



La résilience des données est un impératif pour les entreprises d'aujourd'hui

Le modèle de maturité de la résilience des données de Veeam guide les entreprises sur la voie de la réduction des risques



Quoi et pourquoi : le modèle de maturité de la résilience des données

Alors que les entreprises continuaient à chercher à améliorer la résilience des données en 2024, les cadres dirigeants pensaient souvent à tort que leurs organisations se situaient déjà bien au-dessus de la moyenne en termes d'efficacité de leur personnel, de leurs processus et de leurs technologies. Voyant cet état d'esprit comme une tendance inquiétante, Veeam a mis sur pied un consortium d'experts du secteur afin de quantifier la situation globale des entreprises et de formuler des recommandations consensuelles sur la manière de progresser vers une meilleure résilience des données. Cette enquête révèle que près des trois quarts des entreprises ne sont pas prêtes à réagir en cas de panne. Ce niveau d'excès de confiance a conduit les organisations à sous-estimer leur résilience réelle, ce qui les rend vulnérables.

Le modèle de maturité de la résilience des données de Veeam (DRMM) vise à fournir aux entreprises les informations nécessaires pour les aider à se remettre des interruptions, optimiser leurs ressources et assurer la continuité de leurs opérations. Alors que la résilience des données était autrefois considérée comme une fonction de la seule sauvegarde, les stratégies de sauvegarde traditionnelles s'avèrent insuffisantes face à l'évolution des cybermenaces, aux pressions réglementaires et à la complexité croissante des écosystèmes de données. Assurer une véritable résilience des données nécessite une approche structurée et transversale qui intègre les efforts IT, de sécurité et de conformité dans une stratégie cohérente.

La plupart des entreprises font preuve d'une confiance excessive dans la résilience de leurs données.

30 %+

des entreprises estiment être plus résilientes que leurs fonctionnalités comparées réelles

74 %

sont exposées à des risques liés à la restauration des données



Le schéma directeur de la protection des données

Le modèle de maturité de la résilience des données (DRMM) de Veeam fournit une infrastructure empirique qui permet aux entreprises d'évaluer leur résilience actuelle, d'identifier les lacunes et de mettre en œuvre des améliorations ciblées. Veeam a développé le modèle DRMM en collaboration avec McKinsey, Palo Alto Networks et Splunk, en s'appuyant sur les contributions de plus de 500 cadres dirigeants. Les résultats indiquent que 74 % des entreprises n'utilisent pas ne serait-ce que la moitié des meilleures pratiques identifiées par la recherche sur la résilience, ce qui entraîne une augmentation des risques financiers, opérationnels et de conformité. Le DRMM fournit une approche structurée pour aligner les stratégies commerciales et technologiques, renforcer la gestion des risques et améliorer les fonctionnalités de restauration à grande échelle. En s'appuyant sur ce modèle, les entreprises peuvent passer d'une réponse réactive aux crises à une résilience proactive, pour s'assurer que les données restent un catalyseur de croissance plutôt qu'un point de défaillance.

Les résultats de l'étude montrent que les meilleurs acteurs connaissent généralement :

7 fois

vitesse de restauration plus rapide (MTTR)

4 fois

moins de pertes de données (RPO)

3 fois

moins de temps d'arrêt (RTO)

~10 %

taux de croissance moyen du chiffre d'affaires plus élevé

Dimensions du modèle

Lorsque la société Veeam a décidé d'élaborer le modèle DRMM, elle s'est entourée des plus grands experts de l'efficacité opérationnelle. McKinsey & Company a dirigé les efforts visant à créer un cadre rigoureux et indépendant des fournisseurs. Ce modèle a été conçu pour évaluer la capacité d'une entreprise à assurer la résilience de ses données dans trois dimensions principales.



Stratégie : aligner les aspects métier et les risques

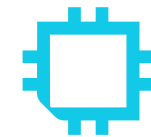
Une stratégie de données claire intègre les **objectifs métier à la planification** de la résilience, pour garantir que les organisations peuvent anticiper les menaces, renforcer la gouvernance et maintenir la conformité.



Personnes et processus : renforcer la résilience par l'alignement et l'action

La véritable résilience repose sur des équipes responsabilisées et une exécution standardisée. En investissant dans des talents qualifiés, un leadership aligné et des protocoles interfonctionnels clairs, les organisations peuvent réagir de manière décisive dans les moments de perturbation.

Des workflows définis et une gouvernance assurent la continuité, tandis que la collaboration et la formation permettent aux équipes de s'adapter et de restaurer rapidement en toute confiance.



Technologie : la pierre angulaire de la résilience

La technologie soutient la résilience dans six domaines clés :

- **Sauvegarde** : protection sécurisée des données en local ou dans plusieurs clouds.
- **Restauration** : restauration agile des systèmes critiques, même à grande échelle.
- **Architecture et portabilité** : évolutivité dans des environnements hétérogènes et souvent hybrides.
- **Sécurité** : prévention et remédiation anticipée contre les cybermenaces.
- **Rapports et renseignements** : visibilité et informations en temps réel pour renforcer la conformité, améliorer la restauration et optimiser les opérations.

En intégrant **stratégie, personnes, processus et technologies**, les entreprises peuvent **réduire les risques, accélérer la restauration et renforcer la résilience à long terme.**

Les quatre horizons de la maturité de la résilience des données

À l'aide de données de l'étude couvrant les principales catégories (stratégie, personnel, processus et six disciplines technologiques sous-jacentes) (sauvegarde, restauration, architecture, sécurité, reporting et renseignements), le DRMM aide les entreprises à évaluer leur capacité à s'assurer que leurs processus métier dépendants de l'informatique sont résilients. Cette évaluation place les organisations dans l'un des quatre horizons de chaque vecteur (et globalement), en fonction de leur niveau de maturité en matière de résilience ainsi que des possibilités d'amélioration :

Basique

Révèle une base avec d'importantes possibilités d'amélioration.

Intermédiaire

Les performances d'une entreprise sont au-dessus du minimum, mais il est probable qu'elles utilisent majoritairement des processus manuels ou des augmentations ad hoc. Il y a encore beaucoup de choses à améliorer, mais l'organisation peut manquer de conscience de ce qui est possible et de ce qui vaut la peine d'être fait.

Avancé

L'organisation commence à passer d'une approche tactique à une approche stratégique et, dans certains cas, elle est plus proactive que réactive. Ils ont investi dans un meilleur personnel et de meilleurs processus et disposent d'une voie vers de meilleurs résultats et avantages.

Le meilleur de sa catégorie

Que ce soit dans le cadre de scénarios d'utilisation spécifiques ou à tous les niveaux, une entreprise exécute des environnements de premier ordre qui résultent sans aucun doute autant du personnel et des processus que des technologies qu'ils ont choisi d'exploiter.

74 %

des organisations se classent en catégories de base et intermédiaires, ce qui met en évidence des possibilités d'amélioration majeures

44 %

30 %

18 %

8 %

Self-optimizing

Le meilleur de sa catégorie

Mature & Adaptive

Avancé

Reliable But Limited

Intermédiaire

Reactive & Manual

Basique

Principaux avantages du DRMM

Utiliser un modèle orienté secteur basé sur des recherches indépendantes peut s'avérer très utile pour les entreprises qui cherchent à évaluer et renforcer leur posture de résilience des données. Voici quelques-uns des avantages du modèle de maturité :

Protection des revenus

Renforcer la faisabilité commerciale et la défense concurrentielle en répondant aux besoins du marché et en fournissant des produits fiables.

Optimisation des coûts

Minimiser les inefficacités, les dépenses informatiques et les coûts liés aux incidents en optimisant l'exploitation, l'infrastructure et la gestion des risques.

Conformité et gestion des risques

Réduire les risques juridiques, réglementaires et commerciaux en minimisant les cyberincidents, les pertes de données et les coûts associés.

Intégrité de la marque et confiance des consommateurs

Protéger la réputation et la confiance des clients grâce à la fiabilité, la disponibilité et un positionnement fort sur le marché.



Pour en savoir plus sur les [cas clients](#) réels de Veeam, cliquez ici.

Élément de preuve

Global Bank améliore la protection de ses revenus grâce à une meilleure résilience

Une banque mondiale qui a suivi les recommandations du modèle de maturité a bénéficié des avantages suivants :

99,99 %

Temps de fonctionnement des applications stratégiques

ZÉRO

Pannes liées à la cybersécurité au cours des trois dernières années.

300 000 \$

Économies par panne grâce à la réduction du MTTR pour les systèmes informatiques critiques

Progresser « vers le haut et vers la droite » dans la maturité de la résilience des données



Une fois que le DRMM a révélé l'état de résilience d'une entreprise, il prescrit également les méthodes et les avantages de progresser par rapport aux conséquences de rester dans l'état actuel. À ce stade, il est temps d'envisager la mise en œuvre des étapes nécessaires pour passer d'un horizon à l'autre en examinant de plus près les indicateurs clés de performance et d'autres métriques de performance pour donner un aperçu de la performance de l'entreprise.

Stratégie

Pour qu'une stratégie de résilience des données soit efficace, les entreprises doivent se demander dans quelle mesure les personnes (dirigeants et équipes), les processus (internes et externes) et la myriade de technologies sont alignés pour atteindre les résultats souhaités.

Personnes et processus

- La direction et les membres du conseil d'administration ont-ils pu superviser et rendre obligatoire la résilience des risques et la gestion des données ?
- Les équipes fonctionnelles sont-elles identifiées pour chacun des domaines technologiques et alignées sur les processus et la stratégie globaux de résilience des données ?
- La direction oblige-t-elle les équipes à être prêtes à exécuter une planification objective et intégrée, des exercices de simulation et une préparation au monde réel ?

Technologie

- L'architecture de sauvegarde des données assure-t-elle une protection complète dans l'ensemble de l'entreprise hétérogène et permet-elle l'inaltérabilité et le respect des règles ?
- Les technologies de restauration des données permettent-elles des restaurations agiles depuis des environnements de production et de protection hétérogènes vers d'autres plateformes à grande échelle ?
- Les technologies de sauvegarde et de sécurité sont-elles inclusives pour assurer une résilience efficace à l'ensemble des clouds hybrides hétérogènes, notamment en ce qui concerne la portabilité des workloads dans toute l'entreprise ?
- **Sécurité des données** : les technologies de sécurité des données s'intègrent-elles à la sauvegarde et à la restauration de manière à aligner la résilience proactive, la prévention proactive et la résilience réactive au sein des équipes et des politiques ?
- Les technologies de production de rapports sur les données offrent-elles une visibilité adéquate, une prévention proactive et une gouvernance adéquates ?

L'intelligence des données est-elle intégrée à toutes les piles technologiques du modèle de résilience des données et l'accélère-t-elle ?

Une approche prescriptive pour favoriser l'amélioration continue

Le DRMM est fondé sur des concepts avec lesquels certains dirigeants sont intrinsèquement d'accord, mais étonnamment, peu d'organisations adoptent ces idées dans leur stratégie et leurs processus de base.

Pas de panique, préparez-vous

Ne commencez pas par le datacenter ; commencez par la salle de conférence. Pour améliorer la résilience de la plupart des entreprises, la clé réside souvent dans l'inclusion d'un plus grand nombre de personnes (parties prenantes et responsables de la mise en œuvre, par exemple) et dans la mise en œuvre de meilleurs processus. Parmi les étapes suivantes à suivre pour élever le niveau d'une entreprise, citons l'implémentation de processus et de pratiques proactives au-delà des bases fondamentales.

Qui d'autre devrait se joindre à la table ?

Comme évoqué plus haut, la résilience des données ne se limite pas à l'informatique. C'est pourquoi les entreprises doivent mobiliser un plus grand nombre de parties prenantes, aux côtés du DSI et du RSSI. En élargissant considérablement les types de parties prenantes de haut niveau qui ont un intérêt direct dans la résilience des données de la société, comme les directeurs de la gestion des risques et les directeurs des données, une

société peut recueillir une évaluation plus large sous différents angles. Cela permet de s'assurer que les stratégies qui en résultent tiennent compte des besoins de l'ensemble de l'organisation, ce qui contribue à assurer le soutien nécessaire pour progresser vers une meilleure résilience.

Aligner la stratégie de données, les personnes, les processus et la technologie

Une fois que toutes les différentes parties prenantes sont dans la pièce, le DRMM est un moyen de les présenter les unes aux autres et de travailler ensemble. Au cours de ces séances de travail DRMM, de nombreuses équipes découvrent qu'elles travaillent en silos et que certaines personnes d'une même entreprise font un travail complémentaire ou contre-productif dans d'autres départements. Ainsi, en réunissant tous ces différents points de vue dans une même pièce avec un objectif commun, les organisations peuvent bien comprendre la réalité de leur situation et être mieux préparées à passer d'un horizon à l'autre.



De la fondation à la révolution : améliorer la résilience des données de votre entreprise

La résilience n'est pas une initiative ponctuelle. C'est un continuum de maturité qui oblige les entreprises à évaluer leur stratégie, leur personnel, leurs processus et leurs technologies de données de manière holistique. Que vous établissiez des pratiques fondamentales, que vous optimisiez les flux de travail existants ou que vous repoussiez les limites de l'innovation, voici comment passer à l'étape suivante.

Fondation

Construire l'infrastructure de base de la résilience

- Définissez une stratégie claire de résilience des données, avec un leadership dédié et des objectifs mesurables.
- Mettez en place des processus de gestion des incidents et des changements qui alignent les équipes chargées de la sécurité, de l'informatique et des données.
- Standardisez les bases de référence de sauvegarde, de restauration et de sécurité pour limiter les risques sur l'ensemble des systèmes stratégiques.

Évolution

Étendre la résilience au-delà de la conformité à des opérations proactives, automatisées et évolutives

- Effectuez des analyses annuelles de l'impact sur les opérations afin d'affiner la tolérance au risque et de suivre les améliorations.
- Mettez en œuvre une formation interfonctionnelle sur la réponse aux incidents, y compris des simulations et des jeux de guerre.
- Automatisez la gouvernance des données et le suivi de leur restauration pour garantir l'application des politiques dans toutes les unités opérationnelles.

Révolution

Assurer la résilience à l'échelle de l'entreprise en intégrant l'intelligence, l'automatisation et le leadership stratégique

- Nommez un responsable de la résilience pour mener une approche cohérente et alignée sur l'entreprise.
- Développez une stratégie de restauration de bout en bout, incluant la mobilité des workloads multcloud et l'évaluation des risques pilotée par intelligence artificielle.
- Déployez une supervision et une analyse prédictive en temps réel pour anticiper et prévenir les défaillances avant qu'elles ne surviennent.

Le parcours de chaque organisation sera différent. Certaines peuvent nécessiter des efforts de remédiation, tandis que d'autres sont prêtes pour des stratégies avancées. Où en est votre organisation aujourd'hui et comment pouvez-vous passer à l'étape suivante ?

Comment **Veeam** peut vous aider

Veeam a pris l'initiative d'associer McKinsey et ses partenaires, ainsi que des experts du secteur informatique, au développement du modèle DRMM. Le DRMM fournit des conseils prescriptifs sur la manière dont les entreprises peuvent améliorer la résilience de leurs données, en mettant l'accent sur des fonctionnalités supplémentaires susceptibles d'améliorer la résilience d'une organisation. Ces recommandations sont indépendantes des fournisseurs en raison de la nature originale du modèle. Pour les y aider, Veeam peut formuler des recommandations spécifiques issues de son portefeuille de produits et de services qui s'alignent sur les directives du DRMM. Veuillez contacter votre partenaire Veeam ou votre responsable de compte Veeam pour en savoir plus.

➔ **Pour plus d'informations sur les solutions pour les grandes entreprises de Veeam, [cliquez ici.](#)**

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](https://www.linkedin.com/company/veeam) et X [@veeam](https://twitter.com/veeam)