6 raisons de protéger vos données SaaS

veeam

SaaS : dynamiser les entreprises d'aujourd'hui

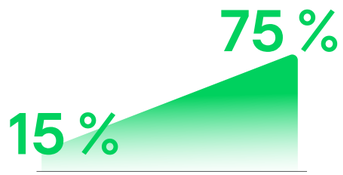
Les applications SaaS sont le moteur de l'entreprise moderne. Entre e-mails, partage de fichiers, données clients et finances, ils permettent aux équipes d'avancer rapidement et de rester connectées. Ils sont flexibles, rentables et évolutifs, et c'est exactement la raison pour laquelle les entreprises les ont adoptés si rapidement.

Mais voici le piège : les données des applications SaaS ne sont pas aussi sécurisées que vous le pensez.

Trop d'entreprises supposent que leur fournisseur SaaS les couvre en matière de protection des données. La réalité ? La plupart des plateformes offrent une rétention à court terme et des outils de restauration élémentaires incapables de suivre la vitesse et l'ampleur des menaces actuelles. Il offre peu de protection contre les suppressions accidentelles, les ransomwares, les erreurs de synchronisation ou les mésaventures d'initiés. Et lorsqu'il s'agit de répondre aux exigences réglementaires, vous devez vous débrouiller par vous-même.

Dans la pratique, c'est le modèle de partage des responsabilités. Le fournisseur garantit la disponibilité des services. Vous gérez les données elles-mêmes : comment elles sont sécurisées, combien de temps elles sont conservées, à quelle vitesse elles peuvent être restaurées.

À mesure que vous recourez à des applications cloud et à des infrastructures hybrides, et que vos équipes sont réparties géographiquement, cette responsabilité devient plus difficile à gérer. De petites lacunes dans la couverture se transforment en problèmes coûteux. Les sauvegardes manquées, les restaurations retardées et les stratégies de rétention non conformes peuvent causer de réels dommages, tant sur le plan financier qu'opérationnel et sur le plan de la réputation.



Actuellement, seules 15 % des entreprises considèrent la sauvegarde des données SaaS comme une priorité absolue. On s'attend à ce que ce chiffre atteigne 75 % d'ici 2028.

Le changement se profile, mais attendre n'est pas une stratégie.

Cet e-book est conçu pour vous aider à prendre de l'avance. Vous y découvrirez précisément où se situent les lacunes communes, pourquoi les outils natifs sont insuffisants et à quoi ressemble réellement une stratégie de protection des données SaaS moderne et résiliente.

Si votre entreprise s'appuie sur le SaaS pour gérer des parties essentielles de l'activité, il ne s'agit pas seulement d'informations utiles. C'est une planification essentielle.

Pourquoi les données des applications SaaS doivent-elles être protégées ?

1. Erreur humaine et suppression accidentelle

Les plateformes SaaS sont essentielles au fonctionnement des entreprises, mais la plupart des équipes sous-estiment à quel point il est facile de perdre des données importantes. Une simple erreur, comme la suppression d'un mauvais fichier, une mauvaise configuration d'une synchronisation ou l'écrasement d'un enregistrement partagé, peut supprimer instantanément des informations critiques du système. Beaucoup pensent que la restauration n'est qu'à quelques clics, mais c'est rarement le cas.

La plupart des plateformes (Microsoft 365, Entra ID, Salesforce) utilisent des corbeilles intégrées qui offrent des périodes de rétention courtes et une portée limitée. Une fois ce délai écoulé, ou si les données contournent entièrement la corbeille, la restauration devient impossible. Très souvent, les données dont vous avez besoin ne sont même pas protégées et certains types de données peuvent ne jamais arriver à la corbeille. Lorsque vous remarquez qu'il manque quelque chose, il est souvent déjà hors de portée.

Ces plateformes sont conçues pour la performance et la collaboration, et non pour une protection à long terme. Et comme les entreprises deviennent de plus en plus dépendantes du SaaS pour leurs principales fonctions, ces lacunes deviennent de plus en plus difficiles à ignorer. Une suppression accidentelle ne doit pas faire dérailler un projet, retarder un audit ou perturber la relation client.

2. Risques juridiques, réglementaires et de conformité

Les réglementations telles que le RGPD, HIPAA et NIS2 ne sont pas de simples cases à cocher, elles ont des conséquences réelles. Nous parlons d'amendes majeures, de maux de tête juridiques et de dommages pour votre marque si vos données ne sont pas stockées, conservées ou restaurées comme l'exige la loi.

Alors que ces cadres deviennent plus stricts et plus globaux, compter uniquement sur des protections intégrées met votre entreprise en danger. Et il ne s'agit pas seulement de cocher des cases de conformité, il s'agit d'avoir un contrôle total au moment le plus important.

En 2024, la pression s'est intensifiée. Les cybercriminels sont devenus plus rusés, les catastrophes naturelles ont mis à mal les infrastructures et de nouvelles réglementations telles que NIS2 ont placé la barre encore plus haut. À l'approche de 2025, les cybercriminels utilisent les ransomwares comme un écran de fumée pour exfiltrer ou corrompre vos données en silence, tandis que l'IA ajoute vitesse et complexité à l'équation.

Pour rester conforme et garder le contrôle, il faut plus que de bonnes intentions. Il faut une vraie stratégie et les bons outils pour la soutenir.

3. Le coût élevé des pertes de données

Les pertes de données ne frappent pas seulement l'IT, mais aussi l'entreprise tout entière. Cela épuise les budgets, fait dérailler les plans et ébranle la confiance des clients. À elles seules, les amendes peuvent atteindre des millions, mais ce n'est qu'un début. Les efforts de restauration détournent les équipes de leurs tâches essentielles, les frais juridiques grimpent en flèche et la productivité stagne. Pendant ce temps, les clients sont frustrés, les offres tombent à l'eau et les concurrents n'hésitent pas à combler les lacunes.

Sur les marchés actuels à évolution rapide, un seul incident de données suffit à mettre une société hors course. L'élan est perdu, les priorités se déplacent vers le contrôle des dégâts, et ce qui a commencé comme une petite erreur devient une crise coûteuse. Trop souvent, les entreprises sous-estiment la vitesse à laquelle les choses peuvent s'envenimer. Ils traitent la perte de données comme un problème informatique… jusqu'à ce qu'il perturbe les revenus, la réputation et les relations.

Voici la vérité : les données sont au centre de tout. Tout en dépend : les opérations, l'expérience client, la conformité et la croissance. Si vous perdez le contrôle de vos données, vous cédez le contrôle de votre entreprise. Et la plupart du temps ? Ce n'était pas une fatalité.

4. Menaces de sécurité interne

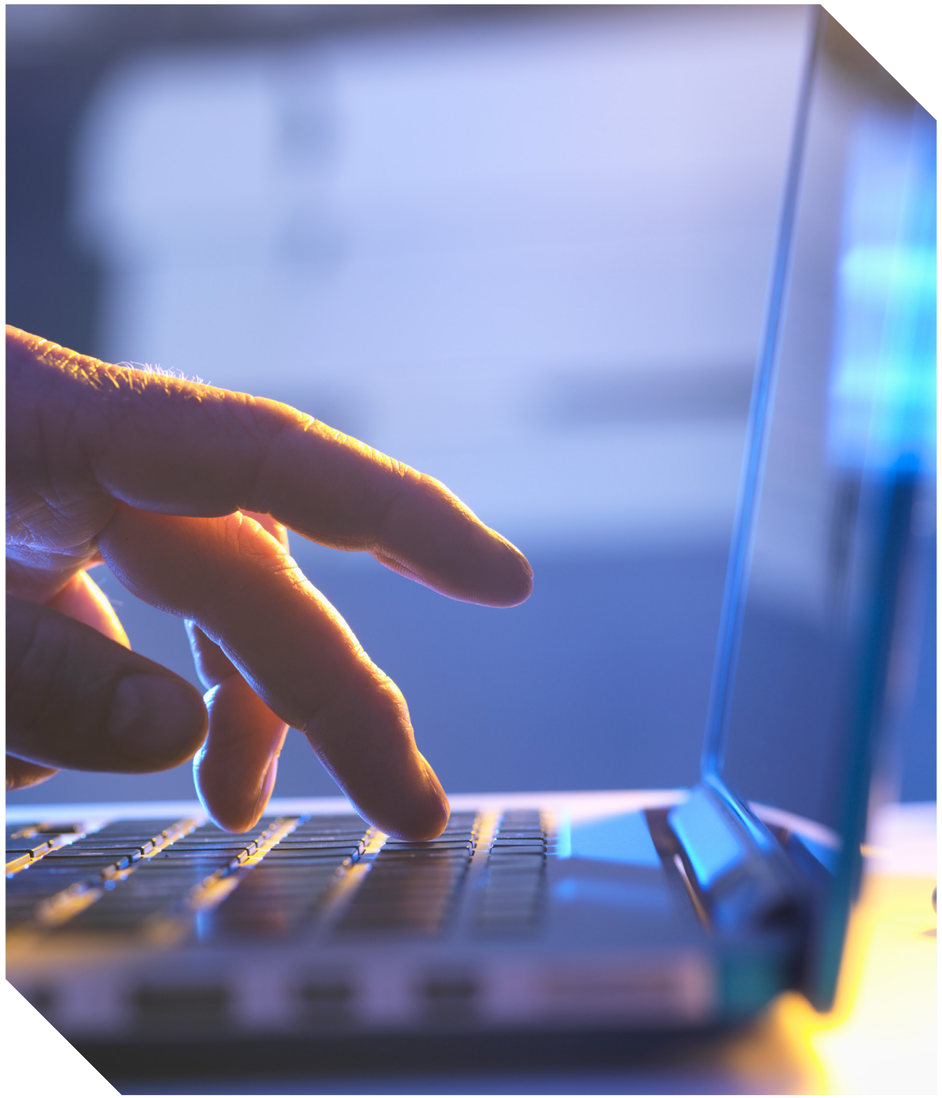
Les menaces internes font partie des risques les plus sous-estimés et des plus dommageables. Les employés, les sous-traitants et les fournisseurs ayant accès à des systèmes sensibles peuvent exposer des données, que ce soit par erreur ou intentionnellement. Une autorisation mal configurée, un partage de fichiers négligent ou une suppression malveillante peuvent passer inaperçus tant que le mal n'est pas fait.

Le travail hybride n'a fait qu'augmenter les enjeux. Avec des équipes dispersées géographiquement et des systèmes plus ouverts que jamais, la surveillance est plus difficile et les menaces internes peuvent échapper aux défenses traditionnelles. Il ne s'agit pas d'attaques qui font la une des journaux de l'extérieur, mais plutôt de brèches discrètes de l'intérieur. Lorsque vous les détectez, vos données stratégiques ont peut-être déjà disparu.

Ce n'est pas une exception rare. Cela se produit dans tous les secteurs, dans toutes les équipes et dans tous les services. Et les conséquences sont graves : confiance rompue, flux de travail bloqués, échecs de conformité et enquêtes coûteuses.

Les menaces internes ne sont pas un « peut-être », mais une préoccupation constante et inévitable. La vraie question est : aurez-vous la visibilité, le contrôle et le plan de reprise nécessaires pour y faire face avant qu'elle ne devienne une crise à part entière ?

5. Cybermenaces



Les cyberattaques deviennent de plus en plus intelligentes et difficiles à contrer. Les ransomwares ont largement dépassé le simple chiffrement de fichiers. Les attaques d'aujourd'hui impliquent souvent des vols de données, des actes de sabotage et des tactiques d'extorsion en plusieurs étapes conçues pour submerger les défenses et bloquer les équipes d'intervention. Le phishing, l'abus de privilèges et les logiciels malveillants furtifs ne sont souvent qu'un début.

L'impact financier peut être énorme. En 2024, le montant moyen des rançons payées au quatrième trimestre s'élevait à plus d'un demi-million de dollars USD. Mais ce chiffre ne tient pas compte de l'ensemble des coûts. Les pertes de chiffre d'affaires, les procédures juridiques, les temps d'arrêt d'exploitation et les dommages causés à la réputation de la marque causent souvent plus de dommages à long terme. Les cadres réglementaires tels que le RGPD et NIS2 font monter les enjeux encore plus : ils obligent les entreprises à démontrer que leurs données ont été protégées avant, pendant et après une attaque.

Avec une infrastructure hybride, des équipes à distance et un nombre croissant de points d'accès, les opportunités pour les cybercriminels ont explosé. Les défenseurs doivent couvrir plus de terrain avec les mêmes ressources, quand ce n'est pas moins. Les menaces basées sur l'IA et l'ingénierie sociale plus sophistiquée ajoutent encore plus de pression aux équipes IT et de sécurité déjà surchargées.

Les ransomwares ne sont plus seulement une question de sécurité. Il s'agit d'un risque commercial qui exige une stratégie moderne à plusieurs niveaux à la hauteur de sa complexité. Les entreprises ont besoin d'être plus rapides, plus intelligentes et entièrement équipées pour y répondre.

6. Assurer la continuité d'activité

Les perturbations peuvent prendre de nombreuses formes (ransomwares, pannes, catastrophes naturelles) et lorsqu'elles surviennent, le compte à rebours commence. La plupart des équipes ne sont pas préparées pour restaurer leurs données assez rapidement. Selon Gartner, la restauration après une attaque par ransomware nécessite souvent plusieurs semaines. Ce genre de retard a des conséquences néfastes à tous les niveaux.

Les temps d'arrêt réduisent le chiffre d'affaires, frustrent les clients et épuisent les ressources internes. Dans des secteurs comme les soins de santé, la finance et le gouvernement, où chaque minute compte, les coûts peuvent grimper rapidement. Les clients s'attendent à de la disponibilité. Lorsque les systèmes s'éteignent, la patience s'épuise et la confiance dans la marque en prend un coup. Dans les environnements complexes, une panne unique affecte souvent de nombreux systèmes, partenaires et utilisateurs finaux. Sans plan fiable, les petits problèmes s'amplifient et la restauration devient plus difficile au fil des heures.

Tous ensemble ? La vitesse de restauration ne consiste pas seulement à remettre les systèmes en ligne. Il s'agit aussi de protéger le travail de vos équipes et la confiance de vos clients, tandis que chaque heure pendant laquelle vos données SaaS sont compromises érode progressivement les deux.

La question qui se pose est donc la suivante : est-ce que c'est un risque qui vaut la peine d'être pris ?

Le rôle des solutions tierces dans la protection des données

Les fournisseurs SaaS n'ont pas été conçus pour assurer une protection complète des données. Leurs outils natifs couvrent le strict minimum. Les plannings de sauvegarde sont rigides, la rétention est courte et les possibilités de restauration sont limitées. Les fonctionnalités essentielles telles que les restaurations granulaires, la rétention étendue et le reporting conforme ne font tout simplement pas partie de l'offre.

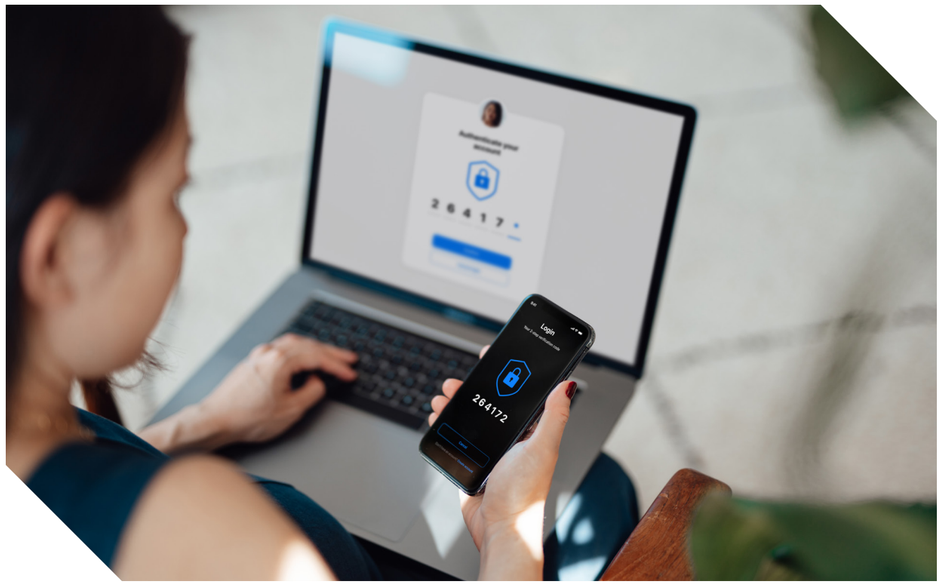
À mesure que les environnements se complexifient, ces limitations créent plus de risques. Les équipes doivent assembler des solutions de contournement, ce qui ajoute du coût et de la complexité sans résoudre le problème sous-jacent. La visibilité est limitée. La flexibilité fait défaut. Et lorsqu'un problème survient, la restauration est souvent lente, incomplète, voire impossible.

Les plateformes SaaS sont essentielles au fonctionnement des entreprises, mais les protections par défaut n'ont pas été conçues pour assurer une résilience à long terme. Sans sauvegarde conçue spécifiquement ni restauration, les entreprises risquent de voir leurs outils essentiels leur faire défaut là où elles en ont le plus besoin.

La question est simple : s'il s'agit des données qui font fonctionner votre entreprise, les protections intégrées sont-elles vraiment suffisantes pour les protéger ?

La protection des données SaaS en action

De plus en plus d'entreprises reconnaissent cette lacune dans la protection des données SaaS — et elles y répondent. D'ici 2028, 90 % des entreprises s'attendent à ce que la sécurité soit intégrée dans une plateforme SaaS de protection des données. Le changement est déjà en cours. Les équipes tournées vers l'avenir dépassent les outils natifs et adoptent des solutions de protection des données SaaS, des plateformes unifiées et des stratégies de restauration hybride qui englobent les environnements cloud, SaaS et locaux.



Ils choisissent des solutions offrant la flexibilité et le contrôle dont ils ont besoin : sauvegardes inaltérables, restauration à un instant précis, rétention à long terme et détection intégrée des menaces. Ce ne sont pas des fonctionnalités bonus. Elles constituent le socle d'une stratégie sérieuse de protection des données.

Pendant ce temps, les risques ne cessent d'augmenter. Les plateformes SaaS gèrent tout, de la vente à la finance en passant par la collaboration. En cas de casse, que ce soit à la suite d'une erreur, d'une attaque ou d'une panne, l'activité est bloquée. Et pour les entreprises qui utilisent encore les paramètres par défaut, la restauration est souvent limitée, lente, voire impossible.

La rétention limitée et la rigidité de la restauration ne résistent pas à la pression du monde réel. Les entreprises ont besoin d'une protection qui évolue avec leurs données, maintient leur conformité et agit rapidement lorsque chaque seconde compte.

Reconnaître le problème est la première étape. Il est maintenant temps de mettre en place la bonne solution.

À quoi ressemble la résilience des données SaaS modernes ?

La manière dont les entreprises gèrent et protègent les données a changé. Les applications SaaS, l'infrastructure hybride et les équipes à distance entraînent un nouveau niveau de complexité. Les cybermenaces évoluent rapidement. Les normes de conformité sont de plus en plus strictes. Et trop d'entreprises s'appuient encore sur des outils obsolètes ou des configurations de plateformes intégrées qui n'ont tout simplement pas été conçues pour répondre aux exigences d'aujourd'hui.

Le guide intitulé 6 caractéristiques essentielles d'une résilience moderne des données SaaS décrit exactement ce dont les entreprises actuelles ont besoin pour rester protégées, assurer leur conformité et garder le contrôle. Vous y découvrirez comment les équipes dirigeantes adoptent des solutions natives cloud qui simplifient les opérations tout en renforçant la sécurité.

- Limitez les retards de restauration grâce à une automatisation basée sur les stratégies rapide et précise.
- Centralisez la protection de l'ensemble des workloads SaaS, cloud et sur site.
- Renforcez la conformité et la sécurité grâce aux contrôles intégrés et à la visibilité en temps réel.

Si vous gérez encore les risques à l'aide d'une mosaïque d'outils vieillissants ou d'hypothèses sur ce qui est couvert, ce guide vous aidera à combler les lacunes.

→ Téléchargez l'e-book pour anticiper la suite.

Ressources complémentaires :

→ 7 raisons cruciales de sauvegarder Microsoft 365

→ 6 raisons de sauvegarder Microsoft Entra ID

→ Principaux scénarios de protection des données Salesforce

À propos de Veeam Software

Veeam®, le n° 1 mondial de la résilience des données, estime que chaque entreprise doit pouvoir se relever après un incident en conservant la confiance et le contrôle de toutes ses données, au moment et à l'endroit voulus. Veeam appelle cela la résilience totale, et nous sommes obsédés par le désir de créer des moyens innovants d'aider nos clients à y parvenir.

Les solutions Veeam sont spécifiquement conçues pour renforcer la résilience des données en offrant la sauvegarde, la restauration, la liberté des données, la sécurité des données et l'intelligence des données. Avec Veeam, les responsables IT et de la sécurité ont la tranquillité d'esprit de savoir que leurs applications et leurs données sont protégées et toujours disponibles dans l'ensemble de leurs environnements cloud, virtuels, physiques, SaaS et Kubernetes.

Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 74 % des entreprises du Global 2000, qui lui font confiance pour le maintien de leur activité. La résilience totale commence avec Veeam.

Pour en savoir plus, rendez-vous sur www.veeam.com/fr **ou suivez Veeam sur LinkedIn** @veeam-software et sur X @veeam.

→ **En savoir plus :** veeam.com/fr