

Datasheet



ActiveProtect Appliance

DP320

Synology

DP320



Robust Data Protection Solution for Edge and Branch Offices

The Synology ActiveProtect DP320 is a purpose-built backup appliance designed for branch offices, remote offices, retail sites, or managed service providers (MSPs). The DP320 can be deployed as an edge server while being managed by ActiveProtect appliances such as the DP7400, DP7200, or DP5200. As a compact desktop unit, companies can store local backups or backup copies and restore data with speed even with minimal resources. The DP320 comes with pre-configured hardware and software, called the ActiveProtect Manager. Synology ActiveProtect is a powerful data protection solution designed to streamline backups, recovery, and protect against ransomware, no matter where your data is located.

- **Rapid deployment**
Set up your backup appliances and start protecting your data within minutes
- **Safeguard all workloads**
Safeguard SaaS, IaaS, VMs, physical devices, and database data via one console
- **Complete visibility**
Deploy towers at branch offices to store backup copies and off-site copies, managed by 1U or 2U appliances
- **Maximize backup & storage efficiency**
Optimize backup efficiency CBT technology and deduplicate data with source-side and server-side deduplication
- **Ransomware defense**
Implement the 3-2-1-1-0 policy for immutable data protection, auto backup verification, off-site backups, and sandboxed DR tests
- **Restore data across platforms**
Recover data across cloud or on-premises platforms with P2V, P2C, V2V, V2C, C2V data recovery
- **Scale at any time**
Tier data to the cloud or on-premises solutions to free up space



Accelerate your deployment

Start backing up your workloads in minutes. Essential configurations, such as disk partitioning and RAID setup, are automatically completed during the initial setup of Synology ActiveProtect. The DP320 comes as a pre-configured backup appliance that includes all the required hardware components.



Workload protection across environments

Consolidate your on-premises, cloud, and virtual workloads on one platform. Safeguard Windows PCs, Macs, Linux, VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, NetApp ONTAP, Nutanix Files, Synology NAS, Microsoft 365 services, Google Workspace services, Oracle Database, Microsoft SQL Server, Azure VM, and Amazon EC2.



Ensure total data visibility

Manage and monitor all your backups, backup copies, and tiered data via a unified console. Implement workload protection policies to safeguard new or existing workloads automatically. Designed for edge and ROBO deployments, the DP320 provides local backup protection or protects additional backup copies across distributed locations.



Boost your backup performance and storage

With Synology ActiveProtect's SURE (Synology Unified Reduction Engine) technology, optimize backup efficiency and maximize storage capacity. With Changed Block Tracking (CBT), only changed data blocks are backed up. This minimizes data transfer and optimizes backup efficiency. Source-side deduplication removes data before transmission while server-side deduplication removes data redundant data across backup appliances.



Advanced protection for your data

The DP320's security mechanism is based on the principle of least-privilege authentication and network protection, ensuring that data is protected at every stage from data access to backups to storage and restoration.

- **Network architecture:** Configure firewall settings to only allow access from devices within specified IP ranges and subnets, and ensure only authorized backup appliances can perform data transmissions. The built-in management port is an isolated interface dedicated to management purposes, separate from data flow, to reduce security risks.
- **Identity and access controls:** Enforce least-privilege access with admin roles, so each user only has the permissions they need. Integrate with Active Directory, LDAP, or SAML 2.0 to use your existing SSO with MFA, and automatically block suspicious IPs to prevent unauthorized login attempts.
- **Encryption:** Prevent sensitive data from being exposed even if the device is stolen by encrypting at the volume level as a way to maintain data confidentiality and meet compliance requirements.
- **Logging and monitoring:** Retain, view, and export logs for regular audits, and receive a periodic summary of backup and recovery activities via email. For real-time visibility, set up SNMP traps, SMTP notifications, or syslog forwarding to integrate with existing monitoring platforms and receive alerts as they happen — so IT can trace user activity and stay on top of things.
- **Updates and maintenance:** ActiveProtect Manager automatically updates to the latest version, keeping your system secure and reducing the risk of data breaches. If vulnerabilities are found, Synology is ready to validate the security issues and release relevant patches or fixes.
- **Ransomware defense:** Meet the 3-2-1-1-0 backup strategy to ensure data resiliency. Verify data automatically during backups to ensure clean copies of your data can be stored. Detect and repair any data errors with self-healing capabilities. Conduct DR drills via ActiveProtect's built-in sandbox. Secure backups with WORM (Write Once Read Many) technology so that no changes or deletions can be made to your data. Safeguard clean copies of your backups off-site in an air-gapped environment via logical or physical isolation.

Migrate and restore data flexibly

Move data seamlessly across cloud and on-premises platforms. Restore data flexibly across cloud, virtual, and physical environments such as Azure VM, Amazon EC2, VMware vSphere, Microsoft Hyper-V, and more. Meet Recovery Time Objectives (RTO) for disaster recovery and ensure fast data access for business continuity requirements. Perform bare-metal recovery, file-level restoration, and download your backups to restore data when needed.

Perform disaster recovery drills regularly in a sandboxed environment without any impact on your production site. Verify your backups and automatically generate recovery videos for audit purposes.

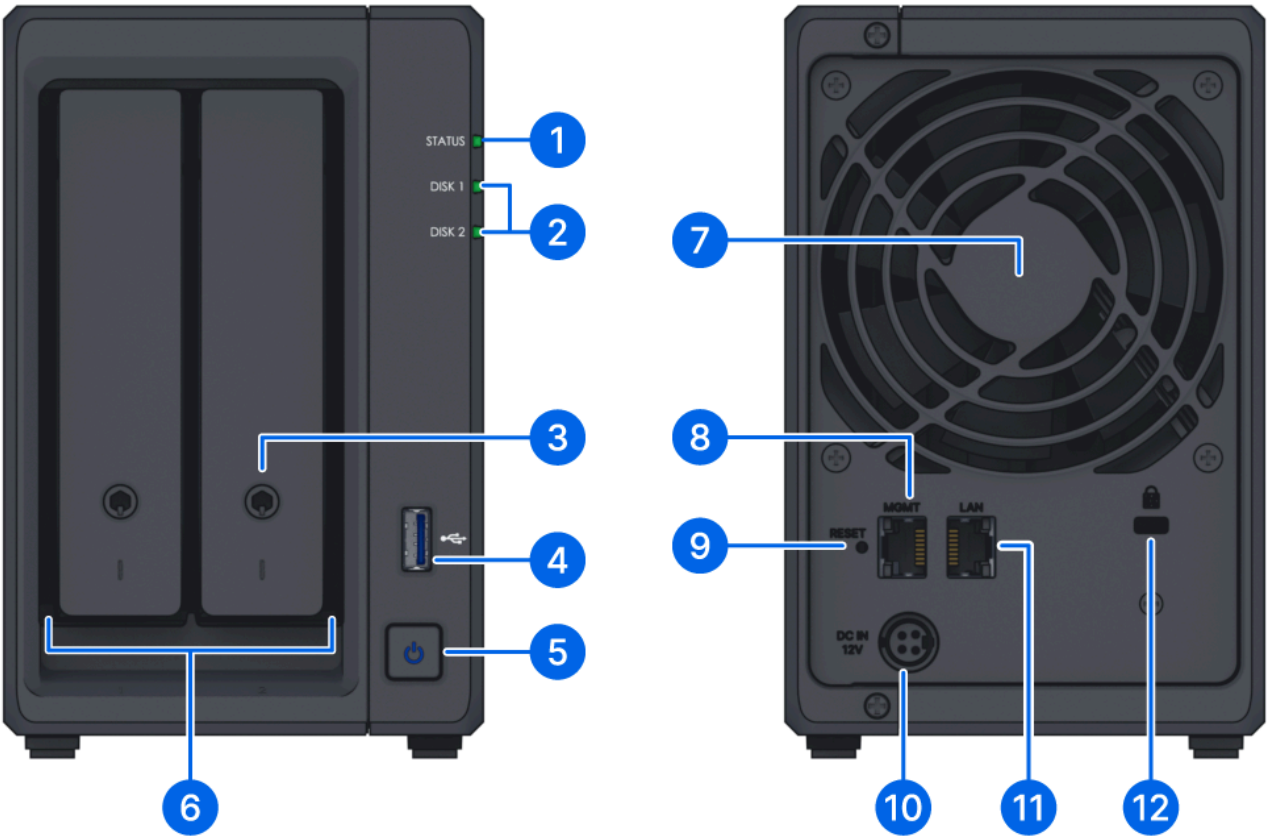


On-demand scalability

Use version tiering to move data to remote storage such as Synology NAS, C2 Object Storage, Wasabi Cloud Storage, Azure Blob Storage, or AWS S3, for easy storage expansion and long-term data retention.

As your business grows, add new DP320 towers and manage them centrally through a 1U or 2U ActiveProtect appliance running ActiveProtect Manager.

Hardware Overview



No.	Name	No.	Name
1.	STATUS Indicator	7.	Fan
2.	Drive Status Indicator	8.	Management Port
3.	Drive Tray Lock	9.	RESET Button
4.	USB 3.2 Gen 1 Port	10.	Power Port
5.	Power Button	11.	1GbE LAN Port
6.	Drive Tray	12.	Kensington Security Slot

Technical Specifications

General	
Raw Capacity ¹	8 TB
Capacity with Tiering ²	Up to 257 TB
Cluster Management Capability ³	Supports up to 10 servers or 500 workloads
Suggested Built-in Restored VM ⁴	1
Notes	<p>1. These values are estimates based on telemetry data and may vary depending on enterprise usage conditions. 2. Long-term archived data can be tiered to remote storage, keeping only the index locally to reduce local space usage. The Capacity with Tiering limit depends on the appliance data usage and the number of tiered workloads and versions. Contact the Synology team for evaluation. 3. ActiveProtect license is required. 4. Maximum number of suggested built-in restore virtual machines</p>

Hardware	
Form Factor	Desktop
CPU	AMD Ryzen R1600 (2 cores)
Memory	8 GB
Storage Configuration	2 × 8 TB 3.5" HDD (RAID 1)
Network Interface	<ul style="list-style-type: none"> • 1 × 1GbE RJ-45 (Data transfer) • 1 × 1GbE RJ-45 (Management)
Product dimensions (HxWxD)	166 × 106 × 223 mm
Weight	2.9 kg
AC Input Power Voltage	100V to 240V AC
Power Frequency	50 / 60Hz, Single Phase
Power Consumption	21.07 W
British Thermal Unit	71.85 BTU/hr
Operating environment	<ul style="list-style-type: none"> • Temperature: 32°F to 104°F (0°C to 45°C) • Relative humidity: 8% to 80% RH
Storage environment	<ul style="list-style-type: none"> • Temperature: -5°F to 140°F (-20°C to 60°C) • Relative humidity: 5% to 95% RH

Environment & Packaging	
Certification	FCC, CE, BSMI, VCCI, RCM, UKCA, EAC, KC, UL, BIS
Environment Safety	RoHS compliant
Package Contents	<ul style="list-style-type: none"> • 1 x DP320 main unit • 1 x Accessory Pack • 1 x Quick Installation Guide • 2 × 3.5" SATA HDD
Warranty	3 Years
Notes	The warranty period begins from the purchase date indicated on the receipt. Learn more about the product's limited warranty.

SYNOLOGY INC. © 2026, Synology Inc. All rights reserved. Synology, the Synology logo are trademarks or registered trademarks of Synology Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Synology may make changes to specification and product descriptions at anytime, without notice.