



SAUVEGARDE DANS LE CLOUD :

Guide d'évaluation et liste de contrôle détaillés d'une **sauvegarde à la demande (BaaS)**

Renforcez l'agilité des données, l'efficacité opérationnelle et la cyber-résilience.



Table des matières

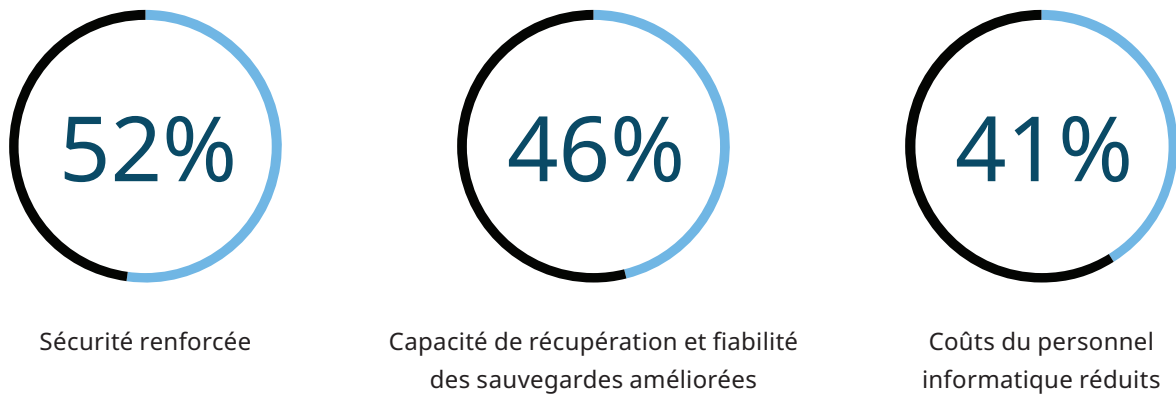
- La sauvegarde à l'ère du cloud.....2**
- Renforcer la protection des données et la liberté opérationnelle4**
- Renforcer la sécurité et la préparation aux ransomwares.....6**
- Bénéficier d'une consommation et de coûts plus flexibles, favoriser le développement durable.....8**
- Liste de contrôle : offres BaaS..... 10**
- Utiliser le BaaS..... 12**

La sauvegarde à l'ère du cloud

Ces dernières années, la modernisation de l'informatique portée par le cloud computing a conduit à une innovation et à une croissance rapides. Les infrastructures informatiques critiques n'ont cependant pas toutes été mises à niveau de manière cohérente ou au même rythme lorsque les entreprises sont passées sur le cloud, ce qui a créé des inefficacités et des cyber-vulnérabilités inacceptables.

Le passage, souvent négligé, à une infrastructure de sauvegarde moderne dans le cloud (au-delà de ce que proposent les fournisseurs de SaaS) peut rendre votre entreprise aussi agile que si vous exécutiez vos applications modernes dans le cloud. La sauvegarde à la demande (BaaS) est en effet un élément fondamental de la continuité de l'activité qui consolide les silos de sauvegarde hérités, créés avant le cloud, tout en améliorant et en renforçant votre expérience, vos opérations et vos coûts liés au cloud. Le BaaS vous permet par ailleurs de maximiser plus efficacement le potentiel de l'ensemble de vos données pour obtenir des informations commerciales et assurer la cyber-résilience de votre entreprise.

Les principaux avantages des services de protection des données basés sur le cloud



Source : [Enterprise Strategy Group](#). « L'évolution des stratégies de protection des données dans le cloud » (en anglais), 2021.

Allez plus loin dans votre transition vers le cloud

Lorsque vous évaluez les offres BaaS, vous devez savoir quelles capacités disponibles prendre en compte, notamment comment vos données seront protégées et comment votre entreprise sera facturée. Ce guide présente les principaux critères d'évaluation et fournit une liste de contrôle pour vous aider dans votre transition vers le cloud.

Avant de comparer les solutions de sauvegarde dans le cloud, vous devez comprendre comment une offre prend en charge ces capacités BaaS essentielles :

1. Renforcer la protection des données et la liberté opérationnelle
2. Renforcer la sécurité et la préparation aux ransomwares
3. Bénéficier d'une consommation et de coûts plus flexibles avec le développement durable

Évaluation des défis actuels

Avant que vous n'évaluiez une offre de sauvegarde dans le cloud, clarifions les principales différences entre un environnement de sauvegarde et de récupération géré en local par votre entreprise (alias auto-géré), et un environnement hébergé dans le cloud géré par un fournisseur de sauvegarde. Le tableau 1 présente 10 défis courants en matière de sauvegarde et de récupération avec des solutions auto-gérées uniquement en local.

10 défis courants en matière de sauvegarde et de récupération avec des solutions auto-gérées uniquement en local

- 1 L'achat d'une infrastructure en silos (par ex. serveurs distincts, cibles de stockage dédiées, etc) est coûteux, ce qui augmente le CapEx
- 2 L'absence de prise en charge de la protection des applications modernes, natives du cloud et SaaS, désavantage l'entreprise par rapport à la concurrence.
- 3 La gestion complexe de la configuration des flux de sauvegarde via plusieurs interfaces utilisateurs fragmentées pour différentes sources de données renforce la frustration du service informatique
- 4 Les passerelles cloud supplémentaires requises pour migrer les données sur site et dans différents clouds publics créent de la complexité
- 5 Les mises à niveau massives et les mises à jour perturbatrices nécessitent de planifier des temps d'arrêt
- 6 Les restaurations lentes qui entraînent le dépassement de l'objectif de délai de récupération (RTO) et/ou les restaurations du dernier point dans le temps uniquement ont un impact négatif sur les objectifs de point de récupération (RPO)
- 7 La déduplication par blocs variables et/ou fixes avec compression augmente les coûts
- 8 Le manque de capacités de protection contre les ransomwares ajoute un risque pour l'entreprise
- 9 L'impossibilité de réutiliser les données fragmentées empêche d'avoir une vision claire des connaissances
- 10 La lenteur du déploiement des capacités modernes freine l'innovation

Tableau 1 : évaluation des environnements de sauvegarde et de récupération locaux auto-gérés

Une entreprise numérique évolue rapidement. Une sauvegarde dans le cloud vous permet de suivre et d'accélérer votre transition vers le cloud et votre transformation numérique.

1 Renforcer la protection des données et la liberté opérationnelle

Les exigences métier et réglementaires relatives aux types d'informations que votre entreprise doit sauvegarder (et leur durée de rétention) changent. Il vous faut une solution de sauvegarde dans le cloud complète, capable de s'adapter rapidement lorsque c'est nécessaire. Si vous n'avez aucun moyen cohérent de prendre en charge les stratégies de rétention et les accords de niveau de service (SLA) pour toutes les applications natives du cloud, de logiciel à la demande (SaaS) et locales, comment pouvez-vous garantir que l'ensemble de vos données sont protégées et que votre personnel informatique, déjà très sollicité, n'est pas surchargé ?

Une sauvegarde dans le cloud peut être bien plus précieuse pour votre entreprise qu'une police d'assurance. Choisissez une offre BaaS dotée des cinq fonctionnalités opérationnelles clés suivantes pour que votre source de données bénéficie de la protection la plus avancée et que vous puissiez être libre au niveau opérationnel :



Prise en charge de vastes sources de données

Les sauvegardes devraient être simples. Aujourd'hui, il est pourtant difficile de gérer la sauvegarde de toutes les données stratégiques des applications de votre environnement, car il existe plusieurs plateformes, services et API dans le cloud, avec des stratégies, des accords de niveau de service et des périodes de rétention différents. Cela crée de la complexité. Pour une simplicité optimale, il faut une solution BaaS unique, capable de prendre en charge un large éventail de charges de travail dans plusieurs environnements et clouds, c'est-à-dire un service qui consolide et protège les charges de travail dans le cloud comme Amazon EC2 et RDS ainsi que les applications SaaS (comme M365) avec un seul service unifié, qui dépasse largement les protections intégrées des fournisseurs de clouds.

Une solution BaaS moderne vous permet d'éliminer les silos de sauvegarde hérités et de mettre en œuvre une protection de classe entreprise complète et cohérente, pour un large éventail de sources de données. Celles-ci comprennent notamment :

- Les applications natives du cloud
- Les charges de travail et applications SaaS
- Les applications cloud développées en interne
- Les serveurs virtuels et physiques
- Les applications traditionnelles et conteneurisées
- Les bases de données relationnelles et distribuées
- Les fichiers et les données non structurées



Avantages à envoyer des copies secondaires de données vers le cloud à d'autres fins que la protection

41 %

Meilleure sécurité par rapport aux ressources locales

38 %

Plus de disponibilité par rapport aux ressources locales

37 %

Évolutivité plus élastique

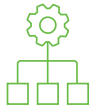
36 %

Capacité à prendre en charge davantage d'utilisateurs finaux en simultané

35 %

Temps de déploiement ou de valorisation plus rapide pour les nouveaux projets

Source : Enterprise Strategy Group. « De la sauvegarde des données à l'intelligence des données », 2022 (en anglais).



Gestion unifiée

Les entreprises créées avant l'avènement du cloud computing ont tendance à gérer elles-mêmes la sauvegarde et la récupération de certaines charges de travail, tout en adoptant pleinement les offres basées sur le cloud telles que M365, Salesforce et Workday. Votre entreprise a besoin que ses données bénéficient du même niveau de protection, peu importe où elles se trouvent et comment elles sont déployées, sans pour autant créer des silos de gestion. Une bonne solution BaaS unifie la gestion de la sauvegarde et de la récupération dans une seule interface utilisateur (UI). Ainsi, même si vous souhaitez utiliser les UI fournies avec vos applications SaaS (par exemple, M365 et SFDC), vous conservez une visibilité complète sur ces dernières, ainsi que sur toutes vos applications et charges de travail locales auto-gérées, par le biais d'une seule et même console. Assurez-vous que la solution BaaS que vous envisagez d'adopter unifie complètement les données de sauvegarde des environnements hybrides et multi-cloud, mais aussi qu'elle vous permet d'effectuer des recherches rapides dans l'ensemble de vos données et de les récupérer n'importe où à partir d'une seule interface.



Simplicité opérationnelle

Les fournisseurs de cloud fonctionnent selon un modèle de responsabilité partagé. Ils garantissent la disponibilité de l'infrastructure. Il vous appartient de protéger les données de votre entreprise. Par exemple, bien que Microsoft 365 (M365) fonctionne dans le cloud sur Microsoft Azure, chacune des applications de productivité M365, ainsi que Teams et SharePoint, possède sa propre stratégie de protection limitée. Alors que la guerre des talents fait rage, les experts informatiques qui consacrent la majorité de leur temps à des tâches routinières telles que la gestion de la protection par charge de travail et les fournisseurs de cloud chercheront de nouvelles façons d'avoir un impact positif plus important sur l'entreprise. Une solution BaaS de niveau entreprise réduit la charge de travail de votre personnel informatique en créant et en exécutant régulièrement des centaines de stratégies. Vos experts auront donc le temps de se consacrer sur l'innovation. Elle sécurise les données, vous donne de la visibilité sur celles-ci, et vous permet de les protéger plus simplement sur plusieurs services cloud et applications locales.



Fiabilité et performance élevées, pas de mises à niveau perturbatrice

Face à l'évolution rapide des entreprises numériques d'aujourd'hui, vos équipes en charge des opérations informatiques et des secteurs d'activité veulent des sauvegardes à la fois flexibles, disponibles, évolutives et fiables. Respectez vos accords de niveau de service (SLA) et accélérez vos résultats opérationnels grâce à une solution BaaS moderne, qui vous permet de disposer des données dont vous avez besoin quand vous en avez besoin, et de contrer les attaques par ransomware. Une sauvegarde dans le cloud n'interrompt pas l'activité : elle est toujours active, mise à jour sur place, et prête à protéger vos données.



Peu ou pas d'empreinte du centre de données

Une infrastructure de sauvegarde héritée comprend généralement une multitude de produits qui rendent vos données plus vulnérables aux cyberattaques. Réaliser une sauvegarde dans le cloud à partir de fournisseurs de solution SaaS individuels signifie qu'un ransomware peut trouver de nombreux points d'entrée. Une seule offre BaaS consolidée, avec peu ou pas de matériel en local, renforce votre protection en réduisant l'empreinte de votre centre de données et donc votre surface d'attaque.

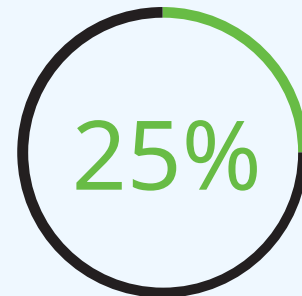
Que demander aux fournisseurs : améliorer la protection de données et la liberté opérationnelle

- Quel est le degré de tolérance de votre entreprise (chefs d'entreprise et propriétaires de l'application) en ce qui concerne les temps d'arrêt pour les mises à jour et les mises à niveau liées à la sauvegarde ?
- Comment votre prochaine solution pourra-t-elle sauvegarder toutes les sources de données disponibles dans votre entreprise ?
- Combien de temps votre personnel consacre-t-il à la gestion des sauvegardes des applications et données SaaS, natives du cloud et locales ?
- Quels sont les processus mis en place pour vous permettre de vous adapter rapidement à l'évolution des exigences réglementaires ou commerciales en matière de protection et de rétention des données ?
- Qu'envisagez-vous de modifier dans votre environnement informatique pour réduire votre infrastructure locale et votre profil de risque en matière de cybersécurité ?

2 Renforcer la sécurité et la préparation aux ransomwares

Les données des entreprises sont attaquées et les cybercriminels s'enrichissent. Selon [Cybersecurity Ventures](#), une entreprise sera victime d'une attaque par ransomware toutes les 2 secondes d'ici 2031, ce qui coûtera à ses victimes 265 milliards d'euros par an. Voilà pourquoi votre entreprise doit non seulement améliorer son agilité informatique, mais aussi renforcer sa posture de sécurité et mieux défendre ses données contre les ransomwares.

Une solution BaaS peut permettre à votre entreprise de ne pas payer de rançon, mais toutes les offres BaaS n'offrent pas les mêmes capacités de préparation aux ransomwares. Assurez-vous d'investir dans une solution BaaS dotée de fonctionnalités anti-ransomware essentielles, notamment :



des entreprises déclarent avoir perdu des données SaaS principalement à la suite d'une suppression malveillante.

Source : [Enterprise Strategy Group](#).
« L'évolution des stratégies de protection des données dans le cloud », 2021 (en anglais).



Snapshots inaltérables

Vos données sont mieux protégées dans une sauvegarde dans le cloud conçue avec des snapshots inaltérables, que les ransomwares ne peuvent pas chiffrer, modifier ou supprimer. Une bonne solution BaaS vous permet de garantir que vos données structurées et non structurées (e-mails, fichiers audio et vidéo, images, etc.) sont sauvegardées et prêtes à être récupérées en cas d'attaque par ransomware.



Détection d'anomalies et alerte

Selon l'enquête « Coût d'une violation de données en 2022 » (en anglais), il faut en moyenne 277 jours pour identifier et contenir une violation. Un délai aussi long permet aux cybercriminels de chiffrer et d'exfiltrer vos données pour les vendre sur le dark web. Il est donc important qu'une offre BaaS soit dotée d'une fonctionnalité puissante de détection d'anomalies automatisée en temps quasi-réel. Une sauvegarde dans le cloud vous permet de suivre en permanence le fonctionnement normal du système, pour repérer rapidement les irrégularités et les comportements anormaux des utilisateurs susceptibles d'indiquer une attaque par ransomware. Ces capacités, associées à des alertes, peuvent signaler un danger potentiel, déclencher des mesures correctives, et ainsi réduire le champ d'action d'une attaque par ransomware.



Contrôles d'accès stricts

Selon l'enquête « [Coût d'une violation de données en 2022](#) » (en anglais), le vecteur d'attaque initial le plus courant en 2022 était les identifiants compromis. Votre entreprise se doit donc de gérer plus efficacement l'identité et les privilèges d'accès de ses utilisateurs. Les meilleures offres BaaS prennent en charge le contrôle d'accès basé sur les rôles (RBAC) granulaire pour empêcher les parties non autorisées de menacer vos données. Recherchez-en une qui inclut également l'authentification multifacteur (MFA) (un processus en deux étapes, qui requiert quelque chose que vous « connaissez » et quelque chose que vous « possédez ») pour authentifier et atténuer les schémas d'hameçonnage et autres piratages de mots de passe.



Isolation des données

Avant l'ère du cloud, une entreprise récupérait généralement ses données en ramenant physiquement sur site les données stockées sur des bandes hors-site. Ce processus n'est cependant plus compatible avec le respect des SLA de récupération des entreprises.

Une solution de BaaS moderne isole les données de votre environnement de production en déplaçant les données de sauvegarde hors-site vers le cloud et en les sécurisant. Une solution de BaaS moderne peut, par exemple, créer isoler les services AWS en déplaçant les données sur un locataire distinct. Si vous devez récupérer rapidement suite à une attaque par ransomware, vous pouvez donc le faire sans réinfecter votre environnement de production.



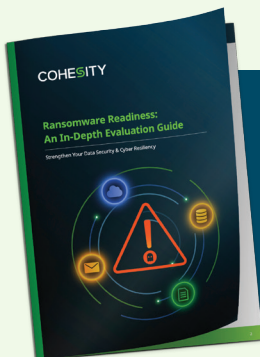
Récupération rapide des données à grande échelle

Étant donné la prévalence des ransomwares et la croissance constante des développements de logiciels malveillants, votre entreprise doit être prête à se remettre rapidement d'une cyberattaque. Vous devez notamment disposer de processus et de technologies qui vous permettent de récupérer vos données à grande échelle en toute confiance.

Il vous faut un service de sauvegarde dans le cloud capable de récupérer rapidement toutes sortes de sources de données (des centaines de VM, de grosses bases de données ou de larges volumes de données non structurées, des données de productivité M365, etc.), instantanément, à grande échelle, à n'importe quel point dans le temps et à n'importe quel emplacement.

Que demander aux fournisseurs : renforcer la sécurité et la préparation aux ransomwares

- Comment défendez-vous l'ensemble de vos différentes applications et charges de travail contre les ransomwares ?
- Comment empêchez-vous aujourd'hui l'accès non autorisé aux données de votre entreprise ?
- Comment prévoyez-vous de récupérer les données en cas d'attaque par ransomware à grande échelle ?



Préparation aux attaques par ransomware : guide d'évaluation détaillé

peut également vous aider dans votre processus de décision.

3 Bénéficier d'une consommation et de coûts plus flexibles, favoriser le développement durable

Dans le milieu professionnel, la nouvelle norme est d'être axé sur les données. Les entreprises s'efforcent donc de plus en plus d'utiliser les données qu'elles collectent et protègent pour découvrir de nouvelles informations et accélérer la mise sur le marché de leurs produits et services. Or, les données qui alimentent les entreprises augmentent à un rythme exponentiel et sont de plus en plus coûteuses à conserver. Adopter un modèle de fournisseur de services est une solution gagnante pour les résultats de l'entreprise ainsi que pour vos équipes en charge de l'informatique et de l'approvisionnement. S'abonner à une solution BaaS permet de consacrer moins de temps à l'approvisionnement, à la conclusion de contrats avec plusieurs fournisseurs de matériel et de cloud pour démarrer. Les abonnements BaaS simplifient également le processus de renouvellement. Une tarification prévisible permet également d'éviter les surprises budgétaires.

Si vous envisagez une solution BaaS pour améliorer votre gestion et votre transparence financières, veillez à choisir un fournisseur qui vous offre à la fois de la prévisibilité et du choix.



Adoption facile

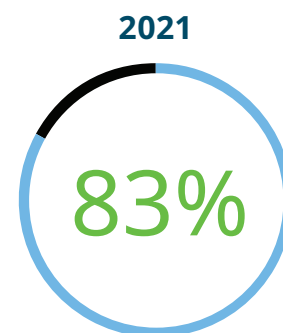
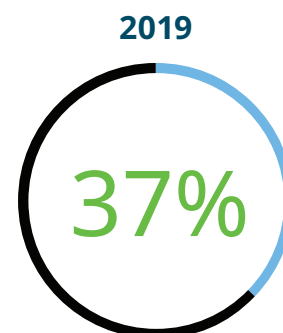
La flexibilité est un élément essentiel pour les entreprises qui envisagent une solution BaaS. Assurez-vous que l'offre BaaS que vous choisissez propose des durées d'engagement gérables (par exemple, un an) et que vous payez uniquement pour la capacité dont vous avez besoin. Vérifiez également si la facturation est facile à comprendre (calculée de manière transparente et granulaire) pour pouvoir prévoir les coûts au maximum. À la différence des offres auto-gérées qui ne proposent qu'une seule option, les solutions BaaS modernes offrent un maximum de flexibilité grâce à de multiples options de licence, notamment des licences frontales, principales ou par utilisateur. Une offre BaaS doit simplifier la mise en œuvre : inscrivez-vous, configurez votre compte, connectez vos sources de données et détectez automatiquement vos charges de travail. Vous devez pouvoir commencer à protéger vos données et vos applications stratégiques en quelques minutes.



Portabilité des licences

Les dirigeants d'entreprise investissent dans l'informatique pour obtenir des résultats commerciaux. Les technologies ne doivent pas vous obliger à changer votre mode de déploiement ni l'endroit où vous prévoyez de les déployer. Si votre entreprise a besoin d'une sauvegarde qui prenne en charge les charges de travail et les applications qui s'exécutent à la fois sur site et dans le cloud, recherchez un fournisseur BaaS qui assure la portabilité des licences entre les modèles de consommation.

Nous envoyons des copies de données secondaires à des services d'infrastructure de cloud public à d'autres fins que la protection (c'est-à-dire dev/test, analyse, etc.)



Source : [Enterprise Strategy Group](#). « De la sauvegarde des données à l'intelligence des données », 2022 (en anglais).



Prise en charge des exigences en matière de souveraineté des données

Dans une récente enquête ESG, les entreprises ont déclaré être de plus en plus préoccupées par les questions de conformité et de souveraineté/localisation des données. Si vos dirigeants misent tout sur le cloud, les offres BaaS peuvent vous permettre de répondre aux exigences de souveraineté des données. La meilleure solution BaaS fonctionne dans les clouds privés des centres de données et sur des clouds publics de premier plan capables de segmenter vos données par régions à travers le monde, conformément aux réglementations nationales et locales.



Une tarification transparente, selon le modèle de paiement « pay-as-you-grow », sans coûts cachés

En période d'incertitude économique, il peut être important de préserver les liquidités pour l'innovation. Avec une solution BaaS, votre entreprise passe d'un système de dépenses d'investissement à un modèle de dépenses opérationnelles plus prévisible. Une bonne solution BaaS élimine également les coûts de provisionnement et les coûts cachés du cloud, notamment les frais d'entrée et de sortie des données. Choisissez une offre qui vous permette de protéger et de consolider vos données de sauvegarde dans le cloud de manière sécurisée et efficace, et qui vous autorise à exploiter davantage vos données pour en tirer des informations et réduire les risques.



Avantages en termes de développement durable

Votre marque est désormais jugée non seulement en fonction de la manière dont vous vous occupez de vos clients et de vos employés, mais aussi en fonction des efforts que vous déployez pour protéger notre planète. La sauvegarde dans le cloud réduit l'empreinte physique du matériel dans votre centre de données et diminue votre consommation d'énergie, ce qui est un objectif clé des initiatives environnementales, sociales et de gouvernance (ESG) des entreprises. Recherchez une offre BaaS alignée sur vos objectifs ESG.



Que demander aux fournisseurs : bénéficier d'une consommation et de coûts plus flexibles grâce au développement durable

- Comment vos investissements en matière de sauvegarde ont-ils évolué au cours des dernières années ?
- Comment votre entreprise a-t-elle optimisé et optimise-t-elle l'informatique pour stimuler l'innovation en période d'incertitude économique ?
- Quels sont les objectifs de votre entreprise en matière d'ESG ?

Liste de contrôle : offres BaaS

Accélérez la modernisation de l'informatique basée sur le cloud avec une solution BaaS. C'est un moyen idéal de faire évoluer vos objectifs de protection de l'ensemble de vos sources de données, de gagner en liberté opérationnelle, de renforcer votre environnement contre les ransomwares et d'optimiser les coûts. Utilisez cette liste de contrôle des capacités clés lorsque vous évaluez les offres BaaS pour identifier la solution la mieux adaptée à votre entreprise.

Capacités		Fournisseur 1	Fournisseur 2	Fournisseur 3
Améliorer la protection de votre source de données et votre liberté opérationnelle	Prise en charge de vastes sources de données	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Gestion unifiée	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Simplicité opérationnelle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Fiabilité et performance élevées, pas de mises à niveau perturbatrice	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Peu ou pas d'empreinte du centre de données	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Renforcer la sécurité et la préparation aux ransomwares	Snapshots inaltérables	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Détection d'anomalies et alerte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Contrôles d'accès stricts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Isolation des données	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Récupération rapide des données à grande échelle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bénéficier d'une consommation et de coûts plus flexibles, favoriser le développement durable	Adoption facile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Portabilité des licences	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Prise en charge des exigences en matière de souveraineté des données	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Une tarification transparente, selon le modèle de paiement « pay-as-you-grow », sans coûts cachés	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Avantages en termes de développement durable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

« L'offre de sauvegarde à la demande de Cohesity nous permet de protéger nos précieuses données utilisateur sans avoir à acheter au préalable une importante infrastructure de stockage supplémentaire. Comme nous n'avons pas eu besoin de nous procurer de matériel, la solution BaaS de Cohesity a été opérationnelle en moins d'une heure. »

Jake Parham

Responsable informatique, Bureau du shérif du comté de St. Johns



Utiliser le BaaS

Modernisez davantage et plus rapidement votre système d'information en adoptant le BaaS. Votre entreprise stimule son agilité grâce à une solution de protection plus simple, plus efficace et plus sécurisée de niveau entreprise pour la grande variété de sources de données sur laquelle elle s'appuie. Respectez les SLA métier et les exigences de conformité. Gagnez du temps et évitez les problèmes de gestion des données informatiques. Atteignez vos objectifs ESG. Tout cela est possible avec la bonne offre BaaS.



En savoir plus sur le BaaS de Cohesity.

COHESITY

© 2023 Cohesity Inc. Tous droits réservés.

Cohesity, le logo Cohesity, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, le logo Helios, DataGovern, SiteContinuity, DataHawk et les autres marques Cohesity sont des marques commerciales ou déposées de Cohesity, Inc. aux États-Unis et/ou dans d'autres pays. Les noms d'autres sociétés et produits peuvent être des marques commerciales des sociétés respectives auxquelles elles sont associées. Ce document (a) est destiné à vous fournir des informations sur Cohesity, son activité et ses produits ; (b) est réputé exact et à jour au moment de sa rédaction, mais est susceptible de modification sans préavis ; et (c) est fourni « TEL QUEL ». Cohesity rejette toutes les conditions, représentations et garanties expresses ou implicites de quelque nature que ce soit.