Ransomware Resilience Challenge

Check each statement that is true of your setup today. Your score updates automatically. There are 20 points available - your total score points you to where the real gaps are.

1 Protecting data wherever it lives

6 pts

- [ ] I know every place my business data lives - endpoints, servers, NAS and cloud services.
- [ ] All my Windows PCs and servers are backed up automatically.
- [ ] My Mac and Linux machines are backed up, not just my Windows machines.
  Coverage and OS-version support vary by platform - confirm your versions are supported.
- [ ] My Microsoft 365 or Google Workspace data is backed up independently.
  Under the shared-responsibility model, your SaaS provider does not back this up for you.
- [ ] My virtual machines (VMware, Hyper-V) are backed up at the hypervisor level.
- [ ] I have identified any critical SaaS apps my backup tool does not cover.
  CRM, accounting and ticketing tools often need a separate plan.

2 Off-site and off-platform copies

5 pts

- [ ] I follow the 3-2-1-1-0 rule, not just 3-2-1.
  Three copies, two media, one off-site, one immutable or offline, with zero errors after a verified restore.
- [ ] At least one backup copy is stored off-site, away from my primary location.
- [ ] My off-site copy is on a separate platform, isolated from my network and credentials.
  If the same admin login can reach it, ransomware that compromises that login can too.
- [ ] My backups are encrypted, both in transit and at rest.
- [ ] I keep enough version history to recover from an attack that went unnoticed for weeks.
  Attackers often dwell before triggering; shallow retention can mean every kept copy is compromised.

3 Making backups **ransomware-resilient** 5 pts

- [ ] At least one backup copy is immutable and cannot be modified or deleted - even by an admin.
  Immutable WORM snapshots or Object Lock is the single most effective backup defense.
- [ ] I have verified a restore recently - for VMs and servers this can be automated with backup verification in Virtual Machine Manager.
  Active Backup for Business runs a trial restore in VMM and records the boot as a video for proof.
- [ ] My backup system is monitored, and I am alerted when a backup fails.
- [ ] I would be alerted to unusual file activity, such as mass encryption, while it is happening.
  Early detection can mean isolating a system before the encryption sweep finishes.
- [ ] I know roughly how long a full recovery would take, and the business can tolerate it.

4 Security culture and access 4 pts

- [ ] Admin access to my NAS and backup system requires multi-factor authentication.
  Compromised credentials are a leading ransomware entry point.
- [ ] My systems and software are kept up to date with security patches.
- [ ] My team knows how to recognize phishing, the most common way ransomware gets in.
- [ ] I follow least-privilege access - people and apps only have permissions they truly need.



0% (0/20)

Check the boxes above to begin the ransomware resilience challenge.
Speak with a solutions expert for tailored advice on safeguarding data and improving ransomware resilience.

Contact us for a business consultation

Based on your results

Every guide below is here for you. The items tied to a box you left unchecked are flagged so you can start where it matters most.

Suggested

Active Backup for Business

Back up PCs, servers and VMs from one console.

Open quick-start guide

Suggested

Snapshot Replication

Immutable WORM snapshots that survive attacks.

Open quick-start guide

Suggested

Hyper Backup

Send an off-site, versioned copy of your data.

Open quick-start guide

Suggested

Synology Drive

Set up secure file sync and sharing for your team.

Open quick-start guide

Suggested

Active Backup for Microsoft 365

Back up Exchange, OneDrive and SharePoint.

Open quick-start guide

Suggested

Active Backup for Google Workspace

Back up Gmail, Drive and shared drives.

Open quick-start guide

Suggested

C2 Object Storage

Cloud immutability with Object Lock, off-network.

Open quick-start guide

Suggested

Secure SignIn

Multi-factor authentication for admin access.

Open quick-start guide

More guides and references

- NAS security
- Active Insight File Activity
- What is an immutable snapshot?
- White paper: Data Protection with Synology Snapshot Technology
- Recover individual files using snapshots
- Replicate snapshots to a remote Synology NAS
- Ensure data consistency of replicated encrypted shared folders