

Les angles morts de la modernisation

Voir clairement dans
un paysage mouvant



Introduction

La modernisation ne se limite plus à définir où les workloads s'exécutent ; elle façonne également la manière dont les applications sont exploitées, sécurisées, gouvernées et restaurées.

Ce qui a commencé comme une stratégie d'efficacité de l'infrastructure est maintenant la colonne vertébrale de l'informatique moderne. Les workloads se déplacent désormais de façon fluide à travers le cloud, les conteneurs et les environnements traditionnels, ce qui augmente la flexibilité — mais aussi la complexité. Ajoutez à cela des architectures pilotées par l'intelligence artificielle et des exigences croissantes en matière de sécurité et de conformité, et les enjeux opérationnels augmentent rapidement.

Il s'agit d'un processus complexe, et entamer puis faire évoluer votre parcours de virtualisation confère à vous et à vos équipes à la fois des **opportunités** et des **responsabilités**.



Opportunité : Construire des systèmes plus intelligents et plus adaptatifs qui évoluent avec votre entreprise.



Responsabilité : Identifier et combler les **angles morts** qui érodent discrètement la résilience.

Reconnaître les angles morts à un stade précoce peut transformer la modernisation d'une course effrénée en une évolution délibérée et continue.

Une virtualisation moderne correctement réalisée n'est pas seulement efficace ; elle est résiliente dès sa conception.

Dans cet e-book, nous explorerons les angles morts les plus courants de la virtualisation, pourquoi ils sont faciles à ignorer et comment développer une résilience des données qui s'étend à toutes les plateformes, applications opérations que vous gérez.

Pour se moderniser efficacement, les entreprises doivent comprendre où apparaissent les angles morts :

1. Architecturalement
2. Opérationnellement
3. Organisationnellement



Du mythe à la méthode : ce que signifie vraiment la virtualisation moderne

Gagner en clarté et en visibilité sur l'ensemble de votre environnement est tout aussi important (si ce n'est plus) que la technologie que vous choisissez.

La virtualisation a beaucoup évolué depuis la simple fusion des serveurs. Elle s'étend désormais aux hyperviseurs, aux clouds et aux conteneurs, créant un écosystème dynamique qui exige de nouvelles façons d'opérer, de sécuriser et de restaurer les workloads. Malgré cela, de nombreuses organisations abordent encore la virtualisation moderne sous l'angle d'hypothèses dépassées qui augmentent les risques et la complexité au lieu de les réduire.

Mythes courants (et ce qui est réellement vrai)



Mythe : la virtualisation basée sur le cloud est toujours plus facile.



Réalité : Cela dépend de votre environnement. Les modèles multicloud et hybrides peuvent rapidement devenir complexes lorsque les machines virtuelles (VM), les conteneurs et les outils de protection des données ne sont pas alignés.



Mythe : Les snapshots sont identiques aux sauvegardes.



Réalité : Bien qu'utiles, les snapshots ne constituent pas une stratégie de résilience. La restauration moderne exige la rétention, l'inaltérabilité, des fonctionnalités hors site et des restaurations cohérentes au niveau des applications — et pas seulement la possibilité de revenir en arrière.



Mythe : Avec la virtualisation moderne, tout doit être remplacé d'un seul coup.



Réalité : Ce n'est pas une approche du tout ou rien. Une virtualisation réussie évolue grâce à des choix délibérés et incrémentiels qui s'adaptent à vos workloads et aux besoins de votre activité.



Mythe : Exécuter des VM dans le cloud public signifie que mes données sont automatiquement sauvegardées.



Réalité : Selon le modèle de partage des responsabilités, vous êtes toujours responsable de vos propres données. Le cloud fournit l'infrastructure, mais vous devez encore en assurer la restauration.



Mythe : Les conteneurs offrent la portabilité des applications partout.



Réalité : Les workloads conteneurisés nécessitent toujours une protection et une gouvernance, comme toute autre infrastructure. La portabilité n'est pas synonyme de résilience, et ce sont les opérations du Jour 2 qui mettent cette résilience le plus à l'épreuve.

La virtualisation moderne n'est pas un saut isolé ; c'est une série d'étapes ciblées qui alignent les plateformes, les compétences et les stratégies de protection. Les organisations qui font la distinction entre le battage médiatique et la réalité peuvent construire des environnements qui non seulement exécutent des applications modernes, mais les protègent avec assurance au fur et à mesure de leur évolution.

Ces mythes persistent parce que la modernisation de la virtualisation est souvent perçue comme une simple mise à niveau technologique, alors qu'elle est en réalité une **stratégie opérationnelle** qui redéfinit la façon dont les personnes, les processus et les plateformes travaillent ensemble.

Ce que les organisations cherchent réellement à accomplir

La virtualisation moderne ne consiste pas à courir après la plateforme ou la tendance la plus récente. Il s'agit d'atteindre les résultats qui comptent le plus, c'est-à-dire innover rapidement, passer à l'échelle avec intelligence et automatisation, et dépenser efficacement.

Dans l'ensemble des secteurs, les équipes informatiques subissent une pression constante pour offrir de nouvelles expériences numériques sans compromettre la sécurité, la conformité ou les performances, et c'est grâce à la virtualisation qu'elles parviennent à suivre le rythme. La modernisation des applications et de l'infrastructure offre la flexibilité nécessaire pour faire évoluer les workloads, adopter de NOUVELLES technologies, intégrer des pipelines d'IA et se préparer à ce qui viendra ensuite.

Les organisations les plus performantes considèrent la virtualisation moderne comme un moyen d'**aligner l'informatique sur les objectifs de l'entreprise**, et non comme une simple idéologie technologique. L'automatisation, l'orchestration et la micro-segmentation ne sont pas des fins en soi : ce sont

des leviers qui permettent d'augmenter la vélocité, de réduire les risques et de créer de la valeur plus rapidement que les concurrents.

Essentiellement, la modernisation ne concerne pas l'emplacement des applications, mais la façon dont ces environnements permettent l'agilité, l'efficacité et l'innovation. Cet alignement dépend de la visibilité et de la protection. Cela signifie savoir ce que vous avez, où il se trouve et comment il peut être restauré au fur et à mesure que des changements se produisent.

Cet alignement entre les objectifs métier et les capacités opérationnelles dépend d'une protection renforcée et d'opérations simplifiées. La visibilité et la résilience transforment la modernisation d'une simple actualisation technologique en un véritable avantage stratégique.



Déclencheurs, compromis et conséquences de la modernisation

Chaque parcours de virtualisation commence par un déclencheur, un moment où le changement devient inévitable.

Peut-être que les systèmes existants ne suffisent plus à votre entreprise. Peut-être que la pression concurrentielle exige désormais une innovation plus rapide. Peut-être qu'une fusion, un dessaisissement ou une nouvelle obligation de conformité vous oblige à revoir le fonctionnement de votre infrastructure.

Chaque déclencheur est porteur à la fois d'urgence et d'opportunité. C'est l'occasion de bâtir des fondations plus intelligentes et plus solides pour l'avenir, plutôt que de simplement colmater les failles.

Au fil du temps, ces angles morts ne se contentent pas de perturber les opérations. Ils sapent la confiance de vos clients, des autorités de contrôle et même de vos propres équipes.

Cependant, lorsque le changement s'accélère, la complexité se cache dans les espaces entre les plateformes, les équipes et les outils. Ces lacunes invisibles peuvent rapidement devenir **des angles morts** et :

1. Amplifier l'impact des temps d'arrêt.
2. Ralentir et compliquer la restauration.
3. Affaiblir la sécurité et la conformité.
4. Créer des lacunes en matière de gouvernance qui apparaissent lors d'audits ou d'incidents

L'objectif n'est pas d'éviter toutes les conséquences, c'est de s'y préparer. La confiance vient de la prévoyance, de la compréhension des enjeux, de l'anticipation de ce qui pourrait mal tourner et de l'intégration de la résilience dans chaque couche de votre environnement.

C'est ainsi que les organisations modernes peuvent transformer le changement d'infrastructure en un avantage durable plutôt qu'en un risque récurrent.



Il existe de nombreuses voies valables pour la modernisation

Aucun parcours de virtualisation moderne ne se ressemble, et c'est bien là tout l'intérêt.

Chaque organisation avance à son propre rythme et dans une direction dictée par ses priorités commerciales, sa maturité technique et sa tolérance au risque.

Certains adoptent une stratégie **cloud-first** ou **cloud native**, tandis que d'autres privilégient la **consolidation hybride** ou la combinaison d'une infrastructure moderne avec des investissements existants. Certains unifient sous une **pile d'un seul fournisseur** qui couvre les VM et Kubernetes. D'autres adoptent les conteneurs **de façon incrémentale**, en partant d'une fondation axée sur la virtualisation, tandis que d'autres **maintiennent délibérément le cap**, alignant leur transformation sur le calendrier qui a le plus de sens pour leur entreprise. Ces voies offrent une perspective, pas une prescription. Ce qui compte le plus, c'est la préparation, la compréhension d'où vous êtes, où vous allez et la façon de renforcer votre résilience en cours de route.

Cependant, chaque nouvelle plateforme, chaque nouvel outil ou chaque nouvelle approche augmente le risque de **fragmentation des données**. Lorsque les données deviennent cloisonnées à travers les clouds, les clusters et les environnements virtuels, la visibilité diminue, les écarts de protection se creusent et les angles morts s'étendent à travers les environnements.

Plus il y a de chemins, plus la complexité opérationnelle augmente, et cette complexité accrue exige un niveau de résilience des données plus élevé.



La modernisation réussit lorsque la prise de conscience se transforme en action, ou lorsque les organisations transforment leurs connaissances en systèmes unifiés capables de s'adapter, de se restaurer et de se développer sans perdre le contrôle de leurs données.



La modernisation s'opère à travers de nombreux modèles cloud

La modernisation ne consiste pas à choisir une plateforme ou un mode de cloud ; il s'agit d'apprendre à fonctionner sur plusieurs d'entre eux à la fois.

Alors que les sections précédentes ont exploré les différentes voies que les organisations peuvent emprunter pour se moderniser, les modèles cloud décrivent comment les applications sont développées, déployées et consommées tout au long de ce parcours. La plupart des environnements modernes ne sont pas purement IaaS, PaaS ou SaaS. Ils constituent un mélange, façonné par les besoins des workloads, les réalités opérationnelles et les priorités de l'entreprise.

Une voie stratégique

Les VM, les conteneurs et les services cloud coexistent souvent dans des datacenters sur site et plusieurs clouds publics. De plus en plus, cela inclut également les emplacements périphériques où les données sont créées et exploitées en temps réel. Ce modèle mixte donne aux entreprises la liberté d'exécuter leurs workloads là où cela est le plus pertinent.

La virtualisation moderne rend cette flexibilité possible. C'est la couche qui rassemble les workloads hétérogènes, unifie la gestion et ancre la modernisation dans la réalité concrète, permettant ainsi aux organisations d'innover plus rapidement et d'optimiser leur montée en puissance sans repartir de zéro.

La réalité opérationnelle

D'un point de vue opérationnel, cette même flexibilité s'accompagne également de complexité. Les workloads se déplacent, les données sont distribuées, et des écarts de protection apparaissent dans les espaces entre les environnements virtuels et cloud.

Les modèles de protection uniformes ne fonctionnent pas non plus lorsque vous travaillez avec un mélange d'environnements. Chaque système évolue et change différemment, ce qui signifie que la résilience doit être conçue pour accompagner cette évolution. Une approche « add-on » — greffer des outils traditionnels sur des plateformes modernes — ajoute malheureusement plus de frictions et de risques. Cette diversité est aujourd'hui la norme. Elle apporte flexibilité

et choix, mais exige aussi une approche plus intentionnelle de la résilience.

Les organisations prospères ne cherchent pas à éliminer la complexité ; elles conçoivent en tenant compte de celle-ci. En reconnaissant la diversité des plateformes, des modèles cloud et des types de workloads en jeu, ils élaborent des stratégies de protection capables de s'adapter à l'évolution des architectures, garantissant que la modernisation reste soutenable, sécurisée et résiliente dans le temps.



Repenser ce que signifie réellement la protection moderne des données

La protection moderne des données va bien au-delà de la simple sauvegarde ou de la couverture de l'infrastructure.

Pour les applications modernes, la résilience doit couvrir les clouds, les clusters Kubernetes et les systèmes hybrides. Autrement dit, ces environnements devraient être capables de protéger non seulement l'endroit où les applications résident, mais aussi la manière dont elles fonctionnent.

En pratique, la protection moderne des données doit exceller dans quatre domaines :



Assurer une visibilité complète dans l'environnement, y compris les applications, les données, l'infrastructure et les interdépendances.



Appliquer une gouvernance et des politiques cohérentes à l'ensemble des applications, plateformes et environnements.



Automatiser une restauration fiable pour garantir des restaurations rapides et prévisibles lorsque cela compte le plus.



Démontrer une préparation continue pour répondre aux exigences en matière de sécurité, de conformité et d'audit.

La protection moderne des données est **adaptée au cloud et aux conteneurs, centrée sur les applications et basée sur les stratégies**, plutôt que maintenue manuellement. Elle est conçue pour la mobilité et l'évolutivité, pas pour une infrastructure statique. Ce type de résilience s'appuie sur une restauration orchestrée et automatisée pour maintenir l'activité des

entreprises et maintenir la préparation non seulement face aux menaces de ransomware, mais aussi pour les audits de conformité et la continuité des opérations.

Les approches traditionnelles, conçues pour des workloads stables et isolées, peinent à suivre le rythme. À mesure que les workloads virtualisées et conteneurisées gagnent en dynamisme, la protection doit devenir **intelligente et intégrée** afin de pouvoir voir votre environnement entier, appliquer la gouvernance automatiquement et restaurer avec précision en cas de perturbation.

En bref, la protection moderne des données ne consiste pas seulement au stockage de copies ; il s'agit de maintenir la confiance. C'est le fondement qui maintient un paysage de virtualisation diversifié résilient, conforme et prêt pour tout ce qui peut arriver.



Élaboration d'un cadre décisionnel pratique

Il n'existe pas de schéma unique à suivre en matière de modernisation. Votre objectif ultime est la clarté, pas la conformité.

La mise en place d'un cadre décisionnel pratique vous permet de visualiser précisément où vous en êtes aujourd'hui, d'identifier les voies de modernisation les mieux adaptées à votre entreprise et de comprendre ce que chaque choix possible implique pour vos opérations, votre visibilité, votre contrôle et votre restauration.

Un cadre pratique aide les organisations à évaluer :

- La combinaison de workloads (par exemple, VMs, conteneurs, services gérés)
- Objectifs de restauration (délai optimal de reprise d'activité et objectif de temps de restauration (RPO/RTO))
- Modèle opérationnel (p. ex., équipes centralisées ou distribuées)
- Exigences en matière de risque et exigences de conformité
- Besoins de portabilité entre les environnements

Certaines organisations sont déjà avancées dans l'adoption du cloud natif. D'autres continuent à fonctionner principalement sur des plateformes virtualisées ou hybrides. Ces deux approches sont valables. L'important est de savoir comment chaque modèle façonne vos exigences en matière de protection des données et de résilience afin de prendre la bonne décision pour votre propre environnement.

Il n'existe pas de voie unique « correcte » — seulement des voies informées. Les organisations qui abordent la modernisation avec des analyses structurées peuvent anticiper la complexité, concevoir leur stratégie pour une résilience

maximale et s'adapter avec confiance et à un rythme maîtrisé à mesure que leurs besoins évoluent.

Les stratégies les plus efficaces commencent par la compréhension, et non par l'urgence. Ils considèrent la protection des données comme **une partie continue et délibérée du progrès**, et non comme une case à cocher, ni comme une réflexion après coup.



La modernisation réussit lorsque la clarté guide chaque décision, et que la visibilité, le contrôle et la restauration restent connectés, quelle que soit l'évolution de vos applications et de votre infrastructure.



Une vérité universelle : chaque parcours de modernisation exige une protection des données

Les applications modernes exigent une résilience moderne.

Elles fonctionnent dans des environnements virtuels distribués, se déplacent entre les clouds et dépendent d'une disponibilité constante pour fournir de la valeur métier. Cela fait de la résilience non seulement un objectif technique, mais aussi un impératif métier.

Quel que soit le mode de modernisation de votre organisation — par la virtualisation, l'adoption du cloud natif ou la consolidation hybride — une vérité demeure : **la protection des données n'est pas négociable.**

Les applications doivent rester protégées contre toute interruption, et vos données doivent pouvoir être restaurées. La restauration doit fonctionner lorsque cela est crucial, et la gouvernance doit rester constante sur toutes les plateformes.

La modernisation ne remplace pas les principes fondamentaux de la résilience ; elle en amplifie l'importance. Plus votre environnement devient dynamique et distribué, plus la visibilité, le contrôle et la restauration sont essentiels pour maintenir la confiance et la continuité.



Les organisations performantes intègrent la protection à chaque étape de leur parcours de modernisation. La virtualisation moderne constitue une fondation qui permet à l'innovation de rester sécurisée, durable et prête à relever les prochains défis.



Favoriser la modernisation, sans imposer la trajectoire

Chaque organisation a son propre parcours de modernisation, et c'est exactement ainsi que cela doit se passer.

Un véritable partenariat consiste à rencontrer les clients où qu'ils se trouvent au cours de leur parcours, et non à leur dicter où ils doivent aller.

C'est là que Veeam fait la différence.

Veeam est **agnostique en matière de plateformes**, conçu pour fonctionner de manière transparente avec les technologies en lesquelles votre organisation a confiance — couvrant les clouds, Kubernetes et les environnements virtuels.

Il aide les équipes à moderniser à leur propre rythme en garantissant une résilience et une protection des données constantes, quelle que soit la mixité des plateformes ou la rapidité avec laquelle les choses évoluent. Avec Veeam, vous réduisez le verrouillage inutile et maintenez votre flexibilité à mesure que les plateformes évoluent, sans perdre le contrôle.

Le résultat est la liberté, la possibilité de choisir la voie qui convient le mieux à votre entreprise, en sachant que vos données, vos applications et vos opérations sont protégées à chaque étape.



Veeam soutient la modernisation selon vos propres modalités. En maintenant une résilience constante, Veeam agit comme une force stabilisatrice et une couche de fiabilité qui assure une progression régulière, sécurisée et préparée à l'avenir.

