Le guide complet sur la

la confidentialité d'entreprise

La plus grande responsabilité de votre organisation et sa plus grande opportunité

Le guide complet sur confidentialité d'entreprise

La plus grande responsabilité de votre organisation
et sa plus grande opportunité

Dans ce guide :

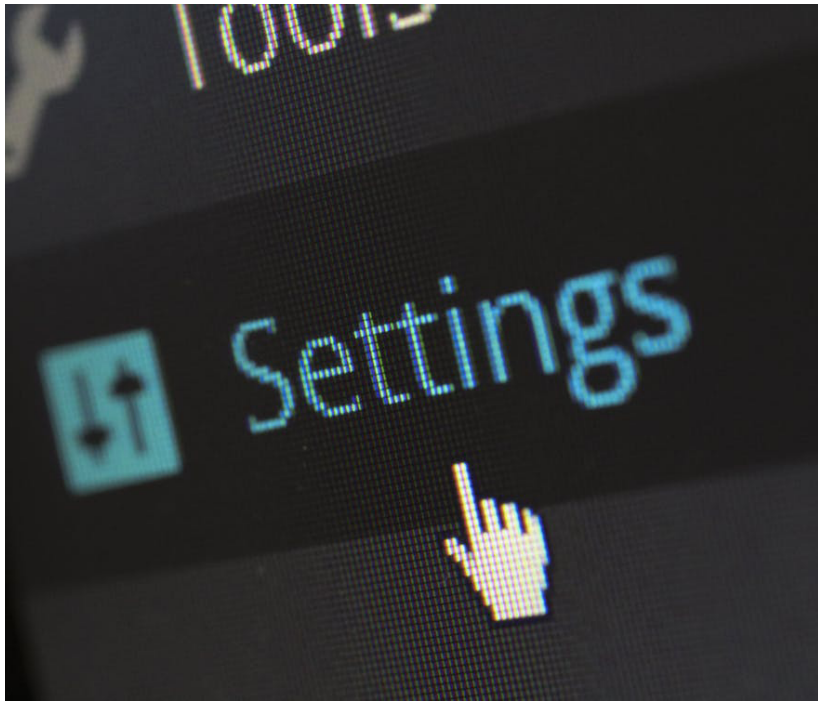
Il n'existe pas de solution de sécurité unique et parfaite.

Si vous avez déjà lu des livres blancs sur la cybersécurité, vous savez à quoi vous attendre : des statistiques effrayantes, une explication des raisons pour lesquelles les choses vont si mal, puis la solution « parfaite » : les outils de cybersécurité de cette entreprise.

Mais ce n'est pas vraiment ainsi que les choses fonctionnent. Le bon ensemble d'outils peut rendre les violations de données moins probables, moins dommageables et moins coûteuses, mais aucune solution technologique unique ne peut remplacer une stratégie de sécurité solide et à plusieurs niveaux.

Vos choix technologiques dans ce domaine sont faits pour accompagner les chefs d'entreprise et leur stratégie de cybersécurité. Indépendamment de ces choix, vous devrez toujours former et préparer votre personnel quant aux bonnes pratiques de sécurité. Vous devez toujours rester vigilant face aux nouveaux risques et travailler avec des contrôleurs de conformité pour les atténuer autant que possible.

Et vous ferez probablement face à une violation de données à un moment donné. Presque toutes les entreprises en font l'expérience. C'est pourquoi il est important d'être réaliste et préparé.



La confidentialité est votre responsabilité et votre avantage.

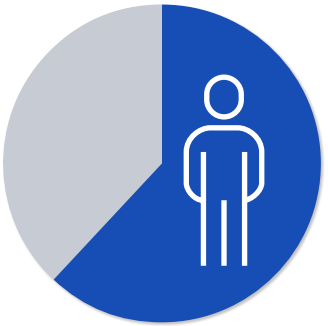
Votre écosystème de partenaires, de clients et d'autres parties prenantes reconnaît que les données deviennent vulnérables lorsqu'elles échappent à un contrôle direct. Dans une récente enquête de Pew Research, 62% des personnes interrogées ont déclaré qu'il était impossible de vivre au quotidien sans que les entreprises ne collectent des données à leur sujet - et 81% pensent qu'elles ont très peu ou pas de contrôle sur les données que ces entreprises collectent.

La même enquête a révélé que 70% des répondants estiment que leurs données sont moins sécurisées qu'il y a 5 ans, et environ 30% déclarent avoir subi une forme de violation de données au cours des 12 derniers mois.

Il est clair que le public a peu confiance dans la manière dont les entreprises collectent et utilisent leurs données. Ainsi, votre organisation peut se démarquer en donnant à vos clients et partenaires l'assurance que leurs données restent privées et sécurisées lorsqu'elles vous sont confiées - et cela peut être un avantage concurrentiel considérable.

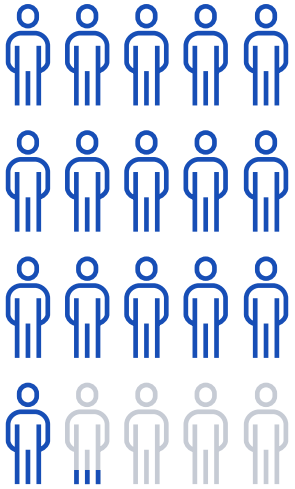
62%

des personnes interrogées ont déclaré qu'il était impossible de vivre au quotidien sans que les entreprises ne collectent des données à leur sujet



81%

qu'elles ont très peu ou pas de contrôle sur les données que ces entreprises collectent



Confidentialité d'entreprise : les fonctionnalités qui permettent aux organisations de ***partager des données de manière sécurisée et sélective*** avec des partenaires, des clients et des consommateurs.

En vous faisant confiance, vos clients et partenaires font de leur vie privée votre responsabilité.

Alors que se passe-t-il ? Si les clients s'interrogent sur la manière dont les entreprises collectent et utilisent leurs données, pourquoi ne prennent-ils pas les choses en main ? Parce qu'ils estiment qu'il n'est pas gérable de garder un contrôle total sur leurs données.

Il est assurément difficile pour un individu de reprendre le contrôle de ses données alors que tant d'entreprises les ont collectées. Une enquête NordPass 2020 a révélé que l'internaute moyen dispose de 100 mots de passe de compte sur les sites Web. Vraisemblablement, si les consommateurs ont pris le temps de créer ces comptes, ils stockent également des informations personnellement identifiables telles que leur adresse, leur numéro de téléphone ou leurs données de carte de paiement.

Les consommateurs se sentent généralement impuissants face aux cyberattaques et aux violations potentielles, mais en même temps, ils savent qu'ils doivent utiliser les services en ligne et les médias sociaux pour participer au monde moderne. Ainsi, ils passent outre leur peur et s'en remettent pour protéger leurs données.

En vous faisant confiance, vos clients et partenaires font de leur vie privée votre responsabilité. Et si votre entreprise a une grave défaillance portant atteinte à la vie privée, elle la considérera comme votre faute, même si ce n'est pas le cas.

Mais il y a un avantage à tout cela. Si vous pouvez protéger de manière proactive les données de vos clients et partenaires plutôt que de simplement réagir en cas de violation, ils resteront à vos côtés. Si vous saisissez l'occasion pendant que d'autres font le strict minimum pour respecter les réglementations de conformité, vous serez un champion de votre département, un champion de votre industrie et un champion des droits des consommateurs.

Confidentialité d'entreprise : le défi de l'ère du cloud

Les données que vous détenez sont précieuses car il ne s'agit pas que de vos données. Elles appartiennent à vos clients, à vos actionnaires et à vos partenaires aussi. Chaque source et groupe d'informations nécessitant un certain accès aux données présente de nouveaux défis de sécurité et d'éthique. Vous devez servir les clients tout en garantissant la sécurité de leurs données financières ou personnelles, en conservant les dossiers RH sans compromettre la confidentialité des employés et en travaillant avec des partenaires tout en gardant leurs secrets commerciaux confidentiels. Chaque cas d'utilisation présente une opportunité d'honorer la confiance d'une partie prenante ou de la trahir.

Les données internes sont tout aussi importantes et tout aussi délicates à protéger. Votre stratégie d'entreprise ou un élément de propriété intellectuelle peut être partagé avec des dizaines d'avocats, de consultants, de cadres, d'employés de bureau, de sous-traitants et d'autres parties prenantes. À moins que vous n'ayez un système qui donne accès à toutes ces parties tout en gardant à l'écart les personnes non autorisées, vos données restent vulnérables.

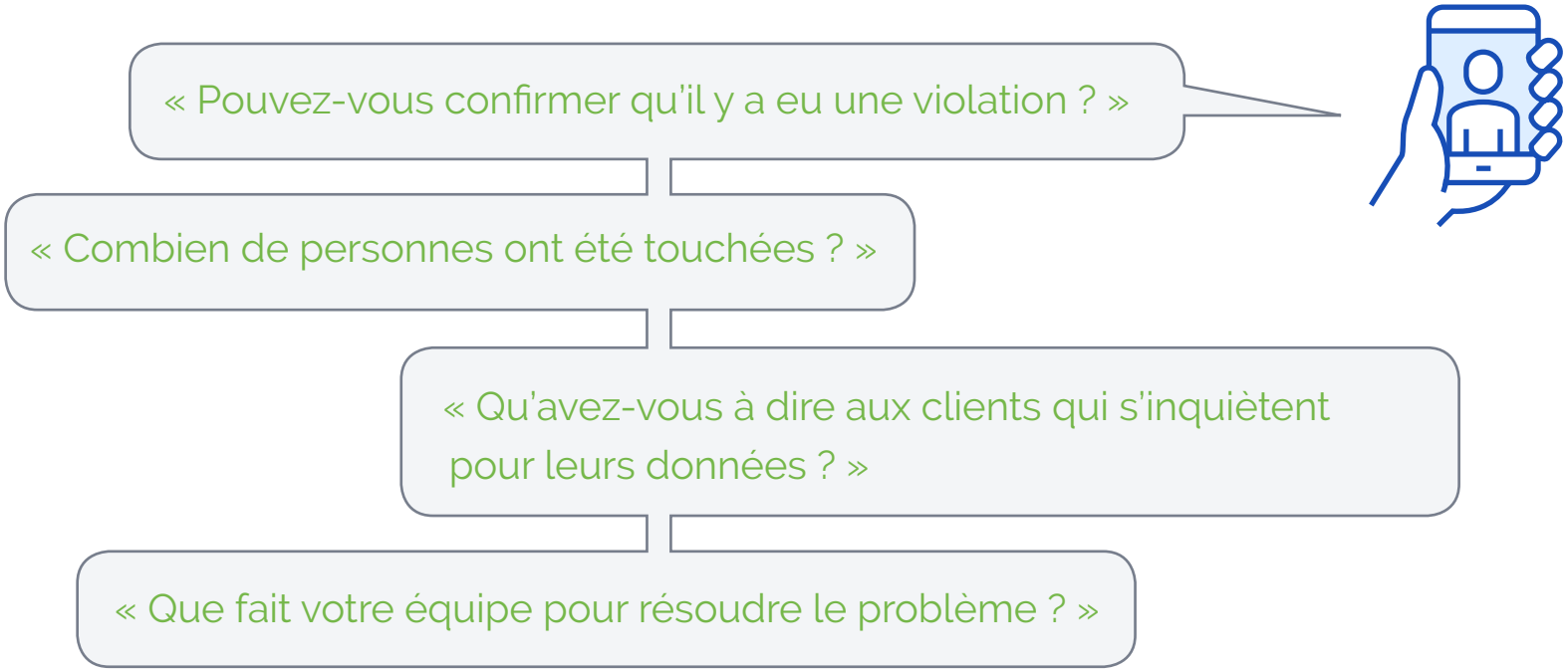
De nombreux défis de l'entreprise se résument ainsi à la confidentialité au sein de celle-ci. Par exemple, la capacité de votre organisation à collecter des informations sensibles, à les utiliser et à les partager rapidement sans les exposer à des pirates ou à des fournisseurs tiers.

La confidentialité d'entreprise intègre votre devoir de permettre la protection, le contrôle et l'accès facile aux données sensibles.
Les organisations qui adoptent ce type de confidentialité - celles qui sécurisent leurs données sans compromettre les flux de travail existants - ouvriront la voie. Le reste de ce guide vous montrera comment y arriver.

Chaque cas d'utilisation présente une opportunité d'honorer la confiance d'une partie prenante ou de la trahir.

Partie 1: Menaces du monde réel sur la confidentialité d'entreprise

Imaginez que vous êtes à la maison en train de vous préparer à aller dormir, lorsque vous recevez un appel d'un journaliste. D'après lui, des données sensibles de vos clients ont été divulguées et exposées.



Vous contactez immédiatement votre équipe de sécurité pour savoir ce qui se passe. Apparemment, c'est aussi la première fois qu'ils en entendent parler.

Qu'aurait-il pu arriver ? Votre équipe va envisager diverses possibilités :

- un employé pourrait avoir accidentellement divulgué les données.
- Une malveillance interne pourrait avoir abouti à une divulgation intentionnelle de données.
- Un pirate informatique aurait pu accéder aux comptes de messagerie des employés.
- Un pirate informatique aurait pu intercepter un e-mail envoyé entre deux employés ou pirater la connexion alors qu'un employé accédait à votre base de données.
- Un cybercriminel pourrait avoir exploité une vulnérabilité de sécurité causée par un tiers ayant accès à vos données. Il peut s'agir de l'entreprise hébergeant vos fichiers, de votre fournisseur de services Internet, d'un partenaire, d'un client ou même du créateur d'une application non approuvée installée sur l'un des ordinateurs de vos employés.

Ce n'est pas une liste complète, loin s'en faut. De nombreuses cyberattaques n'ont pas de point d'entrée clair.

Quoi qu'il en soit, les conséquences des violations prennent au dépourvu même les entreprises les plus préparées. Selon IBM, le coût moyen global d'une violation est de 3,86 millions de dollars. Les coûts tels que l'atteinte à la réputation de la marque, le futur examen du non-respect de certaines régulations et les frais juridiques sont difficiles à prévoir. Les organismes de réglementation et les tribunaux ont une longue mémoire, et la présence (ou l'absence) d'infractions passées pourrait déterminer si un incident futur est traité comme un acte de négligence.

L'employé moyen envoyant plus de 10 000 e-mails chaque année, les données circulent vers et depuis les organisations à grande vitesse. Il n'est pas improbable qu'une violation ait pu être causée par un e-mail imprudent ou un fichier partagé par inadvertance. Pour calculer la quantité de données que votre organisation partage par e-mail, utilisez la calculatrice de partage de données de Virtru.

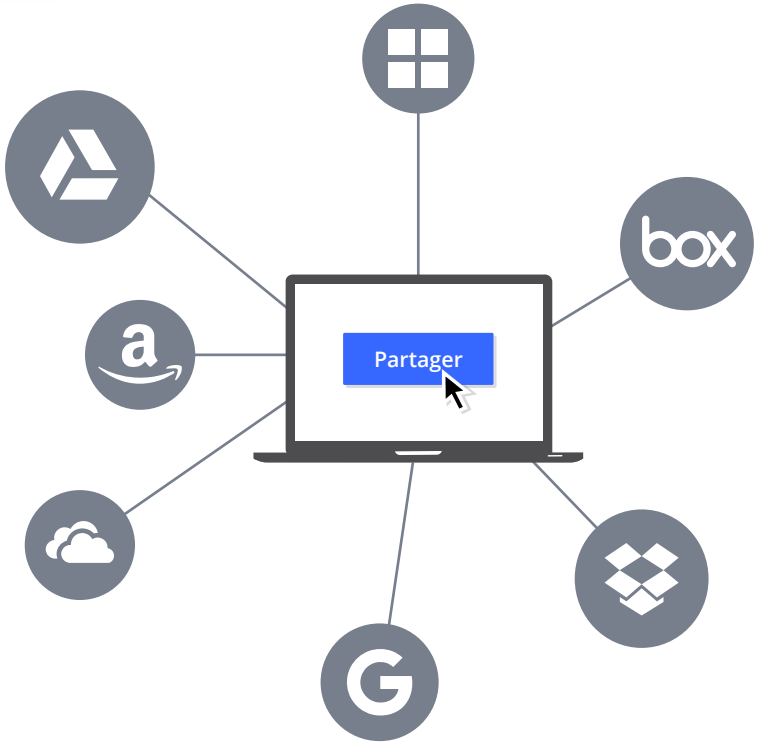
Les organisations peuvent-elles faire confiance aux fournisseurs de cloud ?

Toute personne pouvant accéder à vos données peut potentiellement compromettre leur confidentialité, y compris votre fournisseur de services cloud. Le chiffrement protège contre ce danger en réarrangeant vos données sous une forme illisible. Tant qu'une partie n'a pas accès à la fois aux données et aux clés qui les protègent, vos informations sont en sécurité.

Cependant, les fournisseurs qui chiffrent votre contenu contrôlent généralement à la fois les données et la clé pour les déverrouiller. Cela n'est pas fait dans un but néfaste, mais plutôt pour des raisons de commodité. Cela permet à votre fournisseur de protéger vos données contre les attaques extérieures, tout en les rendant accessibles lorsque vous en avez besoin.

Mais cela signifie également que votre fournisseur de cloud peut lire vos données sous forme de texte brut (non chiffré) et y avoir un accès complet. Cet accès crée un risque inutile pour votre entreprise, vos partenaires et vos clients. Cela entrave également votre capacité à vous conformer à certaines réglementations de conformité, telles que celles relatives aux services d'information de la justice pénale américaine (CJIS), au règlement sur le trafic international d'armes (ITAR), et les exigences en matière de souveraineté des données.

Pour plus d'informations sur la protection des données dans le cloud, lisez la fiche technique de Virtru, Souveraineté et confidentialité des données dans le cloud.



Une violation de la confidentialité des données est une violation des droits

« Nul ne doit être soumis à une ingérence arbitraire dans sa vie privée, sa famille, son domicile ou sa correspondance, ni à des atteintes à son honneur et à sa réputation. Chacun a droit à la protection de la loi contre de telles ingérences ou attaques. »

-Déclaration universelle des droits de l'homme, proclamée par l'Assemblée générale des Nations Unies, 1948

La vie privée n'est pas seulement une nécessité économique : c'est un droit fondamental. Lorsque les clients achètent vos produits, ils sont convaincus que vous pouvez protéger leurs données et identités financières. Lorsque les partenaires collaborent avec vous sur des projets sensibles, ils sont convaincus que vous pouvez protéger ce projet des concurrents, de la presse et du public. Lorsque de nouveaux employés soumettent leur passeport, leurs données de santé et leurs informations de compte bancaire aux RH, ils dépendent de vos contrôles internes pour garder confidentielles leurs données les plus privées.

Si vous ne parvenez pas à protéger ces données, vous ne créez pas seulement des risques pour vos clients ou des coûts supplémentaires pour votre entreprise. Vous trahissez la confiance qui encourage les gens à faire des affaires avec vous.

La plupart des entreprises font de leur mieux pour protéger la cybersécurité en interne, mais vos clients et partenaires ne se soucient pas de la quantité de travail et d'argent que vous consacrez à la cybersécurité. Ils jugent votre entreprise par le succès ou l'échec de vos méthodes.

Mais les anciennes méthodes ne fonctionnent plus.

Partie 2 : Pourquoi la confidentialité d'entreprise est plus importante que jamais

La confidentialité d'entreprise est essentielle dans un paysage numérique en mutation, en particulier à mesure que les effectifs sont de plus en plus largement répartis. Alors que les organisations continuent à faire évoluer leurs façons de communiquer et de partager des informations, leurs approches de sécurité des données parviennent rarement à suivre le rythme et le monde en a pris note.

En conséquence, il existe plusieurs façons de rendre des données vulnérables. Parmi elles, il y a :

1. **Les attaques visant votre organisation interne et votre infrastructure.** Les pirates peuvent cibler vos employés directement sur les outils qu'ils utilisent pour accéder à Internet - et leurs méthodes sont devenues de plus en plus sophistiquées et crédibles. Cela met en péril vos propres données internes, documents de stratégie et communications.

2. **Attaques visant les infrastructures que vous utilisez mais que vous ne possédez pas.** Par exemple, si vous sous-traitez la facturation et que votre partenaire financier a son e-mail piraté, cela peut compromettre vos données. De même, si votre e-mail traverse un serveur mal configuré sur le chemin de votre partenaire, un pirate informatique peut intercepter les données en cours de route. Dans un monde où tant d'informations transitent par e-mail et des milliers d'applications SaaS basées sur le cloud, cela présente de nombreuses opportunités pour que les données soient placées entre de mauvaises mains.

3. **Attaques visant d'autres organisations qui ont des liens avec vos employés ou clients.** Si un membre de votre organisation est lié à une autre entreprise, les pirates peuvent le cibler via son compte de messagerie ou un appareil appartenant à son groupe, accédant ainsi à vos propres données.

   Les dirigeants, les membres du conseil d'administration, les investisseurs et d'autres personnalités de haut rang impliquées dans votre organisation peuvent être particulièrement vulnérables à ces dommages collatéraux, car ils sont plus susceptibles d'être liés à des organisations ciblées. De plus, ils peuvent eux-mêmes être la cible d'un pirate informatique comme un hacktiviste ou un associé mécontent.

4. **Attaques visant l'erreur humaine courante.** Nous avons tous accidentellement envoyé un e-mail à Michel S. au lieu de Michel P., ou peut-être transféré toute une discussion sans vérifier tous les messages précédents pouvant contenir des données et informations sensibles. Plus il est facile de partager des informations, plus vous pouvez faire de dégâts en les partageant accidentellement avec la mauvaise personne. Parlez au mauvais moment et vous pourriez donner un précieux secret à une personne. Mais envoyez une feuille de calcul ou un rapport confidentiel au mauvais groupe ou individu, et vous avez potentiellement compromis des milliers d'enregistrements et donné aux destinataires le pouvoir de partager ces enregistrements avec le public.

Leçons en matière de confidentialité d'entreprise : les données ne sont pas seulement partagées par e-mail - Protection des vidéos

Les vidéos produites par les caméras de surveillance représentent certaines des données les plus sensibles disponibles. En plus de permettre aux entreprises de capturer des séquences vidéo de leurs bâtiments, les sociétés de sécurité fournissent également des caméras vidéo au grand public et aux familles dont certaines capturent l'intérieur de leur maison.

Début 2021, deux violations majeures ont ciblé des images de caméras de sécurité : une impactant Verkada, une entreprise américaine de sécurité du bâtiment, et un autre incident en Chine où des pirates ont eu accès à des milliers de vidéos de caméras de sécurité privées, y compris des images de familles dans leurs maisons et de voyageurs dans les chambres d'hôtel.

Les données sensibles sont partout, qu'elles soient contenues dans une base de données, une correspondance par e-mail, un fichier ou une vidéo en images animées. **Quels types de données sensibles sont confiés à votre entreprise ?**

Partie 3 : Comment Virtru sécurise le partage des données

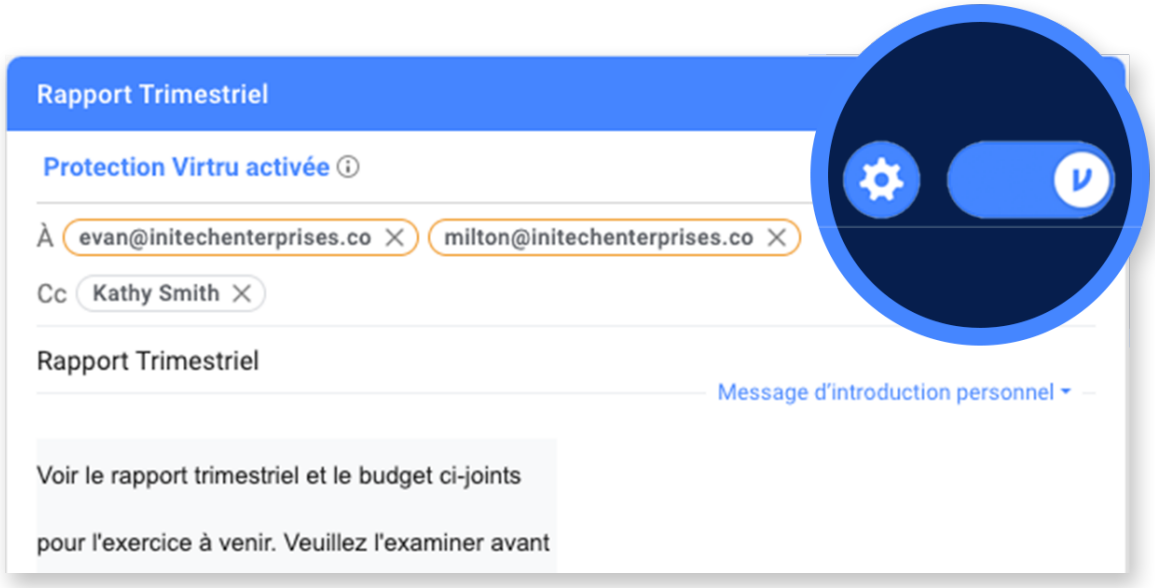
Virtru est une plate-forme de sécurité basée sur le cloud, centrée sur les données et qui permet aux organisations et aux gouvernements de protéger et de partager les données comme ils le souhaitent sans en perdre le contrôle, où qu'elles se trouvent.

Cette plateforme propose un ensemble complet de chiffrement des données, de contrôle d'accès et de gestion des clés contrôlées par l'expéditeur pour protéger les données hautement sensibles dans n'importe quel environnement - auditables et révocables à tout moment.

La technologie pionnière de Virtru, le Trusted Data Format (TDF), est une norme de marquage et de chiffrement des données ouvertes utilisée par plus de 6 000 clients dans le monde.

En quoi le chiffrement des données Virtru est différent

1. **Protégez vos données au niveau de l'objet et partout où elles se déplacent - pas uniquement le périmètre de l'entreprise :** Virtru utilise un chiffrement centré sur les données elles-mêmes pour protéger vos fichiers et vos e-mails tout au long de leur vie numérique. Chaque élément de données est chiffré avant de quitter votre réseau et déchiffré uniquement lorsque le destinataire prévu l'ouvre.



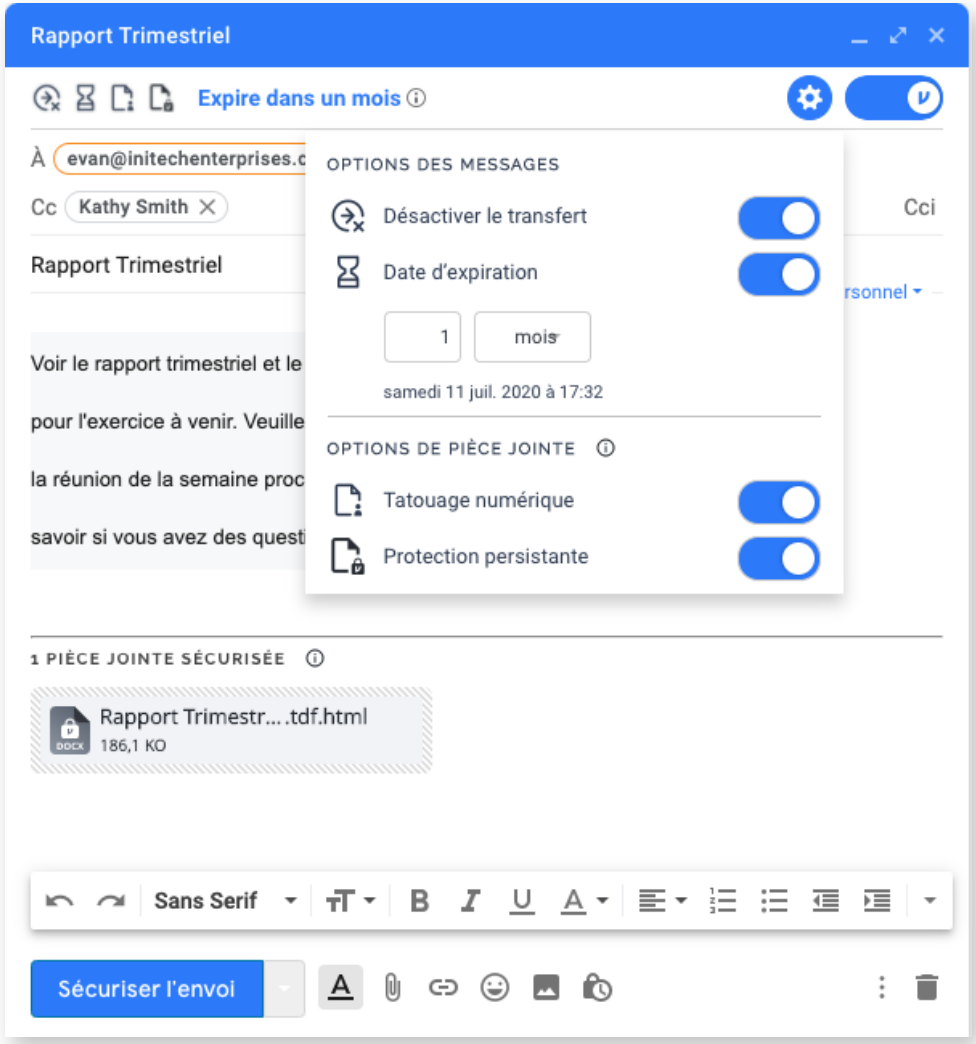
La donnée elle-même (le contenu) est stockée et transmise séparément des clés de chiffrement qui la protègent. Cela signifie que même si des pirates interceptent vos e-mails et vos fichiers, ils ne peuvent pas y accéder car ils n'auront pas les clés de chiffrement.

Nommée Split Knowledge, cette architecture est essentielle pour les organisations qui cherchent à se conformer à la Loi sur la portabilité et la responsabilité de l'assurance maladie (HIPAA), CJIS, ou exigences EAR et RGPD qui restreignent l'accès aux données sensibles par des tiers.

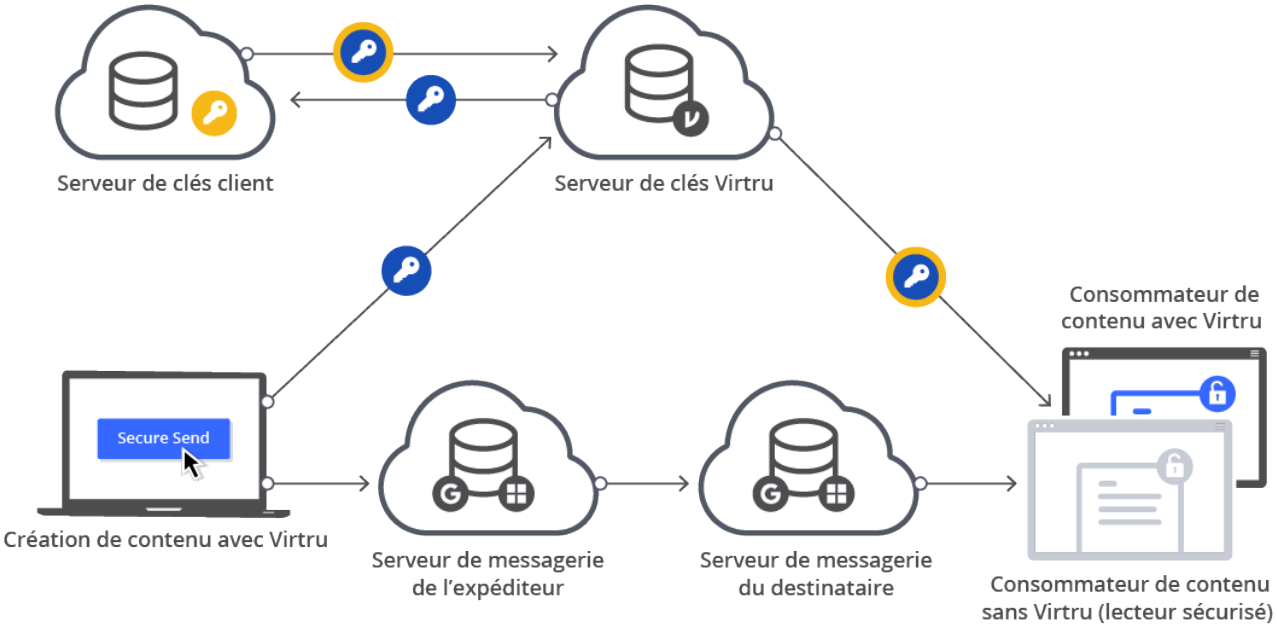
Plus important encore, cela signifie qu'il n'y a pas de point de défaillance unique. Peu importe que vous ne puissiez pas protéger tout le périmètre, car les données elles-mêmes restent en sécurité tout au long de leur parcours.

2. Partagez des données sans compromettre votre capacité à les protéger : il est courant que vous perdiez le contrôle de vos données lorsque vous les partagez à quelqu'un d'autre. Que vous remettiez un fichier à quelqu'un ou que vous envoyiez un e-mail, une fois que ces données ont quitté vos mains, vous devez faire confiance à ce tiers pour les protéger.

Avec Virtru, ce n'est plus le cas. Vous contrôlez toujours qui peut accéder à vos clés de chiffrement, ce qui signifie que vous contrôlez toujours qui peut accéder à vos données. Si vous envoyez un e-mail ou une pièce jointe à la mauvaise personne, vous pouvez révoquer l'accès pour l'empêcher de le lire à l'avenir, même si elle l'a déjà lu une fois. Vous pouvez également définir des limites de temps après lesquelles votre destinataire perdra l'accès, ou désactiver le transfert de fichier ou d'e-mail pour l'empêcher de transmettre du contenu sensible à d'autres destinataires.



3. **Utilisez les solutions cloud de votre choix tout en gardant un contrôle total sur vos données :** En séparant l'emplacement de stockage des clés chiffrement et du contenu, le chiffrement de Virtru vous permet d'exploiter les plates-formes basées sur le cloud tout en garantissant que vos données restent protégées. Il est même possible de gérer vos propres clés sur site ou dans un cloud privé. Même si les fournisseurs de cloud ont accès à votre contenu, celui-ci est chiffré et ces fournisseurs n'ont pas accès aux clés de chiffrement. Les seules personnes (à part vous et les administrateurs de votre organisation) qui peuvent déverrouiller vos données sont les destinataires que vous avez prévus.



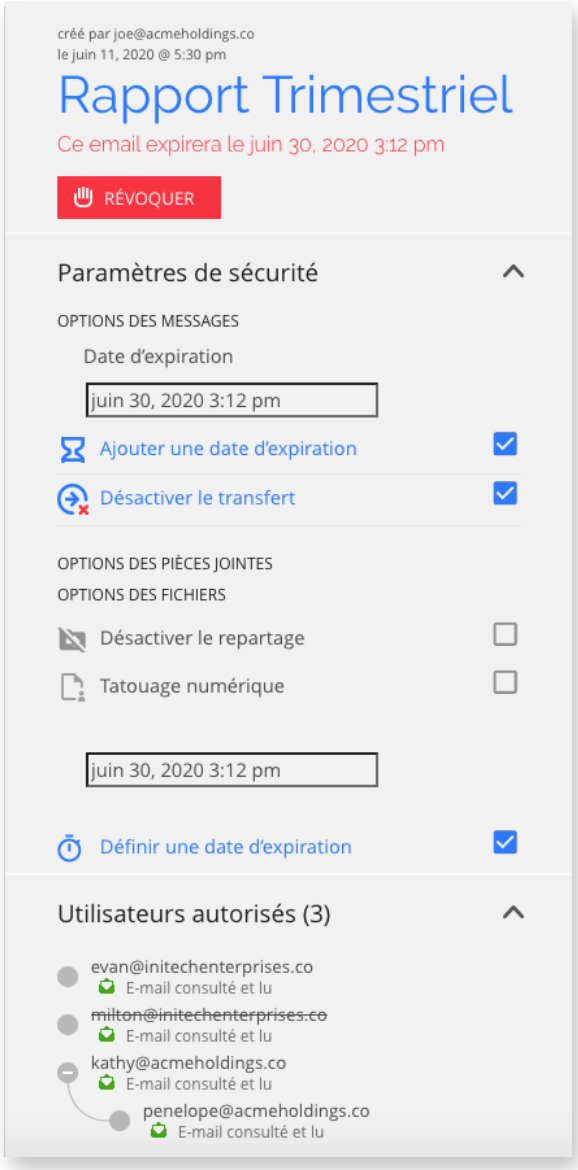
Dans le cas d'une violation de sécurité - lorsque tant de questions sont en suspens - il est inestimable de savoir exactement qui a consulté et partagé les données en question.

4. **Affranchissez-vous de la nécessité de forcer vos clients à se conformer à vos outils :** au lieu d'imposer de nouvelles solutions et technologies à vos clients, Virtru vous permet de travailler avec les outils que vous utilisez déjà et qu'ils ont déjà aussi, tels que Gmail, Google Drive, Microsoft Outlook, iOS et Android. Virtru permet aux clients de recevoir, lire et répondre aux e-mails chiffrés par Virtru sans avoir à installer de nouveau logiciel ni créer de nouvelles informations d'identification comme un nouveau compte où que ce soit.

   Les destinataires peuvent répondre en utilisant leurs comptes de messagerie existants et même envoyer des réponses sécurisées avec des pièces jointes en quelques clics, sans installation ni configuration. Cela augmente considérablement les taux d'adoption par rapport aux portails sécurisés et aux outils de chiffrement de messagerie traditionnels. Cela signifie également que vous pouvez envoyer des messages sécurisés à des clients potentiels, à de nouveaux partenaires et à d'autres personnes qui ne disposent peut-être pas d'un outil de communication sécurisé.

5. **Améliorer la visibilité et le contrôle :** Virtru permet aux employés de surveiller et de contrôler l'accès aux données à l'intérieur et à l'extérieur de l'organisation. Lorsqu'un destinataire accède à des données chiffrées, Virtru en informe l'expéditeur. Même si un message a été transféré ou envoyé à plusieurs destinataires, l'expéditeur peut voir exactement qui a ouvert le message.

   Combinée à des outils tels que la révocation des messages et la désactivation du transfert, cette visibilité fournit un outil puissant pour traiter les violations potentielles. Si les expéditeurs révoquent un message avant son ouverture, Virtru en fournit la preuve, évitant une notification de violation. Si des destinataires non désirés ont déjà accédé à vos données, Virtru devient un outil puissant pour l'atténuation des violations. Vous pouvez empêcher ces destinataires d'ouvrir ou de partager du contenu à l'avenir et isoler votre enquête et résolution de brèche de sécurité uniquement vers les destinataires qui ont déjà obtenu l'accès. Dans le cas d'une violation de sécurité - lorsque tant de questions sont en suspens - il est inestimable de savoir exactement qui a consulté et partagé les données en question.



L'avenir de la confidentialité d'entreprise

L'avenir de la confidentialité d'entreprise est centrée sur les données. Les organisations n'ont plus à choisir entre la sécurisation de leurs données et leur partage. Avec Virtru, ils peuvent réaliser les deux, en toute confiance.

En protégeant la confidentialité de vos données d'entreprise, vous pouvez exploiter toute la puissance du cloud tout en vous assurant la confiance de vos clients. Les entreprises qui peuvent montrer la voie seront toujours récompensées.

Pour en apprendre plus, contactez-nous aujourd'hui pour que nous puissions en discuter.

virtru

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