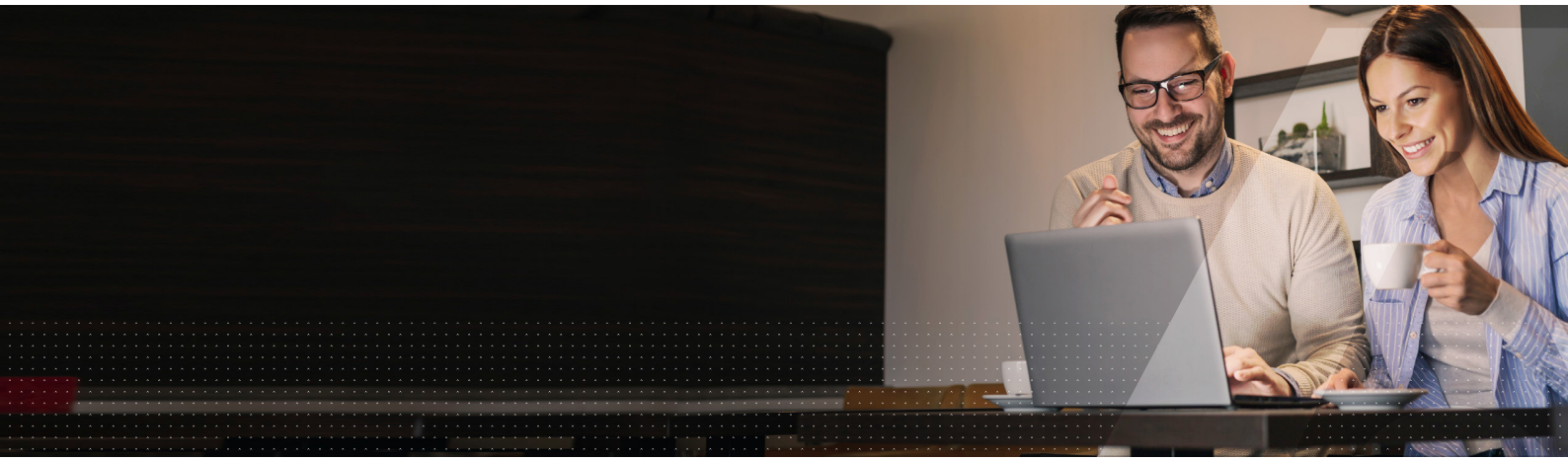
cpl.thalesgroup.com

Google Workspace | THALES
Building a future we can all trust

Les solutions de sécurité de Thales pour Google Workspace

Renforcement de la vie privée et de la confidentialité grâce au chiffrement côté client de Google Workspace et la protection des données et des identités de Thales



Améliorer la gestion des clés pour Google Workspace

Les fournisseurs du cloud comme les entreprises sont en quête de solutions pour renforcer la sécurité du cloud et garantir la conformité. Pour répondre à cette difficulté, Google Workspace offre désormais des modalités de confidentialité améliorées pour Gmail, Google Agenda, les appels sur Google Meet et Google Drive avec le chiffrement côté client (ou CSE pour Client-side encryption) ; une solution qui permet aux entreprises clientes d'avoir un contrôle total sur leurs clés de chiffrement en utilisant CipherTrust Cloud Key Manager et SafeNet Trusted Access, ensemble ou indépendamment.

Adhérant au concept de « sécurité partagée », Google recommande à ses clients d'utiliser un gestionnaire de clés externe (EKM) et un fournisseur d'identité (IDP) pour s'assurer que seules les personnes autorisées et authentifiées puissent accéder aux informations protégées. Seul Thales développe une solution IDP et de gestion des clés indépendante.

Le chiffrement côté client de Google Workspace et la gestion des clés et la protection des identités de Thales : l'alliance parfaite

Les clients utilisant le chiffrement côté client de Google Workspace bénéficient d'une sécurité renforcée et d'une réduction des coûts de déploiement grâce à la solution intégrée de bout en bout de Thales qui contrôle les clés de chiffrement séparément de leurs données sensibles dans le cloud et protège les identités.

Le chiffrement côté client permet aux fournisseurs de services d'héberger des données chiffrées sans avoir la possibilité de les déchiffrer, ce qui protège la vie privée de l'utilisateur. Par exemple, lorsqu'un utilisateur récupère un fichier, la clé de chiffrement correspondante n'est déchiffrée à l'aide des clés fournies par le client qu'après que l'utilisateur a été authentifié dans le cadre d'un processus d'authentification contrôlé par le client.

Utilisé avec CipherTrust Cloud Key Manager, SafeNet Trusted Access (STA) de Thales offre une solution de gestion des clés et IDP indépendante provenant d'un seul et même fournisseur permettant aux clients d'atteindre leurs objectifs commerciaux grâce à un déploiement sans heurts, une expérience utilisateur supérieure et une meilleure rentabilité.

Thales est un partenaire de confiance pour les environnements multicloud. CipherTrust Cloud Key Manager et STA, utilisés ensemble ou indépendamment, permettent aux entreprises de garder le contrôle à la fois de la gestion de leurs clés et de la sécurité des accès tout en évitant la dépendance envers un même fournisseur – ce qui est vital pour le déploiement d'environnements multicloud dans le cadre des initiatives de transformation numérique.

Comment fonctionne cette solution conjointe

Un utilisateur se connecte à Google Workspace et est redirigé vers STA pour l'authentification et la validation d'identité.

- STA authentifie l'utilisateur et crée un token d'authentification.
- Lorsque l'utilisateur crée un fichier chiffré côté client, utilise Gmail ou Google Agenda ou passe un appel via Google Meet, le token d'authentification généré par STA et un token d'autorisation distinct généré par Google sont envoyés à CipherTrust Cloud Key Manager avec une clé de chiffrement des données (DEK) générée par Google.
- CipherTrust Cloud Key Manager valide le token d'authentification généré par STA auprès de STA et valide le token d'autorisation généré par Google auprès de Google.
- Si les deux tokens sont validés, CipherTrust Cloud Key Manager chiffre la DEK avec une clé de chiffrement de clé (KEK) générée par CipherTrust, puis renvoie la DEK chiffrée à Google.
- Les ouvertures ou sauvegardes ultérieures de fichiers nécessitent une validation par CipherTrust Cloud Key Manager qui permettra ou non aux parties autorisées d'ouvrir la KEK et d'accéder à la DEK ainsi qu'au fichier.

Avantages majeurs

Les entreprises qui migrent leurs charges de travail et leurs applications vers le cloud utilisent fréquemment des suites de collaboration telles que Google Workspace. Au-delà d'offrir d'immenses avantages en termes d'accès (n'importe où et à partir de n'importe quel appareil), l'ajout d'une solution externe de chiffrement et de gestion des identités vous donne la possibilité de contrôler vos clés de chiffrement et fournit une couche supplémentaire de confidentialité et de sécurité pour les ressources sensibles de votre entreprise dans le cloud.

Thales est le seul fournisseur de sécurité à offrir une gestion indépendante des clés, des identités et de l'authentification. Les entreprises peuvent ainsi respecter les meilleures pratiques en matière de sécurité du cloud en sécurisant Google Workspace à l'aide du chiffrement côté client.

La solution intégrée de gestion des clés et des accès de Thales offre des avantages tangibles, notamment :

- **Sécurité :** permet aux entreprises de réduire le risque de brèche des données et d'éviter les sanctions en contrôlant elles-mêmes la gestion des clés et la sécurité des accès.
- **Déploiement sans heurts :** l'intégration d'un fournisseur unique avec Google Workspace garantit un déploiement rapide et sans heurts.
- **Expérience utilisateur supérieure :** les utilisateurs bénéficient de modalités SSO pour se connecter à Google Workspace ainsi qu'à leurs autres services et applications cloud.

À retenir

Gestion des clés pour Google Workspace

CipherTrust Cloud Key Manager assure une gestion des clés et un contrôle des politiques externes, pour garantir que seuls les utilisateurs autorisés puissent accéder aux documents chiffrés, à Gmail, à Google Agenda et aux appels passés via Google Meet.

Protection des identités pour CSE

STA fait office d'IDP tiers indépendant et authentifie les utilisateurs pour Google Workspace. STA permet l'authentification pour CSE de Google Workspace via une intégration OIDC.

Amélioration de l'authentification et sécurisation des accès à Google Workspace

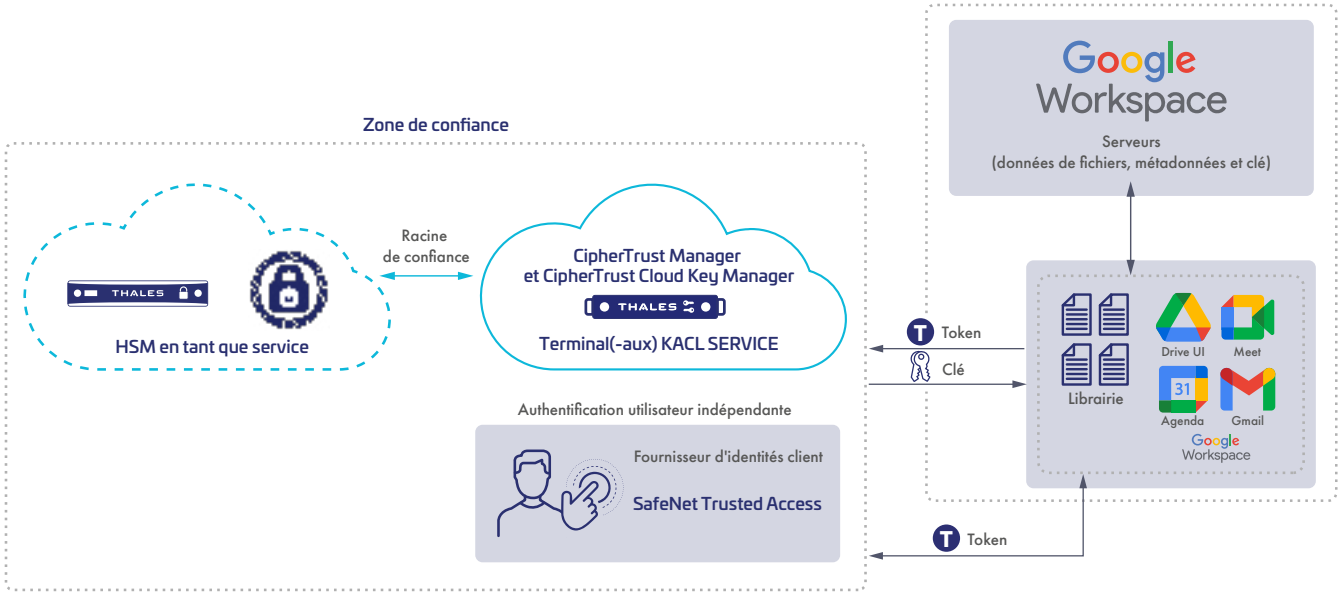
STA s'associe à Google Workspace via une intégration SAML, permettant le SSO et appliquant le niveau d'authentification approprié lorsque les utilisateurs se connectent à leur service Google.

Authentification simple et forte

Appliquez un modèle de sécurité Zéro Trust en mettant en œuvre des modalités où l'accès est subordonné à l'authentification, avec l'utilisation d'une authentification forte et continue, du SSO et de l'authentification multifactorielle pour toutes les ressources. Différentes méthodes d'authentification sont employées, notamment : le standard FIDO, les tokens matériels, les tokens logiciels (applications OTP), l'authentification hors bande (OOB) via notifications push, l'authentification basée sur des certificats (CBA), l'authentification basée sur un motif, l'OOB via SMS et e-mail et l'authentification contextuelle.

Pratique et facile

Il est possible de configurer une modalité de réauthentification pour utiliser les informations d'identification existantes dans un délai prédéterminé, ce qui réduit les frictions au niveau de l'utilisateur sans compromettre la sécurité.



À propos du chiffrement côté client (CSE) de Google Workspace

CSE de Google Workspace aide les clients à renforcer la confidentialité de leurs données et peut répondre à un large éventail d'exigences en matière de souveraineté des données et de conformité. Les clients disposent d'un contrôle direct sur les clés de chiffrement et sur le service d'identité qu'ils choisissent pour accéder à ces clés. Les données des clients sont indéchiffrables pour Google, et les utilisateurs peuvent continuer à profiter des outils de collaboration, à accéder au contenu sur leurs appareils mobiles et à partager des fichiers chiffrés vers l'extérieur.

À propos de Google Workspace

Google Workspace est une plateforme de collaboration et de communication unifiée qui fournit aux entreprises de toutes tailles tout ce dont elles ont besoin pour se connecter, créer et collaborer. Google Workspace comprend des applications telles que Gmail, Google Meet, Google Agenda, Drive, Docs, Sheets, Slides, etc. Pour en savoir plus, rendez-vous sur workspace.google.com.

À propos de la gestion des accès de Thales

Les solutions de gestion des accès et d'authentification de Thales permettent aux entreprises de gérer de manière centralisée et sécurisée les accès à leurs réseaux informatiques et à leurs applications web et cloud avec une approche Zéro Trust. Grâce à un accès conditionnel basé sur des règles d'accès, à un SSO rigoureux et aux méthodes d'authentification universelles, les entreprises peuvent prévenir les brèches efficacement, migrer vers le cloud sans danger et faciliter la mise en conformité réglementaire.

À propos de la protection des données de Thales

La plateforme CipherTrust Data Security est un portefeuille de produits compatibles avec le cloud, conçus pour répondre aux nombreuses difficultés auxquelles sont confrontées les équipes de sécurité dans le cadre de la mise en œuvre de stratégies multicloud. La plateforme offre une gamme inégalée de solutions pour répondre aux besoins de sécurité des données et de gestion des clés de chiffrement. CipherTrust Cloud Key Manager est une composante de cette plateforme.

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.

> cpl.thalesgroup.com/fr <

Nous contacter – Pour consulter les emplacements de tous nos bureaux et nos coordonnées, veuillez vous rendre à la page cpl.thalesgroup.com/fr/contact-us