Lo que realmente se rompe cuando fallan las aplicaciones modernas

Las aplicaciones modernas se mueven rápido. Los fallos se propagan más rápido. Resiliencia que mantiene su negocio en funcionamiento.

Las fallas de las aplicaciones modernas no son solo eventos de pérdida de datos. Cuando algo sale mal, rara vez se trata de un incidente aislado. A menudo, es una falla de dependencia, un error de configuración, un problema de implementación, una brecha de visibilidad u otra cosa que juega en su contra.

Qué se rompe y qué hacer al respecto



POR QUÉ SE ROMPEN LAS APLICACIONES MODERNAS

Las aplicaciones modernas se ejecutan en una infraestructura distribuida, no monolítica. Estos entornos distribuidos ofrecen agilidad y ciclos de desarrollo más cortos, pero también generan nueva complejidad y posibles fallos que exceden las capacidades de las estrategias de protección tradicionales.

Estas estrategias están diseñadas para interrupciones que afectan a un servidor, pero a pocos usuarios. Esto, lamentablemente, no abarca el alcance de las interrupciones modernas, que pueden afectar a cientos de usuarios y dependencias.

UN NUEVO ENFOQUE DE LA RESILIENCIA

Dado que los componentes de las aplicaciones modernas dependen unos de otros, los cambios conllevan riesgos. Es importante entender esas exposiciones.

Con el crecimiento de la IA y los entornos híbridos, el pensamiento a nivel de sistema es clave. Para obtener el mejor resultado, las organizaciones deben proteger su conjunto completo de aplicaciones. Esto debe abarcar los datos, las configuraciones, las políticas, las dependencias, los metadatos y el contexto.

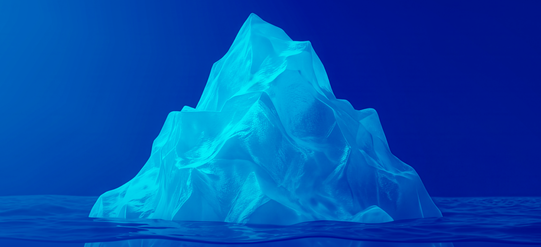
La proactividad también cuenta, ya que los brechas de resiliencia pueden permanecer ocultas hasta que algo se rompe. Las herramientas inteligentes de salud del sistema pueden ayudarle a detectar estas brechas antes de que se conviertan en un problema.

Las aplicaciones modernas se enfrentan a frecuentes interrupciones operativas.

>2/3
de las organizaciones pierden más de $300,000 por hora durante incidentes de TI.
* Informe sobre el estado de las operaciones centrados en IA de PagerDuty 2026

54%
de las víctimas de ransomware utilizaron backups para restaurar datos cifrados el año pasado.
* Informe de ransomware de Sophos 2025

$2 millones
por hora es el costo medio de las interrupciones de TI de alto impacto.
* Pronóstico de observabilidad de New Relic para 2025.



Las fallas ocurren rápido

01
Dependencia rota
Las dependencias de las aplicaciones se rompen. El fallo de un servicio se propaga en cadena y hace que se estanquen las transacciones.

02
Ataque de ransomware
El ransomware afecta a los entornos modernos.
Los atacantes buscan comprometer los backups, no solo los datos.

03
Configuración errónea
Los errores de configuración provocan interrupciones.
Pequeños errores dejan aplicaciones dañadas pero "saludables".

04
Implementación fallida
Las implementaciones fallidas generan una interrupción del negocio.
Las versiones defectuosas dañan los datos y las configuraciones rápidamente.

05
Efecto dominó de las interrupciones
Las interrupciones tienen efecto dominó. Las herramientas fragmentadas en Kubernetes, VMs y SaaS confunden lo que realmente está protegido.

06
Inconsistencia de los datos
Los backup pueden realizarse con éxito incluso cuando se pierden el contexto, los metadatos y las dependencias.

El riesgo para su negocio es real

El tiempo de inactividad implica riesgo. Las consecuencias incluyen:

OPERATIVO
Más apagando fuegos, menos innovación.

FINANCIERO
Cada minuto de tiempo de inactividad tiene un costo.

SEGURIDAD
Mayor exposición al ransomware y a los errores.

ESTRATÉGICO
La confianza se erosiona de arriba a abajo.

La resiliencia moderna es clave

La resiliencia moderna protege el ecosistema completo de aplicaciones al restaurar aplicaciones, datos, gobierno y confianza cuando las organizaciones más lo necesitan.

Criterios principales para una solución de resiliencia eficaz

Restauración automatizada
La recuperación es repetible, validada e integrada, no improvisada a mitad del incidente.

Datos limpios y consistentes
Protege los datos, las políticas, los metadatos, las configuraciones y las dependencias de forma conjunta, no por separado.

Controles de políticas implementados
Los controles de políticas mantienen la coherencia de las cargas de trabajo en todos los clústeres, nubes y tipos de aplicaciones.

Continuidad de la aplicación
Restaura la aplicación completa y su estado operativo en lugar de la reconstrucción manual.

Validación de cumplimiento
El cumplimiento auditable demuestra que las políticas se aplican y que la recuperación es repetible, en lugar de asumirse.

Operaciones seguras
Genere confianza y seguridad. Sabe con certeza qué está protegido, qué está en riesgo y qué se puede recuperar antes de que ocurra un incidente.

Las aplicaciones modernas exigen una resiliencia moderna.

Descubra cómo Veeam Kasten le permite simplificar, proteger y optimizar sus aplicaciones modernas. Libere a su equipo de la complejidad, reduzca el riesgo y asegúrese de que su empresa esté siempre lista, pase lo que pase.

¿Listo para explorar el tema más a fondo? Profundice con el E-book "Por qué las aplicaciones modernas necesitan protección nativa" para aprender cómo la protección nativa resguarda los datos, el contexto, las políticas y las dependencias necesarias para una recuperación completa cuando las aplicaciones modernas fallan.

PROBAR KASTEN

OBTENER E-BOOK

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.