

Datenblatt



ActiveProtect Appliance

DP340

Synology

ActiveProtect Appliance

DP340



Robuste Datenschutzlösung für Edge- und Zweigstellen

Das Synology ActiveProtect DP340 ist ein speziell entwickeltes Datensicherungsgerät für Zweigstellen, Remote-Niederlassungen, Einzelhandelsstandorte oder Managed Service Provider (MSPs). Das DP340 kann als Edge-Server eingesetzt und von ActiveProtect-Geräten wie dem DP7400, DP7200 oder DP5200 verwaltet werden. Als kompakte Desktop-Einheit können Unternehmen lokale Sicherungen oder Sicherungskopien speichern und Daten auch bei begrenzten Ressourcen schnell wiederherstellen. Das DP340 wird mit vorkonfigurierter Hardware und Software, dem sogenannten ActiveProtect Manager, geliefert. Synology ActiveProtect ist eine leistungsstarke Datenschutzlösung, die Datensicherungen und Wiederherstellungen optimiert und vor Ransomware schützt – unabhängig davon, wo sich Ihre Daten befinden.

- **Schnelle Bereitstellung**

Richten Sie Ihre Datensicherungsgeräte ein und beginnen Sie innerhalb weniger Minuten mit dem Schutz Ihrer Daten

- **Alle Workloads schützen**

Schützen Sie SaaS-, IaaS-, VM-, physische Geräte- und Datenbankdaten über eine einzige einheitliche Konsole

- **Umfassende Übersicht**

Stellen Sie Tower in kleinen Niederlassungen oder Zweigstellen bereit, um Sicherungskopien und externe Kopien zu speichern. Die Tower können von 1U- oder 2U-ActiveProtect-Geräten verwaltet werden

- **Effizienz von Datensicherung und Speicher maximieren**

Optimieren Sie die Effizienz der Datensicherung mit der Changed-Block-Tracking-Technologie (CBT) und deduplizieren Sie Daten mit quellseitiger und serverseitiger Deduplizierung

- **Schutz vor Ransomware**

Implementieren Sie die 3-2-1-1-0-Datensicherungsstrategie durch optimierte externe Kopien und unveränderlichen Datenschutz mithilfe benutzerdefinierter Richtlinien von ActiveProtect. Überprüfen Sie Datensicherungen automatisch und führen Sie DR-Tests in einer integrierten

Sandbox-Umgebung innerhalb einer Air-Gap-Umgebung durch.

- **Daten plattformübergreifend wiederherstellen**

Stellen Sie Daten wieder her, ohne an eine einzelne Plattform gebunden zu sein. Stellen Sie Daten flexibel

plattformübergreifend in

Cloud- oder On-Premises-

Umgebungen mit P2V-, P2C-,

V2V-, V2C- und C2V-

Datenwiederherstellung wieder her

- **Jederzeit skalieren**

Lagern Sie Daten auf Cloud-

oder On-Premises-Lösungen

aus, um Speicherplatz auf

Ihrem Datensicherungsgerät

freizugeben



Beschleunigen Sie Ihre Implementierung

Beginnen Sie innerhalb weniger Minuten mit der Sicherung Ihrer Workloads. Wichtige Konfigurationen wie die Festplattenpartitionierung und die RAID-Einrichtung werden während der Ersteinrichtung von Synology ActiveProtect automatisch abgeschlossen. Der DP340 wird als vorkonfiguriertes Sicherungsgerät mit allen erforderlichen Hardwarekomponenten geliefert.



Workload-Schutz in verschiedenen Umgebungen

Konsolidieren Sie Ihre lokalen, Cloud- und virtuellen Workloads auf einer Plattform. Schützen Sie Windows-PCs, Macs, Linux, VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, NetApp ONTAP, Nutanix Files, Synology NAS, Microsoft 365-Dienste, Google Workspace-Dienste, Oracle Database, Microsoft SQL Server, Azure VM und Amazon EC2.



Vollständige Datentransparenz gewährleisten

Verwalten und überwachen Sie alle Ihre Sicherungen, Sicherungskopien und Tiering-Daten über eine einheitliche Konsole. Implementieren Sie Workload-Schutzrichtlinien, um neue oder vorhandene Workloads automatisch zu schützen. Der DP340 wurde für Edge- und ROBO-Implementierungen entwickelt und bietet lokalen Sicherungsschutz oder schützt zusätzliche Sicherungskopien an verteilten Standorten.



Steigern Sie die Leistung Ihrer Sicherungen und optimieren Sie den Speicher

Optimieren Sie mit der SURE-Technologie (Synology Unified Reduction Engine) von Synology ActiveProtect die Effizienz der Sicherungen und maximieren Sie die Speicherkapazität. Mit Changed Block Tracking (CBT) werden nur geänderte Datenblöcke gesichert. Dadurch wird die Datenübertragung minimiert und die Effizienz der Sicherungen optimiert. Die quellseitige Deduplizierung entfernt Daten vor der Übertragung, während die serverseitige Deduplizierung redundante Daten über mehrere Sicherungsgeräte hinweg entfernt.

Erweiterter Schutz für Ihre Daten

Der Sicherheitsmechanismus des DP340 basiert auf dem Prinzip der Authentifizierung mit den geringsten Berechtigungen und des Netzwerkschutzes. Dadurch wird sichergestellt, dass Daten in jeder Phase – vom Datenzugriff über die Sicherung und Speicherung bis zur Wiederherstellung – geschützt sind.

- **Netzwerkarchitektur:** Konfigurieren Sie die Firewall-Einstellungen so, dass nur der Zugriff von Geräten innerhalb bestimmter IP-Bereiche und Subnetze erlaubt wird, und stellen Sie sicher, dass nur autorisierte Sicherungsgeräte Datenübertragungen durchführen können. Der integrierte Verwaltungsport ist eine isolierte, ausschließlich für Verwaltungszwecke vorgesehene Schnittstelle, die vom Datenfluss getrennt ist, um Sicherheitsrisiken zu reduzieren.
- **Identitäts- und Zugriffssteuerung:** Setzen Sie den Zugriff mit den geringsten Berechtigungen über admin-Rollen durch, sodass jeder Benutzer nur die benötigten Berechtigungen besitzt. Integrieren Sie Active Directory, LDAP oder SAML 2.0, um Ihr vorhandenes SSO mit MFA zu verwenden, und blockieren Sie verdächtige IPs automatisch, um unbefugte Anmeldeversuche zu verhindern.
- **Verschlüsselung:** Verhindern Sie, dass vertrauliche Daten offengelegt werden, selbst wenn das Gerät gestohlen wird, indem Sie sie auf volume-Ebene verschlüsseln. So gewährleisten Sie die Vertraulichkeit der Daten und erfüllen Compliance-Anforderungen.
- **Protokollierung und Überwachung:** Bewahren Sie Protokolle für regelmäßige Audits auf, zeigen Sie sie an und exportieren Sie sie. Erhalten Sie außerdem regelmäßig eine Zusammenfassung der Sicherungs- und Wiederherstellungsaktivitäten per E-Mail. Richten Sie für Echtzeittransparenz SNMP-Traps, SMTP-Benachrichtigungen oder syslog-Weiterleitung ein, um vorhandene Überwachungsplattformen zu integrieren und Warnmeldungen in Echtzeit zu erhalten – so kann die IT Benutzeraktivitäten nachverfolgen und stets den Überblick behalten.
- **Updates und Wartung:** ActiveProtect Manager wird automatisch auf die neueste Version aktualisiert, wodurch Ihr System sicher bleibt und das Risiko von Datenschutzverletzungen reduziert wird. Wenn Schwachstellen gefunden werden, ist Synology bereit, die Sicherheitsprobleme zu überprüfen und entsprechende Patches oder Fehlerbehebungen zu veröffentlichen.
- **Ransomware-Schutz:** Setzen Sie die 3-2-1-1-0-Sicherungsstrategie um, um die Ausfallsicherheit der Daten zu gewährleisten. Überprüfen Sie Daten während der Sicherungen automatisch, damit fehlerfreie Kopien Ihrer Daten gespeichert werden können. Erkennen und reparieren Sie Datenfehler mit Funktionen zur Selbstreparatur. Führen Sie DR-Übungen über die integrierte Sandbox von ActiveProtect durch. Schützen Sie Sicherungen mit der WORM-Technologie (Write Once Read Many), sodass Ihre Daten weder geändert noch gelöscht werden können. Bewahren Sie fehlerfreie Kopien Ihrer Sicherungen extern in einer Air-Gap-Umgebung durch logische oder physische Isolierung auf.



Daten flexibel migrieren und wiederherstellen

Verschieben Sie Daten nahtlos zwischen Cloud- und lokalen Plattformen. Stellen Sie Daten flexibel in Cloud-, virtuellen und physischen Umgebungen wie Azure VM, Amazon EC2, VMware vSphere, Microsoft Hyper-V und weiteren Umgebungen wieder her. Erfüllen Sie die Recovery Time Objectives (RTO) für die Notfallwiederherstellung und gewährleisten Sie schnellen Datenzugriff für Anforderungen an die Geschäftskontinuität. Führen Sie Bare-Metal-Wiederherstellungen und Wiederherstellungen auf Dateiebene durch und laden Sie Ihre Sicherungen herunter, um Daten bei Bedarf wiederherzustellen.

Führen Sie regelmäßig Notfallwiederherstellungsübungen in einer Sandbox-Umgebung durch, ohne Ihre Produktionsumgebung zu beeinträchtigen. Überprüfen Sie Ihre Sicherungen und erstellen Sie automatisch Wiederherstellungsvideos für Auditzwecke.

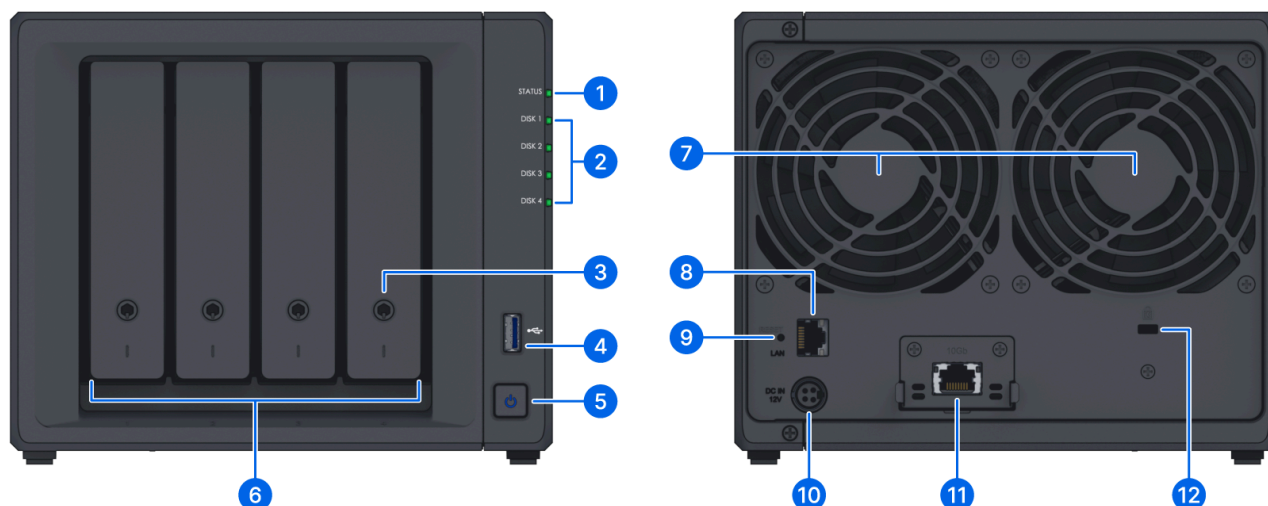


Skalierbarkeit nach Bedarf

Verwenden Sie Version-Tiering, um Daten in einen Remote-Speicher wie Synology NAS, C2 Object Storage, Wasabi Cloud Storage, Azure Blob Storage oder AWS S3 zu verschieben und so den Speicher einfach zu erweitern und Daten langfristig aufzubewahren.

Wenn Ihr Unternehmen wächst, fügen Sie neue DP340-Tower hinzu und verwalten Sie sie zentral über ein 1U- oder 2U-ActiveProtect-Gerät, auf dem ActiveProtect Manager ausgeführt wird.

Hardwareübersicht



Nr.	Name	Nr.	Name
1.	Netzschalter	10.	Netzteil-Lüfter
2.	Betriebsanzeige	11.	PCI-Express-Erweiterungssteckplatz
3.	Warnanzeige	12.	Netzteilanzeigen
4.	Laufwerksstatusanzeigen	13.	Befestigungsbohrungen
5.	Statusanzeige	14.	USB 3.2 Gen 1-Ports
6.	Alarm-Stummschalttaste	15.	10-GbE-RJ-45-Ports
7.	Laufwerksschubladensperren	16.	Reset-Taste
8.	Laufwerksschubladen	17.	Erweiterungsport
9.	Stromanschlüsse	18.	Verwaltungsport

Technische Daten

Allgemein	
Empfohlene Sicherungsquelle	14,5 TB ¹
Empfohlene wiederhergestellte integrierte VM	2 ²
Clusterverwaltungskapazität	Unterstützt bis zu 30 Server oder 1.500 Workloads ³
Notizen	1. Diese Werte sind Schätzungen auf Grundlage von Telemetriedaten und können je nach Nutzungsbedingungen im Unternehmen variieren. 2. Eine ActiveProtect-Lizenz ist erforderlich.

Hardware	
Formfaktor	Desktop
CPU	AMD Ryzen R1600 (2 Kerne)
Speicher	16 GB
Speicherkonfiguration	• 4 × 8 TB 3,5" HDD (RAID 5) • 2 × 400 GB M.2 SSD (RAID 1)
Netzwerk-Interface	• 1 × 10GbE RJ-45 (Datenübertragung) • 1 × 1GbE RJ-45 (Verwaltung)
Produktabmessungen (HxBxT)	166 × 199 × 223 mm
Gewicht	5,2 kg
AC-Eingangsspannung	100 V bis 240 V AC
Stromfrequenz	50 / 60 Hz, einphasig
Stromverbrauch	35,51 W
Britische Wärmeeinheit	121,09 BTU/h
Betriebsumgebung	• Temperatur: 0 °C bis 45 °C (32 °F bis 104 °F) • Relative Luftfeuchtigkeit: 8 % bis 80 % RH
Lagerumgebung	• Temperatur: -20 °C bis 60 °C (-5 °F bis 140 °F) • Relative Luftfeuchtigkeit: 5 % bis 95 % RH

Umwelt & Verpackung	
Zertifizierung	FCC, CE, BSMI, VCCI, RCM, UKCA, EAC, KC, UL, BIS
Umweltsicherheit	RoHS-konform
Packungsinhalt	• 1 x DP340 Hauptgerät • 4 × 3,5" SATA-HDD • 1 x Zubehörpaket • 1 x Schnellinstallationsanleitung
Garantie	3 Jahre
Notizen	Der Garantiezeitraum beginnt mit dem auf dem Kaufbeleg angegebenen Kaufdatum. Erfahren Sie mehr über die eingeschränkte Produktgarantie.

SYNOLOGY INC. © 2026, Synology Inc. Alle Rechte vorbehalten. Synology und das Synology-Logo sind Marken oder eingetragene Marken von Synology Inc. Weitere hier genannte Produkte und Firmennamen sind Marken der entsprechenden Unternehmen. Synology kann ohne vorherige Ankündigung jederzeit Änderungen an den technischen Daten und Produktbeschreibungen vornehmen.