Assurez la souveraineté et la confidentialité des données stockées dans le cloud

Souveraineté des données dans le cloud

Alors que les solutions SaaS et de cloud computing continuent de gagner en popularité, la souveraineté des données est devenue une préoccupation majeure pour les organisations. Elle est une exigence propre à chaque pays selon laquelle les données sont soumises aux lois du pays dans lequel elles sont collectées ou traitées, et doivent rester sur le territoire national. Par conséquent, les organisations doivent porter une attention toute particulière à la manière dont elles gèrent leurs données à différents endroits.

En raison de la nature distribuée du cloud, les organisations s'inquiètent de la capacité à respecter la souveraineté des données et les exigences du RGPD ainsi qu'à garantir une véritable confidentialité des données ainsi qu'une protection contre les accès non autorisés. Mais, l'augmentation des workflows numériques entraîne la nécessité de surmonter ces obstacles. Le chiffrement de bout en bout est la méthode préférée pour partager et héberger en toute sécurité des données dans le cloud et la méthode de gestion des clés de chiffrement est essentielle pour maintenir le contrôle des données pour répondre aux exigences de confidentialité et de souveraineté des données de l'entreprise.

Virtru vous permet d'aller vers le cloud en toute confiance

Chiffrement des e-mails et des fichiers de bout en bout

Protégez les données dès leur création et assurez-vous que seul un destinataire autorisé peut les déchiffrer. Ni Virtru, ni votre fournisseur de services cloud n'auront accès à vos données.

Clés de chiffrement hébergées par le client

Hébergez les clés de chiffrement dans la région géographique requise pour résoudre les problèmes de souveraineté des données et gardez la liberté d'utiliser le fournisseur de cloud de votre choix.

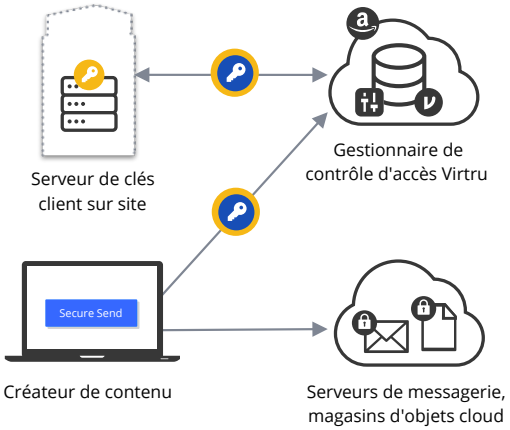
Contrôle d'accès à la demande

Ajoutez ou ajustez des contrôles d'accès, comme la possibilité de révoquer l'accès, de désactiver le transfert et d'ajouter une date d'expiration pour gérer où vont vos données et avec qui elles sont partagées.

Options flexibles de gestion de clés de chiffrement par couches

Décidez de l'emplacement d'hébergement et d'accès des clés de chiffrement afin d'empêcher le déchiffrement de données confidentielles en dehors des régions indiquées.

Clés entièrement hébergées pour une évolutivité sécurisée
Virtru génère une clé de chiffrement unique pour chaque e-mail ou fichier, qui est ensuite protégée par Amazon KMS. Les données chiffrées sont hébergées sur les serveurs de messagerie du fournisseur de cloud, mais stockées séparément de la clé qui peut les déchiffrer dans le cadre d'une architecture à connaissance distribuée. Le gestionnaire de contrôle d'accès (ACM) de Virtru applique les politiques que vous avez définies pour contrôler l'accès aux données chiffrées.



Virtru Customer Key Server (CKS)

Clés hébergées par le client pour un contrôle accru
Ajoutez un chiffrement asymétrique que vous hébergez sur site pour une couche de protection supplémentaire. Créez une paire de clés supplémentaire qui ne quitte jamais votre environnement afin de protéger vos clés de chiffrement sous-jacentes et de bénéficier d'une véritable sécurité de type "Hold Your Own Key". Virtru gère alors uniquement les politiques de sécurité et les échanges de clés.

Intégration HSM pour le plus haut niveau de sécurité
Virtru Customer Key Server (CKS) gère les demandes de chiffrement et de déchiffrement sur la plateforme Virtru et peut être intégré à votre HSM pour gérer les clés privées. Cette méthode s'appuie sur les protocoles PKCS (Public Key Cryptographic Standard) # 11 et KMIP, permettant l'intégration avec divers fabricants de HSM.

Vos données sont votre propriété et Virtru vous aide à ce qu'elles le restent

Virtru répond à votre besoin essentiel de partager et d'héberger des données dans le cloud. Nous facilitons l'accès au cloud car nous proposons un chiffrement de bout en bout qui protège les données des accès tiers ou non autorisés, tout en maintenant facile l'envoi d'un e-mail ou le partage d'un fichier. Virtru sécurise toutes les données que vous jugez importantes et vous permet d'avoir un contrôle total avec des contrôles d'accès comme la révocation des messages et la possibilité d'héberger vos propres clés de chiffrement pour assurer la souveraineté de vos données.

Confidentialité et sécurité avec des normes élevées de protection des données

Virtru est certifié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) avec la Certification de Sécurité de Premier Niveau (CSPN) qui atteste de sa capacité à résister aux cyberattaques et à s'inscrire le cadre d'un besoin croissant de normes élevées de sécurité.

Découvrez comment Virtru peut aider votre organisation à répondre aux exigences de souveraineté des données pour se conformer au RGPD et à d'autres réglementations sur la confidentialité des données. virtru.com/fr/contact-us