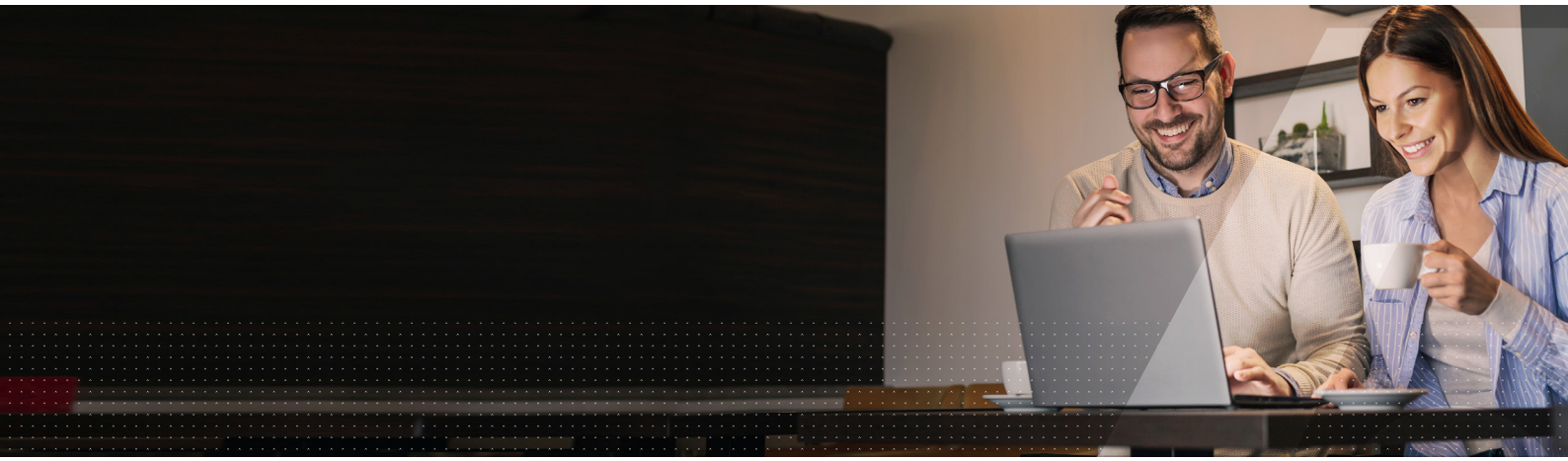
cpl.thalesgroup.com

Google Workspace | THALES Building a future we can all trust

Sicherheitslösungen von Thales für Google Workspace

Verbesserter Datenschutz und erweiterte Vertraulichkeit mit client-seitiger Verschlüsselung von Google Workspace und Thales Data and Identity Protection



Verbesserte Schlüsselverwaltung für Google Workspace

Cloud-Anbieter und Unternehmen möchten Sicherheit und Compliance in der Cloud verbessern. Als Antwort auf diese Herausforderung bietet Google Workspace nun erweiterte Datenschutz- und Vertraulichkeitsoptionen für Gmail, Google Calendar, Anrufe über Google Meet und Google Drive mit client-seitiger Verschlüsselung. Diese Lösung ermöglicht es Unternehmenskunden, mit dem CipherTrust Cloud Key Manager und SafeNet Trusted Access als einzelne Lösungen oder in Kombination die volle Kontrolle über ihre kryptographischen Schlüssel zu gewährleisten.

Gemäß dem Konzept der „Shared Security" (verteilte Sicherheit) empfiehlt Google seinen Kunden den Einsatz einer externen Schlüsselverwaltung (EKM) und eines Identitätsproviders (IDP), um sicherzustellen, dass nur autorisierte und authentifizierte Personen auf geschützte Informationen zugreifen können. Thales ist der einzige Anbieter, der eine unabhängige IDP- und Schlüsselverwaltungslösung entwickelt.

Client-seitige Verschlüsselung von Google Workspace mit Thales Key Management and Identity Protection: Gemeinsam sicherer

Kunden, die die client-seitige Verschlüsselung von Google Workspace nutzen, können mit der integrierten End-to-End-Lösung von Thales, die kryptographische Schlüssel getrennt von ihren sensiblen Daten in der Cloud kontrolliert und Identitäten schützt, eine höhere Sicherheit und einen geringeren Bereitstellungsaufwand erreichen.

Client-seitige kryptographische Schlüssel ermöglichen es Dienstanbietern, verschlüsselte Daten zu hosten, ohne sie zu entschlüsseln, und so die Privatsphäre des Benutzers zu schützen. Wenn ein Benutzer beispielsweise seine Datei abruft, wird der entsprechende Data Encryption Key mit den vom Kunden bereitgestellten Schlüsseln erst entschlüsselt, nachdem der Benutzer eine vom Kunden kontrollierte Authentifizierung durchlaufen hat.

SafeNet Trusted Access (STA) von Thales bietet Kunden in Kombination mit dem CipherTrust Cloud Key Manager eine unabhängige IDP- und Schlüsselverwaltungslösung von einem einzigen Anbieter, der Sie durch eine reibungslose Bereitstellung, eine überragende Benutzererfahrung und eine bessere Wertschöpfung beim Erreichen Ihrer Geschäftsziele unterstützt.

Thales ist ein zuverlässiger Multi-Cloud-Partner. CipherTrust Cloud Key Manager und STA können gemeinsam oder unabhängig voneinander eingesetzt werden und ermöglichen es Unternehmen, die Kontrolle über die Schlüsselverwaltung und die Zugriffssicherheit zu behalten und gleichzeitig die Bindung an einen bestimmten Anbieter zu vermeiden – eine wichtige Voraussetzung für die Unterstützung von Multi-Cloud-Umgebungen im Rahmen von Initiativen zur digitalen Transformation.

So funktioniert die gemeinsame Lösung

Ein Benutzer meldet sich bei Google Workspace an und wird zur Authentifizierung und Identitätsüberprüfung an STA weitergeleitet.

- STA authentifiziert den Benutzer und erstellt ein Authentifizierungs-Token.
- Wenn der Benutzer eine client-seitig verschlüsselte Datei, eine E-Mail in Gmail oder einen Termin in Google Calendar erstellt oder einen Anruf über Google Meet startet, werden das von der STA generierte Authentifizierungs-Token und ein separates, von Google generiertes Autorisierungs-Token zusammen mit einem von Google generierten Data Encryption Key (DEK) an den CipherTrust Cloud Key Manager gesendet.
- Der CipherTrust Cloud Key Manager validiert das von STA generierte Authentifizierungs-Token mit STA und das von Google generierte Autorisierungs-Token mit Google
- Wenn beide Token validiert sind, verschlüsselt CipherTrust Cloud Key Manager den DEK mit einem von CipherTrust generierten Key Encrypting Key (KEK) und gibt den verschlüsselten DEK an Google zurück
- Nachfolgendes Öffnen oder Speichern der Datei erfordert eine Validierung durch den CipherTrust Cloud Key Manager, der es autorisierten Parteien erlaubt, den KEK zu entpacken und auf den DEK und die Datei zuzugreifen.

Wichtige Vorteile

Unternehmen, die Workloads und Anwendungen in die Cloud verlagern, nutzen häufig Collaboration Suites wie Google Workspace. Zusätzliche externe Verschlüsselung und Identität bieten Ihnen nicht nur den Vorteil, einfach und ortsunabhängig Zugriff von jedem Gerät aus zu haben. Sie geben Ihnen auch die Möglichkeit, Ihre kryptographischen Schlüssel zu kontrollieren und stellen eine zusätzliche Ebene der Vertraulichkeit und Sicherheit für Ihre sensiblen Unternehmensressourcen in der Cloud dar.

Thales ist der einzige Anbieter für unabhängige Schlüsselverwaltung, IDP und Authentifizierung, der es Unternehmen ermöglicht, die Best Practices für Cloud-Sicherheit zu erfüllen, um Google Workspace mit client-seitiger Verschlüsselung zu sichern.

Die integrierte Lösung für die Schlüssel- und Zugriffsverwaltung von Thales bietet wichtige Vorteile, darunter:

- **Sicherheit:** Unternehmen können das Risiko von Datenschutzverletzungen und Strafen verringern, indem sie ihre Schlüsselverwaltung und Zugriffssicherheit selbst kontrollieren
- **Reibungslose Bereitstellung:** Die Integration eines einzigen Anbieters in Google Workspace gewährleistet eine schnelle und reibungslose Bereitstellung
- **Überragende Benutzererfahrung:** Benutzer profitieren von der einmaligen Anmeldung sowohl bei Google Workspace als auch bei ihren anderen Cloud-Diensten und -Apps

Highlights

Schlüsselverwaltung für Google Workspace

CipherTrust Cloud Key Manager bietet externe Schlüsselverwaltung und Richtlinienkontrolle, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf verschlüsselte Dokumente, Google Mail, Google Calendar und Anrufe über Google Meet erhalten.

Identitätsschutz für client-seitige Verschlüsselung

STA dient als unabhängiger Drittanbieter-IDP und authentifiziert Benutzer bei Google Workspace. STA ermöglicht die Authentifizierung für die client-seitige Verschlüsselung von Google Workspace über eine OIDC-Integration.

Verbesserte Authentifizierung und sicherer Zugriff auf Google Workspace

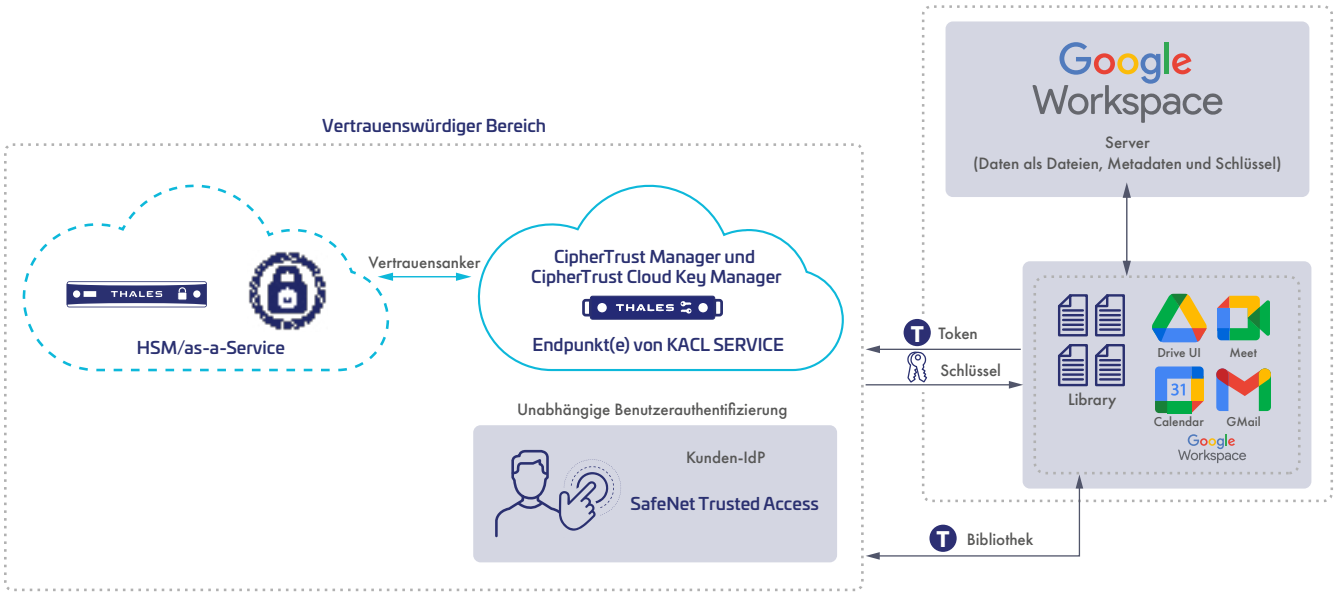
STA ist über eine SAML-Integration mit Google Workspace verbunden, ermöglicht Single Sign-on und erzwingt die entsprechende Authentifizierungsstufe, wenn sich Benutzer bei ihrem Google-Dienst anmelden.

Einfache und sichere Authentifizierung

Nutzen Sie ein Zero-Trust-Sicherheitsmodell, indem Sie Authentifizierungs- und spätere Zugriffskonzepte mit sicherer und kontinuierlicher Authentifizierung, Single Sign-On und Multifaktor-Authentifizierung für alle Ressourcen erzwingen. Zu den Authentifizierungsmethoden gehören: FIDO, Hardware-Tokens, Software-Tokens (OTP-Apps), Out-of-Band-Push-Authentifizierung (OOB), zertifikatsbasierte Authentifizierung (CBA), musterbasierte Authentifizierung, OOB per SMS und E-Mail sowie kontextbezogene Authentifizierung.

Bequem und einfach

Eine Re-Authentifizierung kann so konfiguriert werden, dass innerhalb eines vorab definierten Zeitraums die vorhandenen Anmeldedaten verwendet werden. Dadurch wird sie für den Benutzer bequemer, ohne die Sicherheit zu beeinträchtigen.



Über die client-seitige Verschlüsselung von Google Workspace

Die client-seitige Verschlüsselung von Google Workspace hilft Kunden, die Vertraulichkeit ihrer Daten zu stärken, und kann eine breite Palette von Anforderungen an die Datensouveränität und die Einhaltung von Vorschriften erfüllen. Die Kunden haben direkte Kontrolle über die kryptographischen Schlüssel und den Identitätsdienst, den sie für den Zugriff auf diese Schlüssel einsetzen. Die Kundendaten können von Google nicht entschlüsselt werden, während die Benutzer weiterhin die Vorteile der Kollaboration nutzen, über Mobilgeräte auf Inhalte zugreifen und verschlüsselte Dateien extern austauschen können.

Über Google Workspace

Google Workspace ist eine einheitliche Plattform für Kollaboration und Kommunikation, die Unternehmen jeder Größe alles bietet, was sie benötigen, um sich zu vernetzen, Inhalte zu erstellen und zusammenzuarbeiten. Google Workspace umfasst Anwendungen wie Gmail, Google Meet, Google Calendar, Drive, Docs, Sheets, Slides und mehr. Weitere Informationen erhalten Sie unter workspace.google.com.

Über Thales Access Management

Mit den branchenführenden Lösungen für Zugriffsverwaltung und Authentifizierung von Thales können Unternehmen den Zugriff auf IT-, Web- und Cloud-basierte Anwendungen des Unternehmens mit einem Zero-Trust-Ansatz zentral verwalten und sichern. Durch den Einsatz von richtlinienbasiertem bedingtem Zugriff, striktem SSO und universellen Authentifizierungsmethoden können Unternehmen effektiv Sicherheitsverletzungen verhindern, sicher in die Cloud migrieren und die Einhaltung von Vorschriften vereinfachen.

Über Thales Data Protection

Die CipherTrust Data Security Platform ist ein cloud-fähiges Produktportfolio, das entwickelt wurde, um viele der Herausforderungen zu bewältigen, mit denen Sicherheitsteams beim Einsatz von Multi-Cloud-Strategien konfrontiert sind. Die Plattform bietet eine unvergleichliche Bandbreite an Lösungen für Datensicherheit und Schlüsselverwaltung. Der CipherTrust Cloud Key Manager ist ein Bestandteil der Plattform.

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.

> cpl.thalesgroup.com/de <

Kontakt – Alle Bürostandorte und Kontaktinformationen finden Sie auf cpl.thalesgroup.com/contact-us