Synology®

ActiveProtect Data Recovery Assurance Guide

Ensure confident data recovery with a robust data protection solution

Table of Contents

Overview 01

About this document 02

How ActiveProtect safeguards your backups 03

How ActiveProtect guarantees data recovery 06

Audit your backups to meet compliance and standards 08

Conclusion 10

ActiveProtect Data Recovery Assurance Checklist 11

Overview

With the ever-growing threat of ransomware in today's digital landscape, companies need to be absolutely certain that their data can be successfully recovered when dealing with catastrophic ransomware attacks. According to reports, ransomware attacks have increased nearly **5 times** in the past 5 years.

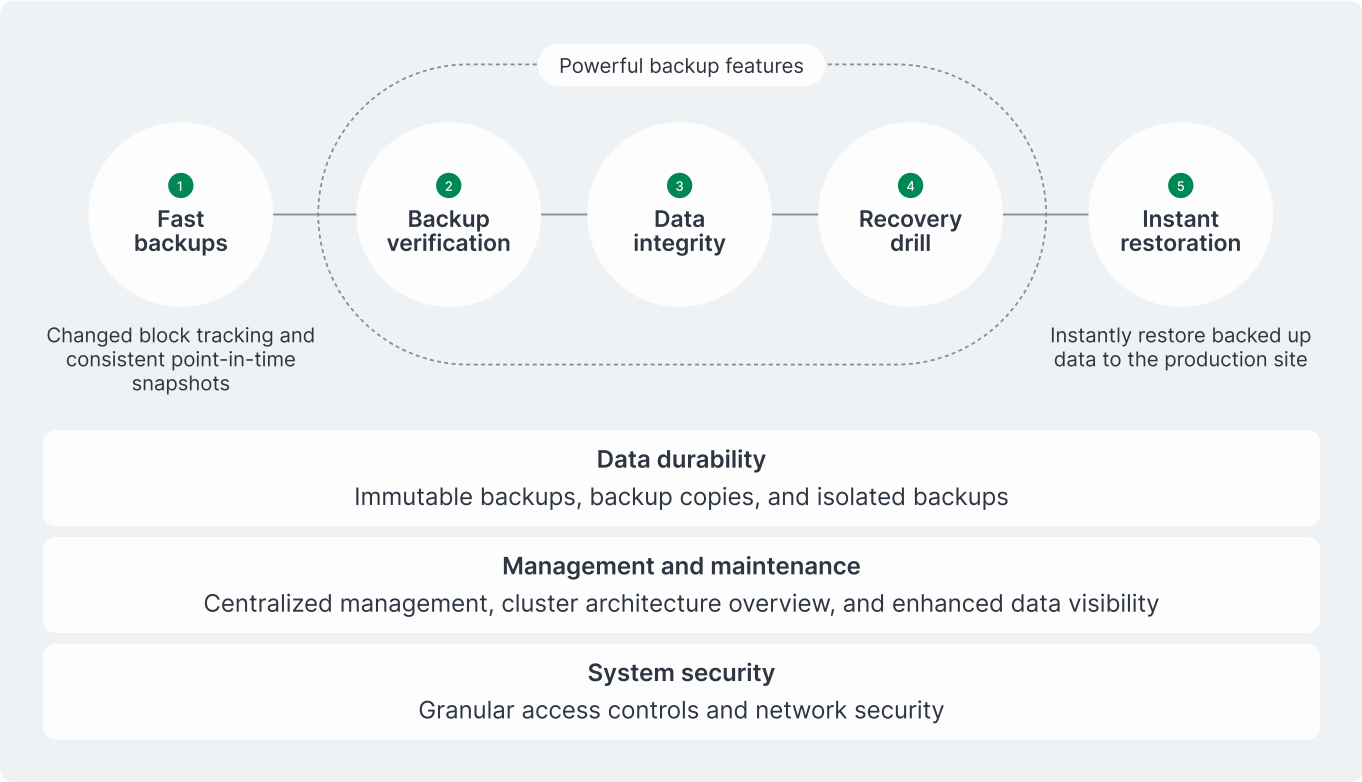
Over 90% of businesses aren't certain they can recover from a ransomware attack, according to Synology's 2025 Enterprise Data Management Survey. Companies need to better protect themselves by implementing a cyber resilient data protection solution in which backups are secured, verified, tested, checked for anomalies, and generates backup reports. These can be kept for auditing purposes and to meet compliance.

Synology ActiveProtect is a one-stop data protection solution that comes with powerful and versatile features to safeguard and verify data so that it can be restored when needed.

About this document

This guide is designed to document best practices for recovering your data with Synology ActiveProtect. It takes an in-depth look at features included in Synology ActiveProtect such as disaster recovery testing, data integrity checks, built-in immutability, and more, so that organisations can follow the 3-2-1-1-0 backup strategy and safely recover data at any time.

This guide is intended for businesses and IT professionals that have implemented or plan on implementing data recovery technologies to safeguard enterprise data.



How ActiveProtect safeguards your backups

In order to ensure your backups are fast, secure, and recoverable, Synology ActiveProtect includes a wide variety of features that empower organisations to store their data safely and ensure data redundancy.

ActiveProtect's modern backup techniques

Synology ActiveProtect uses modern backups techniques that allow users to perform backups quickly, without sacrificing speed. This ensures that source data can be backed up fast, efficiently, accurately, and can be restored to their original state when needed.

A standalone backup image is produced with each backup, with modified blocks being backed up subsequently. This ensures that each backup is a complete snapshot, which can be restored when needed.

Synology ActiveProtect includes an advanced deduplication engine in which redundant data is eliminated from the source and across the cluster with source-side and cross-site deduplication to maximise storage capacity and reduce bandwidth to improve your backup performance and meet recovery point objectives (RPO).

See how Synology ActiveProtect differs from conventional backup solutions: https://sy.to/mfb

Tamper-proof backups with data immutability

ActiveProtect also comes with built-in immutability that essentially locks down your data to prevent data tampering and deletion to ensure the safety of your data.

ActiveProtect comes with customisable protection plans so that users can create an immutable plan which can then be applied to the workloads you select. All backup versions that are a part of the immutable protection plans are then locked down for a set period of time. The retention period is chosen when creating the immutable protection plan.

As an example, if you're performing backups on a daily basis for the next 30 days, each backup version will be locked and cannot be modified or deleted for the next 30 days.

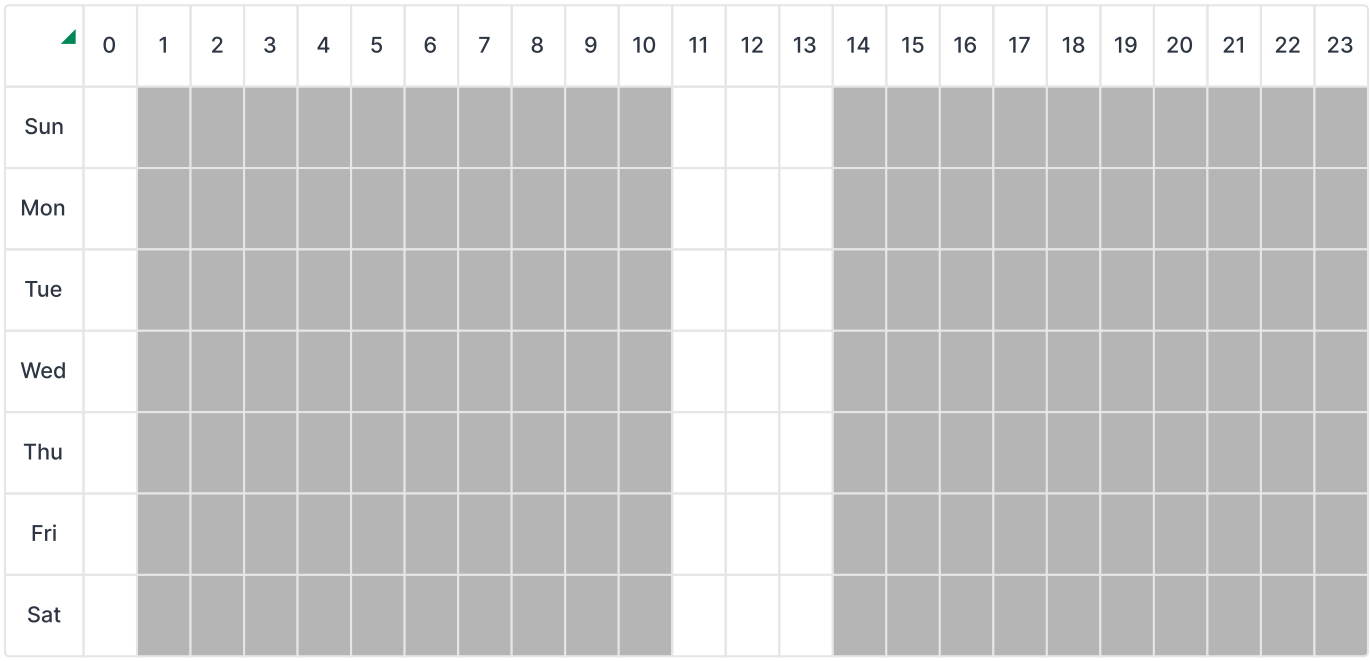
You can further protect your data by safeguarding backup copies on a secondary appliance or on a remote storage of your choice.

See how data immutability works on ActiveProtect: https://sy.to/apmdi

Isolate backups with air-gapping

Access: Allow access

Disallow access



Synology ActiveProtect allows users to create air-gapped backups that are inaccessible as the appliance is disconnected or switched off. This prevents ransomware from accessing the data as the backups are stored offline.

Users can set access periods for their backup appliances by selecting transmission and non-transmission periods throughout the week. Users can also customise access settings to either allow or block access.

To allow access, businesses can enable the network interface cards. If backups are completed ahead of schedule, the appliances automatically revert to isolation mode. Companies can also limit access to specific IP addresses only.

To block access, organisations can completely isolate the backup appliances by deactivating the network interface cards or by shutting down the appliance.

To configure air-gapping with ActiveProtect, view: https://sy.to/apmag

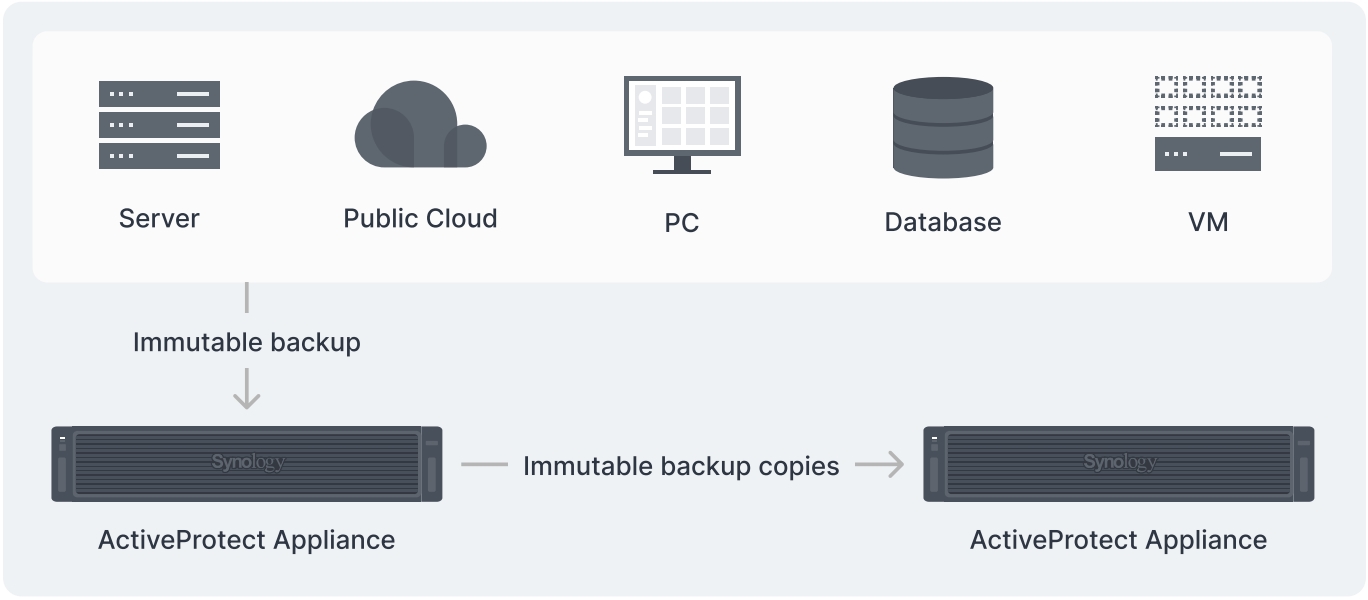
Fortify your defenses with role-based access controls

ActiveProtect comes with multiple features to boost your defences. We recommend setting up user authentication. You can integrate Windows AD and LDAP to centralise user management and set up authentication methods using existing SSO methods to establish multi-factor authentication, or by utilising 2FA to enhance login security and prevent unauthorised access to your data.

In addition, IT admins can restrict employee access to back up, access, or recover data. This prevents privilege abuse and ensures that access is delegated to specified users only.

To manage user authentication with ActiveProtect, view: https://sy.to/apmua

Ensure data redundancy with Synology ActiveProtect



In order to ensure data redundancy, it's best to safeguard multiple copies of your backups.

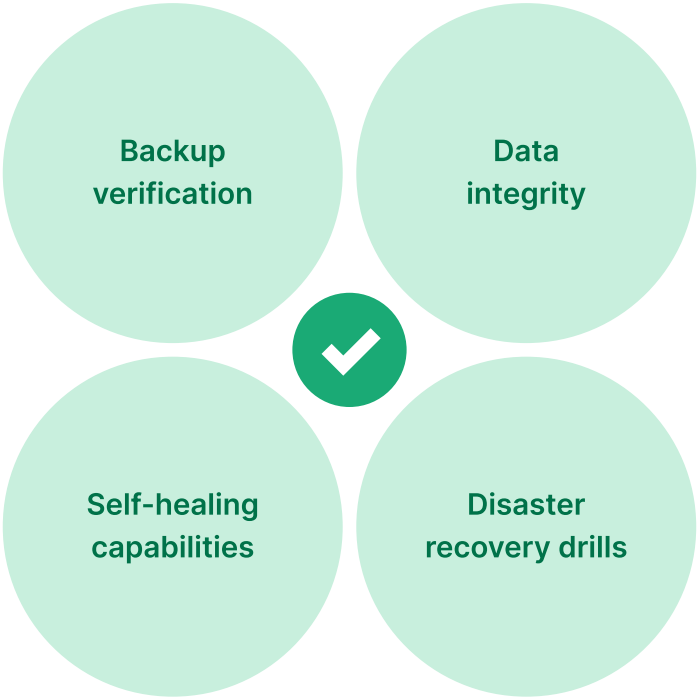
Safeguard immutable copies of your backup onto a secondary backup appliance by creating an air-gapped environment to safeguard against ransomware. Data copies can also be stored onto additional on-prem or cloud repositories such Synology SA or HD Series, select XS or XS+ models or cloud repositories such as C2 Object Storage, Amazon S3, or Wasabi.

This enhances disaster resilience and ensures peace of mind, as clean copies of your data are readily available for recovery in the event of sudden data loss.

To learn more about Synology's on-prem and cloud backup repository solutions, view: https://sy.to/bst

How ActiveProtect guarantees data recovery

With a series of data assurance features such as backup verification, data integrity checks, self-healing capabilities, and disaster recovery testing, there are several ways to ensure that your data is clean and can be successfully recovered when needed.



Self-healing and data integrity safeguards

ActiveProtect proactively detects errors and corrupt data and repairs it with its self-healing capabilities. Btrfs automatically detects and repairs data corruption via data and metadata check summing to ensure zero errors. This ensures data integrity and prevents data corruption.

With Btrfs' built-in file self-healing capabilities, checksums are provided for both data and the metadata, so that two copies of the metadata are generated. The checksums are then verified during each read process. If a mismatch is discovered, this means that there is silent data corruption. The Btrfs file system then automatically detects the corrupt files and then recovers the data via RAID.

With ActiveProtect's data integrity safeguards, only clean copies of your data are stored after verification.

To learn more about Btrfs, view: https://sy.to/apbtrfs

Verify your backups

ActiveProtect automatically verifies backed up workloads by capturing a video of the backup image. This is to confirm that an accurate copy of your data has been preserved. The video is then captured in ActiveProtect's built-in hypervisor and the entire process is recorded. This helps to verify backup reliability and ensure that your backups can be recovered when needed.

Enable backup verification when creating your protection plans. Users will have to configure it under advanced settings. Backup verification is available for virtual machines and physical servers.

To enable backup verification on ActiveProtect, view: https://sy.to/apmbv

Test your backups and instantly restore data via a built-in hypervisor

ActiveProtect comes with a built-in hypervisor for users to create a sandboxed and isolated environment to test data recovery. This allows IT to test their disaster recovery strategies without any impact to the production site.

Physical servers and virtual machines can also be instantly restored to the built-in hypervisor. The backed-up image of physical servers is mounted on the built-in hypervisor, while virtual machines can be restored within minutes. This allows you to quickly validate your backups to ensure recoverability.

To restore backups to the built-in hypervisor, view: https://sy.to/apmbih

Recover off-site data with ease

Data copies stored onto secondary appliances or on-prem or cloud repositories can be restored to the source environment with a click of a button via ActiveProtect's central console.

Granular recovery options such as file or folder-level download or full device recovery are available for workloads such as PCs, physical servers, and virtual machines.

To restore data from ActiveProtect's recovery portal, view: https://sy.to/apmrp

To find out which recovery options are available for each workload, view: https://sy.to/apmrcs

Self-service restoration made simple

Delegate recovery access to specific team members to perform restorations independently without relying on IT admins.

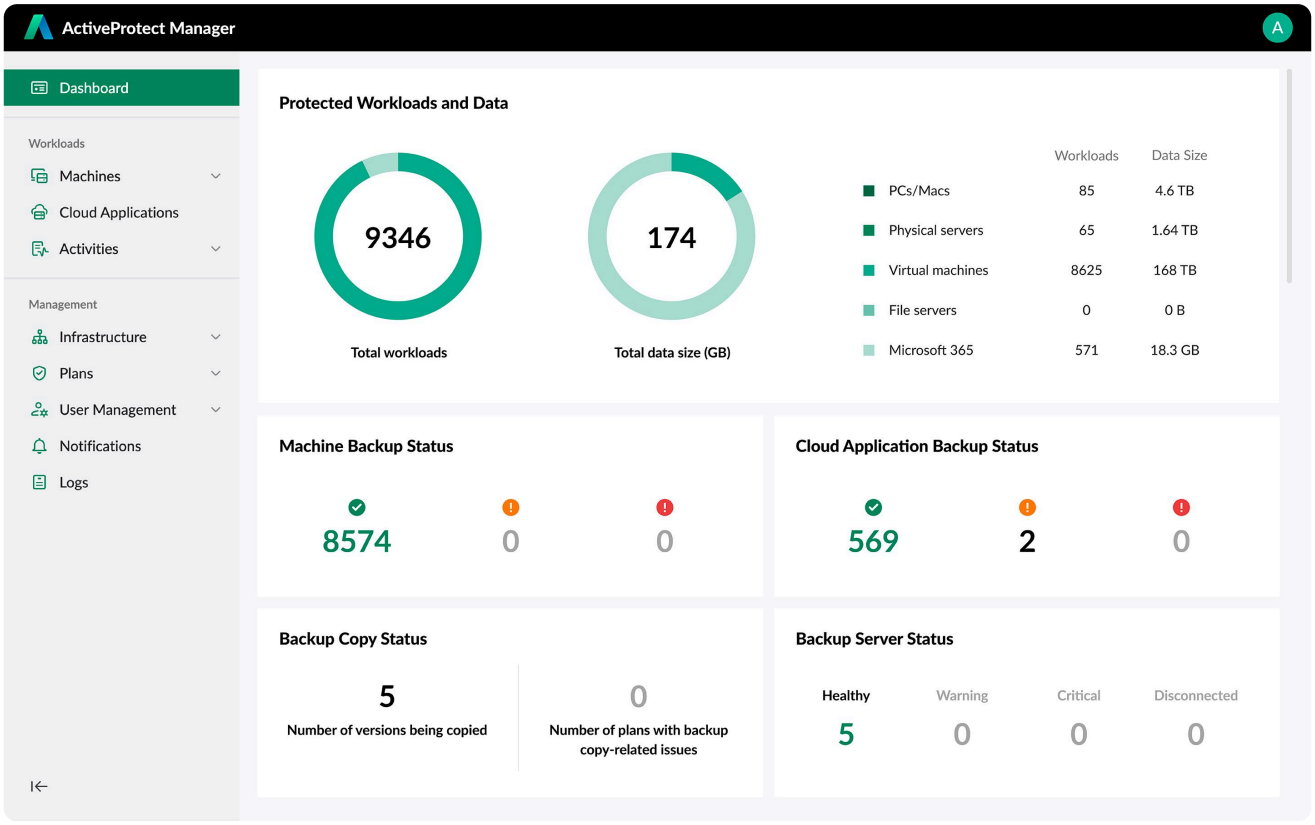
When restoring physical workloads or virtual machines, users with restore permissions can be assigned access to specific backup servers only. This way, they will only be able to restore workloads backed up on those servers via the recovery portal. Users can also be restricted to specific workloads they have access to restore via the recovery portal.

To restore Microsoft 365 data, each user must match their ActiveProtect Manager login accounts with their Microsoft 365 identities to enable SaaS data restoration.

To enable self-service restoration on ActiveProtect, view: https://sy.to/apmssr

Audit your backups with ActiveProtect to meet compliance and standards

Auditing backups is an essential part of the backup strategy to comply with regulations such as HIPAA, ISO 27001, GDPR, and other privacy laws or internal security policies. Regular audits allow organisations to uncover hidden risks, verify, and ensure the safety of their data.



Get a quick overview of your backup environment

ActiveProtect Manager comes with a dashboard that provides an overview of your entire ActiveProtect cluster. Monitor backups in real time by viewing the backup status. Any missed or unsuccessful backups, backup warnings, or errors will also be displayed on the console, allowing users to quickly identify and resolve issues.

The total number of your protected workloads across physical, virtual, and SaaS platforms, the size of the protected data, and the deduplication ratio, which reflects the actual storage space taken up in the appliance, will be displayed on ActiveProtect Manager's dashboard.

In addition, companies will be able to view the status of their backup servers to ensure that there are no warning or critical issues and to check if they are running smoothly and connected to the management server.

The ActiveProtect Manager console also displays the backup duration overview, backup data increase, and total storage usage. The backup duration overview section allows you to monitor backup performance by tracking the duration of your backups. The backup data increase section visually shows the total amount of your data before and after deduplication, highlighting how much storage capacity has been saved.

The total storage usage section at the bottom allows users to track how storage usage has evolved over time (after deduplication). This allows companies to effectively plan their backup infrastructure by keeping future growth in mind.

To navigate ActiveProtect's dashboard, view: https://sy.to/apmnd

Monitor backup tasks proactively

Users can view the status of their ongoing backups and any historic backups underneath the Backup Activities tab. This can be used to identify any workloads that have failed or are only partially successful and to identify any issues. Ongoing and historic restoration activities are under the Restore Activities tab.

The list of backup and recovery activities can then be exported for auditing purposes.

To monitor backup and restore activities with ActiveProtect, view: https://sy.to/apmmbr

Stay on top of your backups by setting up and receiving notifications about the status of your backup tasks. Receive hourly or daily scheduled data reports via email to monitor your backups and restore activity to meet SLA compliance.

To configure notifications with ActiveProtect, view: https://sy.to/apmns

Monitor and audit backup logs

Track your backup activities and your appliances' health and be notified. Generated logs also allow users to gain insights into how ActiveProtect is functioning. In addition to activity logs, this includes advanced system logs, drive information, and connection logs. This is crucial to diagnosing system issues or any performance issues.

Logs can be exported for audit purposes. You can export all logs or logs from a specific time frame only.

Logs can also be forwarded for centralised management and monitoring. This allows IT to track user activity and investigate any breaches or abnormalities. Detailed records of users' actions can be used to identify suspicious activities and meet compliance requirements.

To monitor logs with ActiveProtect, view: https://sy.to/apml

Conclusion

With increasing risk and uncertainty, businesses must be proactive in keeping their data safe and secure. This is the only way to ensure there are no issues with recovery and to be completely confident in their ability to restore clean copies of data if hit by ransomware or sudden data loss.

With ActiveProtect, modern backup and deduplication techniques safeguard data and reduce storage capacity. ActiveProtect also comes with built-in data immutability so that no changes or deletions can be made to your data, and physical or logical air-gapping capabilities to isolate clean copies of your data for guaranteed recovery.

Conduct automatic backup verification to ensure your backups are healthy. In addition, self-healing and data integrity safeguards are included to detect errors, repair data, and prevent data corruption. ActiveProtect also comes with a built-in hypervisor so that users can test their backups to ensure there won't be any issues during data recovery.

Meet compliance and standards by using ActiveProtect’s dashboard for a quick overview into your backup environment. In addition, monitor backup tasks, receive notifications proactively via scheduled daily reports, and audit backup logs to see if there are any backup issues or system issues. This is how ActiveProtect ensures data recovery.

ActiveProtect Data Recovery Assurance Checklist

See if your organisation has implemented a secure data protection solution to ensure confident data recovery and maintain business continuity.

A. Data and workload protection

- [ ] Backed up on-prem devices such as Macs, Windows PCs, Windows Servers, Linux servers, NetApp ONTAP, Nutanix Files, and more
- [ ] Backed up virtual machines such as Microsoft Hyper-V and VMware
- [ ] Backed up databases such as Oracle Database and Microsoft SQL Server
- [ ] Backed up SaaS workloads such as Microsoft 365 accounts

B. Data backup strategy

- [ ] Verify your backups to ensure an accurate copy of your data is preserved
- [ ] Enable automatic self-healing capabilities to ensure data integrity
- [ ] Automatically back up, schedule, or trigger event-based backups to safeguard your data
- [ ] Set immutable data protection policies for your backups and backup copies
- [ ] Select an off-site location to store your data
- [ ] Set air-gapping policies to store isolated copies of data
- [ ] Set retention policies to safeguard your data for a specific period of time

C. Data recovery strategy

- [ ] Run disaster recovery drills with a built-in hypervisor
- [ ] Leverage P2V or V2V migration for instant data restoration or cross-platform data restoration
- [ ] Leverage bare-metal or file-level restoration to recover entire devices or select files only
- [ ] Enable self-service restoration for employees to restore data from the recovery portal

D. Access controls and notifications

- [ ] Monitor and manage the entire backup environment from an intuitive dashboard
- [ ] Audit logs related to backup and restore activities, drives, connectivity, and more, to track user activity and ensure compliance
- [ ] Set role-based access controls to limit employee access to data
- [ ] Configure domain settings to integrate Windows AD and LDAP to authenticate user identity
- [ ] Leverage SSO, 2FA, and MFA to enhance login security
- [ ] Configure email notifications to receive alerts for critical events and more, in real time
- [ ] Receive scheduled data protection reports to stay on top of tasks

Too many unchecked boxes? Speak to a Synology expert about ActiveProtect and see how we can help fill those gaps.

https://sy.to/pjdts

Synology®

SYNOLOGY INC.

9F., No.1, Yuandong Rd.
New Taipei City 220632
Taiwan

SYNOLOGY AMERICA CORP.

3535 Factoria Blvd SE,
Suite #200, Bellevue,
WA 98006
USA

SYNOLOGY FRANCE

102 Terrasse Boieldieu
(TOUR W) 92800 Puteaux
France

SYNOLOGY GMBH

3535 Factoria Blvd SE #200
Bellevue, WA 98006
Tel: +1 425 818 1587

SYNOLOGY JAPAN CO., LTD.

4F, No. 3-1-2,
Higashikanda,
Chiyoda-ku, Tokyo, 101-0031

SYNOLOGY SHANGHAI

3535 Factoria Blvd SE #200
Bellevue, WA 98006
Tel: +1 425 818 1587

SYNOLOGY UK LTD.

Unit 5 Danbury Court,
Linford Wood,
Milton Keynes, MK14 6PL,
United Kingdom

synology.com