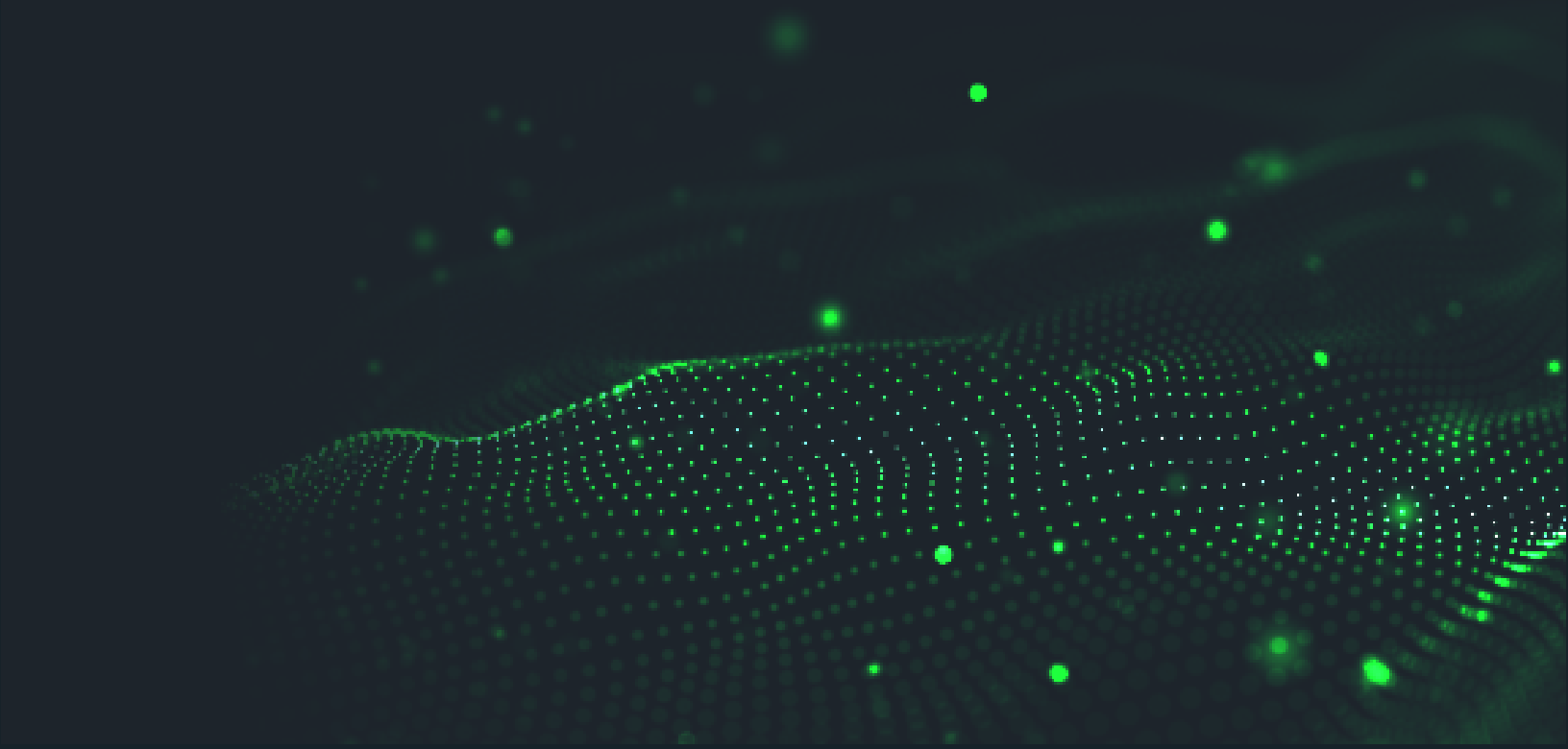
Pourquoi utiliser une plateforme moderne de sécurité et de gestion des données

COHESITY



COHESITY

Table des matières

COHESITY

Synthèse

Aujourd'hui, la ressource la plus importante d'une entreprise, ce sont ses données. Et vos dirigeants le savent. Ils savent également que les cyberattaques, les erreurs humaines ou les catastrophes naturelles peuvent survenir à tout moment et avoir un impact significatif. Ils ont mis en place des solutions de sauvegarde et de restauration pour atténuer l'impact de ces risques.

Mais les processus et les produits utilisés ces dernières décennies n'ont pas été conçus pour répondre aux besoins actuels et futurs des entreprises. Nombre de ces solutions ont été conçues pour une tâche spécifique, entraînant une approche fragmentée des données qui augmente les risques, les coûts et la complexité. En outre, les menaces modernes exigent une approche intégrée, qui associe de manière transparente la sécurité et la gestion des données. Or, les outils plus anciens les considèrent comme des mondes distincts.

Ces limitations amènent de nombreuses entreprises à réévaluer leurs stratégies de sécurité et de gestion des données. Après avoir mené des recherches approfondies et pris en compte le retour sur investissement (ROI), le coût total de possession (TCO) et le profil de risque de leur patrimoine de données actuel, elles se tournent vers des plateformes modernes qui offrent une meilleure protection, des temps de restauration plus rapides, une meilleure évolutivité et une plus grande extensibilité.

Ainsi, lorsque vous décidez de vous intéresser de plus près à une solution moderne, la première question que vous vous posez est la suivante : « Par où commencer ? » C'est sur ce point que nous allons nous concentrer ici.

Vous essayez de comprendre l'intérêt d'un outil récent, ou devez effectuer l'analyse de rentabilité d'un nouvel outil ? Nous verrons pourquoi certaines personnes restent chez leurs fournisseurs historiques, discuterons de l'impact de conserver votre solution actuelle, et examinerons la valeur ajoutée d'une solution plus récente.

> « Notre solution de longue date n'avait pas évolué avec le temps. Il fallait trop de temps pour résoudre des problèmes périodiques. Si une machine virtuelle tombait en panne, notre équipe technique devait la reconstruire à partir des données sauvegardées, ce qui prenait des jours »
>
> - **Luis Suarez**, directeur des systèmes d'information, H.I.G. Capital

COHESITY

Idées reçues sur les offres modernes de gestion et de sécurité des données

Comme pour tout changement, il peut être difficile de basculer sur une solution moderne de sécurité et de gestion des données, surtout si vous ou votre entreprise appréhendez la transition. Commencez par déterminer quels critères sont importants pour vous (par exemple, la conformité, le coût, etc.) et utilisez-les pour évaluer les options qui s'offrent à vous. Vous découvrirez peut-être que la situation actuelle n'est pas idéale. Lisez la suite pour comprendre pourquoi tant d'entreprises envisagent une nouvelle approche.

$ Coût

Lorsque vous changez de solution, il peut y avoir des coûts initiaux liés au nouveau matériel, aux licences logicielles et à la formation du personnel. Cet investissement peut sembler démesuré, surtout si vous êtes satisfait de votre solution actuelle.

Réfléchissez à ceci : maintenir une solution existante pourrait en fait vous coûter plus cher à long terme. Pourquoi ? Les licences et la maintenance peuvent être coûteuses. Selon une enquête réalisée par Deloitte, les départements informatiques consacrent en moyenne plus de 55 % de leur budget technologique à la maintenance des opérations commerciales, et seulement 19 % au développement de solutions innovantes. La croissance des données s'accompagne d'une augmentation des frais de stockage.

Sécurité

Qu'est-ce qui est le plus sûr : l'option moderne ou vos anciennes solutions ? Pour beaucoup, ces dernières permettent aux entreprises de mieux contrôler leurs informations sensibles et sont moins exposées aux cyberattaques.

Réfléchissez à ceci : les solutions traditionnelles ont leurs propres failles de sécurité. Elles sont exposées à un risque accru de fuite et de perte de données liées à des altérations physiques, à des catastrophes naturelles ou à des capacités de protection obsolètes, ce qui peut avoir un impact sur les relations clients et engendrer des coûts élevés. En fait, IBM a indiqué que le coût mondial moyen d'une violation de données en 2023 était de 4,45 millions d'euros, soit une augmentation de 15 % sur les trois dernières années.

COHESITY

Migration des données

C'est un processus pénible. Migrer des données peut être chronophage et coûteux. De plus, si vous changez de solution, vous risquez d'être confronté à de nouveaux défis.

Réfléchissez à ceci : si vous conservez votre solution actuelle, vous risquez de passer à côté des avantages d'une nouvelle solution. Migrer les données de votre entreprise peut lui permettre de gagner en efficacité, et d'améliorer la sécurité ainsi que la qualité des données. Par ailleurs, la plupart des solutions modernes possèdent des capacités visant à simplifier le processus de migration.

Conformité

Dans les secteurs très réglementés, la capacité d'une nouvelle plateforme de sécurité des données à répondre aux exigences réglementaires peut susciter des inquiétudes. Les entreprises préfèrent peut-être s'en tenir à des solutions existantes dont la conformité a été prouvée, plutôt que de prendre le risque perçu d'adopter une nouvelle plateforme.

Réfléchissez à ceci : les solutions modernes sont en fait très sécurisées. Elles intègrent des fonctionnalités de sécurité comme le chiffrement, la gestion des accès et une protection avancée contre les menaces, qui permettent de se conformer plus facilement à des réglementations telles que le RGPD et l'HIPAA. Les solutions traditionnelles ne permettent pas toujours de restreindre l'accès aux données qu'elles contiennent. Elles n'ont pas non plus été conçues pour répondre aux menaces actuelles. De nombreux fournisseurs ont donc bricolé des fonctionnalités et des capacités supplémentaires pour rester à jour, augmentant ainsi la complexité et les risques.

Adoption

Il peut être difficile de changer, en particulier pour les grandes entreprises dont la culture et les méthodes de travail sont bien ancrées. Les équipes peuvent être réticentes à l'idée d'adopter de nouvelles technologies, simplement parce que « nous avons toujours fait autrement » ou parce qu'il peut être difficile d'apprendre quelque chose de nouveau.

Réfléchissez à ceci : la plupart des solutions récentes sont construites en respectant les bonnes pratiques en matière d'interface utilisateur (UI), et sont conçues pour être à la fois conviviales et faciles à adopter. Beaucoup déploient également leur logiciel à la demande (SaaS). Votre entreprise n'a alors pas à se préoccuper de gérer l'application ou les mises à niveau et les correctifs de sécurité.

Satisfaction actuelle

De même, certains peuvent préférer s'en tenir à ce qui fonctionne pour eux. Certains décideurs peuvent ne pas comprendre pleinement les capacités et les avantages des solutions modernes de sécurité des données, et ainsi passer à côté de la valeur ajoutée d'offres plus récentes.

Réfléchissez à ceci : de quoi allez-vous avoir besoin pour affronter les dix prochaines années ? Votre solution actuelle va-t-elle continuer à vous servir pendant une autre décennie, ou voulez-vous quelque chose qui intègre les dernières nouveautés les plus remarquables (par exemple, la solution propose-t-elle des capacités d'IA pour éclairer la prise de décision ? Est-elle native du cloud ?)

COHESITY

Le coût de l'inaction

Nous savons tous qu'il y aura des inondations et, qu'un jour ou l'autre, il y aura une panne d'électricité. Vous êtes probablement préparé à ces situations. Mais qu'en est-il des événements encore plus imprévisibles, par exemple une cyberattaque ? La question n'est pas de savoir si elle aura lieu, mais quand, et il est donc tout aussi important d'avoir une stratégie en place. Même si votre solution actuelle vous satisfait, le fait est que les solutions traditionnelles n'ont pas été conçues pour répondre aux besoins du monde d'aujourd'hui. Avant de décider de conserver votre fournisseur actuel, réfléchissez donc à l'impact que cette décision pourrait avoir sur votre entreprise.

Silos de données. Les systèmes en place gèrent de nombreux silos de données qui limitent la capacité d'une entreprise à gérer des volumes croissants de données et à évoluer. Cela peut vous empêcher de vous adapter à l'évolution des besoins de votre entreprise, créer des problèmes de performance et diminuer la productivité. Les silos provoquent également des inefficacités qui augmentent les coûts opérationnels. Par exemple, un rapport IDC a révélé que les entreprises qui avaient adopté une solution moderne avaient économisé plus de 720 000 euros en temps de travail par an, car elles avaient eu besoin de 7,2 employés à temps plein en moins pour gérer leur infrastructure informatique.

Surface d'attaque plus large. Aujourd'hui, les entreprises conservent leurs données dans plusieurs environnements (par exemple, dans le cloud, en mode SaaS et en local), ce qui élargit la surface d'attaque et complique la sécurité. Chaque environnement peut nécessiter une approche différente de la protection des données, et leur niveau de sécurité peut varier de l'un à l'autre.

Stratégie de sécurité obsolète. Les solutions traditionnelles n'ayant pas été conçues pour le paysage actuel des menaces, elles sont plus exposées aux vulnérabilités et aux exploits connus. Les cybercriminels peuvent ainsi se servir de ces failles pour obtenir un accès non autorisé aux systèmes, voler des données sensibles ou perturber les opérations. Voilà pourquoi tant d'entreprises paient la rançon. Selon Compliance Week, Change Healthcare, une unité Optum d'UnitedHealth, aurait payé 22 millions d'euros pour récupérer ses données après une attaque par ransomware début 2024.

Maintenance du système. Les frais de licence et de maintenance peuvent coûter aux entreprises des milliers d'euros par an. De plus, le temps nécessaire pour faire les mises à niveau ne peut être consacré à des tâches à plus forte valeur ajoutée susceptibles de favoriser l'innovation, la différenciation des produits et les initiatives de sécurité. En outre, à mesure que de nouvelles

COHESITY

solutions arrivent sur le marché, trouver les compétences nécessaires pour exploiter un système plus ancien devient de plus en plus difficile et coûteux.

Productivité des employés. Au fil des ans, les entreprises ont ajouté de nouveaux produits à leur pile technologique pour répondre à des besoins spécifiques. En fait, l'entreprise moyenne compte plus de 130 outils de cybersécurité différents, qui fonctionnent tous avec une vision séparée des données qu'ils protègent. Les utilisateurs doivent constamment passer d'un système à l'autre, et donc les équipes perdent en productivité. Cela pose également des problèmes de personnel, car il est plus difficile de trouver des employés capables d'utiliser des solutions anciennes et complexes.

Temps de réponse. Selon une étude mandatée par Cohesity, 79 % des personnes interrogées ont été victimes d'attaques par ransomware entre juin et décembre 2023, et seulement 7 % d'entre elles ont pu restaurer et rétablir leur processus opérationnel dans un délai de 1 à 3 jours. Cela s'explique en partie par le fait que les anciennes solutions ne prennent pas en charge les nouvelles applications, ou n'offrent pas les capacités nécessaires pour les protéger. Ce problème est amplifié par le fait que la plupart des entreprises consacrent la majeure partie de leur budget de cybersécurité à la protection et à la détection, et seulement une fraction à la réponse et à la restauration. Toutefois, comme ces données le suggèrent, les attaques vont se produire quoi qu'il arrive. Il est donc impératif d'investir dans les deux à parts égales pour atteindre les objectifs de RTO/RPO.

[2] https://www.cohesity.com/fr/press/cohesity-research-reveals-most-companies-pay-millions-in-ransoms-breaking-their-do-not-pay-policies/

COHESITY

Les avantages d'une plateforme moderne de sécurité et de gestion des données

Nous avons examiné les problèmes liés aux anciennes technologies et expliqué ce qu'une solution moderne n'est pas. Nous n'avons toutefois pas évoqué d'alternative, ni indiqué les éléments à prendre en compte pour moderniser vos efforts de sauvegarde et de restauration. Nous recommandons en général de rechercher les caractéristiques suivantes.

Simple à utiliser

Une plateforme moderne de gestion et de sécurité des données doit offrir une expérience cohérente et transparente partout : dans l'infrastructure (en local, dans le cloud, à la périphérie) et dans les charges de travail. Elle doit également être orientée API et pouvoir s'intégrer facilement à d'autres systèmes informatiques. Cela permet ainsi d'intégrer, de traiter et d'analyser facilement les données dans d'autres systèmes et outils, au lieu de créer un réseau complexe de solutions. En centralisant tout en un seul endroit, les entreprises peuvent éliminer les silos et permettre au personnel informatique de gérer plus efficacement de gros patrimoines de données. Par exemple, une importante compagnie d'assurance a économisé 2 millions d'euros par an en coûts de sauvegarde et a permis à sa petite équipe de gérer plus simplement un plus gros volume de données.

Conçue pour évoluer

Les plateformes de données modernes doivent être très évolutives pour pouvoir traiter les gros volumes de données que génèrent les applications et les appareils modernes, ainsi que les volumes croissants de données et d'utilisateurs. Cela permet d'étendre de manière transparente la capacité et les performances en fonction de l'évolution des besoins de l'entreprise. La plateforme doit également être capable de traiter des données provenant de sources très diverses (machines virtuelles, bases de données d'entreprise, NAS,

Avant et après : l'histoire de Hyatt

Pour Hyatt, leader mondial de l'hôtellerie, il était devenu impossible de gérer plusieurs produits informatiques hérités dans le monde entier, d'autant plus le volume de données de certains de ses établissements avait augmenté de 20 %. Pour gagner en efficacité, son équipe informatique a opté pour une solution moderne permettant de garantir une réplication des données de grande qualité et des capacités de dev/test agiles entre ses différents centres de données.

Hyatt a ainsi réduit la durée de réplication des données de plusieurs jours à quelques minutes et a vu sa capacité réduite de 40 %.

Lisez l'étude de cas

COHESITY

SaaS, sources de données dans le cloud), et notamment des données structurées et non structurées.

Sécurité fiable

Une plateforme moderne repose sur les principes du Zero Trust, notamment le contrôle d'accès basé sur les rôles (RBAC), l'authentification multifacteur (MFA), l'immuabilité et le chiffrement des données au repos/en transit. Les données sensibles sont ainsi sécurisées et protégées contre les accès non autorisés et les cyberattaques. Elle permet également d'identifier les données sensibles, de les stocker de manière sécurisée, de détecter les attaques et de regrouper les capacités de réponse aux cyber incidents. Enfin, la solution que vous choisissez devrait idéalement pouvoir s'intégrer à d'autres outils de sécurité existants et émergents afin de renforcer la posture de sécurité de votre entreprise.

Restauration rapide

En cas de cyberattaque ou d'interruption imprévue, une plateforme moderne permet de restaurer les bases de données stratégiques rapidement sans surprise. Les entreprises sont capables de faire cela grâce à des sauvegardes incrémentales et à des snapshots qui sont stockés dans un lieu séparé et ne peuvent pas être modifiés. C'est particulièrement important pour des raisons de conformité. Une plateforme moderne proposera également des options de restauration instantanée et granulaire, afin que les entreprises puissent rapidement restaurer des fichiers, des bases de données ou des applications spécifiques sans avoir à restaurer des sauvegardes entières. Grâce à ces capacités, des entreprises du Fortune 500 ont divisé par 10 leur temps de restauration.

Axée sur les données

Toute plateforme moderne de gestion des données devrait prendre en charge une gamme d'outils d'analyse et de visualisation des données, notamment l'analyse basée sur SQL, le machine learning (ML) et le traitement automatique du langage naturel (NLP), afin que les entreprises puissent extraire des informations et de la valeur de leurs données. Elle devrait également offrir des capacités d'IA. Tous les fournisseurs n'en proposent pas, mais elles permettent aux entreprises de collecter plus rapidement des informations.

Avant et après : Pearl River Community College

Les universités sont récemment devenues les cibles privilégiées des usurpations d'identité et des attaques par ransomware. Pour protéger les informations des étudiants et assurer le bon déroulement des opérations en cas de sinistre, le Pearl River Community College a opté pour une solution moderne de sécurité et de gestion des données proposant des contrôles d'accès, notamment le MFA, des sauvegardes immuables, un quorum et des capacités d'isolation des données.

« Nos primes d'assurance seraient beaucoup plus élevées sans ces capacités. Nous n'aurions peut-être même pas réussi à nous faire assurer » a déclaré Matt Logan, leur DSI.

Lisez l'étude de cas

COHESITY

La suite de votre parcours

Migrer vers une solution moderne de sécurité et de gestion des données peut sembler un défi de taille, surtout si votre solution existante s'est avérée fiable au fil des ans. Mais face à l'augmentation du nombre d'attaques et à l'évolution de la nature des cyberévénements, le statu quo n'est plus suffisant. Les grandes entreprises se préparent donc à l'avenir en protégeant leurs données à l'aide de solutions modernes de sécurité et de gestion.

Voici les prochaines étapes que nous vous recommandons de suivre :

1. **Déterminez pourquoi vous souhaitez changer de solution.**
   - Fixez des objectifs de RTO et de RPO, de stockage, de coûts d'exploitation, etc.
2. **Décrivez les cas d'usage que vous souhaitez prendre en charge et les fonctionnalités importantes.**
3. **Évaluez le ROI et le TCO d'une plateforme de données moderne par rapport à votre solution actuelle. Comparez principalement :**
   - L'efficacité de la protection des données
   - L'efficacité opérationnelle
   - Le risque et la conformité
4. **Élaborez une analyse de rentabilité. Pour convaincre les principales parties prenantes, veillez à :**
   - Démontrer comment la nouvelle technologie s'aligne sur les objectifs stratégiques de l'entreprise.
   - Définir clairement les problèmes auxquels la solution moderne répondra.
   - Expliquer la nouvelle technologie et son fonctionnement.
   - Prendre en compte le coût et les critères d'une cyber-assurance.
   - Quantifier les avantages, notamment les économies de coûts, les gains de productivité et l'amélioration des capacités (c'est-à-dire le ROI)
   - Décrire les prochaines étapes du déploiement de la solution, en abordant les risques potentiels et la manière dont vous les atténuerez.

Une fois que vous avez obtenu l'adhésion à une solution et que vous êtes prêt à sélectionner un fournisseur, évaluez vos données, l'endroit où elles se trouvent et les dépendances de votre équipe. Vous devrez également réfléchir à des processus de gouvernance des données pour maintenir une hygiène à long terme.

COHESITY

À propos de Cohesity

Cohesity est un leader de la sécurité et de la gestion des données alimentées par l'IA. Cohesity s'appuie sur un vaste écosystème de partenaires pour vous permettre de protéger, de gérer et de valoriser plus facilement vos données, que ce soit dans le centre de données, à la périphérie ou dans le cloud. Cohesity permet aux entreprises de se défendre contre les menaces de cybersécurité grâce à ses capacités complètes de sécurité et de gestion des données, notamment des snapshots de sauvegarde immuables, une détection des menaces basée sur l'IA, la surveillance des comportements malveillants et une restauration rapide à grande échelle. Les solutions Cohesity sont fournies à la demande, en mode auto-géré ou par un partenaire équipé de la technologie Cohesity. Cohesity est basée à San Jose, en Californie, et les plus grandes entreprises du monde lui font confiance.

COHESITY

www.cohesity.com

2000052-001-EN 7-2024