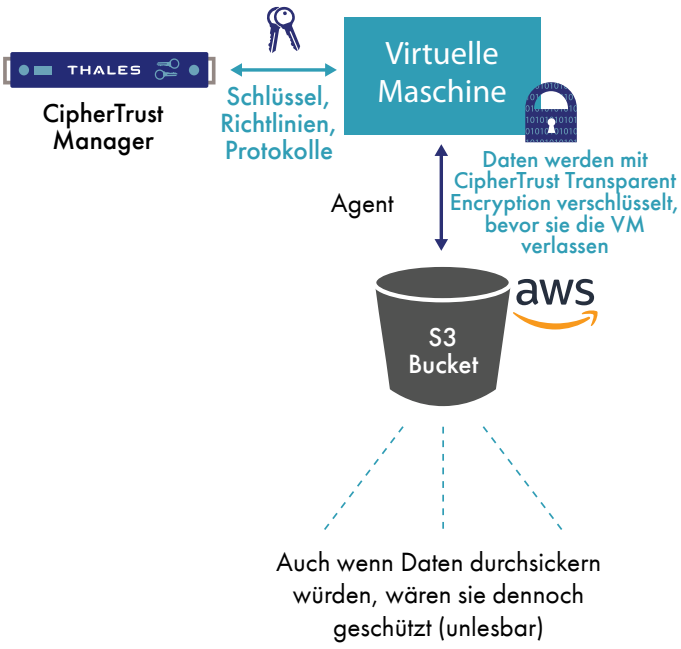
cpl.thalesgroup.com/de

THALES

Fortschrittliche Datensicherung für Amazon S3 mit CipherTrust Transparent Encryption

DIE HERAUSFORDERUNG: Vermeidung von Datenverletzungen durch falsch konfigurierte Amazon-S3-Sicherheitseinstellungen

Amazon Simple Storage Service (S3) ist eine der führenden Cloud-Speicherlösungen und wird von Unternehmen auf der ganzen Welt für eine Vielzahl von Anwendungsfällen genutzt. Amazon-S3-Buckets haben sich zu einem der am häufigsten verwendeten Cloud-Speicher für alle Daten von Serverprotokollen bis hin zu Kundendaten entwickelt. Schlecht konfigurierte S3-Buckets verursachten in der Vergangenheit jedoch eine große Anzahl von Datenverletzungen. Amazon bietet zwar eine Reihe von Sicherheitsservices und -funktionen an, die seine Kunden zum Schutz ihrer Assets nutzen können, letztlich legt der Cloud-Anbieter die Verantwortung für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten in der Cloud sowie für die Erfüllung spezifischer Geschäftsanforderungen an den Informationsschutz jedoch in die Hände seiner Kunden.



DIE LÖSUNG: CipherTrust Transparent Encryption für Amazon S3

In einer Public-Cloud-Umgebung müssen Unternehmen sensible Daten schützen und die vollständige Hoheit und Kontrolle sowohl über ihre Daten als auch über die zugehörigen kryptographischen Schlüssel und Richtlinien behalten.

Mit CipherTrust Transparent Encryption vereinfacht Thales die Sicherung von Amazon-S3-Objekten und hilft bei der Einhaltung von Datensicherheitsvorschriften. CipherTrust Transparent Encryption kann nahtlos für Objekte in Amazon S3 eingesetzt werden und bietet eine transparente und automatisierte Verschlüsselung von sensiblen Daten an, die in S3-Buckets gespeichert sind. Dabei werden keinerlei Änderungen an Anwendungen, Datenbanken, Infrastruktur oder Geschäftspraktiken vorgenommen.

Highlights:

- **Transparente Verschlüsselung von Daten in der Cloud.** Bietet transparente Verschlüsselung von sensiblen Daten, die in Amazon S3-Buckets gespeichert sind.
- **Schlüsselschutz in der Hand des Kunden.** Behalten Sie mit einer FIPS 140-2-konformen Lösung die Kontrolle und die Hoheit über kryptographische Schlüssel – on premises oder in der Cloud.
- **Schnelle Bereitstellung und Implementierung.** Einfache Bereitstellung von Agents, die auf Amazon EC2 und lokalen Servern laufen, ohne dass Anwendungen oder das Datenbankschema geändert werden müssen.
- **Aufgabentrennung.** Fügen Sie eine granulare Zugriffsverwaltung und Zugriffskontrollen für privilegierte Benutzer hinzu, die vom Sicherheitsteam kontrolliert werden.

Vorteile

CipherTrust Transparent Encryption für Amazon S3. Stärkt die Datensicherheit mit Kontrollen zum Schutz vor nicht autorisiertem Zugriff, die auf granularen Zugriffsrichtlinien basieren. Das betrifft unter anderem die Benutzeridentität (z. B. für Administratoren mit Root-Privilegien) und -prozesse.

- Neue S3-Bucket-Zugriffskontrollen, um den Zugriff auf autorisierte Hosts zu beschränken.
- Angreifern wird der Zugriff auf geschützte Buckets verweigert, selbst wenn die Buckets falsch konfiguriert und offen sind.
- Beschleunigt die Erkennung von Datenschutzverletzungen und erfüllt Compliance-Anforderungen mit detaillierter Protokollierung des Zugriffs auf Dateien, 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. Verschlüsselungs-Agents arbeiten auf Amazon-EC2-Recheninstanzen und anderen Servern, die auf S3-Buckets, Elastic Block Storage (EBS) und lokalen Speicher zugreifen.

Funktionen

- Transparente Verschlüsselung und Zugriffskontrolle für Daten in S3-Buckets.
- Die Kontrolle des Zugriffs privilegierter Benutzer ermöglichen es Benutzern mit Root-Zugriff, ihre Arbeit zu erledigen, ohne dass Daten missbräuchlich verwendet werden können.
- Die Protokollierung des Datenzugriffs beschleunigt die Erkennung von Bedrohungen und erleichtert die Forensik.
- Nutzt ausschließlich starke, standardbasierte Verschlüsselungsprotokolle wie Advanced Encryption Standard (AES) zur Datenverschlüsselung und elliptische Kurvenkryptographie (ECC) für den Schlüsselaustausch.
- Vereinfacht die Schlüsselverwaltung in On-Premises- und Multi-Cloud-Implementierungen durch zentrale Kontrolle über den FIPS-140-2-konformen CipherTrust Manager.

CipherTrust Manager

Der CipherTrust Manager zentralisiert die Schlüssel-, Richtlinien- und Protokollverwaltung für CipherTrust Transparent Encryption. Er ist sowohl virtuell als auch als physisches Gerät erhältlich und speichert Masterschlüssel sicher mit einem starken Vertrauensanker. Die entsprechenden Anwendungen können sowohl on-premises als auch in privaten oder öffentlichen Cloud-Infrastrukturen bereitgestellt werden. So sind Unternehmen in der Lage, gesetzliche Vorgaben, behördliche Auflagen sowie bewährte Branchenverfahren für Datensicherheit umzusetzen.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. 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.