Cosa si rompe realmente quando le app moderne falliscono?

Le app moderne vanno veloci. I guasti si propagano più rapidamente. La resilienza garantisce l'operatività della tua azienda.

I malfunzionamenti delle applicazioni moderne non si traducono soltanto in perdite di dati. Quando qualcosa va storto, raramente si tratta di un episodio isolato. Spesso si tratta di un guasto di dipendenza, un errore di configurazione, un problema di implementazione, una mancanza di visibilità o qualcos'altro che ostacola il corretto funzionamento.

Cosa non funziona e come intervenire



PERCHÉ LE APPLICAZIONI MODERNE FALLISCONO

Le applicazioni moderne funzionano su infrastrutture distribuite — non monolitiche —. Questi ambienti distribuiti favoriscono l'agilità e cicli di sviluppo più brevi, ma introducono anche nuove complessità e possibili punti di guasto che superano i limiti delle strategie di protezione tradizionali.

Queste strategie sono concepite per gestire interruzioni del servizio che interessano un singolo server, ma coinvolgono pochi utenti. Purtroppo questo non copre la portata delle interruzioni del servizio moderne, che possono avere ripercussioni a catena su centinaia di utenti e dipendenze.

UN NUOVO APPROCCIO ALLA RESILIENZA

Poiché i componenti delle app moderne dipendono gli uni dagli altri, le modifiche comportano dei rischi. È importante comprendere tali esposizioni.

Con la crescita dell'intelligenza artificiale e degli ambienti ibridi, il pensiero a livello di sistema è fondamentale. Per ottenere il miglior risultato, le organizzazioni devono proteggere l'intero parco applicazioni. Questo dovrebbe includere dati, configurazioni, politiche, dipendenze, metadati e contesto.

Anche la proattività è importante, poiché le lacune nella resilienza possono rimanere nascoste fino a quando qualcosa non si rompe. Strumenti di monitoraggio dello stato di salute del sistema possono aiutarti a individuare queste lacune prima che diventino un problema.

Le applicazioni moderne sono soggette a frequenti interruzioni operative.

>2/3
delle organizzazioni perde oltre $ 300.000 ogni ora durante incidenti informatici.
[1] PagerDuty 2024 State of AI-First Operations Report

54%
delle vittime di ransomware hanno utilizzato backup per ripristinare dati crittografati nell'ultimo anno.
[1] Rapporto Sophos sullo stato del ransomware 2025

$ 2 mln
per ora è il costo mediano delle interruzioni del servizio IT ad alto impatto.
[1] Previsioni di osservabilità di New Relic per il 2025.



I guasti avvengono rapidamente

01
Dipendenza interrotta
Le dipendenze dell'applicazione si guastano. Un singolo servizio che non funziona può innescare un effetto a catena, bloccando le transazioni.

02
Attacco ransomware
Il ransomware ha un impatto sugli ambienti moderni.
Gli aggressori prendono di mira i backup, non solo i dati.

03
Configurazione errata
Le configurazioni errate causano interruzioni del servizio. Piccoli errori possono compromettere le applicazioni senza che i sistemi ne rilevino il malfunzionamento.

04
Implementazione non riuscita
Le implementazioni non riuscite causano interruzioni dell'attività aziendale.
Le versioni difettose compromettono rapidamente dati e configurazioni.

05
Effetti a catena delle interruzioni del servizio
Le interruzioni del servizio producono effetti a catena. La frammentazione degli strumenti utilizzati in ambienti Kubernetes, VM e SaaS rende poco chiaro quali sistemi siano effettivamente protetti.

06
Incoerenza dei dati
I backup possono riuscire anche se il contesto, i metadati e le dipendenze si perdono.

Il rischio per la tua azienda è reale

L'interruzione è sinonimo di rischio. Le conseguenze includono:

OPERATIVO
Più gestione delle emergenze, meno innovazione.

FINANZIARIO
Ogni minuto di interruzione ha un costo.

SICUREZZA
Maggiore esposizione a ransomware ed errori.

STRATEGICO
La fiducia si erode dall'alto verso il basso.

La resilienza moderna è fondamentale.

La resilienza moderna protegge l'intero ecosistema applicativo ripristinando applicazioni, dati, governance e fiducia nei momenti in cui le organizzazioni ne hanno più bisogno.

Criteri principali per una soluzione di resilienza efficace

Ripristino automatico
Il ripristino è ripetibile, validato e integrato, mai improvvisato durante un incidente.

Dati puliti e coerenti
Protegge dati, policy, metadata, configurazioni e dipendenze insieme, non separatamente.

Vincoli di policy applicati rigorosamente
I vincoli di policy mantengono la coerenza dei carichi di lavoro in ogni cluster, cloud e tipo di applicazione.

Continuità dell'applicazione
Ripristina l'intera applicazione e il suo stato operativo anziché ricostruirla manualmente.

Validazione della conformità
La verificabilità della conformità dimostra che le politiche vengono applicate e che il ripristino è ripetibile, anziché dato per scontato.

Operazioni sicure
Costruisci fiducia e sicurezza. Sei certo di ciò che è protetto, a rischio e ripristinabile prima che si verifichi un incidente.

Le applicazioni moderne richiedono una resilienza moderna.

Scopri come Veeam Kasten ti consente di semplificare, mettere in sicurezza e ottimizzare le tue applicazioni moderne. Libera il tuo team dalla complessità, riduci il rischio e assicurati che la tua azienda sia sempre pronta, qualunque cosa accada.

Pronti ad approfondire l'argomento? Approfondisci con l'e-book "Perché le applicazioni moderne necessitano di protezione nativa" per capire come la protezione nativa salvaguarda i dati, il contesto, le politiche e le dipendenze necessari per un ripristino completo in caso di guasto delle applicazioni moderne.

PROVA KASTEN

OTTIENI L'E-BOOK

© 2026 Veeam Software. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi registrati sono proprietà dei rispettivi titolari.