

Building Ransomware-Resilient Backup

A practical guide to the 3-2-1-1-0 rule, immutability and recovery testing

STORAGE

Published October 2026 · cybertechinsights.com

EXECUTIVE SUMMARY

Backups are now a primary target

Ransomware operators have learned that encrypting production systems is only half the job. If an organisation can restore quickly from clean backups, the attacker has little leverage. As a result, modern attacks routinely look for backup servers, delete snapshots, change retention settings and steal backup administrator credentials before they encrypt anything.

This whitepaper explains how to design a backup architecture that survives that kind of attack. It uses the widely adopted **3-2-1-1-0 rule** as a framework, then covers immutability, credential isolation, recovery testing and the questions to ask when evaluating storage and backup vendors.

Key takeaways

- Treat the backup environment as a high-value security zone, not an IT utility.
- At least one copy of every critical dataset should be immutable or offline.
- Backup administration must use separate identities, MFA and a separate management network.
- A backup only counts once it has been restored and verified — test regularly.

FRAMEWORK

The 3-2-1-1-0 rule explained

The original 3-2-1 rule — three copies of data, on two different media, with one copy offsite — was designed for hardware failure and site disasters. The extended 3-2-1-1-0 version adds two requirements aimed at deliberate, malicious data destruction.

Rule	Requirement	Why it matters
3	Keep at least three copies of data: production plus two backups.	A single backup copy is a single point of failure.
2	Store backups on at least two different types of media or platforms.	One flaw, bug or vendor issue should not affect every copy.
1	Keep at least one copy offsite or in a separate cloud account/region.	Protects against site loss and local compromise.
1	Keep at least one copy immutable or offline (air-gapped).	Attackers with admin access cannot alter or delete it.
0	Zero errors: verify backups and run recovery tests.	Unverified backups often fail when they are needed most.

DESIGN

Making at least one copy immutable

Immutability means that once a backup is written, it cannot be modified or deleted until a retention period expires — even by an administrator. There are several practical ways to achieve it:

- **Object storage with object lock (WORM).** Many on-premises and cloud object stores support write-once-read-many retention. Use compliance-style locking where available, so retention cannot be shortened by an admin.
- **Hardened repositories.** Linux-based backup repositories with immutable file flags, single-use credentials and no interactive remote access.
- **Offline media.** Tape or removable media that is physically disconnected once written remains one of the simplest air gaps.
- **Separate cloud tenancy.** Copies sent to a cloud account that production administrators cannot sign in to.

Whichever approach you choose, set retention to cover the time an attacker might remain undetected in the environment. Restoring from a backup that already contains the attacker's tools simply restarts the incident.

SECURITY

Isolating backup administration

Most backup compromises start with stolen credentials rather than a flaw in the backup software. Reduce that risk by removing every shortcut between the production domain and the backup environment:

- Do not join backup servers to the production Active Directory domain; use separate, dedicated accounts.
- Require phishing-resistant multi-factor authentication for backup consoles and storage management.
- Place backup infrastructure on a separate management network with tightly restricted inbound access.
- Apply four-eyes approval for destructive actions such as deleting backups or reducing retention, where supported.
- Send backup and storage logs to a security monitoring platform and alert on deletions and policy changes.

RECOVERY

Testing recovery, not just backups

A successful backup job only proves that data was copied. Recovery testing proves that the business can operate again. Agree recovery time objectives (RTO) and recovery point objectives (RPO) with business owners for each critical system, then test against them.

- **Automated verification:** mount or boot backups in an isolated sandbox and run health checks after each job.
- **Scheduled restore drills:** restore complete applications — not just files — at least quarterly.
- **Clean-room recovery:** plan where you will rebuild if production identity systems are compromised.
- **Runbooks:** document the order of restoration, dependencies and contacts, and keep an offline copy.

BUYER GUIDANCE

Questions to ask storage and backup vendors

- How is immutability enforced, and can any administrator shorten or bypass retention?
- Can the backup environment run with identities that are completely separate from production?
- Which actions can require multi-person approval?
- How are backups verified automatically, and what does a failed verification look like?
- How long does a full restore of our largest application take at our data volumes?
- What logs and alerts are available for security monitoring, and in what format?

Checklist: ransomware-resilient backup

- Inventory critical systems and agree RTO/RPO with business owners.
- Confirm three copies on two media types, with one offsite.
- Enable immutability or an offline copy for every critical dataset.
- Separate backup identities, enforce MFA and isolate the management network.
- Monitor and alert on backup deletions and retention changes.
- Run automated verification and quarterly full restore drills.

About Cyber Tech Insights: a B2B publication providing research and resources for technology and business decision-makers. This document is for general information only and does not constitute professional advice. © 2026 Cyber Tech Insights.