Enterprise-grade backup and recovery that never leaves your network.

A unified data-protection platform for Windows, Linux and Hyper-V workloads. Application-consistent backups of files, databases, Active Directory, bare-metal server images and virtual machines, encrypted at the source with AES-256-GCM and held on storage you own, with automated recovery verification and built-in diagnostics.

AES-256
encryption before data leaves the server

2FA
authenticator sign-in on every dashboard

No cloud
your data stays on your own NAS

Signed
updates verified by digital signature

Workload coverage

Files and folders
Full, differential and incremental backups, with open and locked files captured through Windows shadow copies.

SQL Server, MySQL, PostgreSQL
SQL Server full, differential and transaction-log backups. MySQL, MariaDB and PostgreSQL dumps on their own timetable.

Server image and System State
Bare-metal images of the critical volumes and the Windows System State, for recovery onto new hardware.

Active Directory
An Active Directory snapshot on domain controllers, alongside System State.

Hyper-V virtual machines NEW
Whole machines, disks and settings, backed up from the Hyper-V host and restored with one Restore VM button. Other platforms: install inside the virtual server.

Linux servers NEW
A Linux edition for files, MySQL, MariaDB and PostgreSQL, with the same dashboard and encryption.

Data protection engine

Three schedules in one job
Incremental daily, differential weekly and full monthly, for example. Only changed files are stored between full backups.

Retention and second copy
Old backups are removed as whole chains. Each backup can go to a second destination for a 3-2-1 layout.

Multi-core compression NEW
Compression uses up to half of the server's processor cores, so large jobs finish sooner without starving the server.

Verified every time
Each backup is read back and checked after it is written. Partial sets are never left looking like good ones.

Scheduled test restores
A real restore of the latest chain to a scratch folder, with the result logged and e-mailed, ready for an audit file.

Browse and restore
Restore single files, folders or everything, to the original or another location. Restores are never blocked by licence expiry.

Defence-in-depth security

- **AES-256-GCM** encryption on the server, in authenticated blocks
- Key from your passphrase through **PBKDF2-SHA256**, 600,000 rounds
- Three ways back in: passphrase, offline key file, vendor recovery
- NAS share connected **only while a job runs**, with a dedicated account
- **Two-factor sign-in** and 15-character passwords for every account
- Password change every six months; no admin or administrator user names
- Lockout after five failed attempts, sign-out after 15 idle minutes
- IP allow-list, full audit log, and **digitally signed** updates only

Operational resilience

Server jobs that fix themselves

Image and Active Directory jobs check Windows first, reset stuck snapshot components with your permission, and retry. The server and its applications are never restarted.

Resume after a restart

If the server restarts or loses power during a backup, the job starts again by itself when the server is back.

Alerts that reach someone

E-mail on failure, missed backup, low NAS space, security events, and before a licence or password runs out.

OmniBot and human support NEW

Say a backup failed and OmniBot reads the logs on the server and explains the cause and the fix, offline. A short form passes you to our support team.

Friendlier to antivirus NEW

Works through Windows' own interfaces instead of command-line tools that security products distrust, with a self-test for each server.

Standalone by design

Every server runs its own backups and reports by e-mail. No central system whose compromise would expose every site.

Ready for your next audit

OmniBackup provides the technical backup controls that healthcare and data-protection frameworks ask for, including ADHICS (Abu Dhabi), HIPAA, GDPR and ISO 27001: encrypted copies, restricted access, tested restores and records to show the auditor. It helps you meet these requirements; your organisation remains responsible for its policies and its audit.

Technical specifications

Windows	Windows Server 2016, 2019, 2022 and 2025; Windows 10 and 11 (64-bit)
Linux	64-bit Intel/AMD distributions with systemd (Ubuntu, Debian, RHEL, Rocky, Alma, SUSE): files, MySQL, MariaDB, PostgreSQL
Virtual machines	Whole-VM backup and restore from a Hyper-V host. On VMware and other platforms, installed inside each virtual server
Databases	Microsoft SQL Server, MySQL, MariaDB, PostgreSQL
Backup storage	Any SMB share: Synology, QNAP, TrueNAS, Asustor, TerraMaster, WD, or another Windows server. Local or USB disk for file and database jobs
Backup types	Full, differential, incremental; SQL transaction log; System State; bare-metal image; Active Directory snapshot
Encryption	AES-256-GCM, PBKDF2-SHA256 key derivation, secrets at rest protected by Windows DPAPI
Management	HTTPS dashboard served by the server itself; administrator and read-only users; per-site branding
Updates	Checked monthly; installed only with a valid digital signature. Offline servers can be updated with the installer
Server image jobs	Use the Windows Server Backup feature (installed automatically where possible); destination must be a network share

Licensing (per server, USD)

- ✓ **1 year: $149** per server, with all updates and e-mail support
- ✓ **3 years: $450** per server, with all updates and e-mail support
- ✓ **Lifetime: $499** per server, never expires, 12 months of updates
- ✓ **30-day trial** with every feature; one licence per physical or virtual server

Try it on your own server

Download the 30-day trial, or ask us for a quotation and installation.

ramtechuae.com/omnibackup

Tel: +971 3 7800813

Synology, QNAP, TrueNAS, Microsoft, Windows, Hyper-V, VMware and other names are trademarks of their owners, used only to describe compatibility.