cpl.thalesgroup.com/de

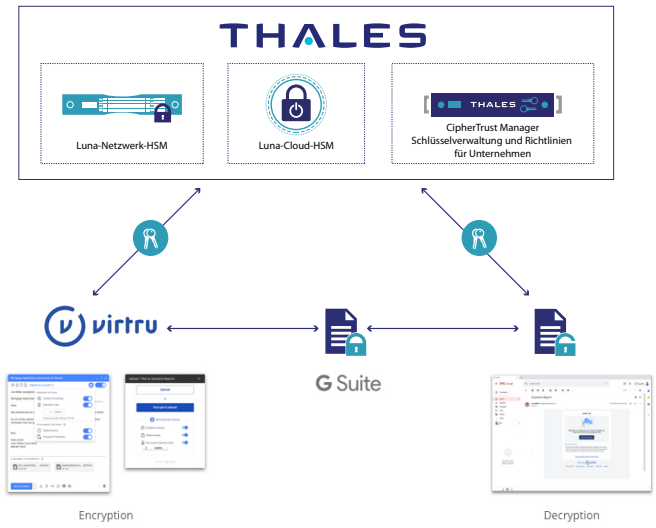
Gewährleisten Sie echten Datenschutz, indem Sie Ihre eigenen kryptographischen Schlüssel für die Google Cloud hosten

Erreichen Sie Zero-Trust-Sicherheit für Gmail und Google Drive, indem Sie die Unternehmenslösungen für Schlüsselverwaltung und die Speicherung von Hardware-Schlüsseln von Thales mit der nahtlosen Schnittstelle von Virtru für End-to-End-E-Mail- und Dateischutz integrieren.

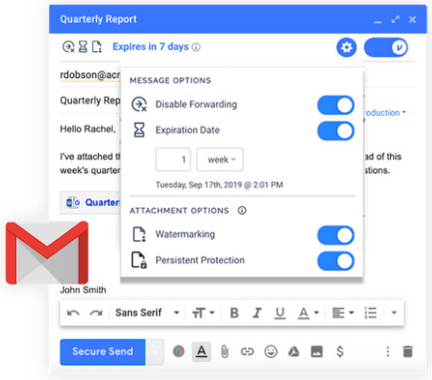
Thales und Virtru bieten maßgeschneiderte HSM-Schlüsselverwaltung für G-Suite-Unternehmen

Bei der Migration in die Cloud möchten viele Unternehmen die Sicherheit ihrer Daten gewährleisten – oft mithilfe von Kryptographie – und dabei weiterhin ohne Beeinträchtigung Informationen teilen und prüfen sowie auf diese zugreifen können. Obwohl viele Anbieter von Cloud-Diensten versuchen, dieses Gleichgewicht herzustellen, zwingen die meisten Sie dazu, sich zu entscheiden: entweder Sie geben die vollständigen Kontrolle über Ihre kryptographischen Schlüssel auf oder Sie verlieren die Kontrolle darüber, wohin die Daten gesendet und wie sie verarbeitet werden.

Die Datenschutzlösungen von Thales und Virtru machen solche Kompromisse überflüssig, indem sie es Unternehmen ermöglichen, ihre eigenen Schlüssel zu hosten – ob on-premises oder in der Cloud – ohne die Kontrolle an Drittanbieter abzugeben oder die Workflows von Gmail und Google Drive für das Teilen von Daten zu beeinträchtigen. Unternehmen können den Enterprise Key Manager oder die Hardware-Sicherheitsmodule (HSM) von Thales nutzen, um die Schlüssel zu speichern und zu verwalten, die für die Verschlüsselung, Authentifizierung, Autorisierung und Nutzung von Daten verwendet werden, die durch die Client-seitigen G-Suite-Endpunkte von Virtru geschützt sind. Die Schlüssel bleiben ebenso wie die E-Mails und Dateien, die sie sichern, unter Ihrer vollen Kontrolle. So können Daten während ihres gesamten Lebenszyklus nach dem Zero-Trust-Ansatz geschützt und granular geprüft werden.



Verschlüsseln Sie G-Suite- und Gmail-Daten unter Beibehaltung der vollständigen Eigentümerschaft an den Schlüsseln



Steuern Sie die Nachrichtensicherheit direkt über die Google-Mail-Taskleiste

Drei Optionen zum Sichern und Verwalten von Schlüsseln

- **Luna-Netzwerk-Hardware-Sicherheitsmodule (HSM) von Thales** Die Luna-Netzwerk-HSMs von Thales sind speziell entwickelte Hardware-Appliances, die kryptographisches Material auf vertrauenswürdige Weise speichern. Luna-HSMs schützen den gesamten Lebenszyklus der kryptographischen Schlüssel innerhalb der manipulationssicheren, gemäß FIPS 140-2 Level 3 validierten Grenzen der Appliance. Der einzigartige Ansatz von Thales, kryptographische Schlüssel in Hardware zu schützen, macht diese Appliances zu den vertrauenswürdigsten Allzweck-HSMs auf dem Markt und stellt sicher, dass kryptographische Schlüssel immer sowohl physisch als auch logisch geschützt sind.
- **Thales Cloud HSM Service.** Thales Cloud HSM Service ist ein Cloud-nativ gehosteter Dienst, der auf der Technologie der Luna-Netzwerk-HSMs basiert. Unternehmen können wichtige Speichermedien jetzt einfacher und kostengünstiger einsetzen, ohne dass Hardware gekauft, bereitgestellt und gewartet werden muss. Obwohl es sich um einen gehosteten Dienst handelt, haben die Kunden alleinigen Zugriff auf ihre Schlüssel und behalten die volle Kontrolle über die Hardware, ohne dass sonstige Personen Zugriff darauf haben.
- **CipherTrust Key Manager (CTM).** CipherTrust Key Manager ist eine zentralisierte Plattform für die Verwaltung von kryptographischen Inhalten (Schlüssel und zugehörige Daten) und Anwendungen, die on-premises, in der Cloud oder in hybriden Umgebungen betrieben werden kann. Er ist als physische oder virtuelle Appliance erhältlich und Kunden können aus flexiblen Optionen wählen, die gemäß FIPS 140-2 Level 1 oder 3 zertifizierte Versionen umfassen. Mit dem CTM können Kunden ihre kryptographischen Schlüssel von Virtru zusammen mit einer Vielzahl von Schlüsseln für andere Verschlüsselungslösungen von Drittanbietern oder mit dem Rest des Verschlüsselungsportfolios von Thales verwalten. Mit dem CTM sind Unternehmen in der Lage, Virtru einfach in ihre umfassende Sicherheitsstrategie einzufügen, ohne dass dabei zusätzlicher administrativer Aufwand entsteht.

Vertrauenswürdige, kundengesteuerte Schlüsselverwaltung für maximale Privatsphäre und Datenzugriffskontrolle

Zero-Trust-Cloud-Sicherheit

Die Split-Knowledge-Architektur trennt Schlüssel von Inhalten, während die nahtlose HSM-Schlüsselspeicherung oder die Schlüsselverwaltung für Unternehmen eine zusätzliche, vom Kunden kontrollierte Sicherheitsebene hinzufügen. Dadurch sind Sie nie gezwungen, Thales, Virtru, Google oder einem Anbieter von Cloud-Diensten den Zugriff auf Ihre Daten anzuvertrauen.

End-to-End-Verschlüsselung und dauerhafte Kontrolle

Schützen Sie Google Mail und Drive mit einer End-to-End-Verschlüsselung, die den unbefugten Zugriff auf Daten verhindert, die in der Google Cloud gespeichert und außerhalb Ihres Ökosystems freigegeben werden. Deaktivieren Sie die Weiterleitung, stellen Sie ein Ablaufdatum ein und widerrufen Sie den Zugriff. Markieren Sie Dateien mit Wasserzeichen, um Datenverlust vorzubeugen, und kontrollieren Sie die Weitergabe und das Teilen von Daten permanent.

Granulare Prüfpfade

Zeigen Sie an, wann und wo bei der digitalen Weitergabe und dem Teilen von Daten auf sensible E-Mails und Dateien zugegriffen wurde, und passen Sie die Kontrollen an sich ändernde Datenschutz- und Compliance-Anforderungen an. Die HSMs und der CTM von Thales protokollieren den Zugriff auf kryptographische Schlüssel und Änderungen des Schlüsselstatus auf sichere Weise und ermöglichen so umfassende Einblicke, mit denen Sie die Datenkontrolle und die Einhaltung gesetzlicher Vorschriften nachweisen können.

Datenschutz in der Cloud für globale Unternehmen

Datenresidenz und Compliance

Erfüllen Sie Datenschutz- und Residenzanforderungen für die gemeinsame Nutzung von Daten in der Cloud, indem Sie entscheiden, wo die Schlüssel zum Schutz dieser Daten gespeichert werden. Darüber hinaus erleichtert die Validierung gemäß FIPS 140-2 Level 3 des CTM und der HSMs von Thales die Einhaltung von Vorschriften wie PCI DSS und HIPAA.

Echter Cloud-Datenschutz

Hosten Sie mit den Cloud-basierten HSM-Angeboten von Thales Ihre eigenen Schlüssel in der Cloud und nutzen Sie Cloud-First-Strategien, damit Unbefugte niemals auf Ihre Google-Cloud-Daten zugreifen können und diese privat bleiben. Erhältlich entweder als Cloud-basiertes HSM-as-a-Service oder als von einem CSP gehostete Appliance – Sie können die Option wählen, die am besten zu Ihrer Architektur und Ihrem Betriebsmodell passt.

Schutz vor staatlicher Überwachung

Vermeiden Sie rechtliche Anordnungen, die Sicherheits- und Cloud-Anbieter dazu zwingen, Ihre Daten ohne Genehmigung an Regierungen weiterzugeben. Wenn Sie Ihre eigenen kryptographischen Schlüssel kontrollieren, haben Anbieter von Cloud-Diensten niemals die Möglichkeit, Ihre Daten in einem lesbaren Zustand an Dritte weiterzugeben. Mit Thales und Virtru können nur Sie auf Datenanfragen der Regierung reagieren.

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.

Über Virtru

Wir bei Virtru ermöglichen es Unternehmen, die Macht der Daten zu nutzen und gleichzeitig die Kontrolle zu behalten. Unser Portfolio an Datenschutztechnologien ermöglicht die Kontrolle von Daten während ihres gesamten Lebenszyklus.

Kontaktieren Sie uns noch heute und erfahren Sie, wie Thales und Virtru die HSM-Schlüsselverwaltung in der Google Cloud vereinfachen.

> cpl.thalesgroup.com/de <

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