Protection des informations d'entreprise grâce à la spécification TDF et à la plateforme de données approuvée de Virtru

Protection des données et contrôle d'accès multiplateforme intégré

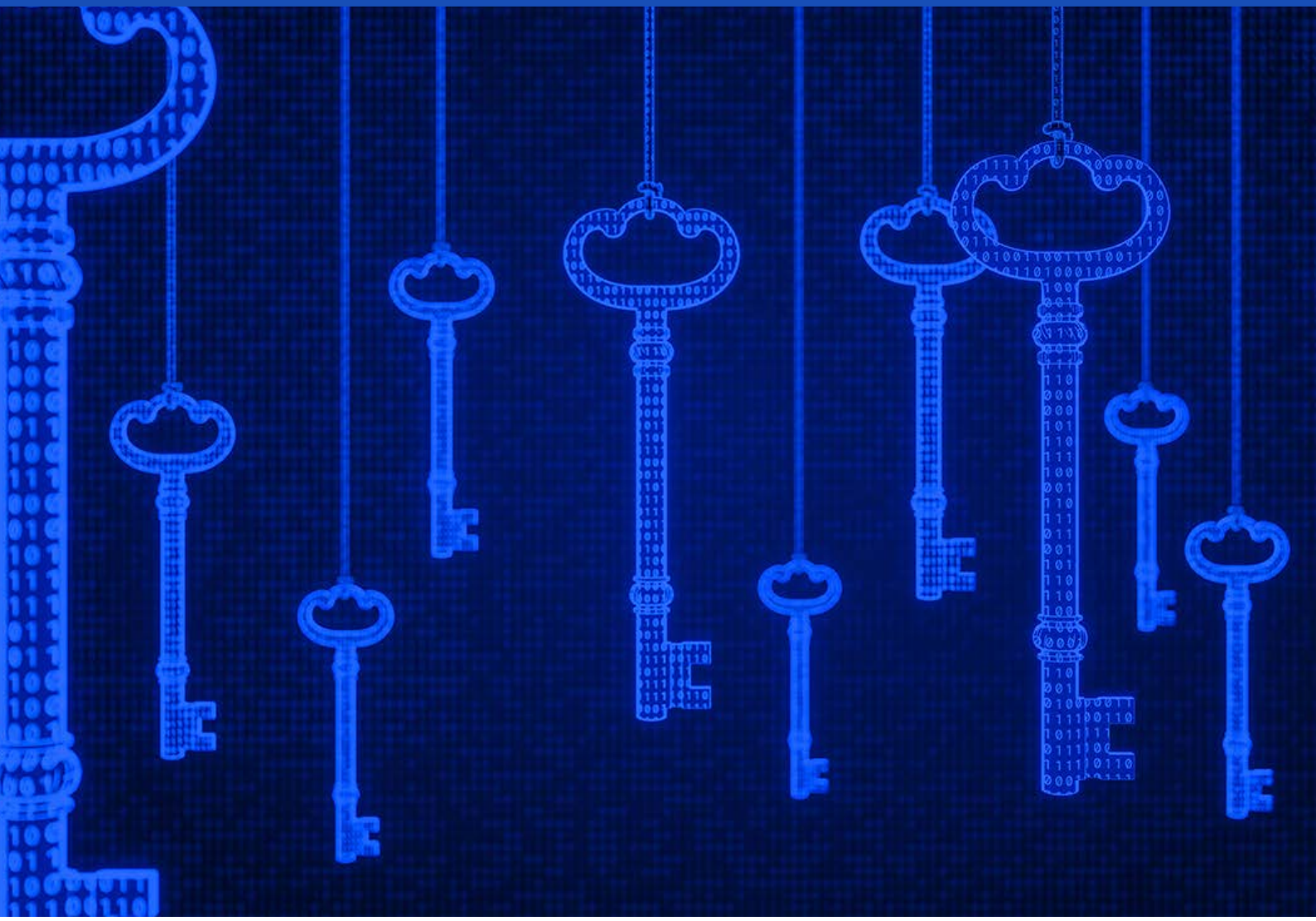


Table des matières

1. La nécessité d'une nouvelle approche de la protection des données

Dans un contexte de croissance des applications cloud et de mobilité accrue des effectifs, la plupart des entreprises rencontrent des difficultés pour protéger, partager et contrôler des informations sensibles. Les solutions existantes demandent beaucoup trop d'efforts de la part des créateurs de contenu comme des consommateurs, et elles ne garantissent pas de protections persistantes une fois que les informations quittent le domaine d'origine.

> **Protections centrées sur les données persistantes :** les protections modernes, qui accompagnent les objets de données individuels (corps d'e-mail, fichiers, champs de base de données) plutôt que de rester liées aux applications ou aux réseaux, permettent enfin de surmonter ces défis tenaces en matière de sécurité des données. Pouvant être appliquées côté client ou par chiffrement au niveau objet, ces protections occupent désormais une place centrale grâce à leur capacité à accompagner les données elles-mêmes, sans avoir à tenir compte du type de serveur ou d'écosystème cloud qu'elles traversent. Elles offrent aux entreprises la simplicité qu'elles espèrent depuis si longtemps en matière de contrôle, de visibilité et de chiffrement.

Si ce type de protection est largement reconnu comme un composant essentiel à toute solution visant à surmonter ces difficultés (parmi d'autres), la complexité technique et un manque de capacités de contrôle entravent encore leur adoption généralisée, ainsi que celle des systèmes de chiffrement côté client étroitement liés. Ces technologies avaient encore récemment la réputation d'être trop compliquées pour permettre un usage et une adoption plus répandus.

Par exemple, les technologies de chiffrement d'e-mail avancé côté client, telles que les spécifications PGP (Pretty Good Privacy) et S/MIME (Secure/Multipurpose Internet Mail Extensions), exigent des connaissances techniques poussées et ne permettent pas un partage facile des données. Les outils de gestion des droits numériques (GDN) développés pour la protection des documents peuvent compliquer le partage de contenu entre différents environnements cloud, les rendant ainsi essentiellement inutilisables pour la plupart des cas d'utilisation en entreprise. Cette situation a conduit les entreprises à se fier excessivement à des approches insuffisantes concernant la protection des données, telles que les outils de sécurité périmétrique et des offres de gestion des droits en silos.

2. Obligations en matière de protection des données pour les entreprises modernes

Les technologies de protection existantes n'ont pas été conçues pour répondre aux besoins les plus importants de l'entreprise moderne :

Facilité d'utilisation pour les créateurs et consommateurs de contenu

La collaboration sur le cloud a renforcé les attentes en matière de convivialité autour des outils de sécurité modernes. Si les dispositifs de protection des données perturbent le travail des utilisateurs finaux existants, ces derniers s'en passeront purement et simplement, même si cela implique de partager des données non protégées. Par ailleurs, les entreprises d'aujourd'hui partagent des données avec un grand nombre d'organisations, de prestataires de services et d'applications cloud. Pour être efficaces, les protections doivent accompagner les données où qu'elles aillent, et l'expérience utilisateur doit rester uniforme sur toutes les plateformes. La moindre complexité peut suffire à freiner l'adoption des technologies les plus sûres.

Vérification et contrôle multiplateformes

Une protection complète des données va au-delà de leur simple sécurisation. Qu'elles soient partagées volontairement avec des partenaires, des clients ou autres parties prenantes par leur propriétaire, ou qu'elles soient partagées par un collaborateur du propriétaire sans que ce dernier n'en soit informé, la plupart des données finissent à un moment ou un autre par quitter l'organisation. Il est vital que les entreprises soient en mesure de surveiller le parcours de ces données et d'en gérer les droits d'accès, y compris après qu'elles ont été partagées et consommées, faute de quoi sécurité et collaboration deviennent vite incompatibles.

Sécurité flexible

Entre le respect de la conformité, la réglementation en matière de domiciliation des données et les politiques de confidentialité des entreprises, difficile de trouver des organisations partageant exactement les mêmes obligations de sécurité. Les solutions de protection des données se doivent ainsi de proposer des options de configuration flexibles pour satisfaire les exigences en matière de confidentialité, le goût du risque des différentes entreprises et les divers scénarios de collaboration.

Plus particulièrement, c'est la méthode de chiffrement qui doit répondre aux besoins des clients. Pour ne plus avoir à faire de compromis entre sécurité et facilité d'utilisation, les organisations doivent être en mesure de décider où leurs clés de chiffrement sont stockées, qui peut y accéder et comment elles sont gérées.

Virtru a été fondée dans l'optique de rassembler ces qualités sur une seule et même plateforme de partage de données homogène et conviviale. Virtru a pour mission d'exploiter pleinement la puissance des données en créant un monde dans lequel elles n'échappent jamais au contrôle de leur propriétaire. À cette fin, Virtru s'efforce d'éliminer le compromis entre protection des données et facilité d'utilisation en faisant de la protection centrée sur les données la nouvelle norme pour les organisations professionnelles.

Les entreprises sont sans cesse confrontées à de nouvelles obligations en matière de protection des données et de confidentialité, et se doivent de tenir le rythme. Dans ce contexte, l'approche novatrice de Virtru vient combler nombre de lacunes des anciennes technologies en matière de convivialité, de contrôle et de sécurité.

3. Le socle des solutions Virtru : la spécification TDF (Trusted Data Format - Format de données approuvé)

De nombreuses solutions de protection des données modernes effectuent des contrôles de sécurité par plateforme (au repos) ou par connexion (en transit). Les propriétaires de données ne peuvent souvent rien faire d'autre qu'espérer que chaque système ou fournisseur pouvant stocker ou transmettre leur contenu a mis en place des contrôles de sécurité et des politiques d'accès aux données adéquats. Si et lorsqu'elles comptent sur ces tiers pour protéger leur contenu, les entreprises doivent renoncer au contrôle qu'elles ont sur leurs données dès qu'elles sont partagées ou transmises et stockées.

Le format TDF est né de la nécessité d'une approche ouverte et interopérable qui permettrait aux protections d'accompagner les données sans contraindre les collaborateurs et les destinataires à adopter au préalable un système particulier. Il peut être considéré comme une protection ponctuelle pour chaque type de données.

Le format **TDF (Trusted Data Format - Format de données approuvé)** est un format de fichier XML à norme ouverte utilisée par la communauté du renseignement des États-Unis afin d'appliquer un balisage et des fonctionnalités de sécurité au niveau des fichiers. Ces fonctionnalités comprennent notamment la création d'assertions fondées sur des propriétés de données ou sur des balises, l'association cryptographique et le chiffrement des données. Le TDF est une norme ouverte et ne nécessite aucune technologie propriétaire ou brevetée. Son utilisation est donc gratuite pour tous.

Initialement développé par Will Ackerly, DPT et cofondateur de Virtru, pour le compte de la communauté du renseignement des États-Unis, le TDF est un format à norme ouverte permettant de placer un enveloppeur autour de tout type de contenu et de ses métadonnées, y compris les assertions de métadonnées.

Ces assertions sont des exigences issues de stratégies grâce auxquelles un créateur de contenu peut définir et appliquer une large gamme de politiques portant sur le contenu fourni au destinataire. Elles permettent par exemple de faire expirer les droits d'accès au contenu du destinataire à une date prévue, d'appliquer des exigences de mise en dépôt de clés, d'autoriser ou d'interdire le transfert de contenu par les destinataires, ou encore d'effectuer un suivi des transferts de contenu. Il protège également l'intégrité des données par le biais d'associations inviolables de ces assertions de métadonnées. Assurant à la fois confidentialité et intégrité, le TDF protège le contenu de tout dispositif espion ou intermédiaire malveillant qui chercherait à y accéder ou à l'altérer.

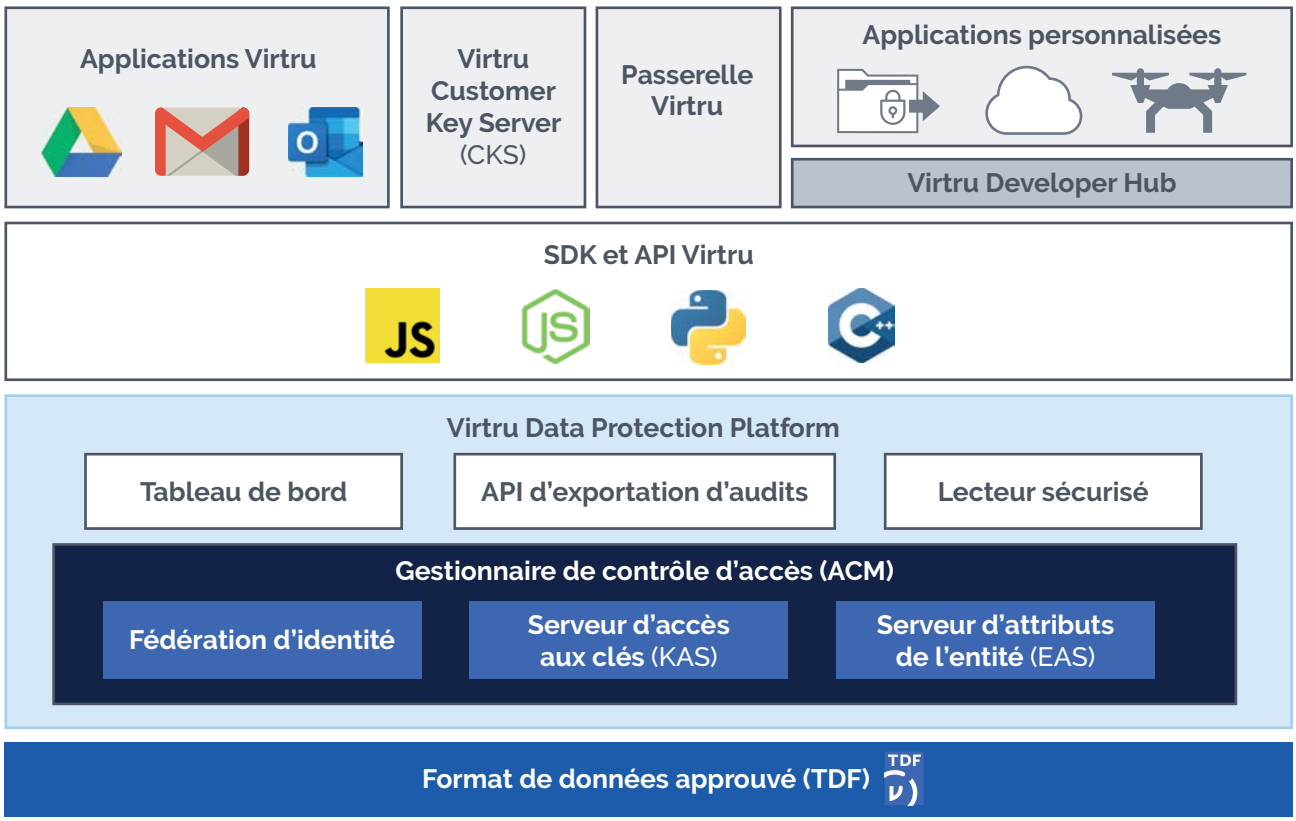
En 2013, la communauté du renseignement des États-Unis a formellement adopté une version du TDF propre aux pouvoirs publics, qui comprend une classification et des marquages de contrôle standardisés, en tant que format interagences standard pour la protection des données sur plusieurs plateformes.

4. Le TDF en pratique : la plateforme de données approuvée (TDP) de Virtru

Le TDF fait de Virtru une solution bien plus complète que celles qui se contentent de chiffrer du contenu en transit sans fournir ni vérification ni contrôle persistant. Là où la plupart des anciennes solutions se limitent aux e-mails, la plateforme de données approuvée de Virtru permet aux entreprises de protéger tout type de contenu partagé par e-mail, par le biais de services de partage de fichiers et par d'autres applications commerciales.

Virtru s'appuie sur le TDF pour mettre à disposition une plateforme de type SaaS (Software as a Service) permettant d'assurer le contrôle des accès, l'application des politiques et la gestion des clés. Les politiques de protection des données sont appliquées par le biais d'intégrations fluides à des applications de productivité courantes, telles que Google G Suite, Microsoft Office 365 et Microsoft Exchange, ou à d'autres applications SaaS comme Salesforce, WorkDay et NetSuite. Les développeurs tiers peuvent s'appuyer sur les SDK Virtru pour intégrer le format TDF à Google Cloud Platform (GCP) et à Amazon Web Services (AWS), de façon à incorporer une protection des données persistante au niveau de l'objet dans leurs applications et workflows personnalisés.

La configuration et l'application de ces politiques s'effectuent de manière centralisée, et vous avez la possibilité de définir des avertissements si vous le souhaitez. Virtru offre également des contrôles flexibles, à la demande, tels que la possibilité de vérifier les accès, de les révoquer ou de leur attribuer une date d'expiration, ainsi que de restreindre le partage du contenu protégé, même en dehors de l'entreprise. Les clients gardent un contrôle total sur les clés utilisées pour la protection de leurs informations.



Architecture la plateforme de données approuvée (TDP) de Virtru

La TDP de Virtru fait oublier les limites des anciennes solutions pour répondre aux besoins de protection des entreprises travaillant dans le cloud :

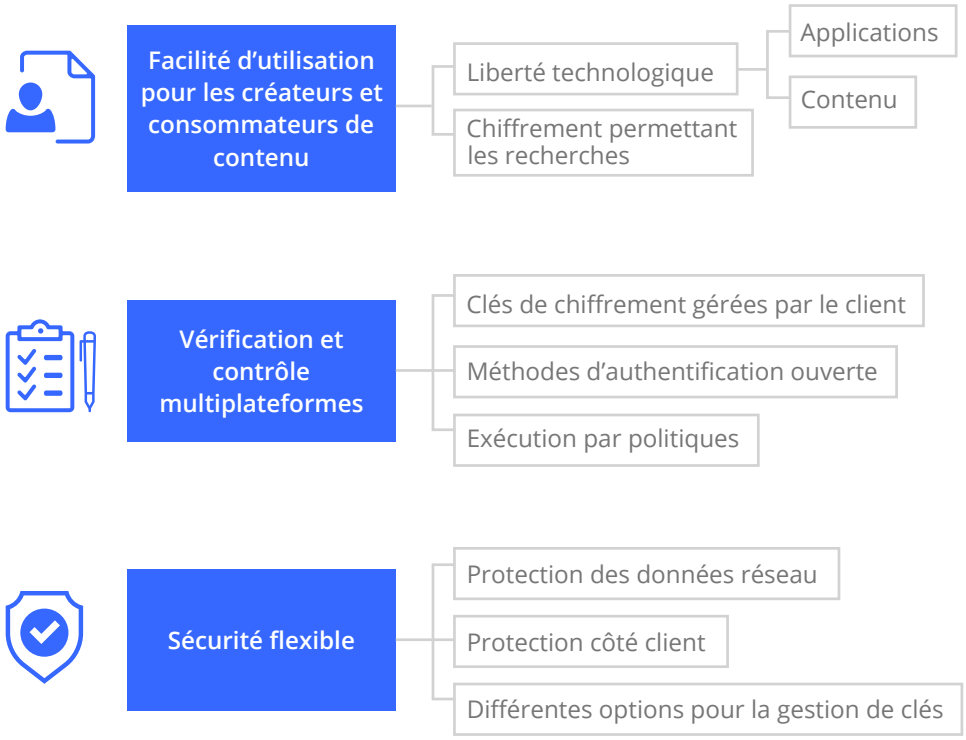
Protection persistante : la TDP de Virtru permet aux entreprises de protéger tous les types de contenu de leur création à la fin de leur cycle de vie.

Partage facilité : la TDP de Virtru permet aux utilisateurs de partager du contenu sécurisé avec tout destinataire au sein de l'entreprise ou en dehors, sans qu'il soit nécessaire de procéder à un échange de clés ou à une autre complexité d'ordre technique.

Intégration transparente aux workflows existants : la TDP de Virtru est conçue pour s'intégrer facilement aux applications et workflows existants, ce qui vous permet de renforcer la sécurité sans incidence sur la productivité des utilisateurs.

Pour répondre à ces besoins, la TDP de Virtru se concentre sur trois aspects essentiels :

- Facilité d'utilisation pour les créateurs et consommateurs de contenu
- Vérification et contrôle multiplateformes
- Sécurité flexible



Trois exigences essentielles pour la protection des données des entreprises

Initialement conçue pour satisfaire les exigences strictes de la communauté du renseignement des États-Unis, la TDP de Virtru offre un haut niveau de sécurité et de contrôle d'accès, tout en garantissant un taux d'adoption élevé par les utilisateurs.

La suite de ce document se penche en détail sur ces exigences, les modalités d'implémentation de la TDP de Virtru, ainsi que son architecture fonctionnelle.

4.1 Facilité d'utilisation pour les créateurs et consommateurs de contenu

Les entreprises modernes utilisent un large éventail d'applications cloud et sur site, ainsi que de multiples plateformes de stockage cloud, et leurs utilisateurs doivent échanger du contenu dans de nombreux formats différents. Pour une sécurisation efficace des données d'entreprise, la TDP de Virtru a été conçue pour maintenir l'hétérogénéité des applications, des clouds et des contenus tout en assurant un workflow fluide pour les créateurs de contenu, les consommateurs de contenu et les administrateurs de systèmes informatiques. Associée à la technologie de recherche brevetée de Virtru, cette multiplicité vous permet d'intégrer la TDP de Virtru à vos infrastructures informatiques et sécurisées en place, sans incidence sur les workflows existants.

4.1.1 Applications offrant une liberté technologique

Pour garantir une adoption et une acceptation généralisées, les technologies de protection des données doivent s'intégrer parfaitement aux applications traditionnelles de messagerie et de stockage cloud, ainsi qu'à d'autres outils commerciaux. Cette intégration est gage de facilité d'utilisation et supprime les obstacles à l'adoption, aucune connaissance ou expertise technique particulière n'étant requise.

L'architecture de la TDP de Virtru est conçue pour assurer une intégration facile à tout type d'application. Une fois intégrées à une application existante, les bibliothèques Virtru assurent trois fonctions :

- Permettre le chiffrement de bout en bout côté client ou la protection côté serveur dès la création.
- Communiquer avec le gestionnaire de contrôle d'accès Virtru et Virtru Dashboard pour le contrôle d'accès, la gestion des clés et l'application des politiques.
- Activer le déchiffrement lorsque l'application reçoit du contenu protégé et que le consommateur de ce contenu est authentifié et dispose des autorisations nécessaires.

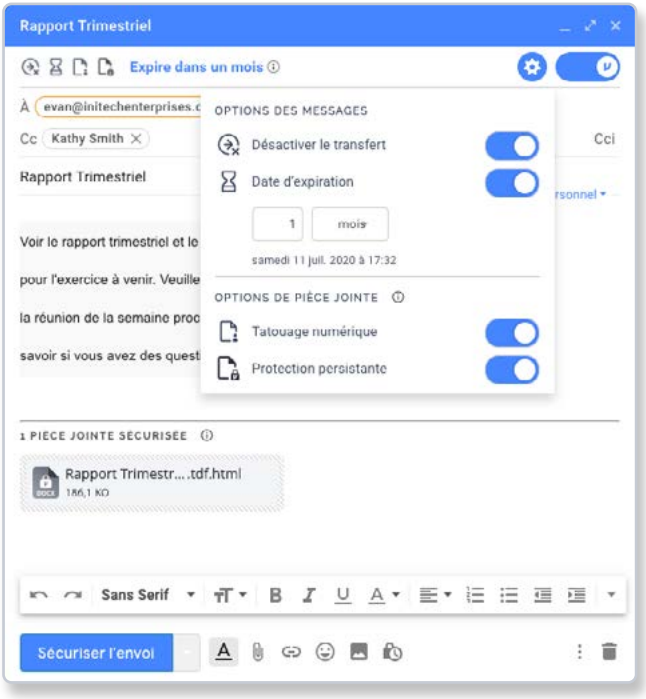
Secure User-First Technology de Virtru

Le contrôle d'accès multiplateforme et la facilité d'utilisation inédite de Virtru reposent sur une technologie breveté grâce à laquelle :

- Les destinataires peuvent déchiffrer et consommer du contenu protégé dans leur navigateur en toute sécurité sans avoir à télécharger ou à installer de logiciel supplémentaire.
- Les destinataires peuvent s'authentifier et consommer du contenu chiffré à l'aide de leurs identifiants existants. Pas besoin de créer de nouveaux noms d'utilisateur ou mots de passe.
- Les expéditeurs et les administrateurs peuvent chercher du contenu chiffré aussi simplement que du contenu non protégé.

Une fois Virtru déployé, la protection est intégrée aux interfaces natives des applications destinées aux utilisateurs finaux, et les processus de chiffrement et de déchiffrement s'effectuent de façon transparente.

À titre d'exemple, Virtru a parfaitement intégré son système de protection des données côté client à des services de messagerie électronique très populaires tels que l'application Web Gmail (Google) et l'application de bureau Outlook (Microsoft). Les utilisateurs voient simplement un bouton permettant de lancer le chiffrement et de nouveaux éléments de menu pour les contrôles d'accès, qui gèrent notamment la révocation et l'expiration. Toutes ces options s'intègrent à l'interface utilisateur native de l'application client sans la transformer.



La solution de chiffrement de bout en bout facile à utiliser de Virtru est directement intégrée à Gmail.

Contenu

Le contenu sensible se présente sous diverses formes : e-mails, documents Microsoft Office, vidéos, images, fichiers audio et formats de fichier propriétaires. Pour garantir un niveau de contrôle et de sécurité maximum sans qu'il soit nécessaire d'acquérir et de gérer plusieurs plateformes, les services de protection des données doivent prendre en charge tous les types de contenu.

La TDP de Virtru s'appuie sur le TDF pour protéger de façon homogène tous types de contenu, qu'il s'agisse d'e-mails, de documents ou d'autres formats de données et éléments. Assurant à la fois confidentialité et intégrité, le TDF protège le contenu de tout dispositif espion ou intermédiaire malveillant qui chercherait à y accéder ou à l'altérer. La fluidité du TDF sur tous les types de contenu garantit que cette protection supplémentaire ne nuit en rien à la convivialité.

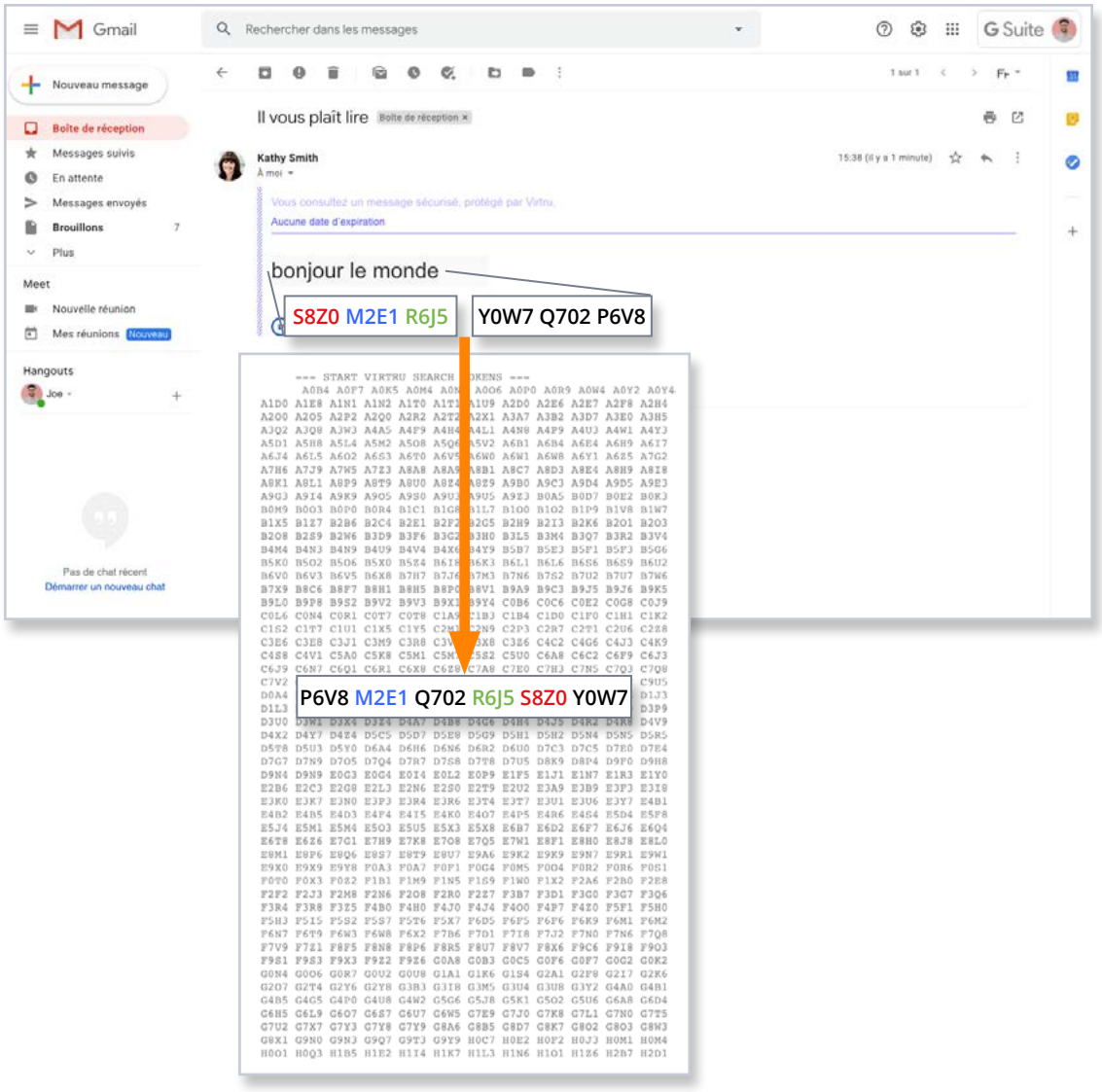
4.1.2 Chiffrement permettant les recherches

En matière de recherche et d'e-Discovery, le compromis entre convivialité et sécurité est particulièrement important. Si le chiffrement côté client est considéré comme le niveau de protection le plus élevé pour les données d'entreprise, les approches côté client traditionnelles, comme PGP et S/MIME, empêchent les utilisateurs finaux et les administrateurs d'effectuer des recherches dans le contenu protégé. Cette limite contraint les entreprises à sacrifier la sécurité au profit des capacités de recherches, dont elles ont besoin pour effectuer des vérifications, des suspensions pour raisons juridiques et d'autres activités dans le cadre de la procédure d'e-Discovery.

Grâce à sa technologie brevetée de chiffrement consultable, la TDP de Virtru offre la seule approche de protection côté client qui permet également d'effectuer des recherches dans le contenu chiffré de façon simple. Le chiffrement consultable de Virtru ajoute des jetons au contenu protégé. Ces jetons permettent aux utilisateurs d'effectuer des recherches côté client sur ce contenu sans révéler les critères de recherche aux serveurs de Virtru ou à d'autres tiers.

Chaque entreprise cliente de la TDP de Virtru reçoit automatiquement une clé de recherche partagée entre ses membres. Concernant les clients de messagerie Virtru, cette clé de recherche permet de générer des jetons de quatre caractères alphanumériques (par ex., a0b1 x9u3 b4u8) pour chaque mot du corps d'un e-mail. Ces jetons sont ensuite insérés dans l'e-mail lui-même, avec plusieurs jetons aléatoires supplémentaires pour la protection contre les attaques par corrélation.

Lorsqu'un utilisateur cherche un message dans la boîte de réception ou une solution d'archivage d'e-mails, des jetons sont générés pour chaque terme saisi et ajoutés à la demande de recherche. Le client de messagerie natif de l'utilisateur est ainsi en mesure de récupérer et d'afficher les résultats de recherche sans obtenir l'accès au terme de recherche ou au contenu sous-jacent. Cet accès n'est également jamais fourni aux serveurs Virtru, ce qui assure l'intégrité des workflows utilisateur existants et la sécurité des données.



Virtru remplace les termes recherchés par des jetons pour permettre de réaliser des recherches chiffrées sans dévoiler le texte brut de la recherche au fournisseur de messagerie.

4.2 Vérification et contrôle multiplateformes

La gestion des clés, la distribution et l'authentification des destinataires ont toujours été des difficultés importantes pour les utilisateurs d'anciennes technologies de protection des données. Pour répondre au besoin de partage étendu sans abandonner le contrôle d'accès, les solutions modernes doivent autoriser les créateurs de contenu à gérer l'accès à leurs données facilement, tout en permettant aux administrateurs d'appliquer automatiquement des contrôles et aux destinataires de s'authentifier de façon homogène à l'aide des identifiants et des workflows existants.

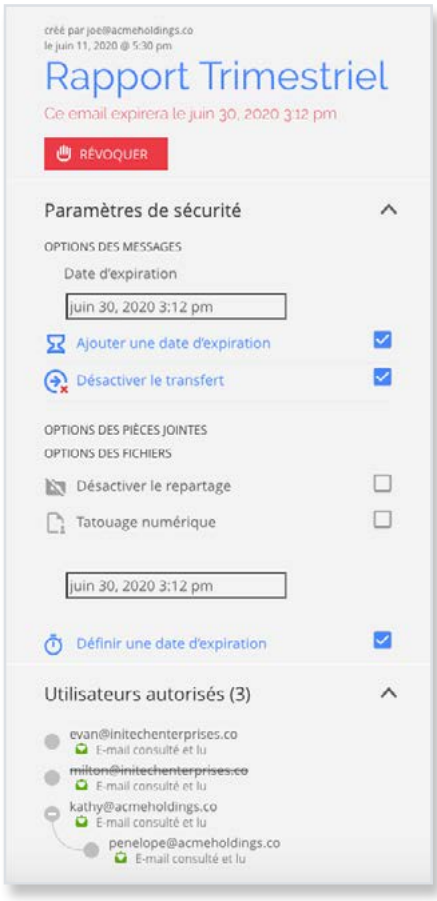
En outre, ces technologies doivent être en mesure de protéger les données transmises sur différents serveurs ou systèmes et d'offrir une visibilité persistance pour des audits rationalisés, un domaine dans lequel les solutions de GDN n'ont jamais été à la hauteur. Si nombre de ces produits fournissent des fonctionnalités de contrôle d'accès pour les données échangées au sein d'une même organisation, ils ne proposent pas de protections persistantes niveau objet. Or ces dernières sont indispensables pour les entreprises modernes qui souhaitent partager des données sensibles avec différents destinataires externes.

4.2.1 Gestion des clés de chiffrement et contrôle d'accès

L'architecture de la TDP de Virtru a notamment pour avantage de permettre aux propriétaires de contenu de gérer les clés de chiffrement pour exercer un contrôle granulaire sur l'identité des utilisateurs pouvant accéder à des documents sensibles et sur la durée de leur accès. Des clés individuelles sont créées pour chaque élément de contenu et chaque consommateur autorisé, permettant ainsi aux créateurs de contenu de gérer les accès à un niveau véritablement granulaire.

Les utilisateurs et les administrateurs peuvent, par le biais d'un client doté d'une extension Virtru ou d'un tableau de bord en ligne, révoquer les accès à du contenu, contrôler le transfert, définir des dates d'expiration, consulter des confirmations de lecture et des journaux d'audit, tatouer numériquement des fichiers et désactiver le téléchargement de pièces jointes. Ces contrôles sont disponibles tout au long du cycle de vie du contenu, sans tenir compte du fait qu'il ait été ouvert ou partagé.

Imaginons qu'un expéditeur envoie malencontreusement du contenu sensible en pièce jointe d'un e-mail à une liste de destinataires, parmi lesquels figure un tiers externe qui ne doit pas consulter ce contenu. Lorsqu'il réalise son erreur, le créateur de contenu peut simplement révoquer l'accès du destinataire accidentel à ce message. Cela n'aura aucune incidence sur les autres consommateurs. La révocation est immédiate et seul le propriétaire du contenu peut l'annuler.



Fonctionnalités d'audit et de contrôle d'accès dans Virtru Dashboard

4.2.2 Méthodes d'authentification ouverte

Plus de collaboration demande plus de protection. Les utilisateurs finaux n'ont qu'une tolérance très limitée pour les technologies de protection des données qui persistent uniquement lors du partage avec certains utilisateurs.

L'un des problèmes les plus importants des anciennes technologies de gestion des droits et de protection des données est qu'elles n'assurent plus cette protection en cas de communication avec des destinataires arbitraires utilisant des technologies ou des réseaux cloud différents.

Dans le cas du chiffrement d'e-mails par clés publiques, l'expéditeur et le destinataire doivent avoir implémenté la même technologie avant tout échange. Si le destinataire n'a pas de clé publique, l'identification des parties est impossible et cette technologie devient inutilisable pour l'échange d'e-mails protégés.

Les anciennes technologies de gestion des droits imposent également de sévères restrictions d'accessibilité aux expéditeurs et aux destinataires. Bien qu'elles permettent d'appliquer des autorisations d'utilisation aux données, les destinataires autorisés peuvent uniquement accéder à ces données s'ils font partie du même réseau que le créateur du contenu d'origine. Ces limites mettent expéditeurs et destinataires devant un choix inconfortable : soit le destinataire modifie ses workflows et adopte une nouvelle technologie lui permettant de s'identifier de manière adéquate, soit l'expéditeur partage ses données sans aucune protection.

Virtru élimine ce problème en évitant de dépendre de la disponibilité d'une clé publique du côté de l'expéditeur et de systèmes de portails ou de répertoires cloud séparés. La TDP de Virtru procède aux vérifications d'identité et aux autorisations d'accès à l'aide de services d'identification existants tels qu'OAuth, OpenID et SAML, ou par le biais d'une simple identification par e-mail avec des codes de vérification.

Les destinataires peuvent ainsi accéder à des données protégées quels que soient leur plateforme et leur fournisseur de services cloud. Les expéditeurs peuvent imposer des restrictions d'utilisation de leurs données sans craindre que les destinataires autorisés ne puissent pas y avoir accès.

Pour davantage de flexibilité et de sécurité, les méthodes d'authentification existantes d'un destinataire (par exemple, clés publiques et l'authentification à deux facteurs) peuvent être utilisées pour vérifier l'identité du destinataire sans avoir à créer de complexités supplémentaires. Cette approche est rendue possible par la nature hautement flexible de la gestion des clés au sein de la TDP de Virtru.

4.2.3 Exécution fondée sur les politiques

Les solutions de protection doivent étendre les possibilités de contrôle à la fois aux créateurs de contenu et aux administrateurs gérant leurs services informatiques. Cette nécessité complique l'équilibre entre visibilité et sécurité, dans la mesure où les données doivent être protégées des tiers tout en restant accessibles aux administrateurs internes et compatibles avec les autres politiques de domaine à appliquer.

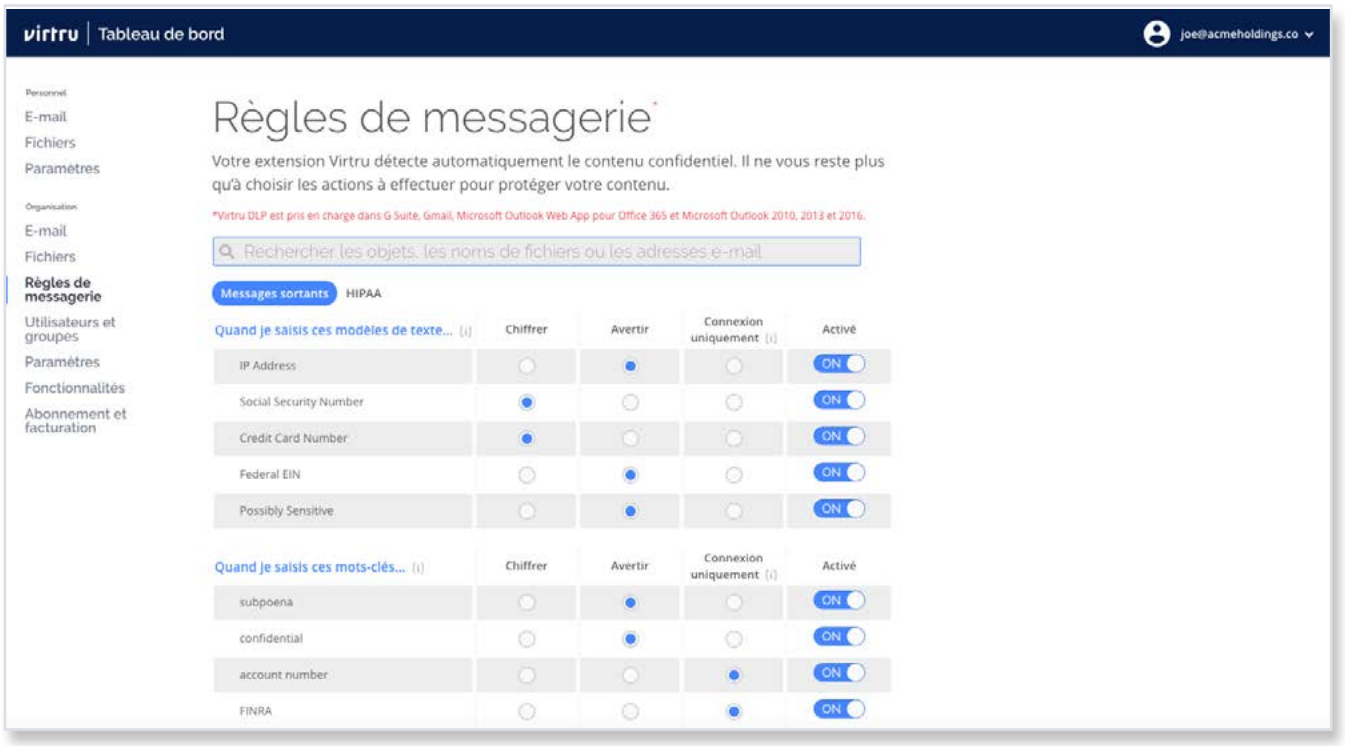
La plupart des technologies de protection des données permettent aux administrateurs de configurer des règles assurant l'exécution automatique du chiffrement, du réacheminement et d'autres actions sur le contenu quittant leur organisation, mais elles exigent souvent que les clients abandonnent pour cela l'accès à leurs données.

À l'inverse, le système de politiques appliqué par Virtru garantit aux administrateurs un contrôle à l'échelle de l'organisation sans compromis sur la sécurité ou le confort d'utilisation. Depuis Virtru Dashboard, les directeurs et administrateurs peuvent créer des politiques afin d'analyser le contenu des utilisateurs finaux côté client ou au niveau du serveur avant qu'il ne quitte l'organisation.

Des règles peuvent être définies pour chiffrer du contenu, prévenir les utilisateurs finaux, ajouter des destinataires, supprimer des pièces jointes et effectuer d'autres actions selon que les e-mails et les fichiers présentent ou non certains critères prédéfinis, par exemple la présence de phrases clés ou de modèles de texte.

Afin que les règles concernent toutes les données quittant le domaine, y compris celles n'ayant pas été créées sur un client doté d'une extension Virtru, la TDP offre une protection des données réseau qui analyse le contenu au niveau du serveur avant qu'il n'atteigne les destinataires prévus. Ces fonctionnalités peuvent être configurées pour toute l'entreprise, pour certains utilisateurs, pour des unités d'organisation ou pour d'autres groupes déjà configurés sur le domaine.

Les politiques peuvent être appliquées aux données entrantes et sortantes, et peuvent même être créées de sorte à intégrer vos solutions de protection contre la perte de données et d'archivage d'e-mails existantes à la TDP de Virtru.



Des règles de messagerie peuvent être configurées dans Virtru Dashboard pour DLP, qui détecte automatiquement les données confidentielles, et applique des protections et des contrôles définis par l'administrateur.

La TDP de Virtru propose également quelque chose jusqu'ici inédit : l'application de politiques côté client. Une fois les politiques configurées par un administrateur au sein de l'entreprise, ces règles peuvent être automatiquement téléchargées sur chaque extension de navigateur, application mobile et plug-in de bureau Virtru exécuté sur l'appareil d'un utilisateur final.

Dans la mesure où ces règles opèrent sur l'ordinateur de chaque expéditeur et non sur les serveurs de Virtru, la plateforme n'a pas besoin d'accéder au contenu client pour appliquer les politiques côté client. Les administrateurs peuvent utiliser ces fonctionnalités côté client pour sensibiliser les employés en configurant des règles destinées à les prévenir directement sur leur appareil avant qu'ils ne partagent des données sensibles.

4.3 Sécurité flexible

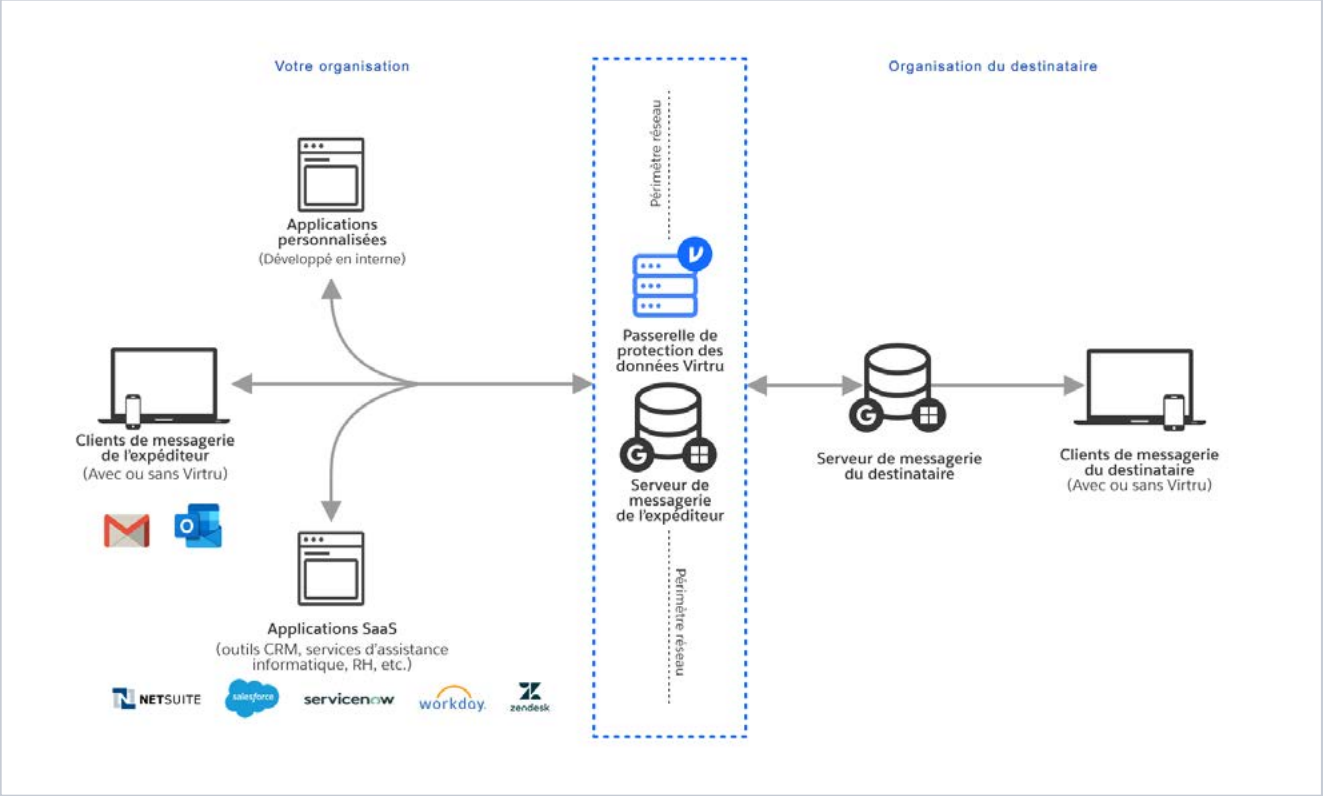
Virtru propose un éventail d'options de protection, de chiffrement et de confidentialité des données bien plus large que celui des anciennes solutions. Si les technologies fondées sur les clés publiques fournissent un chiffrement côté client, elles le font aux dépens de la convivialité et du choix. Les technologies de chiffrement par portail ne protègent pas les données au niveau objet, ce qui expose inutilement le contenu aux dispositifs espions et peut conduire à des brèches ou à d'autres types de perte de confidentialité. En s'appuyant sur la protection niveau objet du TDF, Virtru offre la solution la plus conviviale pour assurer la protection de vos données de façon fiable et durable.

4.3.1 Protection au niveau du réseau grâce à la passerelle de protection des données Virtru

Afin de garantir une sécurité généralisée, les politiques de protection des données doivent être applicables quelle que soit l'origine des données. Il est important que les administrateurs sachent que les données de leur entreprise seront partagées de manière sécurisée, y compris lorsque les créateurs de contenu ou les applications n'appliquent pas de mesures de protection de leur côté. C'est pour cette raison que la TDP de Virtru prend en charge la protection des données au niveau du réseau à l'aide de la passerelle de protection des données Virtru, de façon à sécuriser automatiquement toute donnée partagée par un utilisateur, un appareil ou une application (que l'hébergement ait lieu sur le cloud ou sur site).

La passerelle de protection des données Virtru permet aux organisations d'appliquer des politiques de protection des données à toutes les données entrantes ou sortantes d'un e-mail, d'un partage de fichier ou d'une autre application cloud. Elle joue un rôle complémentaire par rapport aux plug-ins côté client de Virtru en fournissant un mécanisme pour la protection du contenu, y compris lorsque ce contenu est partagé à partir d'un appareil ne disposant pas de Virtru.

La passerelle de protection des données Virtru peut être déployée au sein d'infrastructures sur site ou de solutions IaaS telles qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) ou Microsoft Azure IaaS. Bien que la passerelle puisse être ajoutée à tout type de workflow d'application, elle est le plus souvent intégrée à Microsoft Office 365, Exchange et G Suite, ou à des workflows de messagerie automatisés initiés par des applications SaaS professionnelles, comme Salesforce et Workday.



La passerelle de protection des données Virtru protège les e-mails en provenance de clients de messagerie sur lesquels Virtru n'est pas installé. Elle sécurise les workflows de messagerie automatisés des applications SaaS et personnalisées.

Dans le cas des e-mails, la passerelle peut être déployée à tout point du flux de distribution d'une entreprise, ce qui lui permet de relayer les messages ou d'en assurer la remise finale. En plus de la protection niveau objet de Virtru, la passerelle prend également en charge les technologies de sécurité et de validation standard pour les messageries du secteur telles que Transport Layer Security (TLS), Sender Policy Framework (SPF), Domain Keys Identified Email (DKIM) et Domain Message Authentication Reporting & Conformance (DMARC).

La passerelle de protection des données Virtru est déployée par le biais de conteneurs Docker afin de permettre des déploiements flexibles et évolutifs horizontalement sur différentes infrastructures. Elle utilise un agent de transfert d'e-mails (MTA) conforme aux normes en vigueur, toute communication s'effectue ainsi via le protocole SMTP (Simple Mail Transport Protocol). Elle est configurée de manière à accepter le trafic SMTP des fournisseurs de messagerie électronique vers et depuis la passerelle.

Pour chaque e-mail protégé, la passerelle génère un nouveau jeu de clés de chiffrement. Tout comme les plug-ins côté client de Virtru, la passerelle communique avec le centre de contrôle Virtru pour gérer l'accès aux données protégées et fournir une visibilité aux administrateurs et aux utilisateurs finaux.

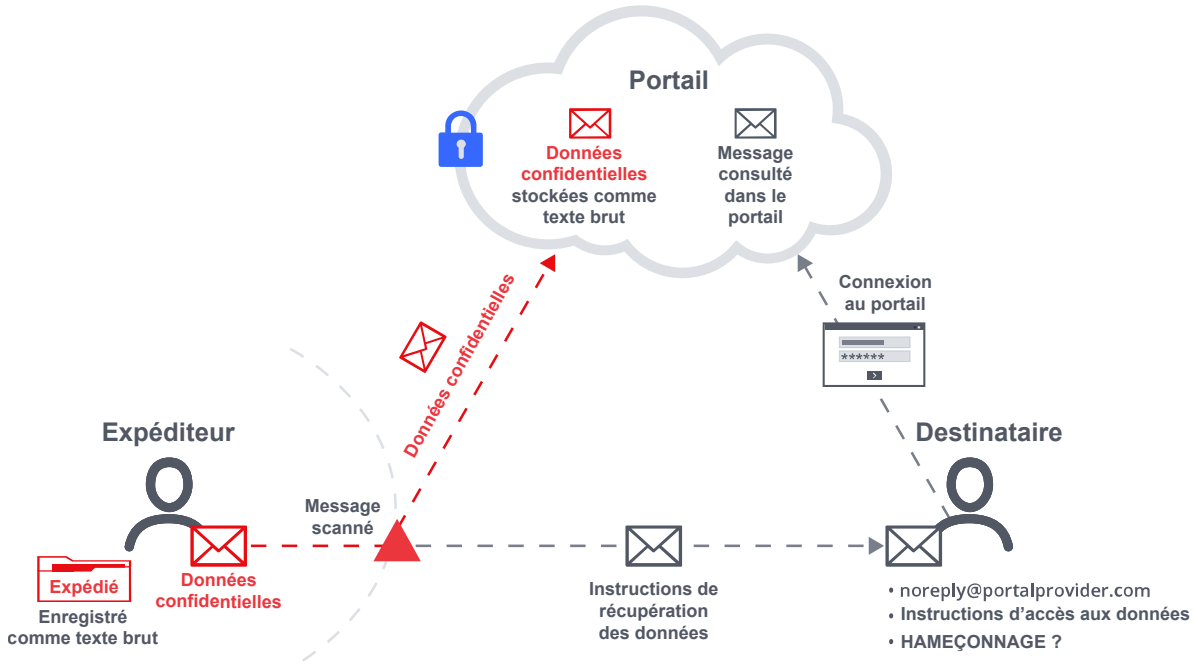
4.3.2 Chiffrement de bout en bout côté client via la protection du point d'extrémité

Pour des raisons de conformité réglementaire, de domiciliation des données et de confidentialité d'entreprise, un chiffrement peut être nécessaire dès la création du contenu sur le point d'extrémité utilisateur et doit persister jusqu'à ce qu'une partie autorisée demande à y accéder. La protection côté client prévient les accès non autorisés et garantit que les fournisseurs cloud n'ont pas accès au contenu déchiffré. Elle rend ainsi le chiffrement de bout en bout fondamentalement plus sécurisé que les approches basées sur un portail, comme TLS. Dans de nombreux cas, le chiffrement de bout en bout côté client s'inscrit dans les exigences de règlements strictes en matière de confidentialité des données, comme CNIL, HDS, EAR et bien d'autres.

Solutions basées sur TLS

- Seulement chiffré lors du transfert
- Le contenu peut ne pas être chiffré lors du stockage
- Possibilité de non-conformité réglementaire
- Aucune visibilité ni fonctionnalité de contrôle
- Intégré à la plupart des fournisseurs de messagerie
- Le destinataire doit prendre en charge le chiffrement TLS

Solutions basées sur un portail



- Le contenu peut être stocké non chiffré
- Moins de contrôle et de visibilité sur les données
- Dépend grandement des règles
- Le destinataire doit créer un nom d'utilisateur et un mot de passe

Solutions de bout en bout de Virtru

- Chiffrement permanent
- Les données restent protégées, où qu'elles aillent
- Architecture de clé à connaissance répartie/ « Zero Trust »
- Utilisation de comptes existants
- Aucun nom d'utilisateur ni mot de passe

Le chiffrement de bout en bout permet également de satisfaire les exigences en matière de domiciliation des données. De nombreuses organisations sont contraintes de ne stocker leur contenu que dans certaines zones géographiques, mais souhaitent malgré tout utiliser des fournisseurs de plateformes cloud internationaux. En confiant le chiffrement côté client à la TDP de Virtru et en stockant les clés de chiffrement dans la zone géographique qui leur est imposée, elles sont en mesure de satisfaire ces exigences de domiciliation des données tout en continuant à utiliser le fournisseur de solutions cloud de leur choix.

Quelles que soient les exigences en matière de réglementation ou de domiciliation des données, le chiffrement de bout en bout est la méthode privilégiée pour garantir la confidentialité et la sécurité des données des entreprises. Lors de l'utilisation de technologies de chiffrement par portail et de méthodes de sécurité reposant sur TLS, du texte brut peut être transmis ou stocké en clair, ce qui rend possible son accès par des tiers non autorisés, comme des ingénieurs du fournisseur de la plateforme cloud. Les technologies côté client garantissent que seuls les créateurs et les consommateurs autorisés pourront accéder au contenu déchiffré.

Le chiffrement de bout en bout était jusqu'ici effectué au moyen d'anciennes technologies reposant sur une infrastructure à clés publiques, comme PGP ou S/MIME pour la messagerie. Bien que très sûres, ces technologies sont difficiles à implémenter et à gérer, et requièrent un échange de clés manuel complexe. Elles ne permettent pas non plus aux créateurs de contenu d'exercer de contrôle sur les données (par ex., révocation, expiration des droits d'accès, suivi des transferts) une fois partagées. En conséquence, seules les entreprises dotées de matériel de pointe sont en mesure de les adopter, et les services informatiques se rabattent bien souvent sur des solutions de sécurité périmétrique.

La TDP de Virtru comble ces lacunes en fournissant un véritable chiffrement de bout en bout pouvant être utilisé de façon quasi universelle. Le contenu est chiffré dès sa création, sur l'appareil du créateur, et avant qu'il ne soit partagé. Le déchiffrement du contenu n'a lieu qu'une fois que la demande de l'appareil consommateur est soumise et que le destinataire est authentifié et autorisé à le consulter. Avec cette architecture, le contenu est protégé de sa création à sa consommation et n'est jamais disponible sous forme non chiffrée pour les prestataires de services ou les systèmes de stockage intermédiaires.

Cas d'utilisation courants de la protection de bout en bout côté client sur la TDP de Virtru

Protection contre la surveillance des pouvoirs publics	Empêcher la surveillance non autorisée et dissimulée des données cloud par les pouvoirs publics grâce à la gestion du stockage des clés de chiffrement et de leurs accès.
Exigences en matière de domiciliation des données	Décider de l'emplacement de stockage et d'accès des clés de chiffrement afin d'empêcher le déchiffrement de données sensibles en dehors des régions indiquées.
Conformité au regard du RGPD	Satisfaire les exigences du RGPD de l'Union européenne à l'aide d'un chiffrement en phase avec « l'état des connaissances » tel que défini dans l'article 32 du règlement.
Conformité au regard des CJIS	Partager sur le cloud les connaissances judiciaires en matière de criminalité en les protégeant avant qu'elles ne quittent l'appareil de l'utilisateur final.
Conformité au regard des réglementations HDS et EAR	Satisfaire les exigences de conformité du partage sur le cloud de données techniques réglementées liées à des applications et des initiatives hautement sensibles notamment liées à l'armée, à la défense ou aux télécommunications, entre autres.

4.3.3 Différentes options pour la gestion de clés

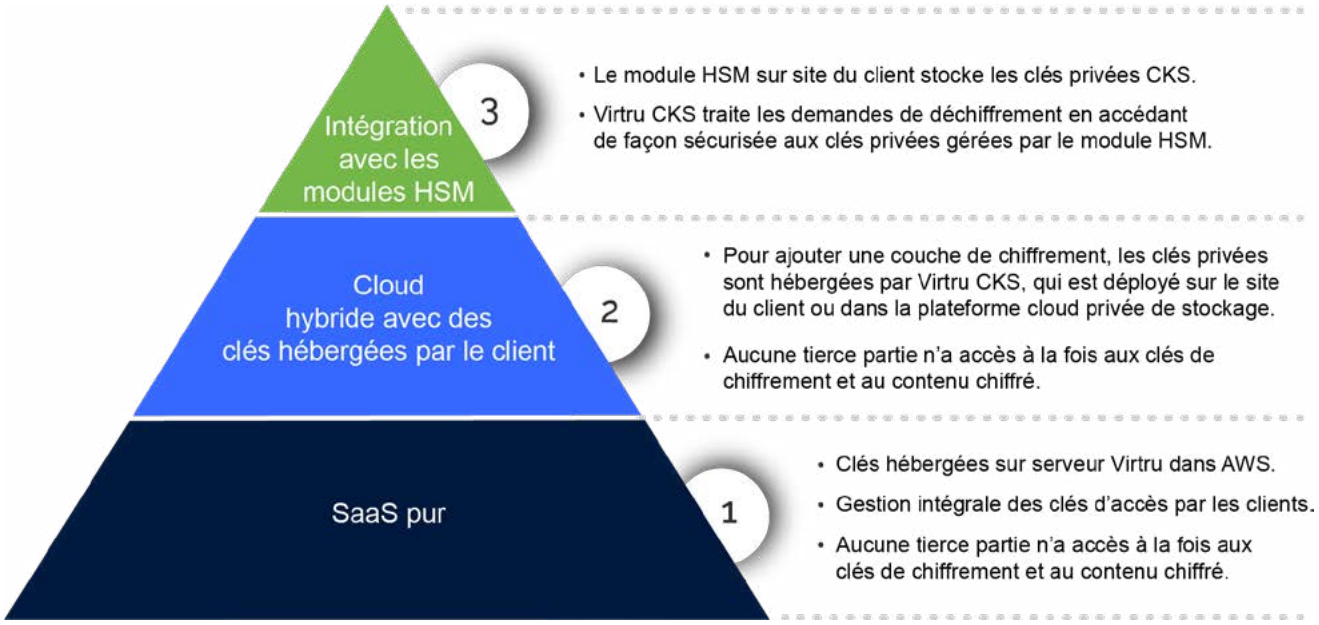
La diversité des réglementations en matière de confidentialité, de sécurité d'entreprise et de domiciliation des données requiert différentes précautions dans la gestion des clés de chiffrement. C'est pourquoi la TDP de Virtru offre aux entreprises trois niveaux d'options pour le stockage et la transmission des clés :

- SaaS pur
- Cloud hybride avec des clés hébergées par le client
- Intégration des modules HSM

SaaS pur

L'option de gestion des clés par SaaS pur de la TDP de Virtru s'appuie sur une architecture à connaissance répartie, au sein de laquelle le contenu chiffré est stocké séparément de la clé permettant le déverrouiller. Une clé de données symétrique AES 256 bits est créée sur le client pour protéger chaque e-mail et fichier. Cette clé est ensuite distribuée via un canal protégé par TLS sécurisé vers le gestionnaire de contrôle d'accès Virtru (décrit dans la section suivante sur l'architecture fonctionnelle de la TDP). Le service KMS d'Amazon renforce la protection des clés de données symétriques à l'aide d'une couche supplémentaire de chiffrement asymétrique, elle-même protégée par un ensemble de modules HSM gérés par AWS. Le contenu est transmis sous forme chiffrée par le biais des canaux traditionnels, et il n'est jamais stocké en clair sur un système cloud ou par un prestataire de services. Les clés sont hébergées séparément sur la TDP de Virtru, mais leur accès reste géré par le créateur de contenu et les administrateurs de l'entreprise.

Grâce à cette architecture à connaissance répartie, une brèche de sécurité simple ne permet pas d'exposer le contenu chiffré. Toute tentative d'attaque devrait en effet pénétrer non seulement le serveur de la TDP de Virtru, mais également l'appareil client ou le fournisseur de messagerie électronique du destinataire pour déchiffrer le contenu.



Trois configurations de gestion de clés proposées sur la TDP de Virtru

Si la méthode de SaaS pur satisfait la plupart des exigences de chiffrement, certaines entreprises requièrent un contrôle intégral et un accès exclusif aux clés protégeant leurs données. Les fournisseurs de plateforme cloud et les anciens fournisseurs de solutions de sécurité ont tenté de répondre à ce besoin par des solutions de gestion au sein desquelles les clés sont détenues par le client, mais celles-ci exigent que les organisations aient suffisamment confiance en ces fournisseurs pour leur laisser la possession de clés chiffrant directement leur contenu. Or, s'ils ont accès à ces clés, les anciens fournisseurs peuvent également accéder au contenu en texte clair sous-jacent accessible dans ces solutions.

Cloud hybride avec des clés hébergées par le client

La configuration de cloud hybride de Virtru tire parti des clés hébergées par le client pour fournir un service de distribution de clés qui empêche les tiers d'accès au contenu non protégé ou aux clés qui servent directement à le chiffrer. Cela est rendu possible grâce à Virtru Customer Key Server (CKS). Le serveur CKS est un appareil physique entièrement hébergé sur site par le client ou dans la plateforme de stockage cloud privée de son choix. Il ajoute un chiffrement asymétrique au SaaS pur de Virtru afin que le client puisse disposer d'un accès intégral et exclusif aux clés de chiffrement.

Lorsqu'une entreprise partage du contenu suivant ce modèle, le client Virtru émetteur génère une clé de message chiffrée à l'aide d'une clé publique CKS. L'hôte CKS héberge la clé privée nécessaire pour déchiffrer la clé publique et désenvelopper la clé de message, mais seule l'entreprise peut y accéder dans la mesure où elle héberge le CKS en local. Les serveurs de Virtru stockent uniquement les clés chiffrées, et ne peuvent donc jamais accéder aux clés de message déchiffrées.

Les clients Virtru récepteurs, à savoir Virtru Secure Reader ou un appareil, client ou serveur doté d'une extension Virtru, disposent également de paires de clés publiques/privées. Le serveur CKS renveloppe les clés de message avec la clé publique du client récepteur avant qu'elle ne soit transmise aux serveurs de Virtru et au client récepteur lui-même. Le client récepteur (situé dans les locaux du destinataire) contient la clé privée nécessaire pour déverrouiller la clé de message renveloppée et enfin déchiffrer le contenu.

Intégration avec les modules HSM

Les organisations qui disposent de processus de sécurité et d'exigences de pointe peuvent exploiter leur infrastructure HSM existante grâce à notre intégration dédiée. Cette option de déploiement vient renforcer l'option associée aux clés hébergées par le client décrite ci-dessus. Les clés privées de l'organisation cliente sont stockées dans un module HSM sur site et Virtru CKS sert uniquement à faciliter la communication entre le module HSM et le gestionnaire de contrôle d'accès Virtru. Le serveur CKS s'appuie sur les protocoles PKCS #11 et KMIP pour traiter les demandes de chiffrement et de déchiffrement tout en accédant de façon sécurisée aux clés privées gérées par le module HSM. Le gestionnaire de contrôle d'accès Virtru prend toujours en charge les workflows d'autorisation en amont.

5. La TDP : architecture fonctionnelle

L'architecture de la TDP de Virtru est constituée de quatre grands composants décrits ci-dessous et résumés dans la figure ci-dessous.

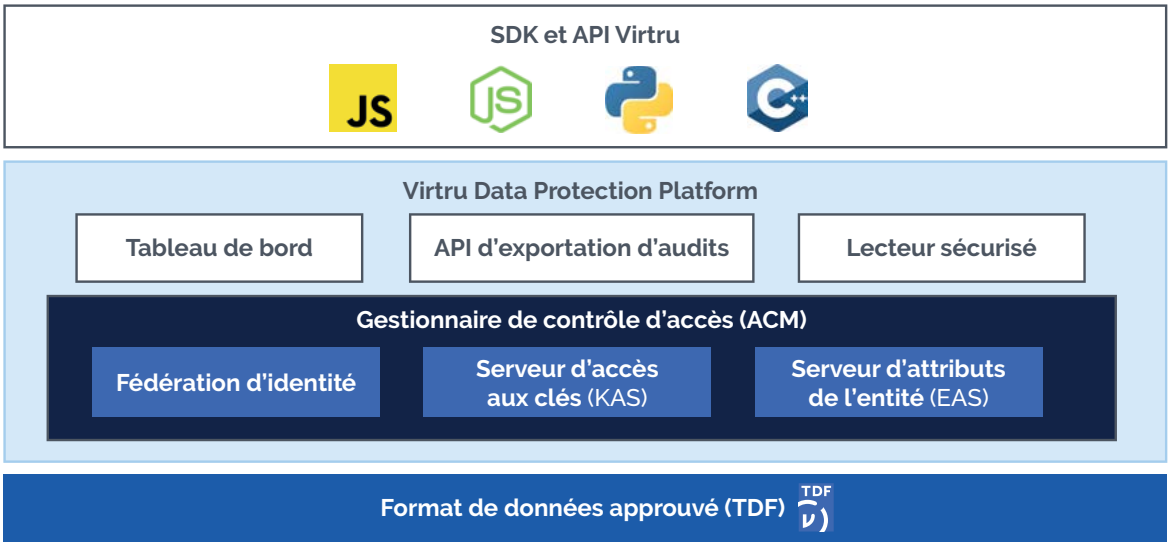
Gestionnaire de contrôle d'accès : Composant essentiel de l'architecture de gestion des clés SaaS de Virtru qui permet aux organisations de définir, d'appliquer et de gérer des politiques destinées à protéger les données et à contrôler l'accès à celles-ci. Le gestionnaire de contrôle d'accès Virtru héberge les clés de chiffrement, et gère les politiques et les attributs d'entité associés. Il traite également les workflows d'authentification et d'autorisation à l'aide d'identité fédérée pour réguler l'accès aux clés de chiffrement et s'assurer que seuls les parties autorisées peuvent accéder au contenu protégé.

Tableau de bord : Panneau d'administration centralisé qui permet de visualiser l'ensemble des données protégées, des accès et des activités partagées, ainsi que de gérer les utilisateurs et les groupes, de configurer la règle de contenu d'e-mail pour la protection contre la perte de données et de définir d'autres paramètres de l'organisation.

API d'exportation d'audits : Prend en charge l'exportation et l'intégration des journaux d'événements Virtru, y compris ceux correspondant aux activités d'administration, de contrôle d'accès et de protection, à l'aide des outils de gestion des événements et des informations de sécurité (SIEM) et des processus du centre des opérations de sécurité (SOC) afin de surveiller les comportements, de détecter et de résoudre des incidents, de réaliser des analyses détaillées et de gérer la conformité.

Lecteur sécurisé : Application sécurisée basée sur un navigateur Web qui offre un accès homogène aux messages et aux fichiers protégés pour les destinataires et les collaborateurs externes.

API et SDK Virtru : outils permettant aux développeurs d'accéder à la plateforme Virtru pour pouvoir intégrer des protections centrées sur les données et des fonctionnalités de contrôle de façon indépendante dans leurs applications et workflows. Actuellement disponible pour les applications JavaScript, Node.js, C++ et Python côté client.



L'architecture de la TDP de Virtru

Fonctions et opérations de gestion de clés de chiffrement Virtru.

Stockage de clés	Dans une architecture à connaissance répartie, les clés de chiffrement sont toujours stockées séparément du contenu chiffré : les clés symétriques sont hébergées dans l'infrastructure de gestion des clés SaaS de Virtru et des clés asymétriques supplémentaires peuvent être hébergées exclusivement sur le site du client grâce à Virtru CKS.
Gestion de politiques	Les assertions de métadonnées de TDF réalisées à l'aide de politiques de contrôle sont liées au contenu chiffré pour permettre l'expiration, la désactivation du transfert, le tatouage numérique au moment du chiffrement, la révocation et l'affichage des accusés de réception pour le contenu partagé.
Authentification	Réalisée par le gestionnaire de contrôle d'accès Virtru lorsque les destinataires tentent d'accéder à du contenu protégé à l'aide de leurs identifiants existants. Prise en charge d'OAuth, de SAML, d'OpenID ou d'un workflow d'e-mail comprenant un lien ou un code de vérification.
Autorisation	Gérée par le gestionnaire de contrôle d'accès Virtru. Après l'authentification, le gestionnaire analyse la politique associée aux données chiffrées pour vérifier si l'identité authentifiée est autorisée à accéder aux données.
Transmission de clés	Les clés sont toujours transmises séparément du contenu protégé : elles sont partagées par TLS entre les serveurs et les clients Virtru avec la confidentialité persistante parfaite (PFS).

5.1 Fonctionnement de la TDP de Virtru

La TDP de Virtru utilise une approche à connaissance répartie pour la protection des données. Le contenu et les clés de chiffrement sont stockées séparément, de sorte que seules les parties autorisées peuvent accéder à du contenu non chiffré. Cette architecture fait que Virtru ne peut jamais accéder à du contenu non chiffré ni déchiffrer du contenu utilisateur en dehors des clients Virtru contrôlés par les clients. Seuls les destinataires autorisés par le créateur de contenu peuvent accéder au contenu protégé et le déchiffrer.

Lorsqu'un utilisateur active la protection Virtru, toutes les activités de chiffrement ont lieu sur les clients dotés d'une extension Virtru à l'aide de clés de chiffrement symétriques AES-256 bits générées par le client. Des clés de chiffrement à objet séparé sont générées pour le chiffrement de chaque e-mail ou fichier. Lors de l'envoi ou du téléchargement de contenu chiffré, le client Virtru l'ayant créé transmet ces clés et les politiques associées au gestionnaire de contrôle d'accès Virtru par le biais d'une connexion TLS sécurisée.

Le gestionnaire de contrôle d'accès Virtru est un service SaaS qui régule l'accès au contenu protégé. Elle distribue des clés de chiffrement aux parties autorisées, applique des politiques de contrôle d'accès et communique avec les services d'identité fédérée pour l'authentification des utilisateurs. Le tableau de bord met également des interfaces de gestion à la disposition des utilisateurs finaux et des administrateurs.

Les banques d'objets telles qu'Amazon Web Services (AWS) S3, ou les serveurs de messagerie comme Google G Suite, Microsoft Exchange et Office 365, stockent du contenu chiffré. L'architecture Virtru « Zero Trust » assure que clés et le contenu sont séparés en permanence. Si la plateforme Virtru contient les clés, elle ne peut pas accéder au contenu. Si elle dispose du contenu, elle n'a pas accès aux clés.

Virtru permet aux parties autorisées de recevoir et de déchiffrer du contenu protégé sans avoir à installer l'un de ses logiciels. Pour accéder au contenu protégé, les destinataires doivent s'identifier sur la TDP de Virtru. Ils utilisent pour cela les identifiants de leur compte de messagerie existant, et n'ont pas à définir de nouveaux noms d'utilisateur et de nouveaux mots de passe. La TDP de Virtru prend en charge l'authentification fédérée via OAuth, SAML et OpenID, et permet aux parties autorisées d'accéder au contenu protégé, une fois qu'elles se sont authentifiées.

Les sections suivantes expliquent comment ces activités d'authentification et de gestion de clés au sein des composants de la TDP de Virtru sont rendues possibles par des normes ouvertes et des implémentations de chiffrement spécifiques.

5.1.1 Normes et protocoles de la TDP de Virtru

L'utilisation de normes ouvertes et de protocoles existants, et non des approches propriétaires des fournisseurs, offre un niveau de sécurité et d'interopérabilité plus élevé pour la TDP de Virtru. Les experts en sécurité se focalisent sur les meilleures normes, garantissant par là une innovation continue et une grande réactivité face aux nouvelles menaces. En outre, l'utilisation de normes simplifie nettement l'intégration à d'autres applications.

Outre la norme TDF, l'architecture de la TDP de Virtru s'appuie sur plusieurs normes ouvertes et sur des protocoles largement reconnus par la communauté des solutions de sécurité. Par exemple, Virtru Dashboard repose en grande partie sur le protocole KMIP (Key Management Interoperability Protocol) de l'Organization for the Advancement of Structured Information Standards (OASIS). Le protocole KMIP favorise les communications entre un serveur de gestion de clés et les clients de chiffrement/déchiffrement. De plus, il stocke et protège les clés de chiffrement et d'autres informations sensibles en lien avec le chiffrement de contenu par le modèle objet KMIP. Les possibilités de communication et de stockage/protection offertes par KMIP font de lui un protocole naturellement adapté à la TDP de Virtru.

La TDP de Virtru utilise le protocole KMIP de diverses manières. Premièrement, elle utilise et étend le modèle objet KMIP afin d'assurer la prise en charge du stockage et de la protection des clés de contrôle d'accès et des clés à connaissance répartie (abordées plus en détail dans la section suivante). Deuxièmement, elle utilise des mécanismes de transport compatibles avec KMIP, à savoir le protocole HTTP (Hypertext Transfer Protocol) sur TLS à l'aide de JSON (JavaScript Object Notation), pour permettre les communications entre les serveurs de chiffrement et les clients. Virtru a quelque peu détourné KMIP de sa vocation d'origine en l'enrichissant afin d'améliorer sa convivialité au service de la TDP.

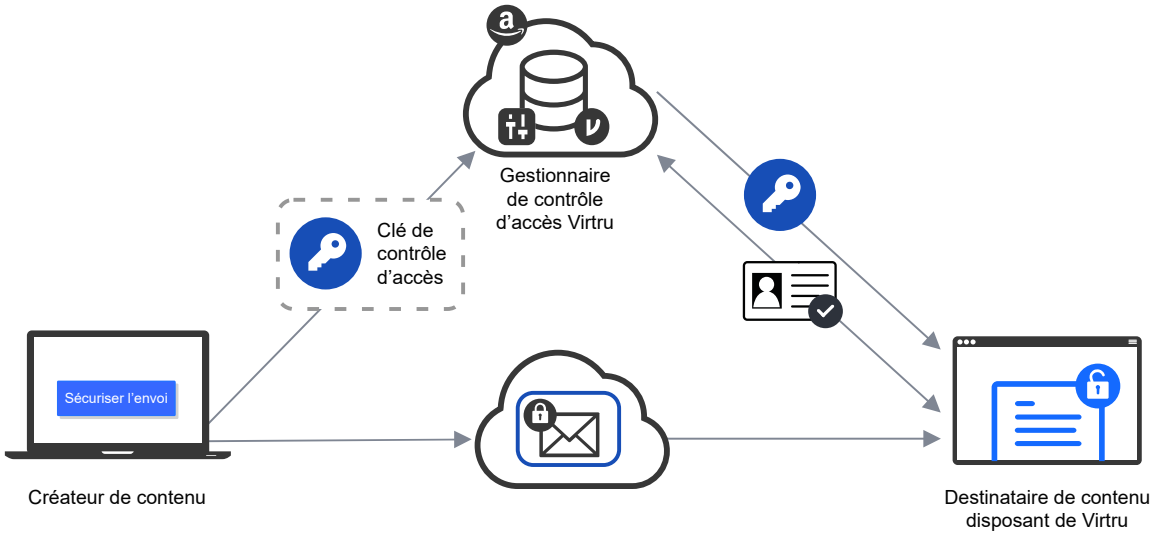
Les serveurs de la TDP de Virtru sont conçus pour être fédérés et distribués, ce qui signifie que les clients peuvent choisir l'emplacement de stockage et de distribution de leurs clés. Les applications dotées d'une extension Virtru sont conçues de manière à spécifier un pointeur dirigé vers le serveur de gestion de clés adéquat au moment du chiffrement. Le logiciel côté client du destinataire sait ainsi où aller pour récupérer la clé de déchiffrement.

5.1.2 Modes d'implémentation du chiffrement sur la TDP de Virtru

Le modèle de chiffrement de Virtru est implémenté de deux façons. Le premier mode d'implémentation est le plus souvent utilisé lorsque le consommateur du contenu utilise un service compatible avec Virtru, comme Microsoft Outlook ou Google G Suite, et que Virtru est installé sur le point d'extrémité.

Pour ce premier mode, une seule clé secrète, la clé de contrôle d'accès, est utilisée pour chiffrer le contenu à l'aide du mode Galois/Counter AES 256 bits. Cette clé est transférée de manière sécurisée de l'appareil client du destinataire jusqu'au gestionnaire de contrôle d'accès Virtru au moyen du protocole ECDHE (Échange de clés Diffie-Hellman basé sur les courbes elliptiques). Cette connexion, au même titre que les autres transmissions de clés du processus, est protégée par confidentialité persistante parfaite (PFS), une propriété qui garantit le caractère éphémère des clés d'établissement de session. Parallèlement au transfert de la clé, le contenu chiffré est directement envoyé au destinataire par les canaux traditionnels.

Gestion et échange de clés : Virtru SaaS, le destinataire dispose de Virtru



Lors du chiffrement initial et de l'envoi :

- Le client Virtru crée une clé symétrique AES 256-GCM unique, la clé de contrôle d'accès, pour chiffrer le message.
- La politique de la clé de contrôle d'accès est mise à jour lors de l'ajout des destinataires et de l'application des contrôles d'accès afin de déterminer qui peut accéder à la clé, pendant combien de temps et si les destinataires peuvent la partager ou la transférer.
- Le message chiffré est envoyé au serveur de messagerie cloud et la clé de contrôle d'accès est transmise du client au gestionnaire de contrôle d'accès.

Lorsqu'il reçoit une tentative de connexion, le gestionnaire de contrôle d'accès réalise les actions suivantes :

- Il authentifie l'identité du destinataire.
- Il autorise cette identité en fonction de la politique associée à la clé de contrôle d'accès.
- Il octroi l'accès à la clé de contrôle d'accès (si autorisé).
- Il déchiffre le contenu en vue de l'accès du destinataire.

Le deuxième mode d'implémentation est basé sur le premier mode décrit ci-dessus et est utilisé pour garantir un haut niveau de sécurité et de confidentialité lorsque les consommateurs du contenu ne disposent pas d'une application dotée d'une extension Virtru et doivent accéder aux données protégées par le biais de Secure Reader. Pour ce faire, Virtru doit créer une copie de la charge utile du contenu initial. En effet, sans client Virtru récepteur, le client du destinataire ne peut pas accéder à cette charge utile. Immédiatement après sa copie, la charge utile est chiffrée à l'aide d'une clé distincte, appelée clé de charge utile. La clé de contrôle d'accès du premier mode d'implémentation est ensuite utilisée pour chiffrer la clé de charge utile (et est envoyée à Virtru comme dans le premier mode). À ce moment, une troisième clé, appelée clé à connaissance répartie, est utilisée pour chiffrer une deuxième fois (double chiffrement) la clé de charge utile.

La clé à connaissance répartie joue un rôle crucial : elle sépare les clés du contenu chiffré pour répartir les informations (comme son nom l'indique). Elle est stockée avec la charge utile du contenu initial et est envoyée via des canaux traditionnels, notamment le flux de distribution de l'organisation cliente. En parallèle, la copie du message chiffré et la clé de charge utile doublement chiffrée sont envoyées aux banques d'objets pour être stockées de façon sécurisée dans AWS.

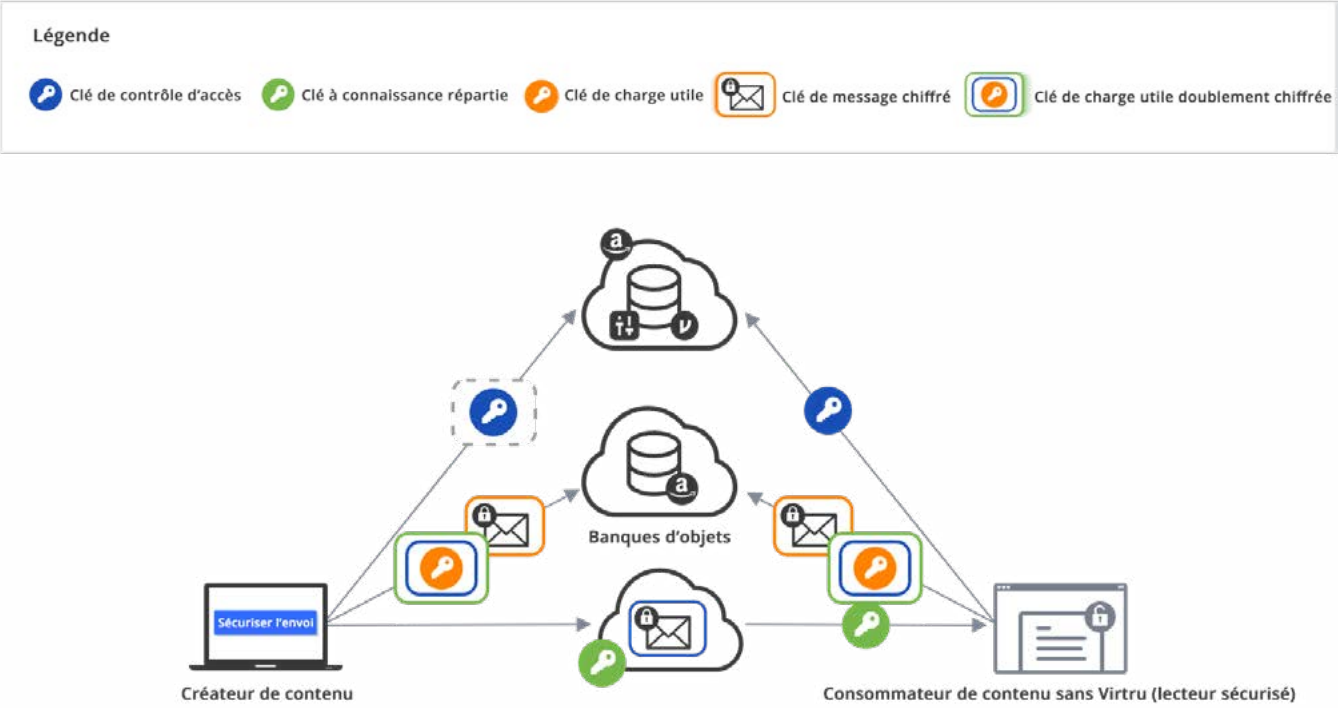
Dans les deux modes d'implémentation, le destinataire autorisé peut accéder à la clé de contrôle d'accès une fois qu'un service de fourniture d'identité tiers a authentifié son identité et que le gestionnaire de contrôle d'accès a autorisé cette identité à consulter le contenu protégé.

Dans le premier mode, Virtru est installé sur le point d'extrémité du destinataire. Par conséquent, une fois le client récepteur authentifié et autorisé, le gestionnaire de contrôle d'accès lui envoie la clé de contrôle d'accès. Le contenu est ensuite déchiffré au sein du client pour assurer un accès homogène, sécurisé et transparent au destinataire.

Dans le second mode, le destinataire est invité à déverrouiller le contenu à l'aide de Virtru Secure Reader, qui initie un workflow d'authentification et d'autorisation pour la clé de contrôle d'accès, ainsi que pour la clé de charge utile doublement chiffrée et la clé à connaissance répartie. Une fois l'authentification et l'autorisation effectuées, la clé à connaissance répartie est utilisée pour lever la première couche de protection autour de la clé de charge utile doublement chiffrée. Le seconde couche est ensuite levée à l'aide de la clé de contrôle d'accès. Enfin, lorsque que la clé de charge utile est déchiffrée, elle peut être utilisée pour déchiffrer la copie du message chiffré et ainsi permettre au destinataire d'accéder au contenu de façon homogène et sécurisée.

Ces workflows avancés de gestion de clés garantissent que Virtru ne peut pas accéder au contenu même lorsqu'elle dispose des clés. Si elle dispose du contenu, elle n'a pas accès aux clés. Malgré la nature complexe de ces opérations de gestion de clés, Virtru ne nécessite aucun échange manuel de clés. Les échanges de clés sont assurés par le gestionnaire de contrôle d'accès Virtru et se déroulent de manière transparente pour les administrateurs comme pour les utilisateurs.

Gestion et échange de clés : Virtru SaaS, Secure Reader



Lors du chiffrement initial et de l'envoi :

- Le client Virtru crée une copie de l'e-mail et le chiffre à l'aide de la clé de charge utile.
- La clé de charge utile est chiffrée à l'aide de la clé de contrôle d'accès.
- La clé de charge utile est chiffrée une seconde fois à l'aide de la clé à connaissance répartie, qui est stockée dans l'e-mail initial et jamais dans l'infrastructure de gestion de clés SaaS de Virtru.
- La copie chiffrée du message et la clé de charge utile doublement chiffrée sont envoyées à des banques d'objets externes, séparément de la clé à connaissance répartie.

À la réception d'une tentative de connexion :

- Le gestionnaire de contrôle d'accès Virtru authentifie l'identité et vérifie si celle-ci est autorisée à accéder au contenu.
- Si l'identité est autorisée, le gestionnaire octroi l'accès à la clé de contrôle d'accès et l'envoie au client récepteur du consommateur du contenu.
- La copie chiffrée du message et la clé de charge utile doublement chiffrée sont envoyées au client récepteur du consommateur du contenu à partir des banques d'objets.
- La clé à connaissance répartie est envoyée au client récepteur du consommateur du contenu dans le message d'origine.
- Dans le client récepteur, la clé à connaissance répartie lève la première couche de chiffrement sur la clé de charge utile. La seconde couche de chiffrement est ensuite levée par la clé de contrôle d'accès.
- Enfin, la clé de charge utile est utilisée pour déchiffrer la copie du message afin de permettre l'accès au sein de Secure Reader.

Étude de cas : sécurisation des communications par e-mail avec la TDP de Virtru

L'étude de cas suivante présente les étapes d'utilisation de la TDP de Virtru pour contrôler les accès, gérer les clés et appliquer des politiques sur les divers services de messagerie électronique. Le processus comporte cinq étapes principales :

Étape 1 : chiffrement du contenu

L'expéditeur place le contenu sur un client de messagerie doté d'une extension Virtru et indique que ce contenu doit être protégé. Le client de messagerie chiffre le contenu avant son envoi. Afin de réaliser le chiffrement, le client de messagerie génère des clés de chiffrement uniques spécialement pour la protection du contenu (ce processus est présenté en détail dans la section précédente). Le client de messagerie crée également une politique de contrôle d'accès pour le contenu, qui définit toute restriction applicable au destinataire en matière de contrôle d'accès (par exemple, une date d'expiration du contenu, le cas échéant) par le biais d'assertions de métadonnées.

Étape 2 : distribution du contenu et gestion du contrôle d'accès

Le client de messagerie de l'expéditeur distribue le contenu par le biais de canaux traditionnels, comme l'envoi d'un message chiffré par e-mail, au serveur de messagerie pour procéder au traitement nécessaire. Parallèlement, le client de messagerie de l'expéditeur s'acquitte également de la gestion du contrôle d'accès. Cela implique le transfert des clés de chiffrement (avec les politiques de contrôle d'accès associées) et des copies du contenu chiffré au gestionnaire de contrôle d'accès Virtru et aux banques d'objets, afin de les stocker jusqu'à ce que le destinataire tente d'accéder à l'e-mail.

Étape 3 : authentification de l'utilisateur

Lorsque le destinataire tente d'accéder au contenu protégé par le biais de son client de messagerie avec extension Virtru, il déclenche une session d'authentification tripartite entre le client de messagerie, le gestionnaire de contrôle d'accès Virtru et le prestataire de services d'identification tiers qui détient les identifiants. Les trois principaux protocoles d'identité fédérée, OAuth, OpenID et SAML (Security Assertion Markup Language), sont pris en charge par Virtru pour l'authentification de l'utilisateur. Étant donné que l'application avec l'extension Virtru coordonne toutes les communications entre le gestionnaire de contrôle d'accès Virtru et le prestataire de services d'identification, le serveur Virtru n'a jamais accès aux identifiants de l'utilisateur.

Étape 4 : distribution des clés et des contrats

Si l'authentification réussit et que le gestionnaire de contrôle d'accès confirme que la politique de la clé de chiffrement autorise cet utilisateur à accéder au contenu, Virtru envoie la clé de contrôle d'accès protégée au client de messagerie avec extension Virtru du destinataire.

Étape 5 : déchiffrement du contenu

Si les termes du contrat de sécurité sont respectés (par exemple, si l'expéditeur n'a pas demandé l'expiration du contenu), le client de messagerie du destinataire utilise la clé pour déchiffrer le contenu protégé, permettant au destinataire autorisé de le consulter.

Cette méthode possède d'importants avantages par rapport aux anciennes approches fondées sur les clés publiques et les portails. Si les approches fondées sur des clés publiques (telles que PGP et S/MIME) assurent bien un chiffrement de bout en bout côté client, elles sont difficiles à utiliser et requièrent un échange de clés manuel compliqué. Les systèmes fondés sur des portails sont relativement simples pour les expéditeurs, mais bien moins commodes pour les destinataires.

Ils offrent également beaucoup moins de sûreté et de confidentialité dans la mesure où ils stockent une copie du contenu sur leur serveur. En cas de faille sur ce serveur, tout le contenu pourrait facilement être exposé à des accès non autorisés, ce qui représenterait des violations majeures de la confidentialité pour un grand nombre d'utilisateurs. Reprenant les avantages du chiffrement de bout en bout côté client, la TDP de Virtru y ajoute visibilité et contrôle persistant, et ce, sans sacrifier la convivialité et la simplicité des e-mails traditionnels.

6. Technologies de confidentialité approuvées de Virtru

Gamme de produits actuelle

Virtru s'intègre à vos outils existants, ce qui vous évite d'avoir à choisir entre facilité d'utilisation et protection des données. Nos technologies de confidentialité flexibles, approuvées et faciles d'utilisation régissent l'accès aux données tout au long de leur cycle de vie : de la création au partage, en passant par le stockage, l'analyse et l'exploitation.
Le portefeuille de produits de Virtru comprend les éléments suivants :

- Des solutions de confidentialité des données qui s'intègrent de manière transparente aux applications les plus fréquemment utilisées, comme les messageries électroniques et les applications de partage de fichiers. Virtru ajoute des fonctionnalités de chiffrement niveau objet, de contrôle d'accès, d'audit, de gestion de clés et d'application de politiques à Microsoft Outlook (Exchange sur site ou Office 365) grâce à un complément Outlook, ainsi qu'à Google Drive et à Gmail (Google G Suite) grâce des extensions de navigateur Chrome. Pour Salesforce, Workday, NetSuite et les autres applications d'entreprise fréquemment utilisées qui échangent automatiquement des données à l'aide de processus de messagerie, la passerelle de protection des données Virtru assure la protection des e-mails et des pièces avec une visibilité ainsi qu'un contrôle permanents, sans perturber les workflows de votre application.
- Un ensemble d'outils de conception de confidentialité adressés aux développeurs, qui peuvent être intégrés facilement à n'importe quel appareil connecté, application ou infrastructure. Le SDK Virtru permet aux organisations d'utiliser la TDP pour intégrer des protections de niveau objet à leurs applications simplement et rapidement. Ces fonctionnalités fournissent un niveau de protection bien plus élevé que celui que la plupart des sociétés sont en mesure de développer en interne. Elles permettent également aux fournisseurs d'applications d'entreprise d'éliminer les points de défaillance uniques, tout comme les solutions standardisées de Virtru.

Fonctionnement de la TDP de Virtru dans les applications internes

Grâce aux SDK Virtru, les organisations disposent d'une console centrale leur permettant de définir des politiques de confidentialité et de contrôler l'accès aux données à partir de l'ensemble des applications qu'elles utilisent, y compris celles qu'elles ont développées en interne.

En tant qu'administrateur, vous serez en mesure d'appliquer des politiques à l'échelle du domaine sur l'ensemble de vos outils collaboratifs, ainsi que de contrôler rapidement les accès sur l'ensemble des applications et des appareils connectés, que ce soit pour des utilisateurs individuels ou pour des groupes. Comme illustré dans le cas d'utilisation ci-dessous, nous souhaitons que les entreprises puissent facilement intégrer des protections aux outils dont elles disposent déjà ou qu'elles développent, tout en garantissant la persistance de ces protections indépendamment de l'emplacement de création et de consommation du contenu.

Analyse sécurisée

Afin de générer des informations pertinentes à partir de leurs modèles d'analyse les plus performants, les institutions doivent avoir accès à d'immenses quantités de données, rassemblées grâce au partage entre organisations.

Bien qu'elles comprennent les avantages des échanges d'informations à plus grande échelle, les organisations sont souvent peu disposées à partager leurs données les plus précieuses avec des collaborateurs spécialisés en analyse, en raison d'un manque de transparence, de contrôle et de maintien de la propriété une fois les données transmises.

La TDP de Virtru impose une restriction d'accès aux ensembles de données en chiffrant toutes les données et en mettant en place des politiques sur leurs serveurs de clés associés. Les points de données fournis par les différentes organisations travaillant sur le projet d'analyse ne sont jamais dévoilés aux autres organisations, et pourtant toutes les parties peuvent accéder facilement aux analyses, aux mesures et aux autres calculs réalisés à partir des points de données.

Appareils connectés

Des fabricants du monde entier se livrent à une concurrence féroce pour développer des appareils connectés et les commercialiser auprès des consommateurs afin de renforcer la connectivité. Mais la vitesse effrénée du développement de produit ne laisse pas toujours suffisamment de temps aux questions de sécurité qui doivent faire l'objet d'une réflexion et d'une implémentation minutieuses.

Les capteurs de l'Internet des objets transfèrent en permanence de larges volumes de données confidentielles entre les appareils et le cloud. Ces données doivent respecter les normes de protection tout au long de leur cycle de vie, de leur collecte à leur analyse en passant par leur transmission, même lorsque l'appareil lui-même n'est pas sécurisé, afin de garantir la confidentialité des clients et la conformité réglementaire.

Grâce aux SDK Virtru, les développeurs et les professionnels de la sécurité peuvent mettre en place une protection persistante dans les appareils connectés, afin de chiffrer les données dès leur collecte et d'ajouter des politiques de contrôle d'accès définies par l'administrateur ou l'utilisateur final. Les données collectées et partagées par les appareils connectés restent ainsi privées et conformes, et les contrôles d'accès, de révocation et d'expiration de la TDP de Virtru aident à protéger les appareils connectés pouvant être perdus ou volés.

Mesures face à la pandémie

Les professionnels des soins de santé qui jouent un rôle important face à la pandémie de coronavirus ont besoin d'un accès aux données pour suivre et ralentir la propagation du virus, ainsi que répartir les ressources là où elles sont le plus nécessaires.

La possibilité de mettre en place des contrôles vérifiables crée une relation de confiance chez les patients et autres parties prenantes qui permet ensuite aux fournisseurs de soins de santé, aux pouvoirs publics et à d'autres institutions de générer rapidement et avec précision de nouvelles informations améliorées. Cela a pour conséquence la création de plans d'action plus efficaces qui nous permettront de remettre plus rapidement sur pied l'économie sans compromis sur la confidentialité.

Comme dans le cas d'utilisation de l'analyse sécurisée décrit ci-dessus, la TDP de Virtru veille à ce que les données soient utilisées uniquement aux fins prévues. Elle inclut également des contrôles renforcés qui permettent aux utilisateurs de partager, d'approuver et de révoquer l'accès à leurs informations confidentielles à tout moment.

Sécurité des applications

Alors que les professionnels de la sécurité des applications concentrent leurs objectifs sur la protection des données et le respect des règlementations en constante évolution, les développeurs élaborent de nouvelles applications et de nouveaux workflows de partage de données à une vitesse inégalée.

Les professionnels de la sécurité ont des difficultés à suivre l'accélération des processus de publication, rendue possible par les outils, conteneurs et plateformes nécessitant peu de code open source. Ce n'est que lorsque des fonctionnalités de chiffrement de bout en bout et de contrôle d'accès sont faciles à utiliser et à implémenter que l'approche DevSecOps devient envisageable.

Grâce à la TDP de Virtru, votre équipe a la possibilité d'ajouter une protection des données niveau objet aux applications et aux workflows en toute simplicité.

7. Conclusion

Les menaces actuelles exigent une solution de protection des données en mesure de fournir un contrôle d'accès persistant, capable de satisfaire les exigences des entreprises en matière de sécurité et suffisamment simple pour permettre une adoption généralisée. En fournissant des contrôles d'accès granulaires pour tout type de contenu tout en simplifiant les interfaces destinées aux expéditeurs, aux destinataires et aux administrateurs, la TDP de Virtru est la première solution qui vous évite d'avoir à choisir entre protection des données et convivialité.

Reposant sur des formats de données et des protocoles ouverts, éprouvés et fondés sur des normes, Virtru offre aux entreprises de toute taille et de tout type une protection hautement évolutive et flexible. Virtru a adopté un modèle fédéré permettant aux organisations d'utiliser les services d'authentification déjà en place et de gérer leurs propres clés de chiffrement à l'aide de serveurs de clés mis à leur disposition par Virtru.

Virtru minimise l'impact sur les applications client, les serveurs cloud et les utilisateurs finaux tout en tirant profit des services de sécurité et de contrôle d'accès avancés de la TDP de Virtru basée sur le cloud. Les API et bibliothèques Virtru permettent une intégration étroite entre le système de protection et vos applications, minimisant la gêne pour les utilisateurs finaux.

La TDP de Virtru dans son ensemble permet aux entreprises de protéger leurs données en toutes circonstances, tout en s'intégrant aux applications commerciales et aux workflows utilisateur existants.

Pour plus d'informations ou pour découvrir la TDP de Virtru en action, contactez-nous afin de programmer une démonstration.
virtru.com/fr/contact-sales

À propos de 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, fondés sur notre plateforme de protection des données ouverte, régit les données tout au long de leur cycle de vie. Plus de 20 000 organisations font confiance à Virtru pour la sécurité des données et la protection de la confidentialité. Pour plus d'informations, rendez-vous sur virtru.com/fr ou suivez-nous sur Twitter @virtruprivacy.