Backup and Disaster Recovery - Full Features Guide

Complete solution breakdown, recovery standards, product options and service inclusions

Local NAS Backup

- Synology DiskStation setup and config
- QNAP NAS for high-performance workloads
- RAID 1 and RAID 5 configuration
- Shared folder backup and versioning
- File server to NAS replication
- Hyper Backup to local and cloud
- Snapshot replication for fast restore
- Drive health monitoring and alerts

Cloud and Offsite Backup

- AWS S3 and Glacier backup
- Azure Blob Storage backup
- Wasabi cloud storage (cost-effective)
- Encrypted upload before transmission
- Offsite NAS-to-NAS replication
- Incremental backup to reduce bandwidth
- Multi-region redundancy options
- Long-term retention and archival

Microsoft 365 Backup

- Exchange mailbox daily snapshots
- SharePoint and Teams data backup
- OneDrive file versioning and backup
- Point-in-time restore per mailbox
- Deleted item recovery beyond MS limit
- Legal hold and eDiscovery support
- Backup admin portal access
- Monthly backup status reports

Server and VM Backup

- Windows Server full image backup
- Bare-metal recovery capability
- Hyper-V VM snapshot backup
- VMware vSphere backup support
- Incremental forever backup mode
- Application-aware backup (SQL, Exchange)
- Off-hours backup scheduling
- Recovery to dissimilar hardware

Backup Monitoring and Management

- Daily automated backup job checks
- Instant alert on backup failure
- Monthly backup health report
- Backup storage usage tracking
- Quarterly scheduled restore test
- Written restore test report
- Backup policy review annually
- Retention period management

Disaster Recovery Planning

- Recovery Time Objective (RTO) definition
- Recovery Point Objective (RPO) definition
- Written DR procedure document
- Step-by-step restore runbook
- Staff DR awareness briefing
- Annual DR plan review
- Emergency contact and escalation list
- PDPA data retention compliance guidance

Backup Solution Comparison

Feature	Basic NAS	NAS + Cloud	Fully Managed
Local NAS backup	Yes	Yes	Yes
Cloud or offsite backup	No	Yes	Yes
Microsoft 365 backup	No	Optional	Yes
Server image backup	No	Optional	Yes
Daily monitoring	No	No	Yes
Failure alerts	No	No	Yes
Monthly health report	No	No	Yes
Quarterly restore test	No	No	Yes
DR plan documentation	No	No	Yes
PDPA compliance guidance	No	No	Yes
Onsite installation	Yes	Yes	Yes
Post-install support 90 days	Yes	Yes	Yes

Recovery Standards and SLAs

Recovery Scenario	Target RTO	Notes
File and Folder Recovery	Under 30 minutes	Restore individual files from NAS or cloud backup
Server Recovery (NAS image)	2 to 4 hours	Restore full server from local NAS image backup
Server Recovery (cloud)	4 to 8 hours	Restore from cloud backup depending on data volume
Microsoft 365 Mailbox	Under 1 hour	Point-in-time restore of individual mailbox data
Full Environment Recovery	8 to 24 hours	Complete bare-metal rebuild from backup with DR plan

Compatible Products and Platforms

Synology DiskStation	DS224+, DS923+, DS1522+, RS1221+ — NAS backup appliances for SME and enterprise.
QNAP NAS	TS-233, TS-464, TBS-h574TX — High-performance NAS for demanding workloads.
Veeam Backup	Server and VM backup for Hyper-V and VMware environments. Industry standard.
Acronis Cyber Protect	Combined backup and cybersecurity. Ransomware protection built in.
MSP360 (CloudBerry)	Cloud backup for AWS, Azure and Wasabi. Flexible retention and scheduling.
Synology C2 Cloud	Synology-native cloud backup. Seamless integration with Synology NAS.
Microsoft 365 Backup	Third-party M365 backup with point-in-time restore for mailbox and SharePoint.
Wasabi Cloud Storage	Cost-effective S3-compatible cloud storage. No egress fees for restore.

Frequently Asked Questions

How often should my business backup data?

For most businesses we recommend daily incremental with weekly full backups. Critical data like accounting and databases should be backed up daily minimum.

What is the difference between backup and disaster recovery?

Backup is copying data to a safe location. DR is the plan to restore systems after a failure. A backup without a tested recovery plan is incomplete. You need both.

Can you backup Microsoft 365 emails and SharePoint?

Yes. Microsoft only retains deleted data for a limited period. We implement third-party M365 backup with daily snapshots and point-in-time recovery for all mailboxes.

How long does recovery take after a ransomware attack?

With a proper backup and DR plan most SME environments restore in 2 to 8 hours. The key is a clean offsite backup not connected to the network during the attack.

Do you monitor backups or just set them up?

We do both. Under managed monitoring we check jobs daily, resolve failures, send monthly health reports and perform quarterly restore tests. You get alerts on failure.

Is cloud backup safe and PDPA compliant?

Yes. All data is encrypted before transmission and stored encrypted at rest. We advise on PDPA-appropriate retention periods and access controls for your industry.