Synology®

ActiveProtect Appliance

DP340

Cyber-resilient Data Protection Solution for Endpoints

The Synology ActiveProtect appliance DP340 is a data protection solution that comes pre-configured with hardware that runs ActiveProtect Manager, an operating system designed specifically for backup purposes. With its ability to perform backups, restore, deduplicate, replicate, and manage while ensuring security, the DP340 is an ideal backup server for your small and medium endpoints. It seamlessly integrates all current and future workloads across multiple sites into clusters, enabling centralized management through a single platform. With immutability, air-gapped backups, and access control, the DP340 protects against ransomware attacks, and secures all your data.

Highlights

- **Deploy quickly**
  Set up your server in minutes
- **Safeguard all workloads**
  Protect VMs, SaaS, databases, physical servers, and more
- **Visibility**
  Monitor servers, and backup status on a centralized platform
- **Reliable backup**
  Verify backups and test your disaster recovery plan in a sandboxed environment
- **Flexible recovery**
  Perform bare-metal, file-level recovery, or P2V/V2V instant restoration to meet your RTO needs
- **Ransomware defense**
  Leverage source-side global deduplication and a specialized backup engine
- **Optimized backup efficiency**
  Perform bare-metal, file-level recovery, or P2V/V2V instant restoration to meet your RTO needs
- **Data security**
  Implement least privilege with access controls, firewall, and isolation for a robust architecture

Quick and seamless deployment

Essential configuration such as disk partitioning and raid array setup will be automatically completed , making deployment fast and effortless so that you can start protecting your data immediately.

Protect workloads with specified policies

Safeguard all your workloads, including VMware vSphere, Microsoft Hyper-V, Windows, macOS, Linux, NetApp ONTAP, Nutanix Files, Microsoft 365 services, Oracle Database, and Microsoft SQL server. Establish policies for companies to meet SLA requirements, and automate data protection by detecting existing and future workloads, ensuring that the workloads are secured under the appropriate policies. View, modify, and manage policies with ease.

Reliable backup and flexible recovery

The DP340 supports self-healing functionality with continuous detection of silent data corruption through Btrfs checksum. It ensures zero errors by repairing corrupt data via RAID technology. To verify the recoverability of backup data, disaster recovery drills can be regularly performed in a sandboxed environment without affecting your primary production site. Backup verification is also available, automatically generating recovery drill videos for auditing purposes. In the event of a disaster, data can be flexibly restored based on your Recovery Time Objectives (RTO) via entire machine restoration, file-level recovery, physical-to-virtual (P2V), or virtual-to-virtual (V2V) methods to restore data to the designated location.

Uncompromised ransomware protection

To prevent ransomware attacks, the DP340 protects data backups and backup copies with immutability and write-once-read-many (WORM) storage to ensure that no one can modify data that has been backed up during the specified retention period. Additionally, it integrates encryption capabilities, enabling

data to be encrypted locally before being backed up to remote destinations. To further enhance security, you can also isolate the remote environment using the air-gap feature.

Optimized backup efficiency

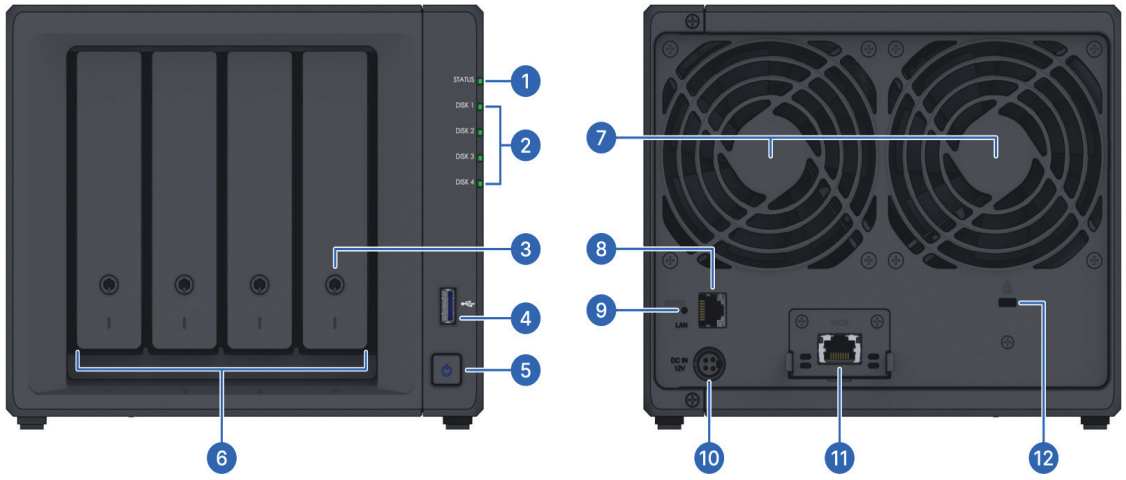
The DP340 optimizes storage space allocation via hardware and software integration. By leveraging SSD cache to store backup-related metadata, optimizing data organization, and consolidating multiple files into a single image, it accelerates data processing. Both backups and backup copies utilize global source-side deduplication, as it compares data at the source and only transmits non-duplicate data to save bandwidth and storage space.

Data security at its core

The DP340's security mechanism is based on the principle of least-privilege authentication and network protection architecture. This mechanism only allows authorized personnel to access data, restricts access to specific devices, and limits access to the backup infrastructure during designated times to ensure data security.

- **For authorized personnel:** Active Directory, LDAP, and SAML 2.0 integration enables enterprises to use existing SSO with MFA and granular permissions to enhance access control.
- **For devices:** Firewall settings can be configured to only allow access from devices within specified IP ranges and subnets. The built-in management port is an isolated interface dedicated for management purposes. It is separate from data flow to reduce security risks.
- **Enhanced isolation:** Remote backup infrastructure can be further secured via air-gapped solutions to achieve network or physical isolation. Combine this with scheduled backups to control network access during specified times or by directly powering devices on or off.

Hardware Overview



1	STATUS Indicator	2	Drive Status Indicator	3	Drive Tray Lock	4	USB 3.2 Gen 1 Port
5	Power Button	6	Drive Trays	7	RESET Button	8	Management Port
9	10GbE LAN Port	10	Power Port	11	Fan	12	Kensington Security Slot

Technical Specifications

General Specifications

Suggested Backup Source	* 14.5 TB (60 Machines or 150 SaaS Users)
Suggested Built-in VM	2
Suggested Cluster Size	Managed in a cluster that supports up to 2,500 servers

* These statistics are based on telemetry data and may vary depending on your company's usage.

Hardware Specifications

Form Factor	Desktop
CPU	AMD R1600 (2 cores)
Memory	16 GB
Storage Configuration	4 × 8 TB HDD (RAID 5) 2 × 400G SSD (RAID 1)
Network Interface	1 × 1GbE RJ-45 Port (Management) 1 × 10GbE RJ-45 Port (Data transfer)
Dimensions (HxWxD)	166 × 199 × 223mm
Weight	5.2 kg
Operating Temperature	32 to 104°F (0 to 45°C)
Storage temperature	-5 to 140°F (-20 to 60°C)

Environment and Packaging

Certification	FCC, CE, UKCA, BSMI, RCM, NCC, VCCI
Environmental safety	RoHS, REACH
Package contents	• 1 x DP340 main unit • 4 × 3.5” SATA HDD • 1 x Adapter • 1 x AC Power Cord • 2 x RJ-45 LAN Cable • 1 x Accessory Pack • 1 x Quick Installation Guide
Warranty	3 years

DP340-2024-ENU-REV001