

DOOMSDAY BACKUP

When everything is encrypted, what can you still restore?

Doomsday Backup is the copy of your business built to stay out of an attacker's reach: locked against change, stored off-site and separated from the credentials ransomware crews steal first. Then we prove it restores.

WHY ORDINARY BACKUPS FAIL ON THE WORST DAY

01

Attackers go for the backups first

With stolen admin credentials, they delete or encrypt every backup they can reach before the ransom note appears.

02

Replication copies the damage

Encrypted and deleted files replicate to your second site as faithfully as good ones do.

03

An untested backup is a guess

A green job report says the job ran. It does not say the application comes back.

Find out what you could restore today.

800-700-7500
www.controllednetworks.com

What a Doomsday Backup engagement puts in place

Designed around your workloads and written into your proposal, so you know exactly what is protected, where it lives and how fast it comes back.

Immutable backup copies

Retention-locked copies designed to refuse changes and deletion for the window you set, even from a compromised admin account.

Geographic replication

A second copy in a separate facility, so a fire, flood or regional outage does not take the backups down with the servers.

Offline / air-gapped archive

For your most critical data: an encrypted copy with no network path back to production.

Restore testing

Scheduled test restores of real workloads, with a report showing what came back and how long it took.

RPO / RTO by workload

How much data each application can afford to lose and how long it can be down: agreed, written down and designed for.

Recovery runbook

Who does what, in what order, with which dependencies. Written before the bad day, not during it.

WHAT EACH APPROACH IS BUILT TO SURVIVE

SCENARIO	REPLICATION ONLY	STANDARD BACKUP	DOOMSDAY BACKUP
Server or storage failure	Yes	Yes	**Yes**
Deletion noticed weeks later	No, deletion replicates	Yes, within retention	**Yes, within retention**
Loss of an entire site	Yes	Only if kept off-site	**Yes, replicated off-site**
Ransomware with admin access	No, encryption replicates	Often reached, deleted	**Immutable, isolated copies**
Proof that it restores	Not tested	Rarely tested	**Tested, with a report**

HOW WE WORK

01

Assess

We inventory critical workloads, dependencies and who can delete today's backups.

02

Design

Protection, isolation, replication and retention matched to each workload.

03

Implement

We build it, seed the copies and document the recovery order.

04

Prove

Test restores on a schedule, with the runbook updated as you change.

Request a ransomware recovery readiness assessment.

We review what you back up, where it lives and who can delete it, then tell you plainly what you could restore.

800-700-7500

www.controllednetworks.com

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

Protection depends on the final design, retention window and operating procedures set out in your written agreement. No backup architecture is immune to every scenario. © 2026 Controlled Networks Solution LLC (CNS). All rights reserved.