O que realmente falha quando as aplicações modernas deixam de funcionar

Aplicativos modernos evoluem rapidamente. As falhas se propagam mais rapidamente. A resiliência mantém seu negócio em operação.

As falhas de aplicações modernas não são apenas eventos de perda de dados. Quando algo dá errado, raramente é um incidente isolado. Frequentemente, trata-se de uma quebra de dependência, um erro de configuração, um problema de implantação, uma lacuna de visibilidade ou outro fator que possa prejudicá-lo.

O que pode falhar e o que fazer a respeito



POR QUE OS APLICATIVOS MODERNOS FALHAM

Aplicativos modernos operam em infraestrutura distribuída — não monolítica. Esses ambientes distribuídos proporcionam agilidade e ciclos de desenvolvimento mais curtos, mas também introduzem novas complexidades e possíveis falhas que excedem os limites das estratégias de proteção tradicionais.

Essas estratégias são criadas para paralisações que atingem um servidor, mas poucos usuários. Infelizmente, isso não abrange o alcance das paralisações modernas, que podem repercutir em centenas de usuários e dependências.

UMA NOVA ABORDAGEM PARA A RESILIÊNCIA

Como os componentes modernos do aplicativo dependem uns dos outros, as alterações trazem riscos. É importante compreender essas vulnerabilidades.

Com o crescimento da IA e dos ambientes híbridos, a abordagem sistêmica é essencial. Para obter o melhor resultado, as organizações devem proteger o seu portfólio de aplicativos inteiro. Isso deve abranger dados, configurações, políticas, dependências, metadados e contexto.

A proatividade também conta. Já que lacunas de resiliência podem permanecer ocultas até que algo falhe. Ferramentas avançadas de monitoramento da saúde do sistema permitem detectar essas falhas antes que elas se transformem em problemas.

Aplicações Modernas Enfrentam Interrupções Operacionais Frequentes

Mais de 2/3
das organizações perdem mais de US$ 300.000 por hora durante incidentes de TI.

* PagerDuty — O Estado das Operações Orientadas por IA 2026

54%
das vítimas de ransomware usaram backups para restaurar dados criptografados no ano passado.

* Sophos — O Estado do Ransomware 2025

US$ 2 milhões
por hora é o custo mediano de paralisações de TI de alto impacto.

* Previsão de Observabilidade 2025 da New Relic

Falhas acontecem rapidamente

01
Dependência quebrada
Dependências de aplicação quebram. Um serviço com falha provoca um efeito cascata, resultando em transações paralisadas.

02
Ataque de ransomware
O ransomware afeta os ambientes modernos. Atacantes têm como alvo os backups, não apenas os dados.

03
Erro de configuração
Erros de configuração causam paralisações. Pequenas falhas fazem com que os aplicativos apresentem problemas, mesmo mantendo o status de "íntegro".

04
Falha na implantação
Implantações com falhas geram interrupção nos negócios. Lançamentos com falhas quebram dados e configurações rapidamente.

05
Efeitos secundários das paralisações
As paralizações têm efeitos secundários. Ferramentas fragmentadas em Kubernetes, VMs e SaaS dificultam a identificação do que está realmente protegido.

06
Inconsistência dos Dados
Os backups podem ser bem-sucedidos mesmo quando o contexto, os metadados e as dependências são perdidos.

O Risco Para o Seu Negócio É Real

Tempo de inatividade é risco. As consequências incluem:

OPERACIONAL
Mais combate a incêndios, menos inovação.

FINANCEIRO
Cada minuto de tempo de inatividade tem um custo.

SEGURANÇA
Maior exposição a ransomware e erros.

ESTRATÉGICA
A confiança se deteriora de cima para baixo.

A Resiliência moderna é fundamental

A resiliência moderna protege todo o ecossistema de aplicações, restaurando aplicações, dados, governança e confiança quando as organizações mais precisam.

Principais Critérios para uma Solução Eficaz de Resiliência

Restauração automatizada
A recuperação é repetível, validada e integrada, não improvisada no meio do incidente.

Dados limpos e consistentes
Protege dados, políticas, metadados, configurações e dependências de forma conjunta, não de maneira isolada.

Diretrizes de políticas reforçadas
Controles de políticas garantem a consistência das cargas de trabalho em todos os clusters, nuvens e tipos de aplicações.

Continuidade de aplicações
Restaura toda a aplicação e seu estado operacional, evitando reconstrução manual.

Validação de conformidade
A conformidade auditável comprova que as políticas são aplicadas e que a recuperação é repetível, em vez de presumida.

Operações com confiança
Construa confiança e credibilidade. Você sabe o que está protegido, o que está em risco e o que pode ser recuperado antes que um incidente aconteça.

Aplicações modernas exigem resiliência igualmente moderna.

Descubra como o Veeam Kasten ajuda a simplificar, proteger e otimizar suas aplicações modernas. Liberte sua equipe da complexidade, reduza riscos e garanta que sua empresa esteja sempre pronta, não importa o que aconteça.

Está pronto para se aprofundar no assunto? Aprofunde-se com o E-book Por que Aplicações Modernas Precisam de Proteção Nativa para entender como a proteção nativa salvaguarda os dados, o contexto, as políticas e as dependências essenciais para uma recuperação completa quando aplicações modernas falham.

EXPERIMENTE KASTEN

OBTER O E-BOOK

© 2026 Veeam Software. Informações confidenciais. Todos os direitos reservados. Todas as marcas comerciais são propriedade dos seus respectivos titulares.