



Backup Security Checklist

8 checks MSPs should run on every customer environment before attackers do.

- ☐ The backup agent runs under a dedicated service account with no domain admin rights and no write access to production shares.
- ☐ Backup storage credentials exist only inside the backup software, stored encrypted, and aren't shared with any other system or user.
- ☐ Backup storage (local and cloud) is used for backups only and isn't mapped or browsable from production.
- ☐ MFA on backup consoles and admin accounts is phishing-resistant (FIDO2 or hardware key), not push-based.
- ☐ Offsite storage is immutable, and its access credentials and encryption keys are documented outside production.
- ☐ Retention reaches further back than a realistic dwell time, set per job and per storage location.
- ☐ Restore tests run on a schedule and after every significant change, with results logged.
- ☐ Each customer and system has a measured RTO from a real restore test and a documented restore order.