Vos 100 premiers jours

avec la Veeam Data Platform

Le guide du dirigeant pour une résilience mesurable

La plupart des organisations supposent être protégées, mais peu l'ont testé.

Dans une récente enquête, 90 % des responsables de la sécurité ont déclaré pouvoir restaurer leurs données dans les limites des objectifs définis. Cependant, parmi les victimes de ransomware, seuls 28 % ont pu restaurer toutes leurs données (Source : Rapport sur la confiance et la résilience des données 2026). La confiance n'est pas synonyme de capacité de restauration démontrée, et c'est dans l'écart entre les deux que les ransomwares l'emportent, que les audits échouent et que les pannes deviennent des crises.

90 %

des responsables de la sécurité ont déclaré être en mesure de restaurer leurs systèmes dans les délais qu'ils s'étaient fixés

28 %

des victimes de ransomware ont pu récupérer l'intégralité de leurs données

Parce que la résilience n'est réelle que si vous pouvez la prouver.

Ce guide adopte une vision stratégique de votre déploiement de la Veeam Data Platform. Au fur et à mesure que votre équipe franchit les étapes techniques du déploiement, ce guide les traduit en résultats pour l'entreprise : les risques réduits, les fonctionnalités acquises et la preuve dont vous disposerez à la fin.

Parce que c'est à vous de décider en matière de tolérance au risque, d'engagements de restauration et de continuité d'activité. Ce guide couvre ce dont vous êtes responsable et ce que vous serez en mesure de communiquer avec confiance au conseil d'administration, aux auditeurs et aux assureurs d'ici le 100e jour.

Voici ce que ce guide met à votre disposition :

1. Les cinq résultats qui distinguent la résilience testée de la protection supposée
2. Ce que cela signifie pour votre fonction : directeur informatique, RSSI ou DAF
3. Les sept cas d'usage couverts par votre investissement, et comment leur activation optimise votre ROI
4. Les questions pertinentes à poser à votre équipe pour vérifier que la résilience est maintenue après le centième jour

De l'exposition à la preuve : les cinq résultats qui comptent

Voici les cinq résultats auxquels votre organisation s'engage en déployant la Veeam Data Platform. Chacun d'eux représente une étape qui vous fait passer d'une simple exposition aux risques à des preuves tangibles de résilience. Ensemble, ils définissent ce qu'est un environnement dont la résilience peut être démontrée et vérifiée.

01. Sous contrôle

Vous connaissez précisément les éléments protégés, leur emplacement et le Standard appliqué. Pas d'hypothèses, pas de lacunes découvertes sous pression.

02. Protégée

Chaque workload stratégique est couvert par un plan sur lequel votre stratégie de continuité d'activité peut s'appuyer. Rien ne passe à travers les mailles du filet quand cela compte le plus.

03. Renforcée

Un attaquant ne peut pas détruire votre capacité à restaurer. Des copies inaltérables existent localement et hors site, vous offrant un point de restauration sain confirmé, indépendamment de l'évolution de l'incident.

04. Capacité de restauration démontrable

Vous pouvez prouver que la restauration fonctionne, pas seulement l'affirmer. Elle est testée, documentée et prête à être présentée à votre conseil d'administration, à vos auditeurs et à votre assureur.

05. Opérationnalisée

La résilience ne dépend pas d'une seule personne ou d'un seul effort héroïque. Il s'appuie sur une responsabilité claire, des rapports structurés et une cadence définie que votre équipe peut maintenir.

Ce que cela signifie pour votre rôle

Directeur informatique/Directeur technique

Lorsque le conseil d'administration vous demande si votre organisation peut restaurer après un incident majeur, vous avez une réponse testée et documentée. Le risque de panne n'est plus une question de confiance, mais une réalité documentée.

RSSI

Vous disposez d'un point de restauration propre et confirmé avant qu'un incident ne devienne une crise, plutôt qu'après. L'analyse des renseignements sur les menaces, les copies inaltérables et les résultats de tests documentés vous fournissent les preuves dont vos assureurs, auditeurs et équipe juridique ont besoin.

DAF

L'éligibilité à une cyberassurance, les conditions de renouvellement et les négociations sur les primes d'assurance sont plus favorables lorsque la capacité de restauration est démontrée plutôt que simplement supposée. Selon les études, les entreprises ayant investi davantage dans la résilience des données n'ont payé une rançon que dans 33 % des cas, contre 52 % pour les autres. Votre investissement dans Veeam est ciblé, prévisible et directement lié à la réduction de l'exposition financière en cas de panne imprévue.

33 %

des organisations ayant davantage investi dans la résilience des données ont versé une rançon.

52 %

des organisations n'ayant pas réalisé ces investissements ont versé une rançon.

Source : Rapport sur la confiance et la résilience des données (2026).

La valeur débloquée

La valeur délivrée par la Veeam Data Platform va bien au-delà d'un seul rôle ou d'un seul incident. Dès les 100 premiers jours, votre organisation débloque des fonctionnalités qui répondent à la véritable complexité des environnements IT modernes : infrastructure hybride, expansion du cloud, contraintes réglementaires et un paysage de menaces en constante évolution.

Ces sept cas d'usage sont au cœur de votre investissement.

Protection et restauration

Lorsqu'un incident survient, la qualité de votre réponse dépend entièrement de la qualité de votre préparation. C'est le socle dont chaque organisation a besoin, quel que soit son secteur ou son infrastructure.

1. **Détection et réponse aux menaces :** Veeam analyse les chaînes de sauvegarde à la recherche d'indicateurs de logiciels malveillants et valide l'intégrité des fichiers avant la restauration, afin que votre organisation restaure proprement plutôt que de réintroduire une menace. Les résultats documentés des analyses soutiennent votre processus de réponse aux incidents et satisfont aux exigences des assureurs.
2. **Reprise après incident vers le cloud :** Lorsque l'infrastructure sur site échoue, Veeam déplace les workloads vers des cibles cloud, conformément à vos objectifs de restauration définis. Votre équipe dispose d'un plan éprouvé et opérationnel plutôt qu'un processus manuel qui risque de ne pas tenir sous pression.

Maîtriser la conformité

La pression réglementaire et les exigences de souveraineté des données augmentent. Votre stratégie de protection des données doit suivre le rythme. Si vous opérez dans un secteur réglementé ou entrez dans un cycle d'audit, c'est là qu'il faut se concentrer en premier.

3. **Gouvernance, risques et conformité :** Veeam génère les rapports prêts à l'audit dont vos équipes de conformité et juridiques ont besoin, incluant les résultats des tests de restauration, l'inventaire de la couverture et la confirmation de la stratégie de rétention, sans nécessiter de collecte manuelle de preuves lors de l'audit.
4. **Souveraineté :** Veeam permet à votre entreprise de contrôler l'emplacement de stockage et de traitement des données de sauvegarde, en respectant les exigences de résidence des données dans toutes les juridictions, sans sacrifier la capacité de restauration.

Gérer la complexité à grande échelle

L'infrastructure moderne ne se trouve pas en un seul endroit. Votre stratégie de protection ne doit pas l'être non plus. Si vous êtes en pleine migration ou si vous exploitez déjà une infrastructure multicloud ou SaaS hybride, c'est là que se concentre le risque opérationnel.

5. **Mobilité des workloads entre les environnements :** Lorsque les workloads se déplacent entre les environnements sur site, cloud et en périphérie, Veeam déplace la protection avec elles. La couverture n'est pas interrompue lorsque votre infrastructure change.
6. **Protection multicloud :** Veeam offre des fonctionnalités de protection et de restauration homogènes sur l'ensemble des fournisseurs de cloud, supprimant ainsi le risque opérationnel lié à des outils fragmentés et à des angles morts entre les plateformes.
7. **SaaS hybride :** Les données stratégiques stockées dans les applications SaaS sont protégées en même temps que les workloads de votre infrastructure, comblant ainsi l'écart de couverture que la plupart des organisations ne découvrent qu'après un incident.

Il ne s'agit pas de fonctionnalités futures ou de modules complémentaires optionnels. Ce sont les avantages dont votre organisation bénéficie au fur et à mesure de son déploiement et de son activation, chacun réduisant une catégorie spécifique de risque et renforçant la confiance de votre équipe de direction lorsque la pression est à son comble. La question n'est pas de savoir si votre organisation a besoin d'un tel niveau de résilience ; c'est la rapidité avec laquelle vous pouvez y arriver.

Le jour 100 n'est pas la ligne d'arrivée. C'est la référence de base. La résilience est une pratique, pas un projet.

Veeam fournit la Veeam DataAI Command Platform, le modèle éprouvé de maturité de confiance en matière de données et d'IA, ainsi que l'expertise technique nécessaire pour guider votre équipe depuis le premier déploiement jusqu'à la résilience pleinement démontrée. Nous sommes là pour vous aider à chaque étape.

Assurez-vous que votre équipe dispose du guide technique des 100 premiers jours et commencez à vous aligner sur la portée, le calendrier et les résultats du déploiement.

La résilience à ce niveau n'est pas une ambition à long terme. Avec le bon plan de déploiement, c'est la réalité à court terme de votre organisation.

À vous de jouer.

Questions importantes à poser régulièrement à votre équipe

- Tous les workloads stratégiques sont-ils couverts, et des lacunes ou défaillances de protection sont-elles restées non résolues ?
- Quand avons-nous testé une restauration complète en conditions réelles pour la dernière fois, et disposons-nous de résultats documentés à l'appui ?
- Si une attaque par ransomware survenait ce soir, serions-nous en mesure d'identifier un point de restauration propre et validé, puis de restaurer nos systèmes sans payer de rançon ?
- Nos équipes juridiques et de conformité peuvent-elles produire des éléments probants sans effort manuel, et notre architecture respecte-t-elle toujours nos obligations réglementaires actuelles ?
- Qui dispose d'un accès en tant qu'administrateur à notre environnement de sauvegarde, et quand avons-nous effectué une revue de ces accès pour la dernière fois ?

À propos de Veeam Software

Veeam, acteur de référence de la confiance des données et de l'IA, est une société spécialisée dans l'aide aux organisations pour garantir que leurs données et leur IA sont pleinement comprises, sécurisées et résilientes, afin de pouvoir accélérer leur innovation en matière d'IA sécurisée à grande échelle. En tant que leader du marché en matière de résilience des données et de gestion de la posture de sécurité des données, Veeam est conçu pour la convergence de l'identité, des données, de la sécurité et des risques liés à l'IA. Le siège de Veeam se trouve à Seattle et la société possède des bureaux dans plus de 30 pays. Veeam protège plus de 550 000 clients dans le monde, dont 82 % des sociétés du Fortune 500. En savoir plus sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.

En savoir plus : veeam.com

