

DOOMSDAY BACKUP

Cuando todo está cifrado, ¿qué puede restaurar todavía?

Doomsday Backup es la copia de su negocio diseñada para quedar fuera del alcance del atacante: bloqueada contra cambios, guardada fuera de sitio y separada de las credenciales que el ransomware roba primero. Y después demostramos que restaura.

POR QUÉ LOS RESPALDOS COMUNES FALLAN EL PEOR DÍA

01

Los atacantes van primero por los respaldos

Con credenciales de administrador robadas, borran o cifran todo respaldo a su alcance antes de que aparezca la nota de rescate.

02

La replicación copia el daño

Los archivos cifrados y borrados se replican a su segundo sitio con la misma fidelidad que los buenos.

03

Un respaldo sin probar es una suposición

Un reporte en verde dice que la tarea corrió. No dice que la aplicación vuelve a funcionar.

Sepa qué podría restaurar hoy.

800-700-7500
www.controllednetworks.com

Lo que un proyecto Doomsday Backup deja instalado

Diseñado alrededor de sus cargas y escrito en su propuesta: qué está protegido, dónde vive y qué tan rápido regresa.

Copias de respaldo inmutables

Copias con bloqueo de retención diseñadas para rechazar cambios y borrado durante el periodo que usted defina, aun desde una cuenta de administrador comprometida.

Replicación geográfica

Una segunda copia en otra instalación, para que un incendio, inundación o falla regional no se lleve los respaldos junto con los servidores.

Archivo fuera de línea (air-gap)

Para sus datos más críticos: una copia cifrada sin ruta de red hacia producción.

Pruebas de restauración

Restauraciones de prueba programadas con cargas reales, y un reporte de qué regresó y cuánto tardó.

RPO / RTO por carga de trabajo

Cuántos datos puede perder cada aplicación y cuánto tiempo puede estar caída: acordado, por escrito y contemplado en el diseño.

Manual de recuperación

Quién hace qué, en qué orden y con qué dependencias. Escrito antes del mal día, no durante.

QUÉ RESISTE CADA ENFOQUE

ESCENARIO	SOLO REPLICACIÓN	RESPALDO COMÚN	DOOMSDAY BACKUP
Falla de servidor o almacenamiento	Sí	Sí	**Sí**
Borrado detectado semanas después	**No, el borrado se replica**	Sí, dentro de la retención	**Sí, dentro de la retención**
Pérdida total de un sitio	Sí	**Solo si está fuera de sitio**	**Sí, replicado fuera de sitio**
Ransomware con acceso admin	**No, el cifrado se replica**	**Suele ser borrado**	**Copias inmutables y aisladas**
Prueba de que restaura	**No se prueba**	**Rara vez se prueba**	**Probado, con reporte**

CÓMO TRABAJAMOS

01

Evaluar

Inventariamos cargas críticas, dependencias y quién puede borrar los respaldos actuales.

02

Diseñar

Protección, aislamiento, replicación y retención según cada carga de trabajo.

03

Implementar

Lo construimos, cargamos las copias y documentamos el orden de recuperación.

04

Comprobar

Restauraciones de prueba programadas y el manual actualizado conforme usted cambia.

Solicite una evaluación de recuperación ante ransomware.

Revisamos qué respalda, dónde vive y quién puede borrarlo, y le decimos con claridad qué podría restaurar.

800-700-7500

www.controllednetworks.com

325 S. River St., 2nd Floor, Hackensack, NJ 07601

La protección depende del diseño final, el periodo de retención y los procedimientos definidos en su contrato. Ninguna arquitectura de respaldo es inmune a todos los escenarios. © 2026 Controlled Networks Solution LLC (CNS). Todos los derechos reservados.