FORTRA

EBOOK (GoAnywhere)

Le contrôle dans le cloud : comment le MFT vous aide à relever vos défis en matière de données ?

Introduction

Ces dernières années, l'évolution rapide et inattendue des opérations métier a révélé de nouveaux défis sur le plan de la sécurité. Si beaucoup se sont débattus pour maintenir la sécurité de leurs données lors de l'adoption de technologies cloud, d'autres ont reconnu la valeur ajoutée d'une solution MFT (transfert de fichiers géré) performante. Nous avons échangé avec un groupe d'experts issus d'un large éventail d'entreprises et de secteurs, et leurs témoignages vous permettront d'appliquer votre initiative cloud de la façon la plus transparente, sécurisée et efficace possible.

La transformation numérique a bouleversé la gestion des entreprises. Cette transformation se produit en grande partie dans l'écosystème cloud. Des déploiements cloud ont lieu dans tous les secteurs et dans toutes les industries. Avec le cloud, nous avons commencé à comprendre les avantages liés au déploiement de services à valeur ajoutée dans l'écosystème cloud, via une gestion efficace des données. Les nombreux autres atouts de la gestion et du stockage des données dans un environnement cloud comprennent notamment : les économies de coût, la flexibilité, la mobilité, une meilleure sécurité des informations, une collaboration renforcée et de nouvelles connaissances issues des données de l'entreprise.
(Reza Alavi | Directeur principal, Technologies et risque numérique | LinkedIn)

Le télétravail a accéléré l'adoption des technologies cloud, mais si les applications collaboratives cloud ont vu leur adoption augmenter, les méthodes de transfert de fichiers sont restées quasiment inchangées. Cette situation semble davantage poussée par la nécessité de rénover ou de remplacer un système donné, et de migrer ce dernier vers le cloud. Pour nous, cet événement a assurément agi comme un catalyseur : nous étions en train d'abandonner le modèle économique sur site au profit d'un système cloud, et nous devions nous assurer que les données étaient sécurisées. Le transfert de fichiers géré nous a permis de déplacer les fichiers tout en bénéficiant de la flexibilité et du contrôle dont nous avions besoin.
(Matthew Hankinson | Gestionnaire d'infrastructure | LinkedIn)

Question 1 : les défis d'une infrastructure sur site

Quels sont les principaux défis liés au transfert des données sur site et dans le cloud ? Comment la technologie adéquate peut-elle aider sur le plan de la productivité, de la sécurité et de la conformité ?

Funso Richard | Chef de la sécurité informatique | LinkedIn
Une gestion inefficace des données constitue le principal défi auquel sont confrontées les organisations. L'utilisation de protocoles sur site pour le transfert de fichiers (dans et hors l'organisation) représente des défis majeurs, comme une sécurité et une mobilité insuffisante, des problèmes de performance, des coûts de maintenance, une productivité impactée et une expérience utilisateur médiocre. Parmi les solutions alternatives, on trouve le transfert des données dans le cloud. Cette pratique comporte toutefois son lot de difficultés, parmi lesquelles une planification inefficace, un coût financier, une mauvaise configuration et une piètre expérience client. Cette dernière, par exemple, pousse les employés à utiliser des solutions de transfert non approuvées pour déplacer les fichiers. Une telle pratique expose l'entreprise à un risque grave de perte, d'exfiltration et de fuite de données.

Pour garantir la protection des données et une productivité optimale, il est vital d'investir dans une technologie de transfert de fichiers adéquate afin de maintenir un fonctionnement efficace et efficient de l'entreprise. Compte tenu de l'accroissement de l'adoption du télétravail et de la dépendance vis-à-vis de la chaîne logistique, les organisations ont besoin d'une technologie de transfert de fichiers à la fois dynamique, fiable et flexible pour pouvoir déplacer leurs données entre plusieurs protocoles, plateformes et environnements. Cette technologie porte un nom : transfert de fichiers géré (MFT). Le MFT intègre des contrôles de sécurité, sans toutefois impacter négativement la productivité ni les performances. Le MFT offre de nombreux avantages : réduction des coûts, gestion centralisée des données, évolutivité, intégration, conformité, accès aux données en temps opportun, processus décisionnel amélioré, expérience utilisateur positive.

Gary Hibberd | Consultant en sécurité | LinkedIn
Le transfert de données (qu'elles soient sur site ou dans le cloud) pose deux questions fondamentales en matière de contrôle : qui a accès aux données, et comment celles-ci sont-elles transférées ? Le volume des données traitées ne cesse de croître, et leur partage sécurisé au sein de nos infrastructures est d'une importance capitale pour toute organisation.

Les défis auxquels nous sommes confrontés concernent la gestion et le contrôle de ces transferts et, lorsque ces transferts se produisent, nous devons déployer des solutions techniques adéquates, comme le transfert de fichiers géré (MFT). Les fonctionnalités de gestion et de surveillance des données d'une solution MFT garantissent l'arrivée à bon port des données. Une solution MFT efficace réduit les risques de conformité en garantissant le maintien de l'intégrité des données. En outre, une telle solution augmentera la productivité en réduisant la surcharge du réseau, tout en rendant les transferts plus rapides et plus fiables.

Michael Barford | Ingénieur solutions | LinkedIn
Concernant les transferts de données sur site, la complexité élevée liée au développement et au maintien de solutions personnalisées pour le traitement des transferts à hauts volumes et hautement complexes constitue encore l'un des défis majeurs. Et pourtant : les organisations ont encore largement recours aux scripts ou à des « solutions maison » pour traiter les transferts internes. Ce choix s'accompagne de coûts de maintenance et d'exploitation particulièrement élevés. Et qui dit coûts élevés, dit taux d'erreur non négligeable. Lorsqu'un fichier est perdu, il faut généralement plusieurs jours pour s'en rendre compte et mobiliser différentes ressources informatiques pour analyser la cause profonde, savoir où se trouve le fichier, traiter celui-ci manuellement et réparer le « script » afin que le problème ne réapparaisse pas à l'avenir. Le problème prend de l'ampleur lorsque les individus qui ont développé la solution maison changent de poste ou quittent l'entreprise, ou lorsque cette solution personnalisée doit être appliquée à plus grande échelle pour pouvoir gérer d'autres cas d'utilisation (impliquant de plus en plus souvent le cloud).

Les exigences de sécurité ou de conformité constituent généralement une autre difficulté. La conformité est un défi extrêmement difficile et coûteux si l'on ne dispose pas d'une solution spécialement conçue, à jour avec les derniers protocoles de sécurité et dotée de fonctionnalités complètes de cryptage, d'audit, de génération de rapport et de séparation des rôles.

Lors du passage au cloud, il est important de veiller à ce que la solution MFT puisse interagir avec de nombreuses plateformes cloud, mais aussi avec des API REST (qui évoluent constamment afin de prendre en compte les cas d'utilisation futurs).

En raison du grand nombre de plateformes et d'interfaces avec lesquelles les entreprises doivent aujourd'hui composer, il est de plus en plus difficile de respecter les exigences en matière de sécurité, d'audit et de maintenabilité des transferts de données. Traditionnellement, les processus de transfert de fichiers sont configurés, puis s'exécutent sans surveillance, ce qui convenait très bien à l'ère des transferts SFTP ou FTP (vous pouviez utiliser le même processus pour plusieurs partenaires commerciaux). Les difficultés apparaissent lorsqu'il devient nécessaire d'adapter le processus : c'est le moment que choisissent généralement les clients pour se tourner vers une solution MFT.

L'utilisation de la technologie adéquate permet aux entreprises de s'adapter plus aisément face aux exigences en constante mutation dans le domaine du transfert de fichiers.

Ray Sutton | Consultant technique | LinkedIn
Les obstacles au transfert des données sont nombreux et concernent principalement la divulgation de ces services auprès de tierces parties (éventuellement via Internet). Pour relever ces défis, vous devez maintenir un environnement performant et sécurisé, mais aussi, dans la plupart des cas, perfectionner la solution de façon à protéger les réseaux et les systèmes au sein de votre organisation. Ce défi concerne également l'univers du cloud : en effet, vous devez également étudier la sécurité offerte par le datacenter (basé sur le cloud) auquel vous vous connectez afin de renforcer la protection des données. Il faut atteindre un équilibre optimal afin de respecter les exigences en matière de productivité du personnel, de sécurité et de conformité. Toute personne interagissant avec vos systèmes doit également avoir la certitude que vous respectez tous les critères de sécurité et disposez d'un processus facile à suivre pour le transfert des données. Cette étape est essentielle pour maintenir une sécurité élevée. Manquer cette étape, ou déployer des processus ou systèmes difficiles, pourrait inciter certaines personnes à rechercher des alternatives plus rapides, ce qui pourrait mettre en péril la façon dont vous soutenez vos solutions cloud ou sur site.

Matthew Hankinson | Gestionnaire d'infrastructure | LinkedIn
Le transfert sécurisé des données exige un juste équilibre entre, d'un côté, répondre aux besoins de l'entreprise et, de l'autre côté, satisfaire les exigences de cybersécurité. Une telle solution doit répondre aux besoins métiers tout en se montrant conforme. Le transfert sécurisé des données doit répondre aux préoccupations de chacun, et une garantie de cybersécurité est exigée d'un point de vue pratique, mais aussi réglementaire.

Les différences clés entre le déplacement de fichiers sur site et dans un environnement cloud ont toujours porté sur le contrôle. Le cloud nous emmène dans un territoire inconnu, où nous devons faire confiance à un prestataire tiers. Aussi, vous devez vous assurer que ce prestataire de services cloud respecte vos standards de sécurité. De même, vous devez parfaitement connaître les différents types de données que vous envoyez. Si les données comportent des informations personnellement identifiables (PII), vous devez vous assurer que le processus s'accompagne de dispositifs de protection supplémentaires. Trop souvent, les gens ne s'interrogent pas sur la nature des données transmises. On leur demande simplement de déplacer un fichier d'un emplacement à un autre, mais en quoi consistent réellement ces données ? Leur fuite éventuelle entraînerait-elle un problème grave pour l'entreprise ? Il est essentiel de disposer d'une solution fiable de transfert de fichiers géré, capable de déployer de telles fonctionnalités de sécurité. Une grande partie du problème consiste à se débarrasser des vieilles habitudes. Après avoir échangé librement les informations pendant de nombreuses années, les utilisateurs doivent désormais réfléchir aux données contenues dans les fichiers, sous peine d'enfreindre des lois sur la vie privée. Nous nous efforçons de sensibiliser les utilisateurs au contenu qu'ils envoient. Nous travaillons sur la mise en place d'un processus standard et de points de passage initiaux permettant d'analyser les requêtes.

Soulos Panagiotis | Responsable mondial de la sécurité informatique | LinkedIn

Les principaux défis liés au transfert de données sur site comprennent notamment :

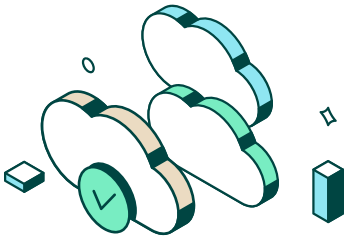
Lacunes de sécurité : les solutions traditionnelles de transfert de fichiers sur site, comme le FTP et le SFTP/FTPS, ne répondent pas à tous les besoins de sécurité actuels de l'entreprise. Le FTP n'a pas été conçu pour assurer la sécurité et ne dispose même pas des contrôles de sécurité les plus élémentaires, comme un canal d'authentification crypté. Le cryptage (p. ex. le cryptage des transferts et du stockage destiné à protéger les données en transit et at rest) est une pensée « après coup », qui exige des étapes et une expertise informatique supplémentaires, rendant ainsi difficiles, coûteux et chronophages l'envoi et le stockage sécurisé de fichiers. En outre, ces solutions ne prennent pas en charge l'échange d'identifiants utilisateur, lequel doit alors être géré par des procédures externes, souvent manuelles et risquant d'être dépourvues de mesures de sécurité (ce qui peut augmenter le risque de divulgation des identifiants).

Automatisation : les solutions traditionnelles ne proposent pas l'automatisation ou la planification des opérations de transfert de fichiers. Des scripts manuels ou des solutions supplémentaires sont généralement requis pour répondre à ces besoins, entraînant un surcoût et la nécessité d'une expertise du côté de l'équipe informatique.

Alertes automatisées : les solutions traditionnelles ne proposent pas de notifications automatisées et doivent être associées à d'autres solutions pour pouvoir informer l'utilisateur en cas d'échec d'un transfert de fichier.

Continuité de l'activité : des plans de reprise après incident (DRP) doivent être élaborés et déployés manuellement, car les solutions traditionnelles n'intègrent aucun mécanisme DRP automatisé. Notons également que les procédures de reprise en cas d'échec de service sont exécutées manuellement.

Problèmes de capacité : les solutions sur site peuvent éprouver des difficultés lors du transfert de fichiers volumineux, notamment en raison de pannes et d'erreurs réseau mineures.



Voici les principales difficultés liées au transfert de données dans le cloud :

Conformité : selon le type d'organisation, des réglementations et/ou normes industrielles spécifiques doivent être respectées. La souveraineté des données doit également être prise en compte lors du stockage et du transfert de données dans le cloud.

Fuites/Violations de données : Des fuites ou violations de données peuvent se produire en cas de compromission du prestataire cloud.

Accès/Déni de service : l'accès aux services peut être bloqué si le prestataire cloud est victime d'une attaque par déni de service ou si l'organisation n'a plus accès à Internet.

Infection par logiciel malveillant : des contrôles anti-malware doivent être mis en place afin d'atténuer le risque à ce que les fichiers stockés et transférés dans le cloud soient infectés par ces mêmes logiciels malveillants.

Enfermement/Blocage propriétaire et portabilité des services : l'utilisation de services cloud doit être évaluée de façon à éviter les situations d'enfermement et de blocage propriétaire tout en favorisant le plus possible la portabilité des services vers un autre fournisseur/prestataire de services cloud. L'enfermement propriétaire (« vendor lock-in ») désigne une situation où le coût du changement de fournisseur est tellement élevé que l'organisation est contrainte de rester avec son fournisseur actuel. Le blocage propriétaire (« vendor lock-out ») désigne, quant à lui, une situation où le fournisseur cesse ses activités et met fin aux services proposés.

En disposant de la technologie adéquate, une organisation peut relever ces défis en s'assurant que cette technologie peut améliorer sa productivité et son efficacité. Les solutions cloud tirent le meilleur parti des caractéristiques du cloud, comme la mise en commun des ressources, son élasticité rapide et le service mesuré. Ce n'est pas tout : les solutions cloud sont conçues et mises en œuvre dans un esprit de sécurité, fournissant ainsi des mécanismes de cryptage adéquats pour protéger les données en transit et at rest. En intégrant des certifications appropriées, des fonctionnalités d'audit et des procédures transparentes, ces solutions permettent même de respecter certains aspects de la conformité.

Cas d'utilisation

Il est facile d'évoquer les avantages d'un système de transfert de fichiers géré en des termes théoriques. Pourtant, les témoignages pratiques ne manquent pas pour attester de l'efficacité du déploiement de GoAnywhere MFT dans le cloud. Voici trois cas d'utilisation particulièrement marquants.

Société pharmaceutique multinationale

L'équipe informatique d'une organisation pharmaceutique internationale devait, entre autres efforts importants, migrer ses services dans le cloud afin d'aboutir à un modèle davantage axé sur l'hybride.

Lors de nos premiers échanges, l'équipe nous a confié qu'elle devait mettre à jour une solution MFT truffée de processus obsolètes et ingérables qui, s'ils n'étaient pas corrigés, pouvaient constituer une menace de sécurité à court terme. L'équipe souhaitait également perfectionner son infrastructure cloud (un projet qui allait rester prioritaire au cours des 12 prochains mois).

Sa solution MFT actuelle était en fin de vie et de support, ce qui rendait difficile la mise à jour des tâches existantes. Parallèlement, le cloud souffrait d'un support limité, ce qui constituait un réel problème pour sa stratégie de migration de services supplémentaires dans le cloud. C'est pourquoi, plus tôt cette année, nous avons finalisé la mise en œuvre de GoAnywhere dans l'environnement de cloud privé de l'organisation.

Distributeur de gaz naturel

Lors de nos premiers échanges, l'entreprise avait sélectionné GoAnywhere MFT comme solution MFT pour la simple raison que nous proposions une offre cloud.

L'entreprise poursuivait un objectif en interne : maintenir le plus de services possible intégrés dans leurs workflows DevOps, exigeant dès lors que tout service déployé devait être compatible avec ses conteneurs ou son infrastructure AWS.

Notre offre de conteneurs était à l'époque relativement maigre, avec une connaissance insuffisante du marché britannique : c'est pourquoi nous avons décidé de déployer notre solution au sein d'AWS.

L'utilisation d'AWS a offert à l'entreprise de nombreux avantages, parmi lesquels l'automatisation d'une grande partie du déploiement avec les processus existants.

Distributeur de produits international

Cette organisation cherchait à réduire l'empreinte de son propre matériel et souhaitait adopter une approche SaaS à l'aide d'une plateforme MFTaaS.

L'organisation a su tirer parti des agents GoAnywhere pour adopter un modèle hybride en nouant un lien de confiance entre les infrastructures sur site et cloud, ce qui l'a aidée à compléter sa stratégie à long terme d'arrêt progressif des services sur site.

La sécurité faisant partie des enjeux majeurs de l'organisation, nous avons proposé une plateforme MFTaaS, notamment grâce à la certification Type 1 SOC-2 que nous avons obtenue.

Dans la plupart des démonstrations auprès de nos clients, le MFTaaS ou le déploiement dans leur cloud privé fait partie des solutions sérieusement envisagées.

Question 2 : les défis du cloud

Quelles sont les conséquences sur le transfert de fichiers géré dans le cadre du passage au cloud ? Quels secteurs d'activité devez-vous prendre en compte ?

Funso Richard | Chef de la sécurité informatique | LinkedIn
L'adoption d'une stratégie cloud exige une planification rigoureuse afin d'éviter toute interruption de l'activité. Idem lorsque les organisations envisagent de migrer le transfert de fichiers géré (MFT) dans le cloud. Une migration du MFT mal exécutée peut entraîner une perte ou une violation de données, des amendes, un surcoût financier considérable, un processus décisionnel inefficace en raison d'un accès aux données retardé, une perte de performance et de productivité, des perturbations logistiques ainsi qu'une expérience utilisateur négative. Pour éviter ces effets néfastes, la mise en place d'une stratégie bien étudiée est indispensable.

Migrer des données dans le cloud s'apparente davantage à une décision commerciale qu'à un processus informatique. La technologie sous-jacente est certes l'affaire du département informatique, mais on doit tenir compte des conséquences économiques avant de procéder à toute migration de données. Le besoin commercial est un facteur clé. Certes, les données sont le carburant de l'économie, mais les performances de l'entreprise dépendent de la qualité de ce même carburant. De la collecte des données jusqu'à leur stockage, en passant par leur protection, leur transmission, leur accès, leur gestion et leur destruction, l'objectif économique doit être pris en compte au moment de sélectionner une solution MFT et une stratégie de migration des données doit obligatoirement être mise en place. Il ne fait aucun doute que le MFT cloud offre de nombreux avantages dans un écosystème hautement mobile et interconnecté : évolutivité des données, mobilité, visibilité, interopérabilité et facilité d'utilisation. Toutefois, les coûts et les ressources qu'exige la mise en œuvre d'une telle solution ne sont pas à négliger. Pour les organisations fortement réglementées, les exigences de conformité jouent un rôle essentiel dans la migration des données dans le cloud. Afin de répondre aux préoccupations de conformité, les organisations doivent choisir des solutions MFT intégrant des contrôles de la conformité et de la sécurité.

Soulos Panagiotis | Responsable mondial de la sécurité informatique | LinkedIn
Il est important de prendre en compte certains éléments clés au moment de choisir une solution de transfert de fichiers géré. La sécurité des données at rest et en transit et la conformité sont en tête des priorités. En aucun cas, le déploiement d'une solution de fichiers gérée dans le cloud ne doit entraîner des irrégularités juridiques, réglementaires ou de conformité. Les performances du service doivent également être examinées. Interopérabilité et portabilité sont deux facteurs clés nécessaires à l'adoption de la solution cloud. Vous devez veiller à ce que la migration des services ait le plus faible impact opérationnel possible (voire zéro impact) sur l'organisation, y compris sur les canaux de communication actuellement ouverts avec les organisations collaboratrices et les clients. Les accords de niveau de service (SLA) doivent faire l'objet d'un examen minutieux, être inclus dans le contrat et couvrir tous les besoins commerciaux.

La formation des utilisateurs (utilisateurs professionnels ou employés informatiques) doit également être prise en compte afin de réduire le risque de défaillance opérationnelle due à un manque de compétences du personnel et pour que ces mêmes utilisateurs, puissent utiliser le service cloud au maximum de ses capacités.

Les utilisateurs professionnels du service, les équipes de sécurité informatique, les équipes chargées du risque opérationnel, les équipes de conformité et juridiques et les équipes des technologies de l'information doivent être impliqués de manière à ce que le service cloud couvre tous les besoins commerciaux.

Gary Hibberd | Consultant en sécurité | LinkedIn
Pour réussir le MFT, l'organisation doit comprendre les outils dont elle dispose ainsi que leur fonctionnement. Passé ce cap, une stratégie de déploiement du MFT doit être établie et communiquée partout dans l'entreprise : il est en effet très probable que tous les secteurs de l'entreprise doivent être pris en compte.

Il convient d'accorder la priorité aux secteurs d'activité qui transfèrent actuellement de grands volumes de données personnelles ou sensibles par e-mail ou FTP, car ce sont ces domaines qui en comprendront les avantages – ainsi que les contrôles employés. Une bonne solution MFT améliorera la sécurité, mais aussi la confidentialité des données.

En déployant le MFT, les organisations peuvent consolider et gérer leurs transferts de données à l'aide d'une plateforme contrôlée et surveillée de manière centralisée, ce qui leur permet de bénéficier d'une excellente visibilité sur les données transférées, mais aussi l'heure/la date et l'auteur du transfert. Ce dispositif de surveillance mis en place, les systèmes MFT contribuent à fournir des preuves qui peuvent être utilisées dans le cadre du processus d'audit interne.

Ray Sutton | Consultant technique | LinkedIn

Quand vous migrez des services dans le cloud, vous devez être conscient des enjeux en termes de risque, de sécurité et de performance. Si le système affiche de piètres performances ou des délais d'attente une fois la migration effectuée, cela risque de pousser vos clients et utilisateurs à ne pas utiliser le service. Pire, ces mêmes clients et utilisateurs risqueront de chercher d'autres moyens pour copier les fichiers. Cela pourrait potentiellement entraîner des problèmes de sécurité, voire la divulgation d'informations confidentielles. La migration vers des solutions cloud n'est pas un simple exercice « lift and shift », surtout lorsqu'on parle de données personnelles ou confidentielles. Récemment encore, nous avons assisté à des failles de sécurité qui auraient pu être évitées si les choses avaient été planifiées et les facteurs de risque étudiés.

Une bonne connaissance de vos données et l'identification des précautions de sécurité à mettre en place figurent parmi les priorités que vous devez vous fixer. Peu importe que vous migriez vers le cloud ou stockiez les données sur site : les règles sont les mêmes. De même, il est vital de mettre en place un cadre de sécurité pour les données et d'être en mesure de manipuler et de sécuriser ces mêmes données. Par exemple, recherchez une solution capable de crypter les données en transit et offrant la possibilité de crypter les données at rest. Envisagez de protéger ces données lorsqu'elles atteignent leur destination finale. Ce n'est pas tout : vous devez également regarder au-delà du bout de la chaîne, par exemple en appliquant un cycle de vie à vos données de façon à contrôler qui peut consulter, éditer, voire imprimer ces mêmes données.

Le cloud offre des possibilités infinies, mais il est essentiel de comprendre la nature même de vos données et la façon dont vous devez protéger cette précieuse ressource.

Questions-réponses : Michael Barford | Ingénieur solutions | LinkedIn

La migration vers le cloud n'est pas un projet à prendre à la légère. Divers facteurs exerceront une influence notable sur cet événement stratégique pour l'entreprise. Dans le cadre du principe de diligence raisonnable, vous devez vous poser les bonnes questions afin de trouver la solution la mieux adaptée à votre vision d'entreprise :

- **Où nos workflows les plus importants s'exécutent-ils, sur site ou dans le cloud ?**
  La réponse à cette question peut vous aider à déterminer l'emplacement idéal de la solution, MFT : dans le cloud, sur site ou dans un modèle hybride.
- **Avons-nous besoin d'une solution MFT « transparente », que les flux d'informations se trouvent sur site, dans le cloud ou dans un modèle hybride ?**
  Aujourd'hui, il est plus fréquent de voir les workflows automatisés combiner technologies traditionnelles (p. ex. le SFTP et le FTPS) et prestataires de services cloud courants. Vous voudrez probablement pouvoir créer des automatisations complexes tout en faisant abstraction de la pile technologique impliquée, de manière à pouvoir vous passer de ressources informatiques et à vous contenter de faibles niveaux de connaissances vis-à-vis de ces automatisations et technologies.
- **Adoptons-nous une infrastructure 100 % cloud ou exploiterons-nous un modèle opérationnel hybride à moyen/long terme ?**
  Dans l'écrasante majorité des entreprises, les cas d'utilisation mêleront infrastructures sur site et cloud. Dans de tels cas, la capacité à déployer le MFT lorsqu'on le désire (sur site/dans le cloud) et à laisser des agents automatiser les processus sur les systèmes à mesure qu'ils sont déployés, peut constituer une capacité essentielle. Les solutions MFT avec agents permettront d'automatiser les workflows impliquant des systèmes sur site, dans le cloud, voire dans des réseaux de clients/partenaires, le tout de manière transparente. Cette stratégie permet une migration sans heurts dans le cloud (et cette migration ne se déroule pas en un seul jour).
- **Avons-nous besoin d'une solution MFT en tant que service cloud, ou devons-nous exploiter une telle solution, nous-mêmes ?**
  Si vous décidez d'exploiter vous-même la solution, il serait sage d'évaluer si la solution s'intègre dans votre stratégie de déploiement existante (en d'autres termes, si elle peut être déployée dans des conteneurs/dockers, est évolutive, offre un équilibrage des charges, etc.).
- **Quels types de données allons-nous traiter ?**
  Vérifiez que les transferts d'informations s'exécutent avec les niveaux de sécurité/conformité appropriés. Dans le cloud, cet exercice peut se révéler plus compliqué : aussi, vous devrez peut-être recourir à des prestataires proposant des certifications, des fonctionnalités comme le cryptage des données at rest, ou bien d'autres caractéristiques adaptées aux besoins de votre entreprise.

Bonnes et mauvaises pratiques

Comme c'est le cas pour toutes les initiatives de sécurité, vous pouvez parfaitement respecter les règles de conformité sans pour autant offrir une sécurité adéquate. Il est parfois aisé de respecter une liste de vérification de la conformité, tout en laissant l'organisation à la merci des menaces. Pour vous aider à prendre les mesures qui s'imposent, nos experts vous prodiguent des conseils, vous indiquant les pièges à éviter et les objectifs à atteindre

✗ MAUVAISES PRATIQUES : Christos Syngelakis | Chef de la sécurité informatique | LinkedIn

Les défis sont nombreux au moment d'aborder la question des transferts de fichiers sécurisés. Les difficultés ne résident pas tant au niveau de l'organisation elle-même, mais dans les activités que celle-ci doit mener en dehors de son environnement. Exemple : un site médical qui doit transférer des fichiers volumineux à des patients, ou une agence marketing qui doit communiquer des fichiers à des tierces parties.

Bon nombre d'entreprises ne disposent pas d'équipe informatique dédiée ou de spécialistes pour les opérations de ce type. Dans bien des cas, le destinataire dispose simplement d'un compte public pour le transfert par e-mail – et de rien d'autre. Les outils d'entreprise mis à votre disposition pour gérer ce type de transaction et respectueux de vos règles organisationnelles ne coïncident guère avec ce scénario.

Parfois, vous avez la possibilité de créer un compte afin que le destinataire puisse accéder aux produits de sécurité que vous utilisez, mais ces outils de communication improvisés s'avèrent généralement très coûteux sur le plan humain, mais aussi des licences pour ce type d'activité. Les gros outils collaboratifs d'entreprise peuvent prendre en charge les transferts de fichier interentreprises, car il s'agit de mécanismes éprouvés entre les deux parties, même si leur capacité à la demande peut s'avérer fortement problématique.

Les niveaux de pouvoir inégaux entre les entreprises peuvent représenter une autre difficulté. Par exemple, lorsque l'autre partie est une administration publique qui souhaite transférer des données, elle pourra insister pour déplacer des données sensibles alors même qu'elle ne dispose pas d'une méthode sécurisée de communication pour toutes ces données. Vous pouvez rencontrer des difficultés avec les limitations de temps, alors même que les chefs d'entreprise voudront que les informations leur soient transférées sans délai. L'utilisateur utilisera n'importe quel logiciel accessible au public pour accomplir la tâche.

Il y a un besoin urgent de solution à la fois facile à déployer et à utiliser, sans que l'utilisateur ni l'autre partie n'ait à faire quoi que ce soit. Des solutions existent, mais celles-ci s'avèrent coûteuses et ne sont pas faciles à gérer. Il existe une grande variété de documents renfermant des informations, et vous ne souhaitez pas que tous ces documents soient à la disposition de tous.

✓ BONNES PRATIQUES : Chris Hodgson | Directeur du développement de l'activité | LinkedIn

Il existe de nombreux protocoles et méthodes de transfert de données avec les clients et les partenaires commerciaux, chacun offrant son lot d'avantages et d'inconvénients. Cette diversité de méthodes de partage de données peut prêter à confusion, et il peut être difficile de devoir gérer ces méthodes tout en garantissant leur conformité. Les produits comme GoAnywhere fournissent une solution de transfert de fichiers sécurisé capable de déplacer les données entre deux terminaux quelconques, que ce soit dans une configuration sur site, cloud ou hybride. GoAnywhere fournit aux utilisateurs et aux administrateurs un cadre de sécurité basé sur les rôles pour la connexion et l'accès au système, via une authentification à deux facteurs, ainsi que le cryptage de l'ensemble des fichiers et des données en transit et at rest. Les entreprises automatisent et rationalisent ainsi plus facilement leurs échanges de données sensibles tout en garantissant le respect des normes industrielles.

Le passage au cloud encourage généralement l'adoption d'une solution de transfert de fichiers sécurisé. Les plateformes cloud fournissent d'excellents outils pour déplacer les données dans leur propre environnement, mais ne permettent pas de transmettre des données entre différents clients cloud. Les solutions comme GoAnywhere peuvent simplifier l'échange de données entre des plateformes cloud hétérogènes, le tout via une interface utilisateur centralisée. Les équipes financières doivent prendre en considération les avantages des transferts de fichier sécurisés au moment de migrer vers de nouveaux systèmes ERP cloud, et ont besoin d'une méthode sûre d'intégration des fichiers et des données avec les systèmes aval ou les partenaires commerciaux.

Conclusion

Le transfert de fichiers est un sujet vaste. Nous disposons d'une infinité de méthodes pour le transfert de données, et il est très difficile de garder un œil attentif sur ces méthodes. Terminés, le FTP (File Transfer Protocol) et le SFTP (Secure File Transfer Protocol) : nous avons adopté de nouvelles méthodes et de nouveaux produits, et tous les fournisseurs sont basés sur le cloud. Cette situation a contribué à créer un monde hétérogène. Certaines organisations ont recours à de vieilles tactiques (comme le SFTP), d'autres ont recours à des API qui reçoivent et envoient continuellement des données auprès de différents tiers et solutions cloud/SaaS. En raison de la grande complexité de toutes ces facettes et des différentes façons de travailler, aucune solution n'est bonne pour tout le monde. Le maintien d'une approche cohérente est un énorme défi, chaque organisation ayant sa propre façon de faire les choses selon ce qu'elle considère juste.

Ensuite, il est vital de pouvoir vérifier l'intégrité des fichiers transmis. Des solutions performantes de validation des fichiers sont disponibles sur le marché. Si vous ingérez de grandes quantités de données et prélevez beaucoup de données à partir des différents services Web que vous proposez, vous pouvez les analyser avant de les transférer à l'aide d'un outil d'analyse en ligne.

Le transfert ne se résume pas toujours à déplacer un fichier d'un point A à un point B : vous devez garantir la sécurité à chaque étape de la transaction. Si le PDG vous demande d'envoyer les fiches budgétaires à un autre emplacement, vous n'enverrez pas ces données par e-mail. Certains outils performants vous permettent de rendre vos fichiers « top secret » et de les protéger.
(Goher Mohammad | Responsable de la sécurité des informations | LinkedIn)

« Le transfert de fichiers est une opération complexe, qu'elle s'exécute dans le cloud, sur site ou selon un modèle hybride. Appliquez-vous des restrictions en fonction de l'extension, ou recherchez-vous la présence de logiciels malveillants dans toutes les données entrantes afin de garantir l'intégrité de vos données, parmi d'autres composants ? En plus d'appliquer un ensemble de contrôles de sécurité, il est vital d'utiliser des modèles réutilisables afin de proposer un modèle de mise en œuvre homogène dans tous vos projets et initiatives où des solutions de transfert de fichiers s'avèrent nécessaires. Que ce soit dans le cadre d'une solution SFTP traditionnelle, d'une suite SDK ou API d'un fournisseur ou d'un bucket S3 doté de stricts contrôles d'accès, il n'existe aucune fonction de migration simple à mettre en œuvre. La classification de ces données (où qu'elles se trouvent) et les contrôles de sécurité qu'implique cette mise en œuvre sont tout aussi importants. »
(Lidia Guiliano | Professionnelle de la sécurité informatique | LinkedIn)

Que votre organisation entame tout juste son parcours vers le cloud ou que sa présence dans le cloud soit déjà solidement établie, la sécurité doit constituer l'une de ses préoccupations premières. La sécurité ne consiste pas à s'assurer simplement que vos données ne sont pas divulguées sur Internet. Les données ne sont pas une entrée statique et ne sont pas confinées à un seul emplacement : elles doivent pouvoir se déplacer pour que votre entreprise fonctionne. L'importance d'une solution de transfert de fichiers géré ne saurait être sous-estimée. Nos experts vous ont présenté des idées inspirantes pour aider votre entreprise à se développer et à grandir dans le cloud en toute sécurité.

Pour en savoir plus sur la façon dont vous pouvez contrôler la sécurité de vos transferts de fichiers, contactez-nous en cliquant ici.

FORTRA

Fortra.com/fr

À propos de Fortra

Fortra est un fournisseur de logiciels de cybersécurité unique sur le marché. Nous créons un avenir plus simple et plus sûr pour nos clients. La fiabilité de nos experts et notre portefeuille de solutions évolutives et intégrées, offrent aux entreprises à travers le monde, maîtrise et équilibre. Nous sommes les artisans du changement positif et votre allié pour vous garantir la tranquillité d'esprit à chaque étape de votre parcours en matière de cybersécurité. Pour en savoir plus, rendez-vous sur fortra.com/fr.

© Fortra, LLC et son groupe d'entreprises. Toutes les marques commerciales et marques déposées sont la propriété de leurs détenteurs respectifs.