tokenization mit Dynamic Data Masking** ermöglicht es Ihnen, das Ausmaß Ihrer Compliance-Überprüfungen zu reduzieren, indem Sie Ihre sensiblen Daten tokenisieren und unverschlüsselte Daten aus Ihrer Umgebung eliminieren.
- **SafeNet High Speed Encryptor (HSE)** schützt Ihre sensiblen Daten auf dem Weg von Ihrem Datencenter zur Cloud oder an andere Orte, einschließlich Audio- und Videostreams in Echtzeit.

Zentralisierte Schlüsselverwaltung und - sicherheit für einfach Handhabung

Verschlüsselung und Tokenisierung ohne entsprechende Schlüsselverewaltung und -sicherheit können zu einer Vielzahl an Verstößen und Compliance-Problemen führen. Mit einer zentralisierten Schlüsselverwaltung können Sie Cloud-Dienste nutzen, ohne die Kontrolle über Ihre Schlüssel den Cloud-Anbietern zu überlassen.

Effiziente Datensicherheitskontrolle:

Mit dem Vormetric Data Security Manager (DSM) der Vormetric Data Security Platform lässt sich das Schlüsselmanagement unternehmensweit zentralisieren. Der DSM kontrolliert Schlüssel und Richtlinien der Produkte der Plattform, einschließlich des Schlüsselmanagements.

Mit den Cloud-Sicherheitslösungen von Thales können Sie für einen einheitlichen Schutz all Ihrer Unternehmensdaten und umfassende Sichtbarkeit und Kontrolle sorgen, sowohl On-Premises als auch in Hybrid- oder Multi-Cloud-Umgebungen.

Der DSM kann in öffentlichen und privaten Clouds oder physisch bereitgestellt werden. So können Sie flexibel sein und Ihre Umgebung stets an die Bedürfnisse des Unternehmens anpassen.

Hohe kryptographische Schlüsselsicherheit:

- **SafeNet Data Protection On Demand (DPoD)** ist eine Cloud-basierte Plattform, auf der eine breite Auswahl an vollständig verwalteten Hardware-Sicherheitsmodulen (HSM) in der Cloud zur Verfügung stehen. Hier können Sie entsprechend der Bedürfnisse Ihres Unternehmens ohne anfängliche Investitionen verschiedene Diente anklicken und in Sekundenschnelle bereitstellen und auf Pay-As-You-Go-Basis bezahlen.
- **SafeNet Luna HSM** bietet Unternehmen die Möglichkeit, in ihrer On-Premises-Umgebung hochsichere, manipulationssichere Geräte mit FIPS 140-2-Zertifizierung anzuwenden, um kryptographische Schlüssel und Abläufe zu generieren und zu sichern. Sie sind auch als dedizierte Geräte über AWS-, Azur und IBM-Clouddienste erhältlich.

Bring-Your-Own-Key

Viele Anbieter von Clouddiensten stellen Data-at-Rest-Verschlüsselung zur Verfügung, bei der die kryptographischen Schlüssel vom Anbieter verwaltet werden. Um sowohl Best Practices als auch Datenschutzvorschriften besser einzuhalten, bieten viele Anbieter jedoch auch Bring-Your-Own-Key (BYOK) Dienste.

BYOK bietet Unternehmen die Möglichkeit, Verschlüsselungscodes oder Schlüsselmaterial für ihre Cloud-nativen Verschlüsselungsdienste selbst zu erstellen und zu importieren. Thales nutzt die BYOK APIs von Cloud-Anbietern, um verschiedene Lösungen und Dienste für mehr Kontrolle und Visibilität anzubieten:

- CipherTrust Cloud Key Manager
- SafeNet Data Protection On Demand
- SafeNet Luna Hardware-Sicherheitsmodul

Es werden unter anderem folgende Clouds unterstützt: Microsoft Azure, Microsoft Office 365, Microsoft Azure Stack, Microsoft Azure National Clouds, Amazon Web Services, Salesforce, Google Cloud Platform und IBM Cloud.

Hold-Your-Own-Key

Mit HYOK können Unternehmen die Verschlüsselungsdienste der Microsoft Azure-Cloud nutzen und sich dabei völlig sicher sein, dass sie den Lebenszyklus der kryptographischen Schlüssel besitzen und kontrollieren.

Dank der Integration zwischen Azure Information Protection und SafeNet Luna HSM können Sie kryptographische Schlüssel statt in der Azure Cloud in Ihren eigenen On-Premises-HSM erstellen und speichern und sie entsprechend Ihrer eigenen Sicherheitsrichtlinien und Compliance-Anforderungen verwalten.

Dadurch haben Sie stets die Kontrolle über den Zugriff auf interne und hochsensible Daten in Verbindung mit Microsoft-Azure-Anwendungen und -Diensten wie Office 365, sodass Sie maximale Sicherheit und Überprüfbarkeit erreichen.

Um Ihre Hybrid-Cloud-Lösungen optimal zu nutzen, müssen Sie sicherstellen, dass Ihre sensiblen Daten schnell und sicher zwischen den verschiedenen Umgebungen übertragen werden können.

Thales Datensicherheit für die Hybrid Cloud

Unternehmen optimieren ihre Investitionen in private und öffentliche Clouds, indem sie Hybrid-Cloud-Lösungen übernehmen. Um das meiste aus diesen Investitionen herauszuholen, muss gewährleistet sein, dass Daten zwischen den verschiedenen Umgebungen schnell und sicher übertragen werden können.

Die Datenschutzlösungen von Thales für Hybrid-Clouds ermöglichen es Ihren Architekten, den idealen Mix zwischen nativen Cloud-Verschlüsselungslösungen und Bring-Your-Own-Encryption-Lösungen zu finden und dabei stets die Kontrolle über kryptographische Schlüssel und Zugriffsregelung zu behalten.

So können Ihre IT- und Sicherheitsteams Ihre Aufgaben nach und nach vereinheitlichen, sodass Sie Ihre sensiblen Daten unabhängig vom aktuellen Speicherort einsehen und kontrollieren können.

Mit den marktführenden Datenschutzlösungen und -experten von Thales wird es so einfach wie noch nie, „alles zu verschlüsseln".

Detailliertere Informationen zu den Produkten von Thales für Cloud-Sicherheit finden Sie auf www.thalesesecurity.com/cloud-security

> thalesgroup.com <

Nord- und Südamerika – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100 Austin, TX 78759 USA • Tel.:+1 888 343 5773 oder +1 512 257 3900 • Fax: +1 954 888 6211 • E-Mail: sales@thalesesec.com
Asien-Pazifik – 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
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