Un groupe industriel international installé en France confie la protection de ses données sur le cloud à Virtru

Après avoir migré vers G Suite, un groupe industriel international installé en France était conscient de la nécessité de prendre des mesures de sécurité supplémentaires afin de renforcer la protection des données confidentielles et de la propriété intellectuelle. Le service chargé de la sécurité numérique s'est rapidement tourné vers Virtru, l'unique partenaire de chiffrement recommandé par Google. La solution de protection des données Virtru pour Gmail a ainsi été déployée dans plusieurs services de l'organisation, dans le but d'améliorer la protection des données confidentielles tout au long de leur cycle de vie.

Grâce à Virtru, le client peut désormais :

- Trouver un équilibre entre l'exploitation efficace et la protection de ses données.
- Assurer la confidentialité de ses contenus relevant de la propriété intellectuelle.
- Améliorer la collaboration entre les équipes internes, les partenaires et les fournisseurs.
- Respecter les exigences de conformité au regard du RGPD.

Confidentialité des données relevant de la propriété intellectuelle

À la suite de la migration vers G Suite, la protection de la propriété intellectuelle était la principale préoccupation de l'organisation. Des données relevant de la propriété intellectuelle étaient régulièrement partagées par le biais de Gmail, à la fois en interne et en externe, entre le service juridique de l'organisation et les mandataires en brevets. L'entreprise était consciente qu'elle ne pouvait pas prendre le risque que ces données se retrouvent entre de mauvaises mains.

Alors qu'elle recherchait une solution pour renforcer la sécurité de ses données confidentielles, l'organisation s'est particulièrement intéressée à deux fonctionnalités Virtru : la révocation des accès et les tatouages numériques. La possibilité de révoquer les accès aux messages et aux pièces jointes est une solution idéale en cas d'e-mails envoyés par erreur ou de changement du niveau de confidentialité des données contenues dans un e-mail, et permet de s'adapter à l'évolution des projets et des partenariats. L'ajout d'un tatouage numérique composé de l'adresse e-mail d'un destinataire renforce la sécurité en contribuant à prévenir les fuites de données.

C'est toutefois la facilité d'utilisation de Virtru pour les employés (des directeurs aux échelons inférieurs) et les partenaires qui a conforté l'organisation dans son choix.

La sécurité à portée de main

L'organisation a opté pour Virtru en raison de son intégration fluide dans les workflows de messages Gmail qu'elle a l'habitude d'utiliser. La protection des données confidentielles (propriété intellectuelle, plans de recherche et de développement, et toutes autres données d'entreprise et juridiques) contre un accès par le distributeur cloud (en l'occurrence Google) a permis au client de bénéficier d'un contrôle total sur ses données et sur les accès, mais également de garantir un conformité totale au règlement général sur la protection des données (RGPD).

La facilité d'utilisation était un critère essentiel. L'équipe chargée de la sécurité numérique savait par expérience que si la solution n'était pas simple d'utilisation, les employés ne l'utiliseraient tout simplement pas. Grâce à l'application mobile Virtru, la protection des données dans les workflows de partage se trouve désormais à portée de main des employés. Les employés activent ou désactivent Virtru selon la classification des données (par exemple confidentielles, hautement confidentielles ou secrètes) avant d'envoyer un e-mail, sans avoir à quitter leur boîte de réception.

Exploitation du potentiel des données

Étant donné qu'elle ne nécessite pas de comptes ou d'identifiants supplémentaires, l'intégration fluide de Virtru dans Gmail favorise l'adoption par les utilisateurs. Elle renforce en outre la sécurité de l'organisation tout en facilitant les collaborations au sein de l'organisation et avec les partenaires externes.

Le déploiement d'une solution de chiffrement conviviale signifie que les employés et les partenaires n'ont plus à faire un choix entre la sécurité et le partage. Ils sont désormais en mesure d'exploiter le potentiel des données et de collaborer en toute confiance. En protégeant les données au niveau objet, Virtru garantit à l'organisation que ses données sont protégées à tout moment. Ainsi, elle n'a pas à se préoccuper de la conformité réglementaire ou des accès non autorisés et peut concentrer ses efforts sur le développement de l'entreprise. ●

N'hésitez pas à nous contacter pour découvrir comment Virtru peut accélérer la mise en place de votre programme de confidentialité en protégeant vos données relevant de la propriété intellectuelle et en empêchant tout accès non autorisé. **virtru.com/fr/contact-sales**

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. À l'origine du format de données approuvé (Trusted Data Format, TDF), la norme sectorielle ouverte pour la protection des données persistante, Virtru propose des technologies de confidentialité flexibles, approuvées et faciles d'utilisation fondées sur sa plateforme de protection des données qui régit l'accès aux données tout au long de leur cycle de vie : de la création au partage, en passant par la transmission, le stockage et l'analyse. Plus de 20 000 organisations de toutes tailles et de tous secteurs 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.