Guide du cloud hybrid

Le cloud en chiffre

Le marché mondial du MFT est en pleine expansion. En 2023, il était évalué à 2,5 milliards de dollars et devrait atteindre 4,52 milliards de dollars d'ici 2029, avec un taux de croissance annuel moyen de 10,2 % selon Globenewsire.

Cette dynamique est alimentée par plusieurs facteurs comme :

- L'augmentation des exigences en matière de sécurité des données et de conformité réglementaire liée à l'informatique telle que : le règlement général sur la protection des données (RGPD) en 2018, le Data Governance Act (DGA) adopté en 2023, le Digital Services Act (DSA) entré en vigueur en 2024, DORA (Digital Operational Resilience Act) apparu en 2024/2025, la réforme de la facturation électronique prévue pour 2026, etc. Ces réglementations instaurent de nouvelles mesures à adopter par les entreprises, sous peine d'amendes, afin de sécuriser, protéger et centraliser les données.

- La croissance du cloud et des environnements informatiques hybrides. Selon Gminsights, le MFT On-Premise représentait 64% des parts de marché en 2024.
  La possibilité de traiter de grandes quantités de données tout en dépensant peu pour le développement de l'infrastructure stimule l'utilisation du cloud. Les méthodes hybrides ont le vent en poupe, car elles intègrent un niveau acceptable de sécurité et de flexibilité. Cela permet un accès à distance tout en étant gérées sur place.

”

Décider de passer au cloud, c'est comme décider de l'achat d'un logiciel ou d'un matériel. Il est donc important de prendre en compte les besoins de votre organisation lorsque vous planifiez votre passage à un environnement de cloud hybride.

Par exemple, allez-vous stocker des informations sensibles dans le cloud ?

Si c'est le cas, dressez une liste des caractéristiques de sécurité dont vous avez besoin et passez-la en revue pour chaque fournisseur de services en ligne et chaque solution que vous évaluez.

Plongeons ensemble dans le vif du sujet !

“

Le cloud hybrid

Selon la norme ISO 17788, le cloud hybride est un modèle de déploiement qui utilise deux modèles différents liés par une technologie appropriée qui permet l'interopérabilité, la portabilité des données et des applications. Un cloud hybride peut être détenu et exploité par une entreprise ou par un tiers, c'est-à-dire qu'il peut exister dans les locaux de l'organisation ou en dehors.

Les scénarios suivants décrivent trois façons dont un environnement de cloud hybride pourrait prendre forme :

Une entreprise manufacturière a besoin d'échanger des fichiers avec des partenaires commerciaux dans le cloud. Elle conserve tout sur site, à l'exception de sa solution de transfert de fichiers sécurisé qu'elle exploite sur une instance au sein de la plateforme informatique cloud qu'elle a choisie pour faciliter la connectivité avec ses partenaires commerciaux.

Une université transfère plusieurs processus de données, notamment le matériel pédagogique et les horaires de cours, vers un cloud privé. Cependant, les données sensibles des étudiants restent sur un serveur interne sécurisé afin d'aider l'université à rester en conformité avec réglementations en vigueur.

Une entreprise IT souhaite réduire la quantité de matériel dans sa salle serveurs. Elle installe donc une machine virtuelle sur Amazon Web Services, puis transpose ses transferts de fichiers vers un ensemble de plateformes en cloud privées et publiques. Les intégrations dans le cloud sont ensuite utilisées pour automatiser les processus entre les serveurs sur site et le cloud. Par exemple, les données utilisateurs mises à jour sont transférées vers des services web tels que SharePoint ou Microsoft CRM.

Le cloud hybride

Quand l’utiliser ?

Vous commencez avec le cloud

Le passage à un cloud hybride peut être une bonne solution intermédiaire si vous n'avez pas encore décidé si un environnement entièrement dans le cloud est approprié pour votre entreprise. Il est aussi, sans doute, plus facile de revenir à un environnement sur site à partir d’un cloud hybride qu'à partir d’un cloud complet, car il y a moins d'éléments en jeu.

Vous souhaitez maintenir la continuité de votre activité

Le cloud hybride est une bonne option si vous cherchez à conserver des sauvegardes sécurisées de données sensibles dans un endroit moins susceptible d'être touché par des pannes de courant ou d'autres causes d'indisponibilité des serveurs. La plupart des plateformes cloud exploitent des serveurs distants dans plusieurs régions, de sorte que même si un site tombe en panne, votre organisation peut être rassurée en sachant que vos données sont disponibles et en sécurité ailleurs dans le monde.

Vous travaillez avec des partenaires commerciaux qui ont migré dans le cloud

L'utilisation d’un cloud hybride vous permet de travailler avec des partenaires commerciaux et d'échanger des données en toute sécurité entre votre environnement sur site et leurs dossiers cloud. Vous bénéficierez de tous les avantages de la simplification et de l'automatisation de vos transferts de fichiers et d'autres processus.

Le cloud et la cybersécurité

Si vous envisagez de stocker des données client ou professionnelles dans le cloud, y compris des numéros de carte de crédit, des adresses physiques, des dates de naissance, la propriété intellectuelle, des données d'employés, des dossiers médicaux, des identifiants personnels ou même des sauvegardes de code logiciel, vous devez vous assurer que vous nous suivons les meilleures pratiques de sécurité cloud bien avant de passer à un cloud hybride.

Voici quelques conseils de cybersécurité à garder à l'esprit :

Maintenez une politique stricte de conservation et de suppression des données client.

Certaines organisations ont besoin de stocker des informations indéfiniment. Cela s'applique au secteur de la santé, par exemple, la conservation des données des patients sur une période de plusieurs décennies aide les praticiens à fournir aux patients des soins de haute qualité. Mais pour ceux qui ne sont pas dans le domaine de la santé, il est utile de savoir quelles lois sur la conservation des données s'appliquent à vous et quand vous devez conserver, voire supprimer, des informations sensibles.

Grâce à ces connaissances, vous saurez exactement combien de temps les données doivent être conservées dans le cloud et comment vous en débarrasser en toute sécurité une fois la période de conservation terminée.

Effectuez les audits de sécurité frequents pour votre environnement de cloud hybride.

Entreprendre un audit peut ne pas sembler être une promenade de santé. Mais les avantages de le faire fréquemment l'emportent largement sur les inconvénients temporaires pour les ressources d'une organisation.

Non seulement vous pouvez prendre une longueur d'avance en repérant les problèmes avant qu'ils ne surviennent, mais vous pouvez également examiner vos fournisseurs tiers et vos intégrations cloud pour vous assurer que l'intégrité de vos données est préservée des deux côtés.

Protégez vos données avec des outils de sécurité spécifiques au cloud.

Les organisations s'appuient fortement sur les applications cloud. Pour assurer la sécurité de vos données, nous vous recommandons de les protéger avec des outils dans ces quatre catégories : les protection DDoS, courtier de sécurité d'accès au cloud, la prévention contre la perte de données et les sauvegardes dans le cloud.

Le chiffrement n’est pas négociable.

Avec l'augmentation inquiétante des violations de données au fil des ans, il n'a jamais été aussi crucial pour les organisations de s'assurer que leurs informations sont correctement sécurisées.

Vos données sont-elles chiffrées en transit vers et depuis les systèmes internes ? La plupart des entreprises répondent par l'affirmative , cependant, le chiffrement dit secondaire , c’est-à-dire protéger les données au repos avec un chiffrement OpenPGP ou AES - est moins souvent appliquée. Les méthodes de chiffrement intégral du disque (ou l'équivalent) sont facilement disponibles dans les environnements en cloud les plus répandus.

La sécurisation des données en transit et au repos est indispensable et devrait figurer sur votre liste des priorités bien avant que les données ne soient stockées dans le cloud.

Automatisation du cloud

L'automatisation est un sujet brûlant pour les professionnels de l'informatique. Elle permet de réduire les tâches manuelles, les erreurs des utilisateurs, de rationaliser et simplifier les processus d'entreprise complexes et d'éliminer les répétitions afin que les employés puissent se concentrer sur d'autres domaines de l'entreprise.

L'automatisation des transferts de fichiers est particulièrement important pour les entreprises qui souhaitent migrer vers le cloud. Cette automatisation s'aligne sur les stratégies de réduction des coûts en éliminant le besoin de plusieurs outils de transferts de fichiers distincts, en remplaçant les processus manuels et en vous donnant plus de contrôle sur le mouvement des données et les connexions avec les partenaires commerciaux.

Comment ça marche ?

Une solution robuste et sécurisée de transferts de fichiers dans le cloud permet aux professionnels de l'informatique, tels que les administrateurs système, les ingénieurs réseau et les programmeurs, de créer des flux de travail de transferts de fichiers.

Ces projets peuvent être facilement configurés pour déplacer et traiter des fichiers dans le cloud, entre environnements et au sein de réseaux privés. Certaines tâches peuvent être automatisées (par exemple, déplacer un fichier d'un dossier à un autre) ou, si vous le préférez, l'ensemble du processus, y compris le chiffrement, peut être automatisé de bout en bout.

Avec des centaines de tâches, de ressources et de déclencheurs au choix, l'automatisation des transferts de fichiers est flexible, simple et puissante. Associés à un planificateur intégré, les flux de travail peuvent être programmés pour s'exécuter à tout moment et les fichiers peuvent être contrôlés dans des dossiers sur des systèmes internes ou basés sur le cloud.

En cas d'échec d'un flux de travail, vous avez la possibilité d'être alerté immédiatement par courrier électronique ou par SMS.

Ainsi, si vous avez une pléthore de processus à gérer, y compris des intégrations web et des transferts de fichiers, l'automatisation dans le cloud devrait être prise en considération lors de la conception de votre nouvel environnement.

Les données stockées dans le cloud doivent respecter les exigences de conformité qui s'appliquent à votre organisation. Les données relatives aux cartes de crédit doivent être traitées et transmises dans le cloud conformément aux directives de la norme PCI DSS. Les informations médicales doivent être sécurisées conformément aux normes HIPAA et HITECH.

Et si vous traitez les données personnelles de citoyens européens (que votre organisation soit située en Europe ou non), vos données cloud doivent respecter les dispositions du RGPD. Les organisations qui ne respectent pas les réglementations, normes ou lois applicables s'exposent à de lourdes amendes et pénalités.

Le marché du cloud

Le marché du cloud d'aujourd'hui offre aux organisations de nombreuses options parmi lesquelles choisir. Les concurrents les plus importants et les plus populaires pour le cloud sont Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud et Oracle Cloud, mais il en existe d'autres qui fournissent un accès public et/ou privé à vos données.

L'option que vous choisirez dépendra de la taille de votre organisation, de votre budget, des exigences de votre entreprise et des normes de sécurité des données auxquelles vous devez vous conformer. Il existe également plusieurs types de « modèles de service » à évaluer. Chaque modèle est livré avec différents services qui sont gérés directement par le fournisseur de services cloud.

Infrastructure en tant que service (IaaS)

Le modèle de service IaaS offre aux organisations un endroit pour installer et exécuter des logiciels prenant en charge le cloud à 100 % dans un environnement hybride ou cloud. Dans ce modèle, le fournisseur de services cloud s'occupe de la gestion de l'infrastructure, tandis que le client est responsable de l'exécution, de la gestion et de la maintenance de tous les systèmes d'exploitation, bases de données ou applications déployés.

Plateforme en tant que service (PaaS)

Le modèle de service PaaS est une option solide pour les développeurs qui souhaitent créer des applications sans acheter le matériel, les logiciels et les autres services nécessaires pour le faire. Avec PaaS, le fournisseur de services cloud héberge des ressources, notamment un système d'exploitation, un serveur, un kit d'outils de programmation, etc. Beaucoup offrent également un espace de stockage, afin que les développeurs d'applications puissent créer, tester, stocker et exécuter leurs créations entièrement dans le cloud.

Plateforme d'intégration en tant que service (iPaaS)

Le modèle de service iPaaS aide le service informatique à intégrer des applications logicielles déployées dans différents environnements. Pour les organisations qui utilisent une approche multi-cloud pour un environnement hybride, l'iPaaS peut maintenir les logiciels et les services connectés entre plusieurs emplacements sur site et dans le cloud.

Logiciel en tant que service (SaaS)

Le modèle de service SaaS permet aux professionnels de l'informatique d'utiliser les logiciels et bases de données intégrés fournis par la plate-forme de cloud computing. Il s'agit d'une approche très pratique des logiciels ; le fournisseur télécharge et héberge le logiciel dans le cloud et fournit également une infrastructure, ce qui réduit la quantité globale de gestion, d'assistance et de maintenance nécessaire pour exécuter le logiciel.

Commencer avec le cloud

À ce stade, vous êtes peut-être prêt à déployer certains de vos processus sur un cloud hybride.

Si vous ne savez pas par où commencer, nous vous suggérons de contacter le fournisseur de services cloud de votre choix. Expliquez votre situation et voyez ce qu'ils suggéreraient. Tous les éditeurs de logiciels que vous utilisez et que vous souhaitez migrer vers le cloud peuvent également vous aider. Ils peuvent avoir de la documentation sur le cloud, des directives ou des bonnes pratiques à partager avec vous.

Voici quelques éléments restants à prendre en compte lors de la migration vers un cloud hybride :

Souhaitez-vous migrer uniquement certains services dans le cloud ou envisagez-vous d'effectuer une transition complète à terme ?

- Si vous avez des applications héritées qui doivent rester sur site, continueront-elles à être interopérables avec les applications que vous exécutez dans le cloud ? Si non, que comptez-vous en faire ?
- Où voulez-vous que vos applications cloud s'installent ? Qui devrait avoir accès à vos données cloud ?
- Remarque : Assurez-vous que les autorisations de base de données et de dossier sont correctement configurées !

Commencer avec le cloud

Sécurisez vos données Cloud hybride

Quel que soit l'emplacement de stockage et quand bien même vos bases de données et vos dossiers sont chiffrés, vous devez toujours vous assurer de chiffrer également vos informations au niveau du fichier. Cela garantit la protection des données internes et externes à chaque couche, réduisant ainsi le risque global de vulnérabilités ou de violations de données.

Si vous utilisez le cloud pour stocker des données, il est inévitable que de nombreuses parties aient accès à ces informations, y compris des partenaires commerciaux, des fournisseurs tiers et des parties prenantes clés.

Cela peut être avantageux : le stockage dans le cloud permet à ces parties de se connecter et de récupérer les informations dont elles ont besoin de n'importe où, sans se limiter aux emplacements physiques ou aux réseaux internes. Toutes les solutions cloud offrent des exigences d'authentification de base et des contrôles de sécurité. Vous pouvez également utiliser une solution de transferts de fichiers sécurisée capable de chiffrer vos informations en transit et au repos, quel que soit leur emplacement.

Le cloud & les transferts de fichiers

Lorsque le cloud hybride est associé à une solution de transferts de fichiers sécurisée, les organisations peuvent déployer leurs processus de transferts dans divers environnements hybrides. Cela permet à l'entreprise de conserver une partie de ses ressources sur site et d'exécuter le reste via un fournisseur de services cloud comme Amazon Web Services ou Microsoft Azure.

La bonne solution de transferts de fichiers doit fournir des protocoles de transfert et de chiffrement de fichiers populaires pris en charge dans un environnement de cloud hybride. Ces protocoles incluent SFTP, FTPS, SCP, AS2 et HTTPS, ainsi que OpenPGP, ZIP avec chiffrement AES et les chiffrements validés FIPS 140-2 pour protéger les informations confidentielles et les données sensibles. Grâce à cette fonctionnalité sécurisée, les fichiers partagés avec les partenaires commerciaux du cloud seront protégés par une connexion sécurisée et les données stockées dans le cloud seront chiffrées au repos.

Le MFT (transferts de fichiers gérés) est une solution sécurisée qui automatise les transferts de fichiers, chiffre les données et rationalise le développement des processus à l'aide d'une approche centralisée. Le logiciel MFT peut déplacer et protéger les fichiers qui résident sur site, dans le cloud public/privé ou dans un environnement hybride, ce qui facilite la mise à l'échelle ou la migration vers différents environnements. Il offre la sécurité et le contrôle dont vous avez besoin pour transmettre et stocker des données en toute sécurité entre les systèmes, les sites, les utilisateurs et les partenaires commerciaux.

La plupart des solutions MFT du marché sont des offres tout-en-un, ce qui signifie qu'elles incluent tout ce dont vous avez besoin pour vos transferts, éliminant ainsi le besoin de solutions logicielles gratuites non sécurisées ou de scripts manuels.

Les logiciels MFT sont généralement dotés d'automatisation, de contrôles de sécurité, de partage sécurisé des e-mails, intégrations cloud et Web, audit et reporting avancés, et possibilité d'améliorer la position de conformité globale de votre organisation.

Lorsque vous implémentez une solution de transferts de fichiers, vous devez déterminer comment et où est-ce que vous souhaitez qu'elle fonctionne.

Tout d'abord, il est généralement facile de configurer une instance MFT dans le cloud. L'installation est rapide et il n'est pas nécessaire de configurer une solution tierce, tout devrait être inclus pour vous.

Après avoir exécuté un assistant d'installation rapide, il vous suffira de configurer vos comptes de partenaires commerciaux et les processus de transferts de fichiers. En ce qui concerne la mise en œuvre, il existe quelques directions que vous pouvez suivre dans un environnement de cloud hybride :

Certains fournisseurs MFT proposent leur solution dans le cadre du marché de la plateforme cloud de votre choix.

Par exemple, Amazon Web Services et Microsoft Azure permettent tous deux aux organisations de télécharger et d'exécuter une instance du logiciel du fournisseur dans leur environnement cloud. Cette approche réduit la nécessité d'utiliser des serveurs, des outils hérités ou d'autres processus sur site.

Une solution MFT cloud complète peut également vous aider à vous conformer aux audits de conformité, aux politiques internes et aux exigences de l'entreprise.

Le cloud & les transferts de fichiers

Vous pouvez choisir de conserver votre solution MFT implémentée sur site, mais d'exécuter une solution de proxy inverse et direct (passerelle DMZ) dans le cloud. Cette solution peut pointer vers des serveurs sur site et aider à assurer la sécurité des services de partage de fichiers dans votre réseau privé lors de l'échange de données avec des partenaires commerciaux dans le cloud. Une passerelle DMZ ne nécessitera pas non plus de ports entrants sur votre réseau et établira des connexions à des systèmes externes pour le compte d'utilisateurs locaux.

Si vous avez décidé de conserver votre solution MFT à 100 % dans un environnement sur site, vous pouvez toujours en intégrer certaines parties dans le cloud. Par exemple, vous pouvez vous connecter uniquement à des dossiers spécifiques dans le cloud. Votre solution établirait ensuite des connexions via des protocoles de transferts de fichiers sécurisés (SFTP, FTPS, HTTPS ou AS2) vers le cloud afin que les fichiers puissent être échangés et récupérés avec des partenaires commerciaux. Les systèmes de fichiers basés sur le cloud, comme Amazon S3, peuvent également être utilisés dans cette instance. Votre solution MFT extraira alors automatiquement les fichiers partagés de ce compartiment dans votre réseau privé.

GoAnywhere MFT

GoAnywhere MFT *est une solution de Managed File Transfer développée par Fortra qui automatise et sécurise les transferts de fichiers en utilisant une approche centralisée au niveau de l'entreprise.*

L'intégration de GoAnywhere dans votre organisation et dans un environnement cloud hybride vous permettra d'économiser du temps et de l'argent, d'améliorer la sécurité, de simplifier les transferts de fichiers et de vous aider à répondre aux exigences de conformité.

La protection des données sensibles est d'une importance capitale dans l'environnement actuel. GoAnywhere fournit une méthode sûre et sécurisée pour transférer automatiquement des informations à l'intérieur et à l'extérieur de votre entreprise. Les transferts de fichiers et les processus d'entreprise connexes seront rationalisés avec GoAnywhere sans que votre équipe n'ait besoin de connaissances préalables en programmation ou en écriture de scripts.

GoAnywhere MFT est flexible, évolutif, hautement disponible et offre des mises à niveau rapides et contrôlables. L'exploitation de GoAnywhere dans un environnement cloud hybride peut aider votre entreprise à réduire les coûts et à protéger les données clés de l'entreprise en cas de panne imprévue ou de sinistre.

BlueFinch ESBD

Contact

Rijswijk – Neufchâteau – Annecy – Paris

France: +33 (0)9 70 75 61 13

Netherlands: +31 (0)8 82 58 33 46

sales@bluefinch-esbd.com

www. bluefinch-esbd.com

Follow us

Prendre rendez-vous