



Data Protection Guide 2025

Secure your data and scale your business with a
streamlined data protection solution



Table of Contents

Key features	04
ActiveProtect appliance	05
C2 Backup for Business	10
Workload protection	14
Safeguard PCs, Macs, and physical servers	15
Protect your file servers	16
Secure your virtual machines	17
Back up databases	18
Safeguard Microsoft 365 services	19
Synology data protection deployment	20
Specs	22

Synology backup and recovery solutions

Synology's cutting-edge data protection solutions allow businesses and organizations worldwide to maintain business continuity and recover data with speed in the face of sudden data loss, downtime, or malware attacks.

Our solutions protect...

23M+

Protected SaaS accounts

2.5M+

Protected endpoints & VMs

Synology data protection solutions

Resilient and reliable backup and recovery solutions that empower enterprises to protect new and existing workloads such as SaaS applications, physical devices, virtual machines, and databases via purpose-built backup appliances and a cloud backup service for fast data recovery and continued service availability.



ActiveProtect appliance

Create high-performance backup clusters with backup appliances and store your data locally to establish total data ownership.



C2 Backup

Secure on-prem and cloud workloads to the cloud with reduced upfront costs and zero hardware maintenance efforts.

Trusted by industry leaders



Key features

Flexible deployment options

Protect your data in minutes. Flexibly choose between storing a wide variety of workloads in clusters via a purpose-built backup appliance or safeguarding backups directly to the cloud.

Automate your data protection

Schedule your backups on a regular basis with time-based or event-based backups to protect against accidental data loss, hardware failure, malware attacks, and more.

Protect against ransomware

Perform immutable backups and store air-gapped backups off-site to meet regulatory compliance.

Role-based access control

Implement access controls to maintain control over business data, delegate admin rights to select employees only, and authenticate users for secure access to data.

Scale as your data grows

Implement an on-demand scalable data backup solution to meet evolving data needs. Store your data with a purpose-built backup appliance or in the cloud without disrupting or transforming your existing backup infrastructure.

ActiveProtect appliance

Simplify your backup management, achieve fast and efficient backup and recovery performance, view your primary backups, backup copies, and archived data no matter where they are stored, restore your data with peace of mind, and scale your backup infrastructure whenever needed.

Synology's purpose-built backup appliances come a variety of features including plan-based workload protection, immutable capabilities, logical and physical isolation, and more, to safeguard your backups and reliably restore your data, in the event of a ransomware attack or sudden data loss.



Optimized backup and recovery performance

Up to

7x faster backup speeds¹

Over

2x faster data recovery speeds¹

Up to

50% data reduction¹

Up to

-99% data transmission^{1,2,3}

ActiveProtect appliance highlights



Quick deployments

Deploy your server within minutes.



Guaranteed data backup

Detect and restore corrupt data, verify backups, and test your disaster recovery strategy in a sandboxed environment via built-in virtual machines.



Protect against ransomware

Secure your data with immutability and isolate your data with air-gapped backups so that a clean copy of your data can be recovered, whenever needed.



Recover with confidence

Leverage bare-metal or file-level restoration to restore data or perform P2V or V2V restoration to instantly recover data.



Prioritize security controls

Safeguard against cyberattacks by executing firewall settings. Super admins can implement passwordless authentication for secure access to backup appliances and delegate admin privileges such as self-service recovery to select employees only.



On-demand scalability

Scale your data with ease to meet changing business requirements.

Note:

1. Performance figures have been obtained through internal testing by Synology Inc.
2. Maximize storage capacity with cross-site deduplication and global deduplication.
3. Eliminate redundant data with source-side deduplication to enable fast data transmission.

Streamline your data protection



Boost your backup performance

Leverage incremental backups and global source-side deduplication to perform backups with speed and reduce overall bandwidth usage and storage consumption.

Automate your backups

Automatically back up all workloads within a protection plan to minimize the risk of data loss. Schedule backups or trigger event-based backups to safeguard all your data.

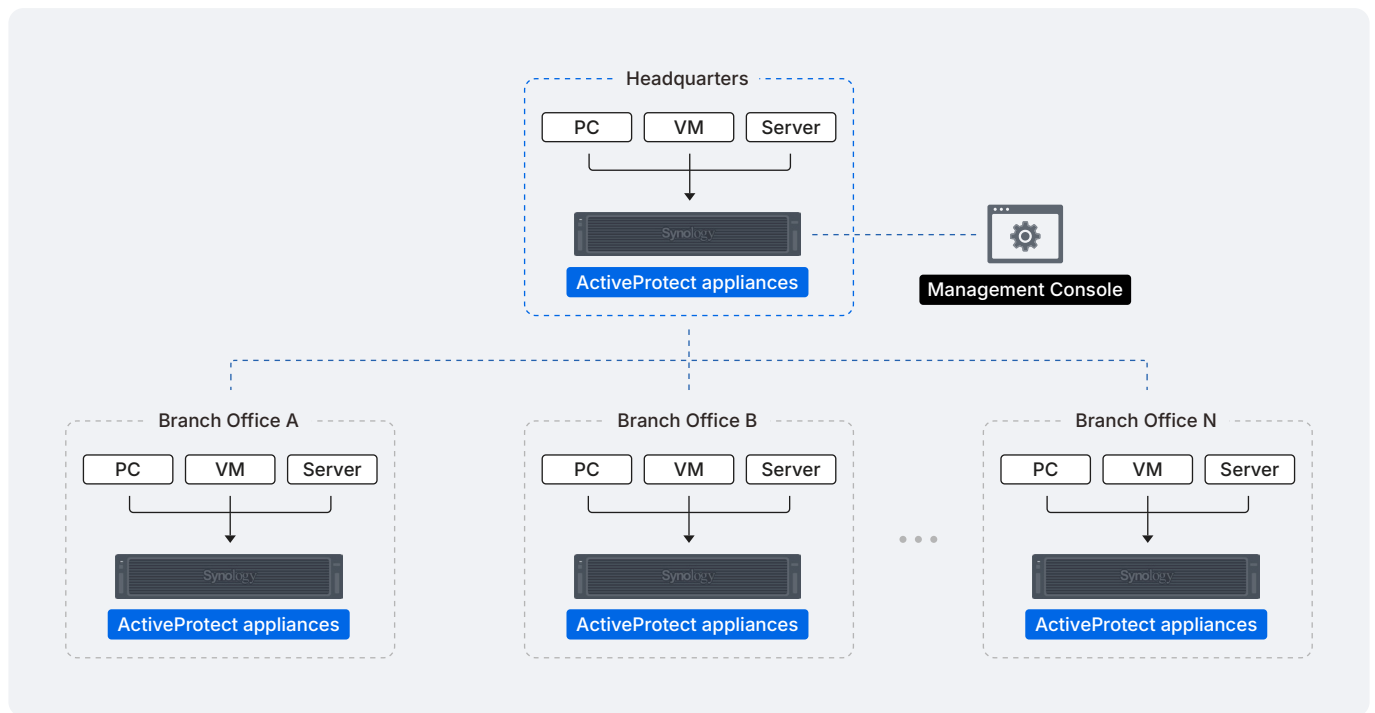
Configure cluster settings with ease

Implement backup settings, backup frequency, retention policies, off-site backups, and more, across your backup infrastructure.

Data protection made simple

Automatically protect new workloads and tie them with custom protection plans to meet and exceed backup SLAs and eliminate data silos.

Monitor and manage all workloads via a cluster



Consolidate and view all your backup appliances

Create a cluster of up to 2,500 backup appliances and monitor and manage up to 150,000 workloads.

Enhance your data visibility

Track all your backup appliances and repositories, view and access your entire backup infrastructure, and retrieve your data, no matter where it is located.

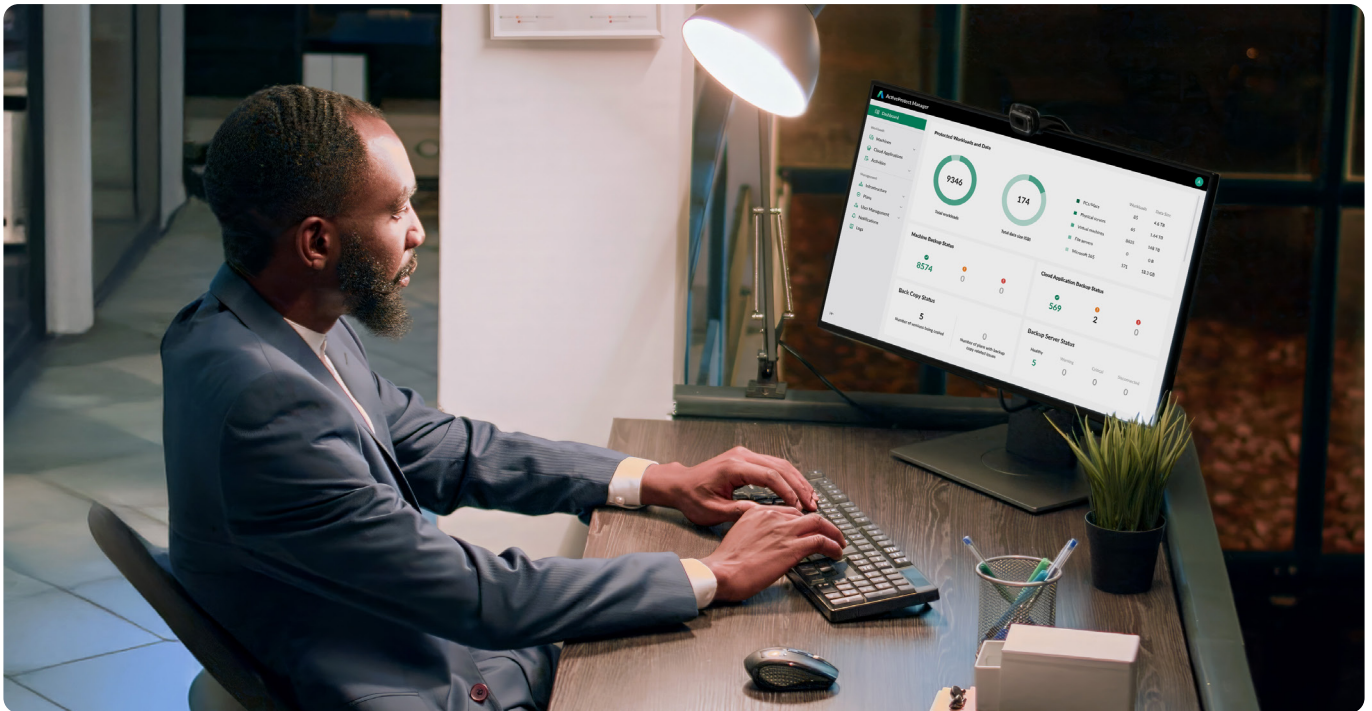
Proactively monitor your backup tasks

Monitor all ongoing backup and restore jobs and notify users if any backup abnormalities are detected. View log activities and receive backup reports to stay on top of your backup tasks.

Scale with ease

Simply add new backup servers to your cluster to meet growing data needs and maintain business continuity by accessing the same data set.

Achieve data redundancy



Automatic backup verification

Ensure accurate copies of your data are preserved as data is automatically checked during backups.

Data integrity safeguards

Detect errors or corrupt data and repair data with self-healing capabilities by setting and implementing a proactive maintenance strategy.

Disaster recovery drills

Perform disaster recovery drills on a regular basis via a built-in virtual machine or test your SaaS accounts without affecting production site to ensure that data can be recovered effectively, in the event of a disaster strike.

Store clean copies of your data

Isolate your data from source environments with logical and physical isolation and prevent data modification or deletion with immutable capabilities, so that a clean copy of your data can be recovered whenever necessary.

Implement access controls

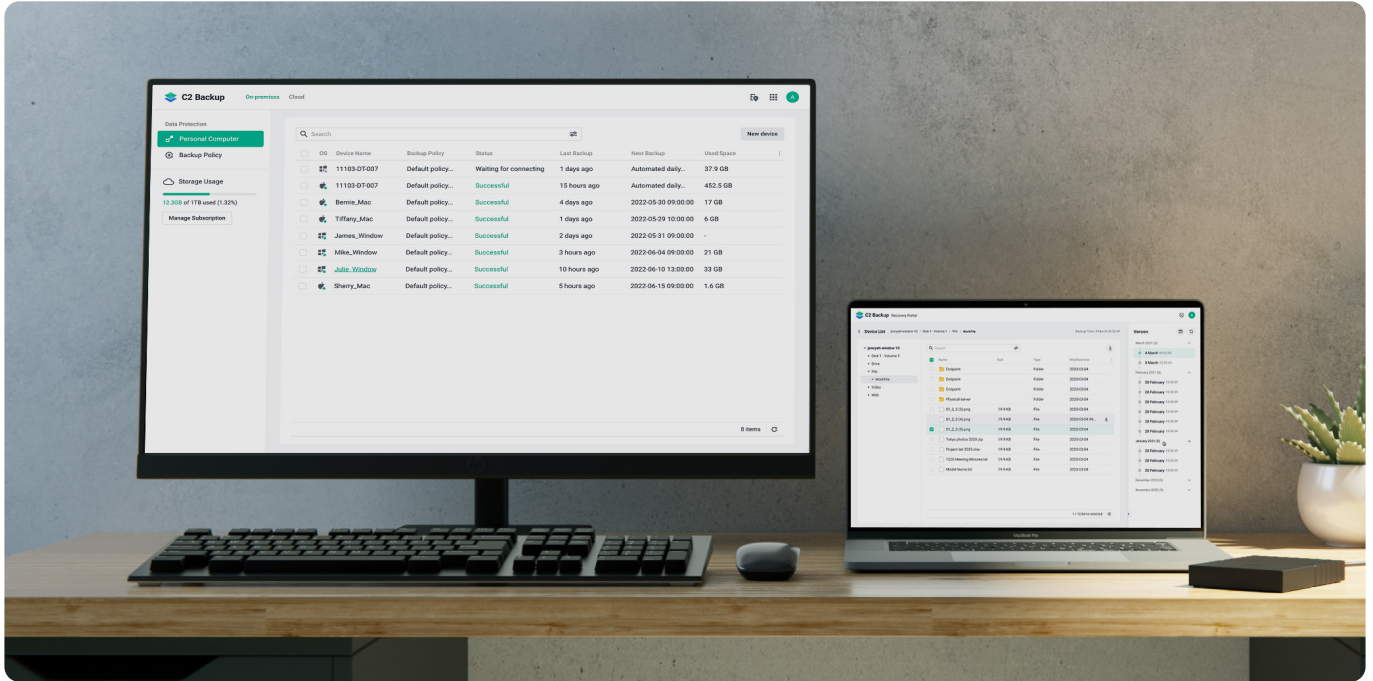
Utilize Active Directory to maintain control of data access, assign users the right to view and restore data, and implement multi-factor authentication to prevent unauthorized access to your data.

Recover data with ease

Flexibly recover your workloads via full device recovery, granular file recovery, or P2V or V2V instant restoration.

C2 Backup for Business

Secure platform to protect on-prem and cloud workloads in the cloud.



Safeguard your workload directly to the cloud

Leverage powerful backup and recovery features to safeguard, monitor, and access previously scattered workloads such as PCs, Macs, servers, and data stored on Microsoft 365 services, directly to the cloud.

C2 Backup for Business Highlights



Automate your backups

Schedule your backups with time or event-based conditions to ensure availability.



Perform ultra-fast backups

Reduce bandwidth usage and storage consumption by backing up changed data only.



Customize your retention policies

Store multiple backup copies directly to the cloud to meet internal or external regulatory compliance.



Data restoration made simple

Restore devices with bare-metal recovery or Microsoft 365 objects with file-level recovery options.



Role-based access control

Control and monitor backup and restore permissions by separating and granting employee access based on their roles and responsibilities at the company.



Free up IT resources

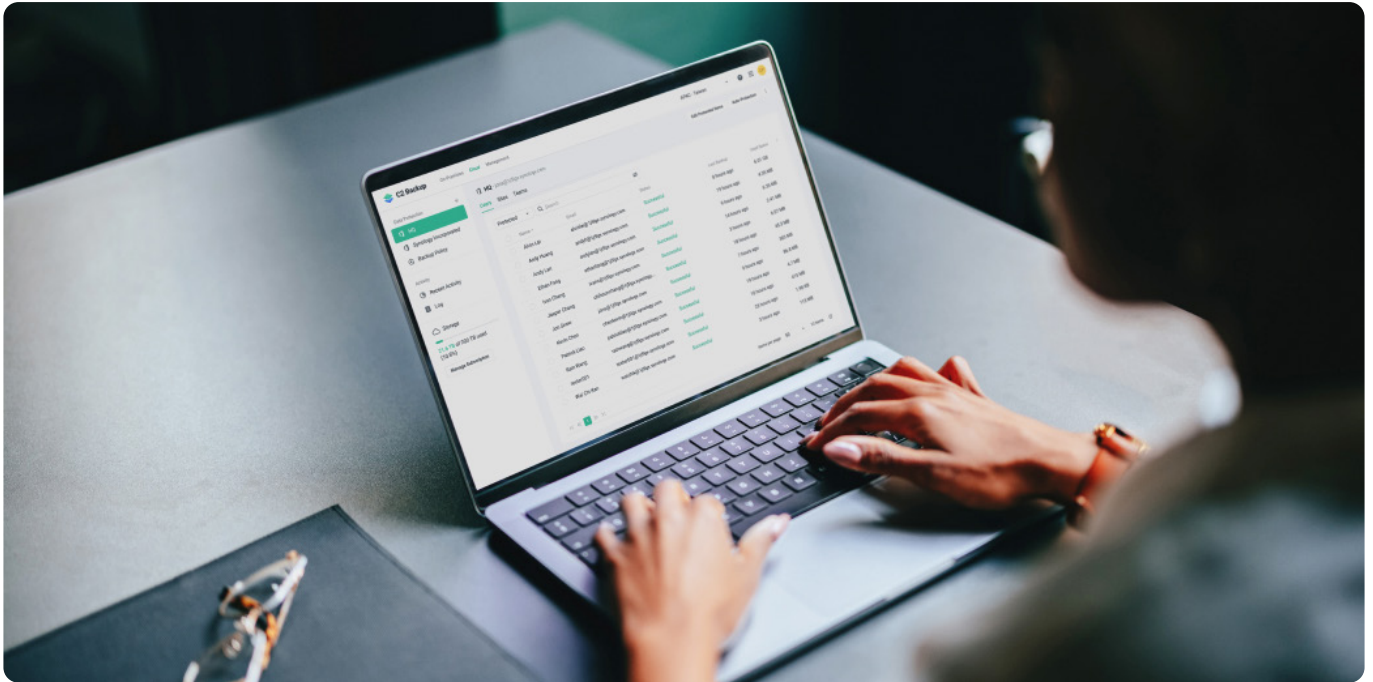
Recover data from a self-service portal with minimal supervision, as long as admin consent has been granted.



Keep an eye on your backups

Receive email alerts, backup status notifications, and scheduled reports to better manage your backups.

Safely store your data in the cloud



Schedule automatic backups

Secure your workloads by setting up time or event-based conditions for continued data protection.

Maximize your storage capacity

Optimize your storage capacity by only backing up changed data as a way to allot more space for future backups.

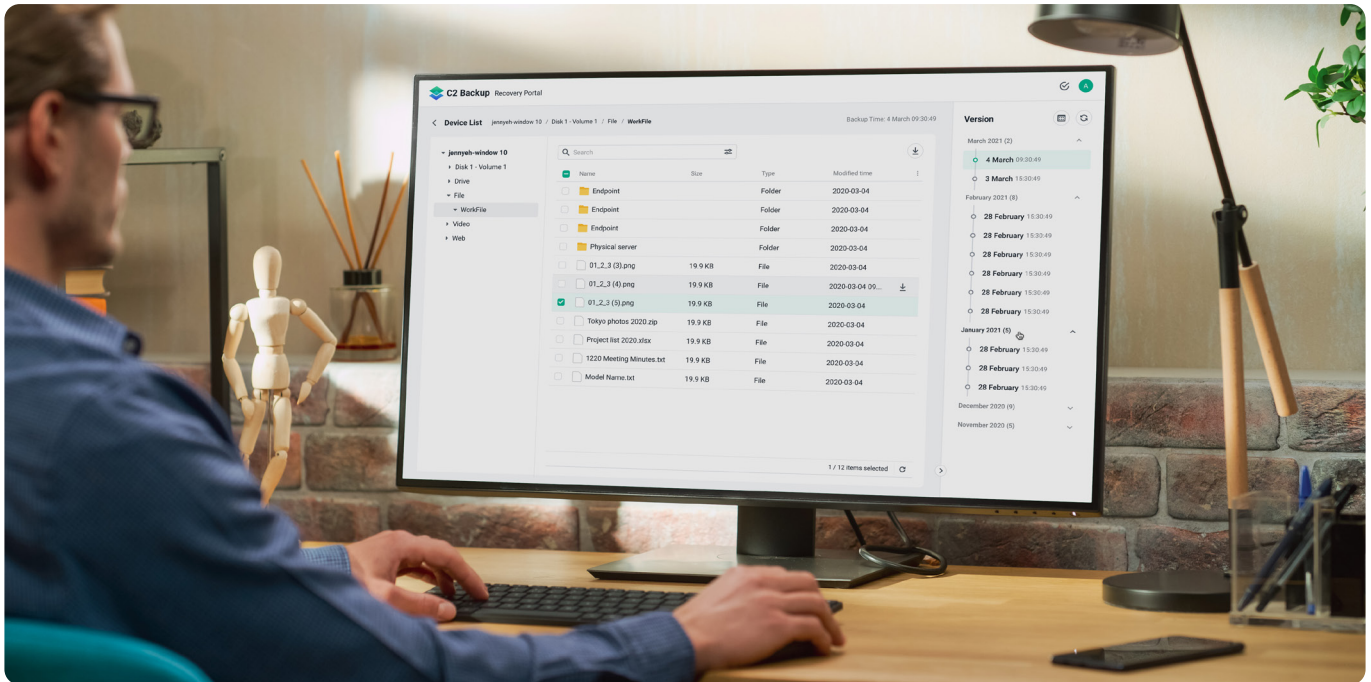
Store data off-site

Back up data directly to the cloud to ensure continued access to your data, no matter where your employees are working from.

Proactively manage your backups

Receive email alerts and notifications on your backup status and view a summary of your backups to better monitor your workloads.

Data restoration made easy



Simplify your data recovery process

Perform bare-metal restoration when restoring Mac or Windows devices or download specific files and folders from the C2 Backup Recovery Portal.

Restore Microsoft 365 data

Restore OneDrive for Business, SharePoint Online, Exchange Online, or Microsoft Teams, to the original tenant or directly download backup versions to your local device.

Restore your devices

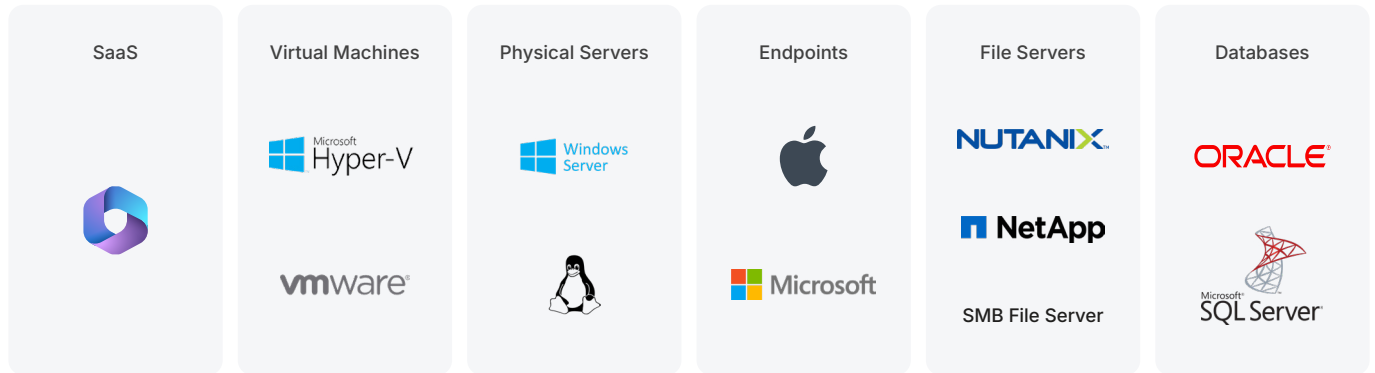
Restore entire devices, including system settings, applications, and more, so that you don't need to spend time setting up Windows PCs from scratch.

Speed up recovery via a self-service portal

Permit authorized employees to initiate self-service recovery as a way to free up IT admin tasks and increase employee autonomy.

Safeguard on-prem and cloud workloads

Boost your cyber resilience by implementing proven on-prem and cloud solutions that safeguard a diverse range of workloads.



Bolster your data protection with a strong backup and recovery plan

Consolidate and back up all your digital data and protect against ransomware attacks and other threats to achieve enterprise data security and ensure business continuity.

Secure business-critical workloads

Safeguard PCs, Macs, and physical servers

Consolidate employee endpoints on a unified console to reduce downtime in the face of sudden data loss.

- Perform ultra-fast backups, minimize data transfer, and save redundant data transmission traffic
- Restore your entire device or perform file-level restoration and select the files that need to be recovered
- Set up role-based access controls to ensure accessibility to business data and minimize security risks within an organization



Mac



Windows PC



Windows Server



Linux

Automate your backups

Set up event or time-based backups to run backups while simultaneously running your endpoints.



Agent-based deployment

Perform backups for large amounts of physical servers in one go by deploying a backup agent.



Protect your file servers

Safeguard mission-critical data stored on file servers to maintain business continuity at all times.

- Safeguard file servers as they are running and perform backups for new or changed data only
- Tamper-proof your backups with built-in immutability and store data for as long as needed
- Free up IT resources by assigning admin access to select employees for self-recovery, as long as they have permission to do so

NUTANIX

Nutanix Files

NetApp

NetApp ONTAP

Deploy with efficiency

Leverage SMB protocol and Windows VSS to perform agentless backups.

Restore with ease

Retrieve entire file shares or specific files to a specific restore point.



Secure your virtual machines

Protect large quantities of business virtual environments on a single platform.

- Perform agentless backups to safeguard your virtual machines with convenience
- Automatically detect and protect new virtual machines to reduce IT efforts
- Leverage built-in hypervisors to verify your backups in a sandboxed environment to ensure that an accurate copy of your data is available, when needed

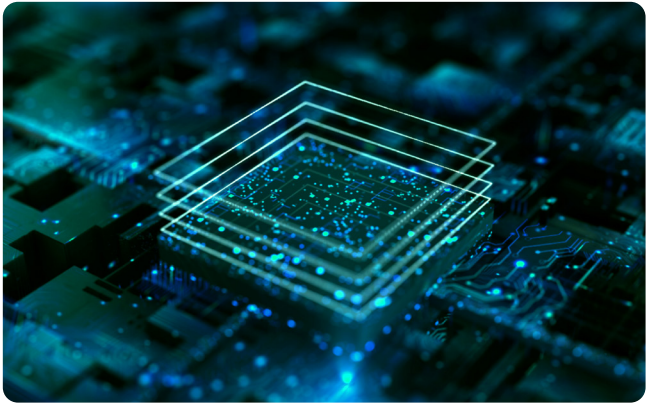
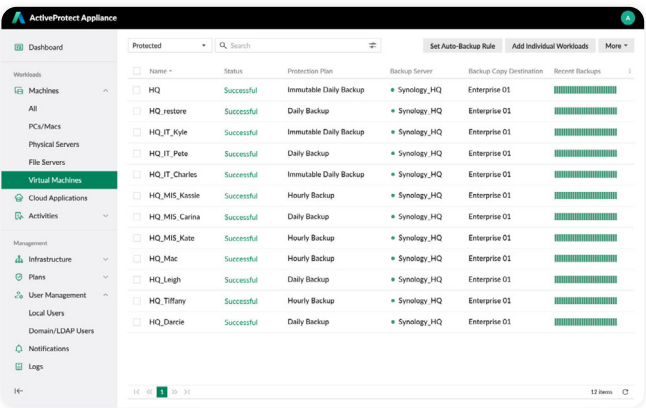


Application-aware backups

Maintain data consistency by performing application-aware backups to prevent data loss.

Instant restoration

Restore virtual machines across hypervisors without being tied down to one console.



Back up databases

Ensure data resiliency even in the face of disaster by securing database data.

- Immutability prevents your data from being modified or deleted by anyone
- Directly restore database data via P2V or V2V migration to minimize disruption
- Granularly restore your databases by downloading each database from the recovery portal as needed

ORACLE®

Oracle Database

Microsoft®
SQL Server®

Microsoft SQL Server

Database-aware backups

Perform application-aware backups to ensure that database data is consistently backed up to prevent data loss.

Data visibility

Check and recover your database data from any previous points in time via the recovery portal.

The screenshot shows the 'Protected' tab in the ActiveProtect Manager interface. It displays a table of protected databases with columns for Name, Status, Database, Protection Plan, Backup Server, Backup Copy Distribution, and Recent Backups. The table lists several databases, all with a 'Successful' status.

Name	Status	Database	Protection Plan	Backup Server	Backup Copy Distribution	Recent Backups
sales_db	Successful	SQL & Oracle	Database Backup	HQ	HQ_Backup_Copy	
sales_performance	Successful	SQL & Oracle	Database Backup	HQ	HQ_Backup_Copy	
crm_customer_data	Successful	SQL	Database Backup	HQ	HQ_Backup_Copy	
warehouse_db	Successful	Oracle	Database Backup	HQ	HQ_Backup_Copy	
customer_accounts	Successful	Oracle	Database Backup	HQ	HQ_Backup_Copy	
crm_db	Successful	Oracle	Database Backup	HQ	HQ_Backup_Copy	

The screenshot shows the 'Self-Service Permissions' tab in the ActiveProtect Manager interface for the 'sales_db' workload. It displays a table of users who can restore backup data for this workload in the Recovery Portal. The table lists several users, all with a status of 'Active'.

Name	Email	Description	Status
Admin_HQ		Super admin with full access	Active
Tam_Sales		Super admin with full access	Active
John_Sales		Super admin with full access	Active
Tiffany_Sales		Super admin with full access	Active

Safeguard a variety of Microsoft 365 services

Centralize backups of Microsoft 365 data for continuous access and better recoverability of your data.

- Safeguard OneDrive for Business, SharePoint Online, Exchange Online, and Microsoft Teams
- Automatically search for and protect new Microsoft 365 objects to meet regulatory compliance
- Granularly restore your Microsoft 365 objects with file or folder-level download options



OneDrive



SharePoint



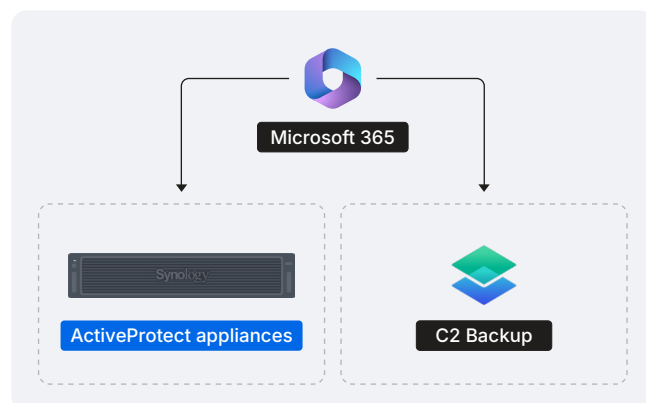
Exchange



Teams

Immutable backups

Prevent data modification or deletion with immutability across your backup infrastructure.



Self-service recovery portal

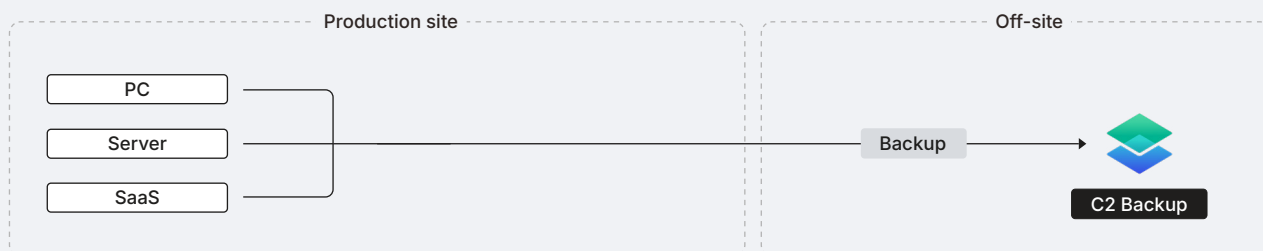
Recover data from a self-service portal, without help from IT admins, as long as employees have been granted permission.



Deploy Anywhere

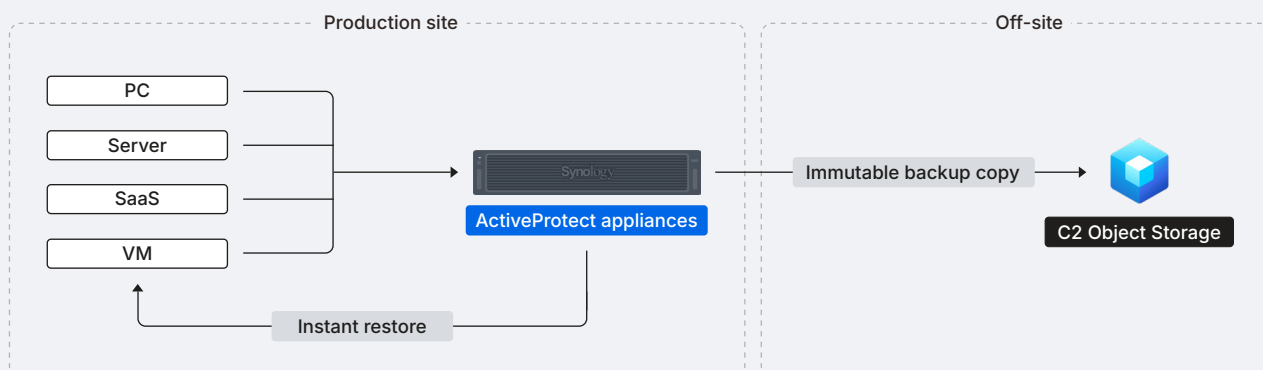
Implement a multi-tiered data protection plan for your organization.

Remote deployment



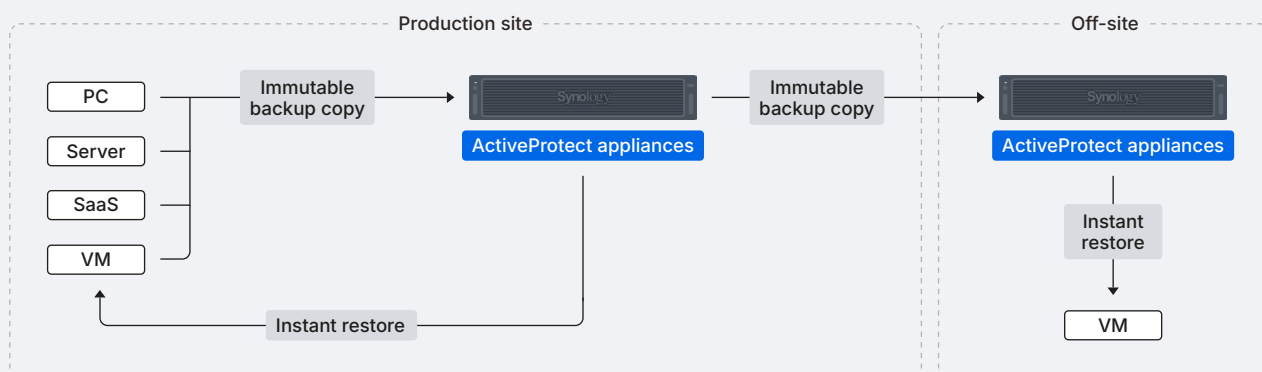
Team members located across the world can back up data stored endpoints such as PCs, Macs, and physical servers, as well as Microsoft 365 services directly to the cloud.

Single-site deployment (Off-site cloud backup)



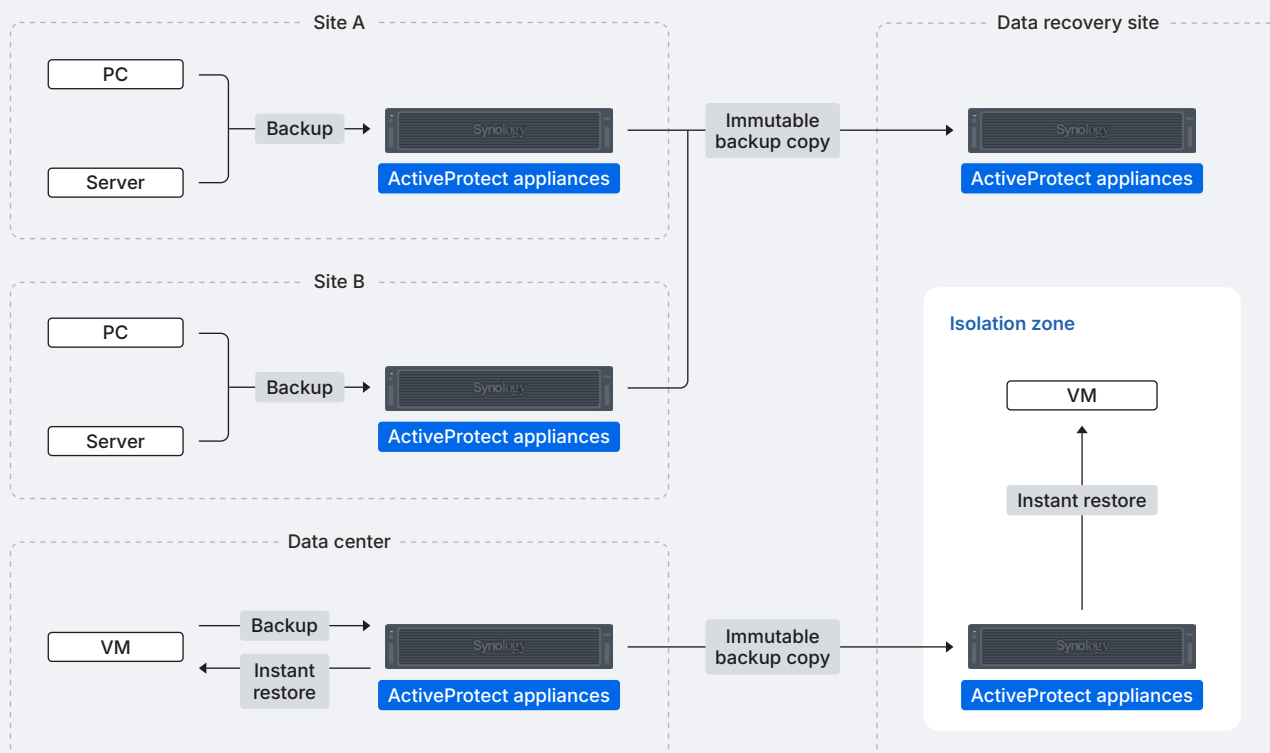
When team members or multiple teams operate from a single location, all endpoints can be backed up onto a central server with ActiveProtect and then copied to the cloud for added redundancy.

Single-site deployment (Off-site remote server)



Safeguard data stored across PCs, servers, Microsoft 365 services, and VMs onto ActiveProtect which can then be backed up to a secondary server or a scalable storage solution.

Multi-site deployment (Disaster recovery)



Sync data from multiple servers onto a central server and continuously back up this data onto a secondary server. Create an isolation zone to preserve clean copies of your backups.

Workload type	Windows PCs and Macs		Windows and Linux physical servers		VMware vSphere and Microsoft Hyper-V virtual machines
Backup solutions available	ActiveProtect appliance	C2 Backup	ActiveProtect appliance (Linux and Windows server)	C2 Backup (Windows server only)	ActiveProtect appliance
Backup scope	<ul style="list-style-type: none"> Entire machines System volumes Custom volumes 	<ul style="list-style-type: none"> Entire device backup Volume backups 	<ul style="list-style-type: none"> Entire machines System volumes Custom volumes 	<ul style="list-style-type: none"> Entire device backup Volume backups 	Entire virtual machine
Backup frequency	<ul style="list-style-type: none"> Manual backups Scheduled backups Event-triggered backups 	<ul style="list-style-type: none"> Scheduled backups (Daily) Event-triggered backups 	<ul style="list-style-type: none"> Manual backups Scheduled backups (Hourly, daily, weekly) 	<ul style="list-style-type: none"> Scheduled backups (Daily) Event-triggered backups 	<ul style="list-style-type: none"> Manual backups Scheduled backups (Hourly, daily, weekly)
Auto protection	 (Via connection key)	—	 (Via connection key)		
Backup verification		—		—	
Application-aware backups	—	—	 (Optional feature)	 (Built-in feature)	
Retention policy	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time
Deduplication		—		—	
Recovery methods	<ul style="list-style-type: none"> Bare-metal restore File or folder level restore 	<ul style="list-style-type: none"> Bare-metal restore 	<ul style="list-style-type: none"> Bare-metal restore File or folder-level restore Perform instant restore or full restore to VMware vSphere, Hyper-V, or a built-in hypervisor 	<ul style="list-style-type: none"> Bare-metal restore 	<ul style="list-style-type: none"> File or folder-level restore Perform instant restore or full restore to VMware vSphere, Hyper-V, or a built-in hypervisor

Workload type	Microsoft 365 services		SMB servers and NetApp ONTAP file servers	Microsoft SQL server and Oracle Database
Backup solutions available	ActiveProtect appliance	C2 Backup	ActiveProtect appliance	ActiveProtect appliance
Backup scope	Back up Microsoft Exchange Mail, contacts, chat, calendars, SharePoint, Teams, M365 groups, archived mailboxes, files and folders	Back up Microsoft Exchange mail, OneDrive files, SharePoint sites, Teams channels and chats	Select folders only	Entire database
Backup frequency	<ul style="list-style-type: none"> Manual backups Scheduled backups (Hourly, daily, weekly) 	<ul style="list-style-type: none"> Scheduled backups (Daily) Event-triggered backups 	<ul style="list-style-type: none"> Manual backups Scheduled backups (Hourly, daily, weekly) 	<ul style="list-style-type: none"> Manual backups Scheduled backups (Hourly, daily, weekly)
Auto protection	✓	✓	—	✓
Backup verification	—	—	—	✓
Application-aware backups	—	—	—	✓
Retention policy	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time 	<ul style="list-style-type: none"> Store all versions Store all versions for a certain number of days to meet long-term retention requirements Apply Grandfather-Father-Son retention policy and/or remove older versions after a set period of time
Deduplication	✓	—	✓	✓
Recovery methods	<ul style="list-style-type: none"> File or folder-level restore 	<ul style="list-style-type: none"> Bare-metal restore Download individual file backup versions 	<ul style="list-style-type: none"> File-level restore 	<ul style="list-style-type: none"> File-level download Database- and instance-level download



SYNOLOGY INC.

9F., No.1, Yuandong Rd.
New Taipei City 22063
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**

Grafenberger Allee 295
40237 Düsseldorf
Deutschland

**SYNOLOGY
JAPAN CO., LTD.**

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

**SYNOLOGY
SHANGHAI**

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist. Shanghai,
China

**SYNOLOGY
UK LTD.**

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



synology.com

© 2025, Synology Inc. All rights reserved. Synology, the Synology logo, and names and logos of Synology products are trademarks of Synology Inc. All other trademarks, logos, company names, and brand names are the property of their respective owners.

Synology reserves the right to make changes to product specifications and descriptions without prior notice.