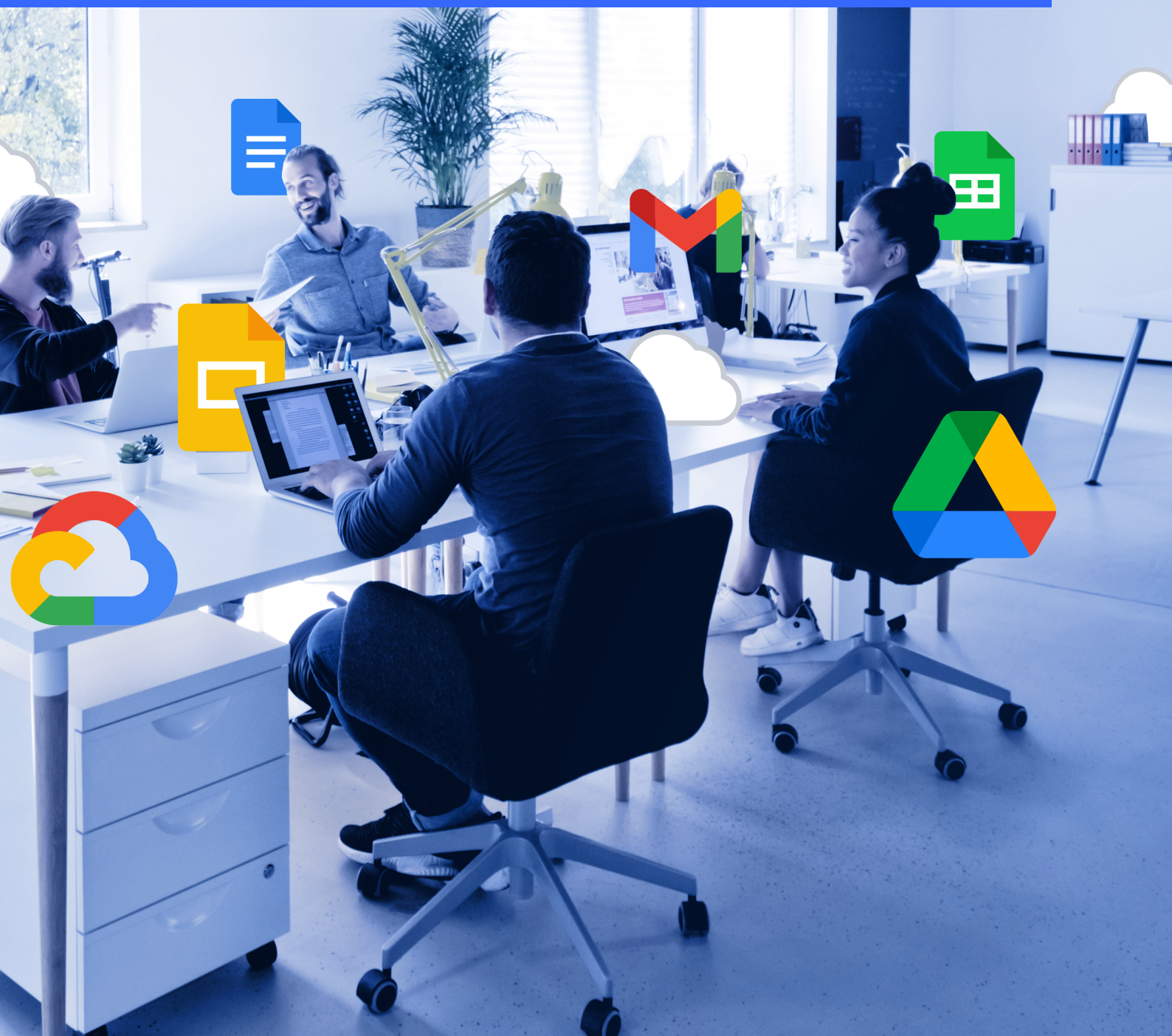
virtru

Le guide complet de la sécurité Zero Trust dans l'écosystème Google

Meilleures pratiques du cloud pour les chefs d'entreprise



Le monde adopte de plus en plus les outils de collaboration basés sur le cloud de Google - pour une bonne raison :

- Ils sont simples et faciles à utiliser.
- Ils sont rentables tout en offrant des fonctionnalités de classe mondiale.
- Ils facilitent une collaboration et un partage de données rapides.
- Ils sont facilement évolutifs.

Mais de nombreuses organisations ont hésité à déplacer tous leurs workflows vers Google Cloud car, historiquement, il n'était pas suffisamment sécurisé pour protéger les informations sensibles partagées par les utilisateurs de l'entreprise ou du gouvernement.

Mais cela a maintenant changé : il est plus sûr que jamais de migrer vers le cloud.

Notamment, Google a annoncé le déploiement du chiffrement côté client Google Workspace en 2021. Cela permet aux entreprises de protéger complètement leurs données, de sorte que même Google ne puisse y accéder.

Mais il existe encore plusieurs aspects de la protection des données que les responsables informatiques et de sécurité doivent prendre en compte afin de protéger efficacement les données qu'ils stockent et partagent dans l'écosystème Google. Ce guide vise à fournir un contexte sur les couches de protection des données Zero Trust qui constituent une stratégie cloud sécurisée sur Google Workspace, Google Cloud Platform (GCP) et au-delà.

Table of Contents

Prendre le contrôle de vos données dans le cloud

Les organisations peuvent hésiter à stocker des données sensibles dans le cloud, de peur qu'elles ne soient pas suffisamment sécurisées ou qu'elles n'aient pas le contrôle total. Historiquement, c'était vrai. Jusqu'à récemment, de nombreuses industries hautement réglementées (telles que l'industrie manufacturière et les organisations gouvernementales) n'étaient tout simplement pas autorisées à utiliser des solutions basées sur le cloud.

De nombreuses organisations mondiales ont également hésité à héberger leurs données sur Google, car elles doivent maintenir la résidence, la souveraineté et le contrôle des données. La plupart des principaux fournisseurs de cloud étant basés aux États-Unis, on craignait que ces organisations ne soient pas en mesure de maintenir la résidence et la souveraineté des données tout en stockant des données sur un serveur en dehors de leur propre pays ou région, mettant en danger les informations privées de leurs clients.

Disposer d'un cadre de protection des données unifié pour Google Cloud aide les entreprises à économiser de l'argent, à réduire la complexité et à gagner en vitesse.

La bonne nouvelle est que Google étend continuellement la capacité de ses clients à chiffrer et à protéger leurs données, tout en préservant la propriété et la souveraineté complètes des données. Depuis Gmail via Google Workspace et Google Cloud Platform, les clients ont la possibilité d'ajouter un chiffrement supplémentaire, ainsi que de gérer les clés de chiffrement en externe, de manière à masquer les données que Google stocke.

Cela vous offre le meilleur des deux mondes : l'efficacité et les capacités de collaboration du cloud, ainsi que l'assurance que vos données restent entièrement sous votre contrôle à tout moment, empêchant ainsi les tiers, y compris Google, d'accéder à vos données.

Pour faire de ce niveau de sécurité une réalité, les organisations doivent sélectionner un partenaire de chiffrement. Étant donné que l'écosystème Google est vaste, les entreprises doivent envisager un partenaire dont les capacités s'étendent sur Google Workspace et Google Cloud Platform, en leur offrant un cadre unique et global pour protéger leurs données conformément aux normes Zero Trust. Disposer d'un cadre de protection des données unifié pour Google Cloud aide les entreprises à économiser de l'argent, à réduire la complexité et à gagner en vitesse.

Google Cloud Partner

Data protection and key management recommended by Google
Virtru est le seul partenaire de sécurité tiers recommandé par Google qui fournit un chiffrement dans l'ensemble de l'écosystème Google, de Gmail à Google Workspace et à Google Cloud Platform.

Apporter un chiffrement de bout en bout à Gmail

De la propriété intellectuelle inestimable aux données sensibles des employés et des clients, la boîte de réception de l'entreprise est un véritable trésor pour les pirates. Un message transmis par erreur ou un clic distrait sur un e-mail de phishing peut être extrêmement dommageable : IBM estime le coût moyen d'une violation de données à 3,86 millions de dollars. Pour les cadres dont les informations particulièrement sensibles, stratégiques et précieuses sont stockées dans leurs boîtes de réception, les enjeux peuvent être encore plus importants.

Les risques d'entreprise tout aussi importants comprennent la conformité réglementaire et les sanctions gouvernementales. Alors que les violations de données sont devenues de plus en plus courantes, les régulateurs gouvernementaux ont accru la surveillance de la confidentialité et de la sécurité des données. Les réglementations américaines telles que HIPAA, CJIS, FERPA, ITAR, CMMC et bien d'autres nécessitent des étapes spécifiques, y compris le chiffrement, pour protéger les informations sensibles. En 2021, un décret de la Maison Blanche sur la cybersécurité a souligné l'importance du chiffrement pour protéger les données gouvernementales, en particulier alors que les cyberattaques continuent d'augmenter en ampleur, en sophistication et en gravité.

Pendant ce temps, l'Union Européenne (UE) exige de larges précautions de sécurité, avec des pénalités sévères en cas de non-conformité qui en ont fait une priorité pour les leaders de la sécurité à travers le monde. En plus d'être passibles d'amendes pour non-conformité, les dirigeants à la tête d'entreprises violées attirent la colère des représentants du gouvernement et sont souvent obligés de témoigner lors d'audiences, amplifiant les dommages causés à la réputation de leurs marques.

Conjugués au besoin croissant de partager des informations sensibles, à la prolifération des appareils mobiles et du travail à distance, ainsi qu'au rythme de la migration vers les plateformes cloud, les risques de sécurité et réglementaires font du chiffrement des e-mails un impératif pour les dirigeants d'entreprise.

Les dirigeants doivent faire de la sécurité complète des e-mails avec chiffrement de bout en bout une priorité stratégique pour l'ensemble de l'organisation. Équiper vos équipes pour chiffrer les messages et les pièces jointes Gmail peut faire la différence entre une situation de risque et une violation coûteuse et dommageable.

« Nous voulons que chacun ait la possibilité de protéger les fichiers qu'il envoie. À un moment donné, tout le monde dans l'entreprise devra partager quelque chose de sensible – peut-être pas tous les jours, peut-être pas toutes les semaines – mais finalement, ils en auront besoin. »

-Ram Avrahami, responsable mondial de l'informatique et des systèmes d'information, NEXT

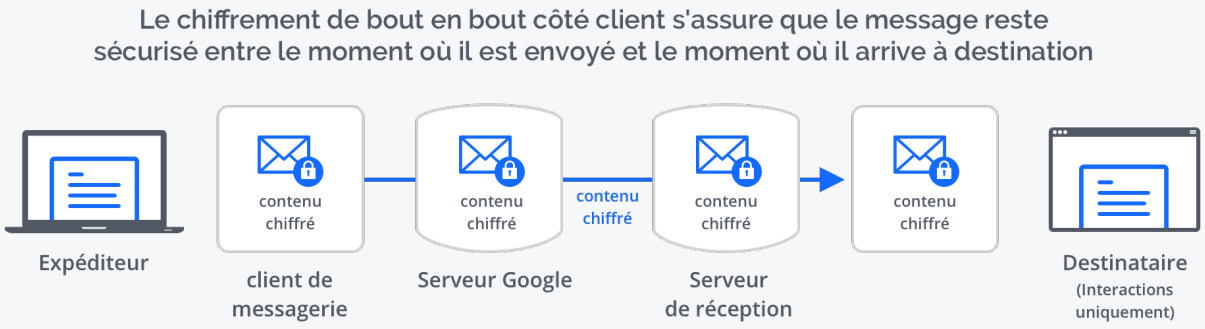
Lire l'étude de cas

Toute solution de chiffrement Gmail viable à trois exigences de base : une protection de bout en bout, la gestion et le contrôle des clés et la facilité d'utilisation.

Chiffrement de bout en bout

Des solutions véritablement sécurisées pour la protection des e-mails d'entreprise utilisent une protection de bout en bout. Votre entreprise ne peut pas se permettre une perte importante de données car un e-mail a été compromis du côté du destinataire. Contrairement aux solutions natives de sécurité de la couche de transport (TLS) de Google et basées sur des portails tiers, le chiffrement de bout en bout protège les données dès leur création, et ce contenu sécurisé reste protégé même après qu'il a été partagé et que les destinataires y ont accédé.

De plus, certains cadres de réglementation et de conformité nécessitent un chiffrement de bout en bout côté client. Ainsi, si vous devez respecter les réglementations de conformité ou maintenir la souveraineté des données, la sécurité des e-mails et des fichiers TLS natifs dans le cloud ne suffira pas.



Le chiffrement de bout en bout côté client s'assure que le message reste sécurisé entre le moment où il est envoyé et le moment où il arrive à destination

Gestion et contrôle des clés

Tout l'intérêt de l'utilisation du chiffrement, au-delà de la protection contre le vol et les fuites de données, est de garder le contrôle total de vos propres données. Lorsque vous utilisez le chiffrement TLS nativement intégré à Gmail, Google détient les clés de votre contenu et doit accéder à ces données afin d'activer la recherche et les analyses de logiciels malveillants. Lorsque vous utilisez un système de portail, le fournisseur de ce portail possède vos clés et a accès à votre contenu. Ce n'est qu'avec une véritable solution de chiffrement de bout en bout côté client que vous obtenez la propriété complète de vos propres clés de chiffrement et un contrôle granulaire sur qui peut déverrouiller et accéder à votre contenu.

Facilité d'utilisation

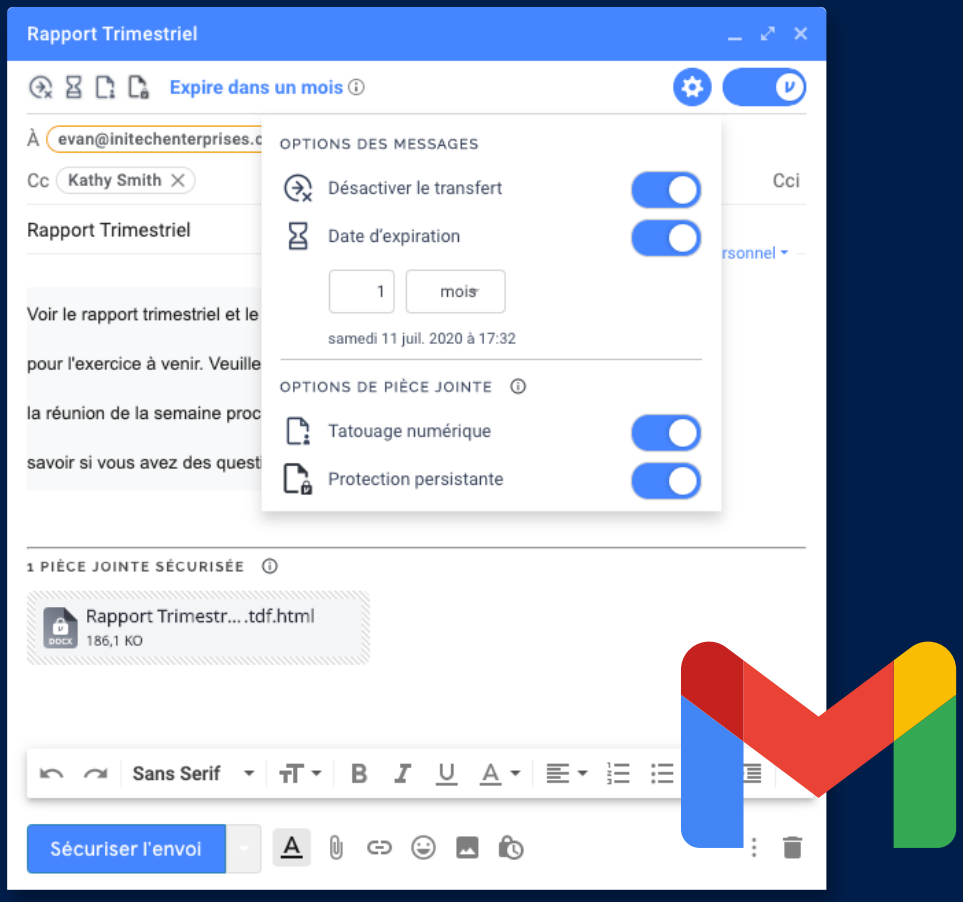
L'un des problèmes que les entreprises rencontrent couramment avec le chiffrement de bout en bout est que les solutions héritées telles que Pretty Good Privacy (PGP) et S/MIME sont difficiles à utiliser. De plus, le service S/MIME hébergé de Google n'empêche pas l'accès des tiers aux données. Google a accès au contenu non crypté, ainsi qu'aux clés de chiffrement qui contrôlent qui peut voir ce contenu.

Pour que le chiffrement des e-mails d'entreprise soit une solution viable, il ne nécessite pas seulement le meilleur en matière de sécurité et de contrôle, il nécessite également de la commodité, en particulier compte tenu du volume d'e-mails entrants et sortants que les entreprises reçoivent quotidiennement. Les entreprises qui migrent vers Google s'attendent à une facilité d'utilisation et à une simplicité, et les anciennes approches de chiffrement de bout en bout ne répondent tout simplement pas aux besoins des dirigeants soucieux de la sécurité.

Responsabilisez les utilisateurs avec Virtru pour Gmail

Lorsqu'il s'agit de protéger les données partagées par e-mail, les responsables de la sécurité doivent accomplir deux choses clés : favoriser des comportements de sécurité solides pour les utilisateurs finaux et créer un filet de sécurité qui capture les informations sensibles qui ont pu passer entre les mailles du filet.

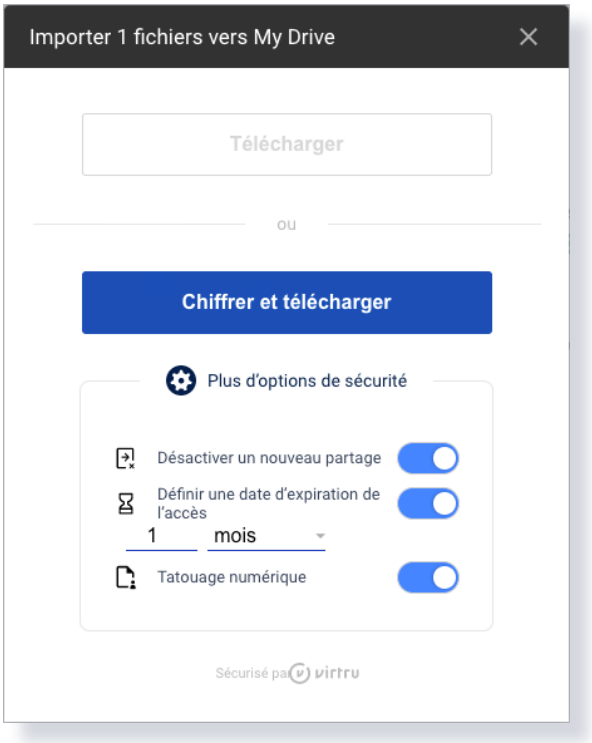
Virtru vous équipe pour faire les deux. Les utilisateurs sont autorisés à protéger leurs propres données et à définir les paramètres d'accès d'un simple clic sur le bouton bleu Virtru, directement dans leur interface Gmail. Les utilisateurs et les administrateurs peuvent conserver une visibilité sur leurs données à tout moment, et ils peuvent choisir de révoquer l'accès à tout moment, même après que les données ont été partagées ou consultées. Les administrateurs peuvent également définir des règles DLP (Data Loss Prevention) personnalisées pour créer un « filet de sécurité » qui chiffre automatiquement les messages contenant certains types de données sensibles. Les administrateurs peuvent également activer automatiquement le chiffrement par défaut pour les utilisateurs qui traitent généralement des données hautement réglementées, garantissant que les informations sont protégées dès qu'un utilisateur commence à rédiger un message.



Accélérer la collaboration sécurisée dans Google Workspace

Les équipes du monde entier aiment déjà utiliser les applications de collaboration de Google. Avec l'annonce en 2021 du chiffrement côté client de Google pour Workspace, les entreprises peuvent utiliser Google Docs, Sheets et Slides avec la certitude qu'elles sont sécurisées et qu'aucun tiers ne peut accéder à leurs données. Les organisations peuvent également ajouter une couche de chiffrement à leurs documents stockés et partagés dans Google Drive, similaire au chiffrement utilisé pour protéger les messages et les pièces jointes Gmail.

Un élément clé de cette couche de sécurité est la gestion indépendante des clés : garantir que les clés de chiffrement permettant de déverrouiller les données sensibles sont stockées et gérées indépendamment de Google. Pour ce faire, les organisations doivent sélectionner un partenaire de gestion de clés agréé Google, tel que Virtru.



Partagez en toute confiance à l'aide de Virtru pour Google Workspace

Virtru fournit un chiffrement de bout en bout des fichiers pour Google Drive, qui complète son chiffrement de bout en bout pour Gmail. Cela protège les fichiers en dehors de l'écosystème Google téléchargés sur Drive, y compris les fichiers PDF, les images, les vidéos, les fichiers CAO et Adobe, etc.

Virtru est également un fournisseur de gestion de clés recommandé par Google pour son chiffrement côté client pour Google Workspace. À ce titre, Virtru sert de gestionnaire de clés tiers de confiance pour sécuriser les clés de vos données hébergées dans le cloud.

L'un des principaux avantages de l'utilisation de Virtru dans l'écosystème Google est que vous bénéficiez d'un cadre unique et complet pour protéger vos données en toute sécurité, partout où elles vivent et se déplacent dans Gmail, Google Drive et Google Workspace.

Lors de l'évaluation de votre partenaire de chiffrement, vous devrez prendre en compte sa gamme complète de fonctionnalités et déterminer si ces fonctionnalités s'étendent à l'ensemble de l'écosystème Google. Le tableau ci-dessous compare Virtru à d'autres clés de chiffrement tiers partenaires. Pour plus de renseignements, consultez la fiche technique de Virtru, *Choisir votre partenaire de gestion des clés de chiffrement pour le chiffrement côté client de Google Workspace*.

Comparer les solutions des partenaires pour Google Workspace, Google Cloud et au-delà

	Capacités de protection des données	Autres fournisseurs	Virtru
Google Workspace	Sécurisation des fichiers natifs de Google (Docs, Sheets et Slides) dans Google Workspace		
	Chiffrement et téléchargement de fichiers statiques dans Google Drive (PDF, Word, Excel, PowerPoint et fichiers image)		
	Usage d'un module de sécurité matérielle (HSM) pour une sécurité maximale		
	Extension de la protection des données aux messages Gmail et leurs pièces jointes		
	Usage d'une solution basée sur le cloud pour améliorer déploiement, la gestion et la facilité d'utilisation à travers votre organisation		

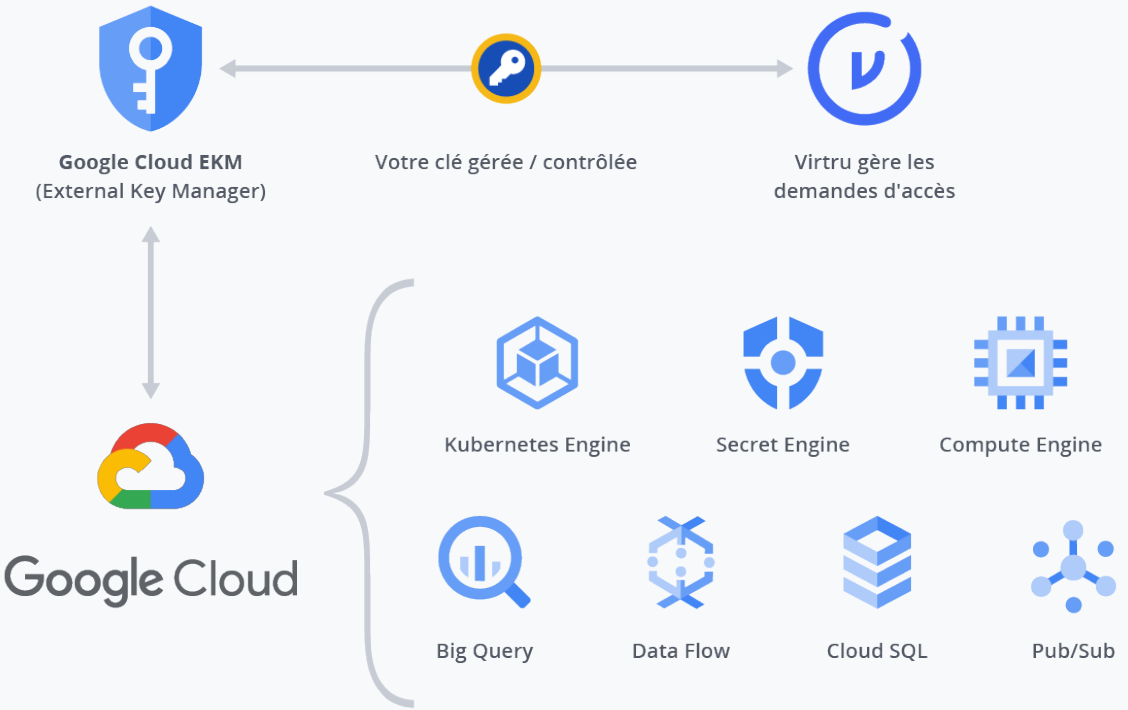
Garantir une confidentialité totale des données pour Google Cloud Platform (GCP)

Avec autant d'entreprises en pleine transformation numérique, beaucoup tirent parti de Google Cloud Platform pour moderniser leurs piles technologiques. Google Cloud Platform offre aux entreprises un environnement polyvalent et évolutif pour créer et héberger leurs architectures système.

À l'instar du chiffrement côté client pour Workspace, Google permet aux entreprises de chiffrer leurs données sur Google Cloud Platform. Comme pour Workspace, cela nécessite un partenaire de gestion des clés externes (EKM).

À partir de 2021, les entreprises pourront utiliser Virtru en tant que partenaire EKM pour gérer en toute sécurité leurs clés de chiffrement séparément de leurs données dans Google Cloud Platform, renforçant ainsi la confidentialité et la souveraineté des données sur l'ensemble de Google Workspace, GCP et d'autres applications cloud. Cette approche Zero Trust de la protection des données peut être utilisée pour protéger les lacs de données, les bases de données et les informations qui transitent par les capacités de cloud computing et d'IA de Google.

Avec la solution de gestion des clés de Virtru en place pour Google Cloud, les entreprises peuvent disposer d'un cadre et d'un langage de politique uniques et mondiaux pour protéger toutes les données de l'écosystème Google Cloud, qu'elles soient générées par les utilisateurs, les appareils ou les systèmes.



Souveraineté des données dans le cloud

Pour les organisations mondiales, le chiffrement de bout en bout résout un problème important : la souveraineté et la résidence des données. La souveraineté des données signifie que les données sont soumises aux lois et règlements de l'emplacement géographique où ces données sont collectées et traitées. La souveraineté des données est une exigence spécifique au pays selon laquelle les données doivent rester à l'intérieur des frontières de la juridiction d'où elles proviennent. Fondamentalement, la souveraineté des données consiste à protéger les données sensibles et privées et à s'assurer qu'elles restent sous le contrôle de leur propriétaire.

Compte tenu de la domination du marché des fournisseurs américains de solutions cloud et logicielles, la plupart des entreprises concurrentes dans l'UE qui exploitent les technologies cloud et collectent des données sur les consommateurs doivent faire face au problème des réglementations américaines par rapport à celles de l'UE dans leur fonctionnement quotidien.

Heureusement, il existe une solution pour ces entreprises, une solution qui permet une pleine participation à l'économie mondiale, maintient les avantages du cloud public et offre un contrôle complet sur l'accès aux données. En novembre 2020, le comité européen de la protection des données (EDPB) a adopté des orientations précisant que le chiffrement de bout en bout est une mesure efficace pour permettre à la fois l'adoption du cloud et les exigences de souveraineté des données de l'UE, qui sont souvent considérées comme la référence mondiale en matière de confidentialité.

Essentiellement, les entreprises concurrentes dans l'UE peuvent associer les contrôles de sécurité stricts offerts par la technologie de cryptage avec les SCC, garantissant la conformité avec la législation européenne post-Schrems II tout en offrant un chemin géré vers l'accès autorisé pour les agences gouvernementales américaines et d'autres entités. C'est là que Virtru peut vous aider.

Virtru a adopté une approche de la sécurité des données qui donne la priorité à la confidentialité et au contrôle entièrement gérés par les clients. La plateforme Virtru garantit que vos données - et celles de vos clients - restent chiffrées et lisibles, même en cas d'activation de la loi américaine Cloud Act.

Comment ? La solution la de Virtru est indépendante de l'infrastructure cloud et du fournisseur, crypto-agile et implémentée de bout en bout par défaut. Les options de gestion des clés chiffrées garantissent qu'aucune entité, y compris les fournisseurs de cloud, n'est en mesure d'accéder aux données sans obtenir le consentement du propriétaire des données, qui a la seule capacité d'accorder l'accès par déchiffrement. En un mot, Virtru soutient collaboration mondiale par biais conformes des données et flux transfrontaliers en s'assurant que:

1. Les données peuvent être stockées sur une solution de cloud computing, y compris ceux qui sont offerts par des fournisseurs américains comprenant les solutions commerciales de Google, Microsoft, et Amazon.

2. Les données sont enveloppées dans une couche de protection (chiffrement) qui ne peut être déverrouillée que par le client ou le destinataire désigné. Bien que les données soient toujours accessibles, elles restent chiffrées et illisibles.

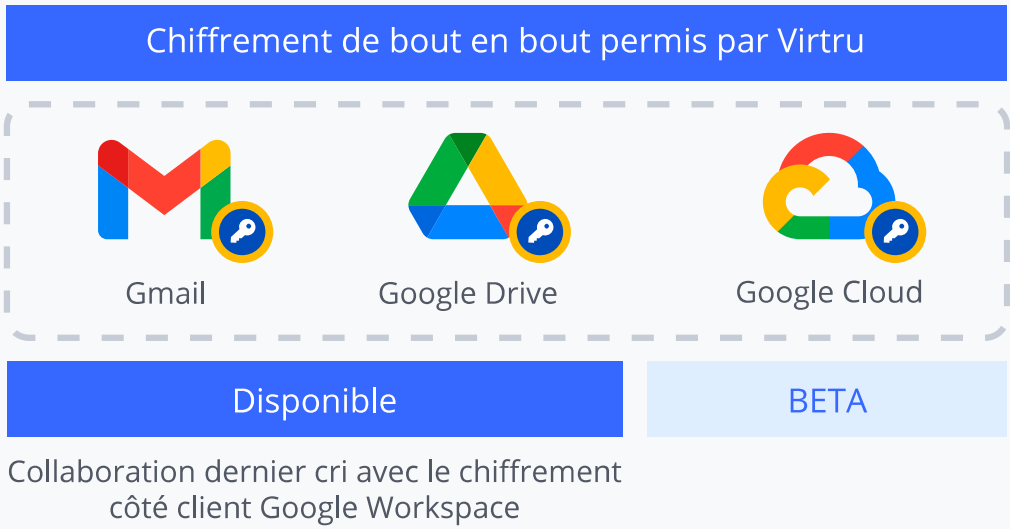
3. Les clés qui déverrouillent cette couche protectrice sont gérées en dehors de la solution cloud. Virtru offre la possibilité de stocker les clés de chiffrement, le cœur du mécanisme de chiffrement, sur site ou dans un cloud privé détenu et géré uniquement par le client, réalisant ainsi la souveraineté des données.

Pour plus de détails sur le maintien de la souveraineté des données dans le cloud, lisez notre guide, *Qui détient les clés de vos données* ?

Virtru sécurise les données dans l'ensemble de votre écosystème Google

Virtru offre le meilleur de la sécurité et de la facilité d'utilisation, dans l'ensemble de l'écosystème de Google.

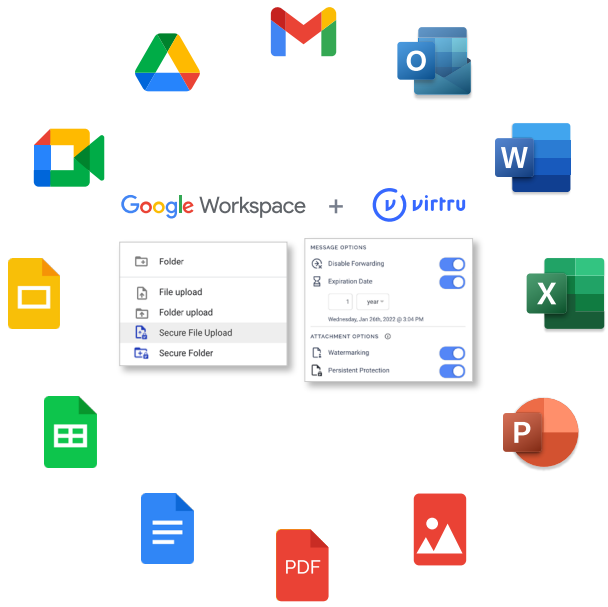
- Pas de logiciel à installer
- Utilisation de votre identité existante
- Gestion de clé Zero Trust
- Facilité d'utilisation pour tous
- Confidentialité, souveraineté, résidence et contrôle des données



Les technologies publiques basées sur des clés fournissent un chiffrement de bout en bout ; cependant, ils le font au détriment de la convivialité. Les technologies de chiffrement basées sur les portails ne chiffrent pas le chemin complet entre l'expéditeur et le destinataire du contenu, et elles introduisent également beaucoup de complexité, obligeant souvent les utilisateurs à créer des informations d'identification ou à télécharger des logiciels supplémentaires. Avec Virtru, vous n'obtenez pas seulement une meilleure sécurité Google, vous bénéficiez d'un contrôle et d'une visibilité totale ; une expérience fluide ; et la commodité pour les utilisateurs, les destinataires et les administrateurs.

Contrairement aux solutions TLS et celles basées sur des portails, Virtru ne se contente pas de chiffrer vos données en transit. Votre message est chiffré dès que vous créez un nouveau brouillon. Étant donné que Virtru utilise un véritable chiffrement de bout en bout côté client, il y a moins de points de vulnérabilité le long du chemin de votre courrier électronique vers la boîte de réception de votre destinataire. Votre message reste en sécurité et aucun tiers ne peut accéder à vos données, y compris Virtru. Votre entreprise garde un contrôle total sur vos clés et votre contenu.

Au-delà du chiffrement, Virtru ajoute également un granulaire contrôle d'accès. Les utilisateurs et les administrateurs peuvent contrôler qui a accès au contenu sensible avec des fonctionnalités telles que la révocation des messages, l'expiration, le contrôle du transfert et le filigrane des fichiers. Virtru ajoute également de puissantes capacités d'audit via le Control Center. Vous pouvez suivre les e-mails et les pièces jointes envoyés à ou à partir de n'importe qui dans votre organisation et tracer où les e-mails sortants ont été transférés.



Enfin, mais c'est important, Virtru est exceptionnellement facile à utiliser, pour toutes les personnes impliquées. Vous pouvez le déployer dans toute votre organisation en quelques minutes, et comme il est directement intégré à l'interface Google, vos utilisateurs n'ont qu'à cliquer sur un bouton pour chiffrer un fichier ou un e-mail. Il n'y a pas d'informations d'identification supplémentaires à retenir. Vous n'avez pas besoin d'échanger les clés manuellement avec votre destinataire.

Que vous ayez besoin de répondre à des exigences réglementaires ou de protéger des informations juridiques, financières ou RH sensibles, le chiffrement est un élément essentiel de la sécurité stratégique de l'entreprise. Virtru fournit le cadre le plus simple, le plus sécurisé et le plus complet pour protéger vos données sur Google Workspace, Google Cloud et au-delà.

Vous voulez découvrir comment Virtru peut ajouter une couche de sécurité à votre écosystème Google ? Contactez-nous pour démarrer la conversation.

virtru

Chez Virtru, nous permettons aux organisations d'exploiter leurs données en toute simplicité tout en gardant le contrôle, quel que soit l'emplacement où elles sont stockées et partagées. Notre portefeuille de solutions et d'outils, basés sur notre plateforme de protection des données ouverte, régit les données tout au long de leur cycle de vie. Plus de 6 000 clients font confiance à Virtru pour la sécurité des données et la protection de la confidentialité.