



Limitez les risques et prenez le contrôle de vos données

Pourquoi vous devriez ajouter l'encryption orientée donnée de Virtru à Microsoft 365

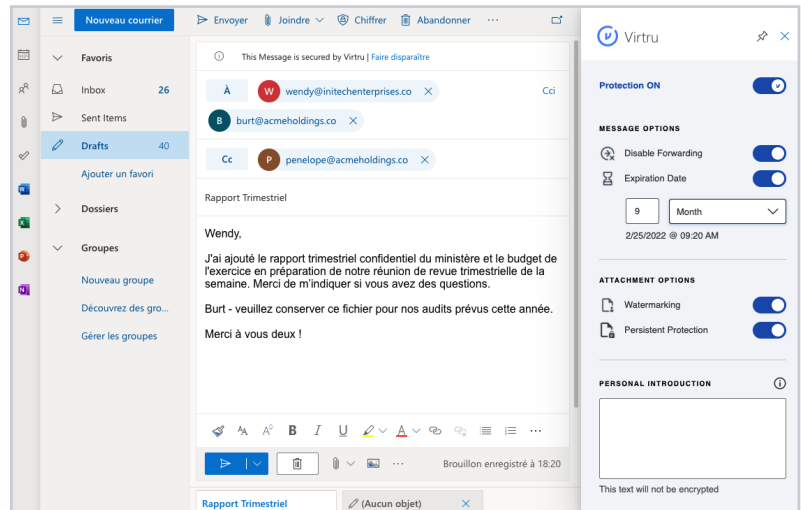
In this Guide

Une solution de protection faite pour vous	2
Résolvez les défis pour rendre le partage de données sécurisé mais simple.....	3
Revue des architectures de chiffrement Virtru et Microsoft	4
Comparez Virtru aux plans Microsoft E3 et E5.....	5
Ce sont vos données et Virtru vous aide à ce que cela continue	10

Une solution de protection faite pour vous

La protection des données partagées dans les workflows nécessite un chiffrement fiable et spécifique ainsi que des contrôles d'accès robustes car les besoins en matière de confidentialité peuvent changer à tout moment. En ce qui concerne Microsoft Outlook, il existe de nombreux fournisseurs de solutions de chiffrement, y compris les plans d'entreprise de Microsoft, parmi lesquels choisir. Le plus important est de trouver la solution qui offre le plus de valeur, des exigences de sécurité à la fonctionnalité clé en passant par la facilité d'utilisation pour votre organisation.

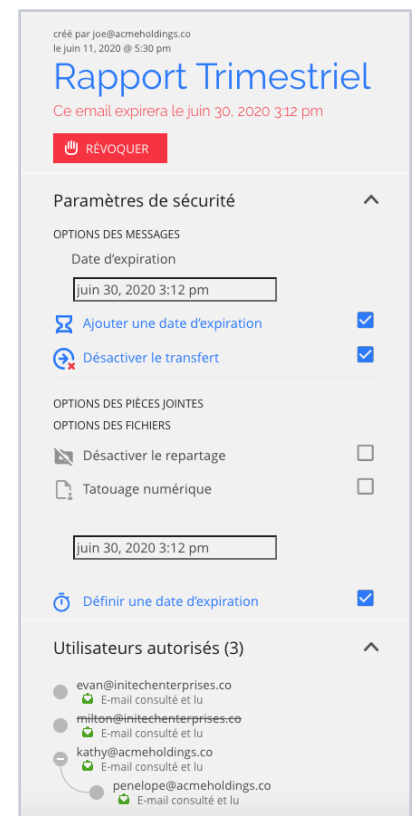
La bonne solution vous aidera à maintenir le contrôle et la visibilité de vos données tout au long de leur cycle de vie, à préserver leur confidentialité et à atténuer les risques de brèche de sécurité. Ceci est possible grâce à une architecture de type Zero Trust, à une gestion flexible des clés de chiffrement, à des options d'interopérabilité et d'intégration cloud et à des contrôles d'accès conviviaux et orientés utilisateurs.



Activer les règles de messagerie DLP pour les modèles de texte dans les messages

Créez une solution de protection des données de bout en bout avec Virtu pour déployer et gérer rapidement et facilement la sécurité à l'échelle de l'organisation, pour améliorer la collaboration, pour contrôler l'accès à vos données et enfin pour permettre le bon alignement de toute l'entreprise. Obtenez exactement ce dont vous avez besoin et ne payez que ce que vous utiliserez. Les produits Virtu pour Microsoft incluent:

- **Outlook** : appliquez le chiffrement Virtu centré sur les données et les contrôles d'accès granulaires directement dans Outlook, et enveloppez chaque objet de données dans sa propre couche de chiffrement, afin d'en contrôler la sécurité en permanence, même une fois partagés avec des tiers.
- **Serveur de clés client (CKS pour Customer Key Server)** : hébergez vos propres clés de chiffrement pour ne jamais avoir à faire confiance à quiconque (y compris Microsoft et Virtu) pour accéder à vos données.
- **Passerelle de protection des données (Gateway)** : sécurisez les e-mails sortants envoyés par des applications telles que Salesforce et Zendesk, et utilisez le chiffrement entrant pour les réponses des outils Workday ou HR afin de protéger les données quand et où cela est nécessaire.



Examiner l'accès aux données et l'activité de transfert, et ajuster les contrôles d'accès

Résolvez les défis pour rendre le partage de données sécurisé mais simple

Notre mission est de vous aider à libérer vos données en vous assurant d'en garder le contrôle partout où celles-ci voyagent et sont partagées. Dans cet esprit, les solutions Virtru vous aident à résoudre vos plus grands défis de partage de données.



Répondez aux exigences de sécurité les plus élevées

Virtru vous aide à répondre aux exigences de conformité telles que CJIS, ITAR, CMMC, GDPR et HIPAA sans un prix exorbitant, tout en étant facile à utiliser pour éviter les erreurs humaines. Nous faisons partie intégrante de votre solution de conformité globale.



Empêcher l'accès de tiers (y compris vos fournisseurs de cloud et de messagerie)

Virtru propose des options de gestion des clés de chiffrement pour prendre en charge la conformité réglementaire, la souveraineté des données et la résidence des données, y compris la possibilité d'héberger vos propres clés afin que vous ayez une couche de sécurité supplémentaire où que vos données se trouvent une fois créées ou partagées. Cela signifie que vous pouvez empêcher tout tiers (y compris Virtru et Microsoft, ainsi que d'autres fournisseurs de cloud, de messagerie et de sécurité) d'accéder à vos données.



Ajoutez facilement le bon niveau de contrôle d'accès à n'importe quel message

Virtru offre des contrôles d'accès granulaires (y compris la révocation, le contrôle du transfert, la date d'expiration, le filigrane et la protection permanente des fichiers) pour chaque utilisateur ou expéditeur ainsi que des contrôles avancés pour les administrateurs pour gérer l'organisation des données en entreprise. Ceux-ci sont disponibles pour tous nos clients dès l'offre de base et pour tous les e-mails, internes comme externes, car tous ont besoin d'une gestion et d'un contrôle fin.



Étendre le chiffrement et le contrôle d'accès aux pièces jointes

Virtru offre des contrôles d'accès flexibles et complets pour les pièces jointes, y compris les fichiers Microsoft Office, les PDF, les fichiers image, etc. Ces contrôles incluent le filigrane pour empêcher le téléchargement ou l'impression, ainsi qu'une protection permanente des fichiers afin que vous gardiez le contrôle et puissiez en révoquer l'accès quel que soit l'endroit où ce fichier est enregistré, y compris le poste de travail de vos destinataires.



Collaborez entre les écosystèmes et les plates-formes et ne vous inquiétez jamais des destinataires utilisant différents clients de messagerie ou ayant des politiques de sécurité moins fiables de la votre.

Virtru fonctionne de manière transparente et identique quel que soit client de messagerie de vos destinataires, sans perdre la sécurité, la résidence ou le contrôle des données. Virtru prend également en charge Google et Microsoft dans des environnements hybrides, ce qui vous permet de maximiser l'agilité et de vous adapter aux nouvelles exigences sans être enfermé dans un seul client de messagerie.



Utilisez une solution facile à gérer et qui réduit le coût total de possession

Virtru se met en œuvre très rapidement pour une plus grande valeur et un meilleur retour sur investissement. Les administrateurs peuvent facilement déployer et gérer les données à l'échelle de l'organisation de façon centralisée. Les utilisateurs sont habilités à protéger les données car il leur est facile d'ajouter un chiffrement et des contrôles d'accès importants. Pour terminer ce cycle de vie des données, les destinataires ont un accès eux aussi très facile sans avoir besoin de créer de nouveaux comptes ou mots de passe. Évitez tous maux de tête liés à la navigation dans de nombreuses pages de solutions, à une documentation contradictoire et à des solutions Microsoft qui se chevauchent mais ne fonctionnent pas.

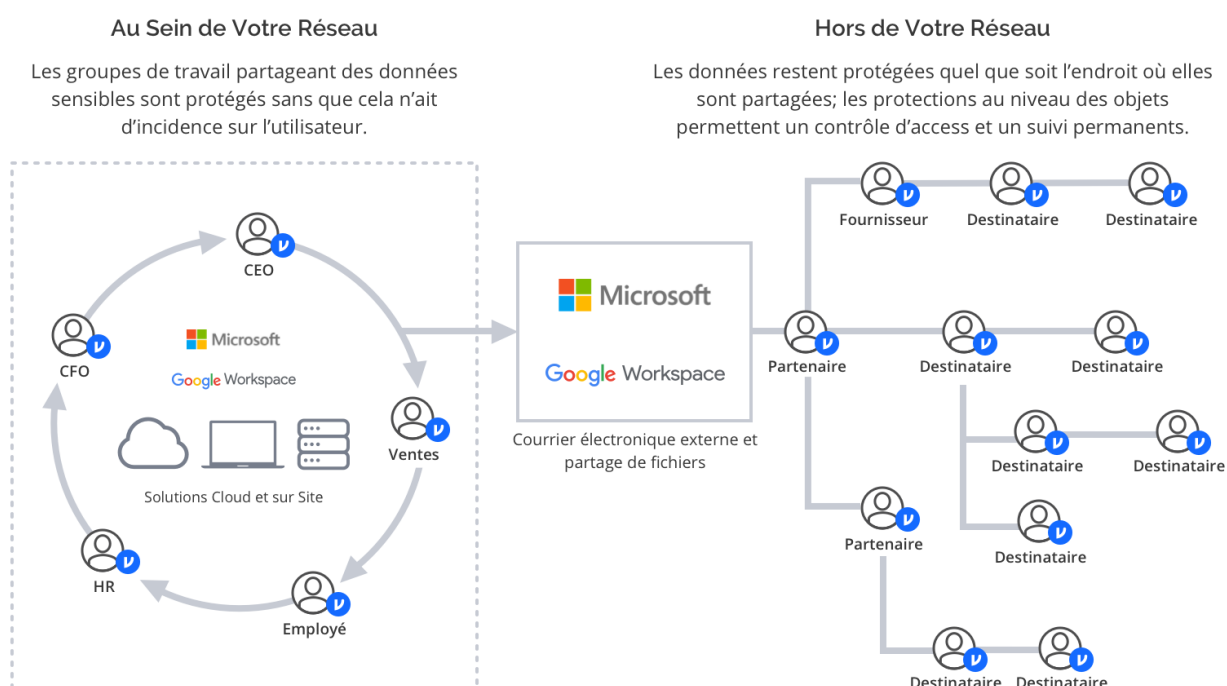
Revue des architectures de chiffrement Virtru et Microsoft

La base de la protection des données de Microsoft pour Outlook est Azure Rights Management (Azure RMS). Il s'agit de la technologie de protection basée sur le cloud utilisée par Azure Information Protection (AIP) pour aider à protéger les fichiers et les e-mails à l'aide de stratégies de chiffrement, d'identité et d'autorisation. La protection persistante d'Azure RMS permet de sécuriser les données car les paramètres de protection restent avec ces données.

Microsoft regroupe ce chiffrement avec d'autres fonctionnalités de sécurité des données pour les entreprises dans des plans d'entreprise. Plus particulièrement, leurs plans E3 et E5 visent à améliorer la collaboration des données en améliorant le chiffrement avec des contrôles d'accès, des règles DLP et des rapports et renseignements sur les données pour respecter les conformités réglementaires et les sécuriser contre les accès non autorisés.

La base de Virtru réside dans la plateforme de données de confiance Virtru qui stocke le contenu chiffré et clés de chiffrement séparément, modèle Zero Trust où tous les composants du système sont authentifiés en permanence. Virtru implémente le format de données de confiance Virtru (TDF - Trusted Data Format) qui maintient les données protégées et sous le contrôle du propriétaire, peu importe où ces données voyagent ou où elles sont enregistrées. Avec le TDF, une organisation peut appliquer des politiques et des règles discrètes tirant parti du contrôle d'accès basé sur les attributs (ABAC) qui accompagnent le contenu.

Pour que vous vous concentriez sur la protection et la conformité des données, Virtru ajoute une valeur supplémentaire pour collaborer en toute sécurité et simplement. Pour garantir la sécurité des données, nous proposons des options de gestion des clés de chiffrement, notamment l'hébergement de vos propres clés de chiffrement (on premise), des options d'intégration transparente de la plateforme et l'interopérabilité du cloud. Pour une fonctionnalité optimale, nous proposons des contrôles d'accès granulaires pour gérer les données partagées en interne ou en externe. De plus, nous offrons la flexibilité de créer un ensemble de services répondant exactement à vos besoins avec une facilité d'utilisation brevetée pour les administrateurs, les utilisateurs et les destinataires afin d'améliorer tout flux de travail de partage de données.



Comparez Virtru aux plans Microsoft E3 et E5

Dans certains domaines clés, Microsoft E3 et E5 n'offrent pas la même valeur de protection des données que Virtru pour votre organisation, en particulier pour les secteurs hautement réglementés. Alors que les plans de niveau gouvernemental à prix élevé de Microsoft peuvent répondre à ces normes de protection des données rigoureuses, Virtru offre le même niveau de protection complète des données à tout client. Le tableau suivant passe en revue les capacités de Microsoft E3 et E5 par rapport à Virtru afin que vous puissiez mieux comprendre comment chaque solution de protection des données correspond à vos besoins.

Capacités		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Chiffrement et gouvernance des données	Envoyer des messages chiffrés avec protection des droits	✓ Centré sur la donnée, chiffrement de bout en bout	✓ Office Message Encryption	✓ Advanced Message Encryption
	Chiffrement et protection des messages au niveau de la donnée pour un contrôle granulaire des accès et à tout moment	✓	✓ Assurez-vous qu'Azure Information Protection (AIP) est utilisée ✗ Anciennes versions de Office Message Encryption	✓ Assurez-vous qu'Azure Information Protection (AIP) est utilisée ✗ Anciennes versions de Office Message Encryption
	Support d'un modèle de sécurité Zero Trust au sein du navigateur, de l'ordinateur et intégré à Outlook mobile	✓ Prise en charge de toutes les façons dont vous utilisez Outlook aujourd'hui	✗	✗ Double Key Encryption dans ce package ne prend uniquement en charge la version bureau d'Outlook sur Windows (pas dans les navigateurs Web ou sur un Mac / iPad)
	Assurez-vous que vos messages (le texte brut) ne peut pas être accédé par un tiers	✓ Virtru (et d'autres fournisseurs, y compris Microsoft) ne peuvent accéder à votre contenu en aucune circonstance - nous gérons simplement les politiques d'accès et les clés entre les différentes parties	✗	⊖ Customer Lockbox - Microsoft ne peut pas accéder à votre contenu sans votre approbation explicite, mais cela montre qu'ils peuvent toujours accéder à votre contenu d'une manière ou d'une autre

Capacités		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Chiffrement et gouvernance des données	Personnaliser les règles DLP	 Définir des règles et des actions pour les modèles de texte, les mots-clés et les destinataires; utilisez notre pack de règles prédéfini pour HIPAA; ou créez vos propres règles personnalisées		 Offre des paramètres de condition et d'action plus avancés, et génère des rapports d'incident.
	Détecter et enquêter sur les menaces avancées	 Offre la possibilité d'enquêter sur les activités suspectes et les accès non autorisés		 Microsoft Defender Advanced Threat Protection (ATP) - prévention des violations et enquête post-violation pour les attaques sophistiquées telles que le hameçonnage et les logiciels malveillants
	Gestion et exploitation des données de façon intelligente	 Le centre de contrôle Virtru permet aux administrateurs de voir quelles données leur organisation protège, de savoir où elles sont, de gérer avec qui elles sont partagées et de s'assurer qu'elles restent sous le contrôle de l'entreprise	 Ne peut indexer que les documents sensibles stockés dans les espaces de travail supportés par Microsoft 365	 Les administrateurs ont une visibilité sur les activités liées au partage de données sensibles, y compris l'emplacement de stockage de ces données, les activités de chiffrement et les journaux de prévention de la perte de données (DLP)
	Chiffrement des e-mails entrants			

Capacités		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Aide à la conformité des réglementations les plus importantes	HIPPA	✓	✓	✓
	GDPR	✓	✗	− Le chiffrement à double clé est la meilleure pratique, mais strictement limité à Outlook sur Windows
	CJIS	✓	✗	✗ Nécessite les plans de services gouvernementaux les plus chers (GCC for state and local government et GCC High for federal)
	CMMC	✓	✗	✗ Nécessite les plans de services gouvernementaux les plus chers
	ITAR	✓	✗	✗ Nécessite les plans de services gouvernementaux les plus chers

Capacités		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Interopérabilité	Fonctionne avec n'importe quel fournisseur de cloud public	✓	✗	✗
	Support des modèles hybrides (A la fois Google et Microsoft)	✓	✗	✗
	Support de tout type de destinataire, quel que soit leur outil de messagerie et leur configuration	✓ Virtru fonctionne quel que soit le client de messagerie ou la configuration de sécurité mis en place par le destinataire et Virtru ne peut jamais accéder à vos données	✗ Si votre courrier électronique voyage en dehors de l'écosystème Microsoft, vous risquez de perdre la sécurité, la résidence et le contrôle des données, et Microsoft peut accéder à vos données	✗ Si votre courrier électronique voyage en dehors de l'écosystème Microsoft, vous risquez de perdre la sécurité, la résidence et le contrôle des données, et Microsoft peut accéder à vos données

Capacités		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Contrôle d'accès Flexibilité et adaptabilité	Contrôles d'accès à la demande disponibles pour les administrateurs, les utilisateurs et les expéditeurs	 Contrôles d'accès granulaires aux messages et pièces jointes, sans configuration nécessaire (ni administrateur, ni utilisateur)	 Contrôles d'accès limités - «ne pas transférer» est la seule fonction disponible	 Cependant, les contrôles d'accès nécessitent une configuration de l'administrateur
	Ajouter et ajuster facilement les dates d'expiration pour les destinataires internes ou externes	 Support for every way you use Outlook today	 Non proposé	 Seuls les administrateurs peuvent modifier les politiques d'expiration et l'expiration est limitée aux destinataires externes
	Révoquer simplement les emails envoyés à des destinataires internes ou externes	 Support for every way you use Outlook today	 Non proposé	 Révocation limitée aux destinataires externes uniquement
	Contrôles d'accès et protection étendue aux pièces jointes (fichiers)	 Watermarking et protection des fichiers persistants pour la plupart des formats de fichiers et ainsi maintenir les contrôles d'accès. Possibilité de révocation de ces accès à tout moment	 les pièces jointes Microsoft Office telles que Word restent chiffrées mais d'autres formats tels que les PDF peuvent être téléchargés sans protection	 les pièces jointes Microsoft Office telles que Word restent chiffrées mais d'autres formats tels que les PDF peuvent être téléchargés sans protection

Ce sont vos données et Virtru vous aide à ce que cela continue

Virtru est une couche transparente de protection des données qui s'ajoute à votre expérience Microsoft native, afin que votre équipe puisse facilement protéger les messages, les pièces jointes et garder le contrôle partout où ces données sont partagées. Que vous utilisiez Outlook à partir d'un navigateur, d'un ordinateur de bureau ou d'un appareil mobile, sur votre PC, Mac, iPad ou téléphone, Virtru vous aide à sécuriser vos données.

Pour répondre à vos besoins, Virtru offre :

- Une protection centrée sur les données et une gouvernance des données de type Zero Trust pour collaborer en toute sécurité avec les destinataires autorisés et garantir qu'aucun tiers ne peut accéder à vos données. (que ce soit Virtru ou Microsoft)
- Options de gestion des clés de chiffrement pour respecter la conformité et la souveraineté de vos données.
- Protection pour sécuriser les messages envoyés et reçus par des applications SaaS personnalisées ou d'entreprise (Salesforce, ServiceNow etc.)
- Prise en charge d'un modèle d'utilisation hybride dans lequel Microsoft et Google sont déployés et utilisés conjointement
- Contrôles d'accès, y compris la révocation instantanée, le contrôle du transfert des messages, la date d'expiration, le filigrane des fichiers et la protection persistante des pièces jointes téléchargées, afin que chacun puisse protéger les données partagées en interne et en externe.
- Facilité d'utilisation et d'administration pour déployer et gérer la sécurité des données, y compris des règles de messagerie personnalisables.
- Adoption rapide par les utilisateurs pour éviter les erreurs humaines lors de l'envoi d'informations sensibles.
- Des renseignements exploitables sur toutes les données pour voir clairement lesquelles vous protégez, où elles vont et qui les a lues ou transmises.
- Accès transparent pour les destinataires sans leur imposer de nouveaux comptes ou mots de passe.

«Le secteur financier est particulièrement vulnérable aux attaques en raison de la prévalence des données sensibles, mais avec la facilité d'utilisation inégalée de Virtru, nous sommes assurés que les données les plus sensibles de nos clients et partenaires sont protégées.»

-Directeur de la sécurité, entreprise de services financiers

Plus de 6 000 clients font confiance à Virtru pour la sécurité des données et la protection de la vie privée.



Découvrez comment Virtru peut activer la confidentialité et la conformité pour Microsoft 365 Outlook. Contactez-nous aujourd'hui su virtru.com/fr/contact-sales