Qu'est-ce qui tombe réellement en panne lorsque les applications modernes sont défaillantes ?

Les applications modernes évoluent vite. Les pannes évoluent encore plus vite. La résilience assure la continuité de votre activité.

Les défaillances des applications modernes ne sont pas seulement des événements de pertes de données. Lorsqu'un problème survient, il s'agit rarement d'un incident isolé. Souvent, il s'agit d'une rupture de dépendance, d'une erreur de configuration, d'un problème de déploiement, d'une perte de visibilité ou de tout autre élément qui joue en votre défaveur.

Ce qui casse et comment y remédier



POURQUOI LES APPLICATIONS MODERNES TOMBENT EN PANNE

Les applications modernes fonctionnent sur une infrastructure distribuée — et non monolithique —. Ces environnements distribués offrent une agilité accrue et des cycles de développement plus courts, mais ils introduisent également une nouvelle complexité et des risques de défaillance qui dépassent les limites des stratégies de protection traditionnelles.

Ces stratégies sont conçues pour les pannes qui touchent un serveur, mais peu d'utilisateurs. Malheureusement, cela rienglobe pas l'ampleur des pannes modernes, qui peuvent avoir des répercussions sur des centaines d'utilisateurs et de dépendances.

UNE NOUVELLE APPROCHE DE LA RÉSILIENCE

Étant donné que les composants des applications modernes dépendent les uns des autres, les changements comportent des risques. Il est important de comprendre ces risques.

Avec l'essor de l'IA et des environnements hybrides, adopter une approche systémique est essentiel. Pour obtenir les meilleurs résultats, les organisations doivent protéger leur parc applicatif entier. Cela doit englober les données, les configurations, les politiques, les dépendances, les métadonnées et le contexte.

La proactivité compte aussi, car les lacunes de résilience peuvent rester cachées jusqu'à ce qu'un incident se produise. Des outils d'analyse intelligente de la santé du système vous permettent de détecter ces lacunes avant qu'elles ne deviennent un problème.

Les applications modernes sont confrontées à des interruptions de fonctionnement fréquentes.

Plus de 2/3
des organisations perdent plus de 300000 $ par heure lors d'incidents informatiques.
* PagerDuty 2026 State of AI-First Operations Report

54%
des victimes de ransomware ont utilisé des sauvegardes pour restaurer des données chiffrées au cours de l'année écoulée.
* Sophos : État du ransomware 2025

2 millions $
par heure est le coût médian des pannes informatiques à fort impact.
* New Relic 2025 Observability Forecast



Les interruptions surviennent rapidement

01
Dépendance rompue
Les dépendances des applications échouent. Il suffit qu'un seul service tombe en panne pour que toute une série de transactions soient bloquées.

02
Attaque par ransomware
Le ransomware a un impact sur les environnements modernes.
Les attaquants ciblent les sauvegardes, pas uniquement les données.

03
Erreur de configuration
Les erreurs de configuration provoquent des pannes.
De petites erreurs rendent des applications défaillantes tout en apparaissant « saines ».

04
Échec du déploiement
Les échecs de déploiement provoquent des interruptions d'activité.
Les versions défectueuses corrompent rapidement les données et les configurations.

05
Répercussions des pannes
Les pannes ont des répercussions. La fragmentation des outils sur Kubernetes, les VM et le SaaS brouille la vision de ce qui est réellement protégé.

06
Incohérence des données
Les sauvegardes peuvent réussir même lorsque le contexte, les métadonnées et les dépendances sont perdus.

Le risque pour votre entreprise est réel.

Les temps d'arrêt sont synonymes de risques. Les conséquences sont notamment les suivantes :

OPÉRATIONNELLES
Plus de gestion de crises, moins d'innovation.

FINANCIÈRES
Chaque minute de temps d'arrêt a un coût.

SÉCURITÉ
Une plus grande exposition aux ransomware et aux erreurs.

STRATÉGIQUES
La confiance s'érode de haut en bas.

La résilience moderne est essentielle.

La résilience moderne protège l'ensemble de l'écosystème applicatif en restaurant les applications, les données, la gouvernance et la confiance lorsque les organisations en ont le plus besoin.

Les principaux critères d'une solution de résilience efficace

Restauration automatisée
La restauration est reproductible, validée et intégrée, et non improvisée en plein incident.

Des données saines et cohérentes
Protège les données, les stratégies, les métadonnées, les configurations et les dépendances ensemble, et non séparément.

Application des garde-fous des stratégies
Les garde-fous prévus par les stratégies assurent la cohérence des workloads sur l'ensemble des clusters, des clouds et des types d'applications.

Continuité des applications
Restaure l'application complète et son état opérationnel au lieu d'une reconstruction manuelle.

Validation de la conformité
Une conformité vérifiable prouve que les politiques sont appliquées et que la restauration est reproductible, plutôt que simplement supposée.

Opérations fiables
Construisez la confiance et l'assurance. Vous êtes sûr de ce qui est protégé, exposé et qui peut être restauré avant qu'un incident survienne.

Les applications modernes exigent une résilience moderne.

Découvrez comment Veeam Kasten vous permet de simplifier, sécuriser et rationaliser vos applications modernes. Libérez votre équipe de la complexité, réduisez les risques et garantissez que votre entreprise est toujours prête, quoi qu'il arrive.

Êtes-vous prête) à explorer le sujet plus en profondeur ? Allez plus loin avec l'e-book « Pourquoi les applications modernes ont besoin d'une protection native » pour découvrir comment la protection native sauvegarde les données, le contexte, les politiques et les dépendances essentielles à une restauration complète lorsque les applications modernes échouent.

ESSAYEZ KASTEN

ACCÉDER À L'E-BOOK

© 2026 Veeam Software. Informations confidentielles. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.