Synology

Datenblatt

ActiveProtect Appliance

DP5200

Letzte Aktualisierung: Oct 15,2026

ActiveProtect Appliance

DP5200



Leistungsstarke Datenschutzlösung für schnell wachsende Unternehmen

Die Synology ActiveProtect DP5200 ist ein speziell entwickeltes Datensicherungsgerät für mittelständische Unternehmen mit schnellem Wachstum, Unternehmen, die flexible Bereitstellungsoptionen benötigen, sowie Managed Service Provider (MSPs). Die ActiveProtect DP5200 ist eine leistungsstarke Lösung für Datensicherung und Wiederherstellung mit vorkonfigurierter Hardware und Software namens ActiveProtect Manager. Sie wurde entwickelt, um Sicherungen und Sicherungskopien zu schützen und Daten vor Ransomware zu bewahren. Die DP5200 ist ein hochdichtes 1U-Datensicherungsgerät, das in Rechenzentren oder gemeinsam genutzten Rack-Umgebungen eingesetzt werden kann, um die Effizienz der Speichernutzung zu maximieren.

- **Schnelle Bereitstellung**
  Datensicherungsgeräte bereitstellen und innerhalb weniger Minuten mit dem Schutz Ihrer Daten beginnen
- **Alle Workloads schützen**
  SaaS, IaaS, VMs, physische Geräte und Datenbanken über eine einzige Konsole schützen
- **Datentransparenz schaffen**
  Bis zu 1.000 Server oder 120.000 Workloads verwalten und überwachen. Bei mittelständischen Unternehmen bereitstellen, um lokale Sicherungen oder Sicherungskopien zu speichern
- **Effizienz von Datensicherung und Speicher maximieren**
  Die Effizienz der Datensicherung mit CBT-Technologie optimieren und Daten durch quellseitige und serverseitige Deduplizierung deduplizieren
- **Schutz vor Ransomware**
  Die 3-2-1-1-0-Richtlinie für unveränderlichen Datenschutz, automatische Überprüfung von Sicherungen, externe Sicherungen und DR-Tests in einer Sandbox implementieren
- **Flexible Wiederherstellung jederzeit und überall**
  Daten über Cloud- oder lokale Plattformen hinweg mit P2V-, P2C-, V2V-, V2C- und C2V-Datenwiederherstellung wiederherstellen

- **Jederzeit skalieren**
  Daten in die Cloud oder auf lokale Lösungen auslagern, um Speicherplatz freizugeben

Vereinfachtes Einrichten

Richten Sie Ihre Unternehmensdaten innerhalb weniger Minuten ein und beginnen Sie mit der Sicherung. Wichtige Konfigurationen wie die Festplattenpartitionierung und die RAID-Einrichtung werden während der Ersteinrichtung von Synology ActiveProtect automatisch abgeschlossen. Der DP5200 wird als vorkonfiguriertes Sicherungsgerät mit allen erforderlichen Hardwarekomponenten geliefert.

Zentralisieren Sie den Schutz Ihrer Workloads

Schützen Sie eine Vielzahl von lokalen, virtuellen und Cloud-Workloads, darunter 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.

Sicherungen verwalten und vollständige Datentransparenz gewährleisten

Verwalten und überwachen Sie alle Ihre Sicherungen, Sicherungskopien und Tiering-Daten über eine einheitliche Konsole. Legen Sie Workload-Schutzrichtlinien fest, um vorhandene und neue Workloads zu schützen. Der DP5200 wurde für wachsende Unternehmen, mittelständische Unternehmen und MSPs entwickelt und bietet lokalen Sicherungsschutz oder speichert zusätzliche Sicherungskopien an verteilten Standorten.

Maximieren Sie Ihre Speicherkapazität

Mit der SURE-Technologie (Synology Unified Reduction Engine) von Synology ActiveProtect werden Sicherungen schneller durchgeführt und die Speicherkapazität optimiert. Nur geänderte Datenblöcke werden gesichert, um die Datenübertragung zu minimieren und die Sicherungseffizienz mit der Changed Block Tracking (CBT)-Technologie zu optimieren. Die quellseitige Deduplizierung entfernt Daten vor der Datenübertragung, während die serverseitige Deduplizierung redundante Daten auf mehreren Sicherungsgeräten entfernt.

Im Kern auf Datensicherheit ausgelegt

Der Sicherheitsmechanismus des DP5200 basiert auf dem Prinzip der Authentifizierung mit geringstmöglichen Berechtigungen und des Netzwerkschutzes. Dadurch wird sichergestellt, dass Daten in jeder Phase geschützt sind – vom Datenzugriff über die Sicherung und Speicherung bis hin zur Wiederherstellung.

- **Netzwerkarchitektur:** Konfigurieren Sie die Firewall-Einstellungen so, dass nur der Zugriff von Geräten innerhalb festgelegter IP-Bereiche und Subnetze zulässig ist, und stellen Sie sicher, dass nur autorisierte Sicherungsgeräte Daten übertragen 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 geringstmöglichen Berechtigungen über admin-Rollen durch, sodass jeder Benutzer nur über die erforderlichen Berechtigungen verfügt. 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 die Daten auf volume-Ebene verschlüsseln. So wahren Sie die Vertraulichkeit der Daten und erfüllen Compliance-Anforderungen.
- **Protokollierung und Monitoring:** 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. Für Echtzeittransparenz richten Sie SNMP-Traps, SMTP-Benachrichtigungen oder syslog-Weiterleitung ein, um vorhandene Monitoring-Plattformen zu integrieren und sofortige Warnmeldungen zu erhalten – so kann die IT Benutzeraktivitäten nachverfolgen und den Überblick behalten.
- **Updates und Wartung:** ActiveProtect Manager aktualisiert sich automatisch auf die neueste Version, hält Ihr System sicher und reduziert das Risiko von Datenschutzverletzungen. 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 und gewährleisten Sie die Datenresilienz. Überprüfen Sie Daten während der Sicherungen automatisch, damit fehlerfreie Kopien Ihrer Daten gespeichert werden können. Erkennen und reparieren Sie Datenfehler mithilfe von Selbstreparaturfunktionen. Führen Sie über die integrierte Sandbox von ActiveProtect DR-Übungen 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 plattformübergreifend wiederherstellen und migrieren

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 für Audit-Zwecke automatisch Wiederherstellungsvideos.

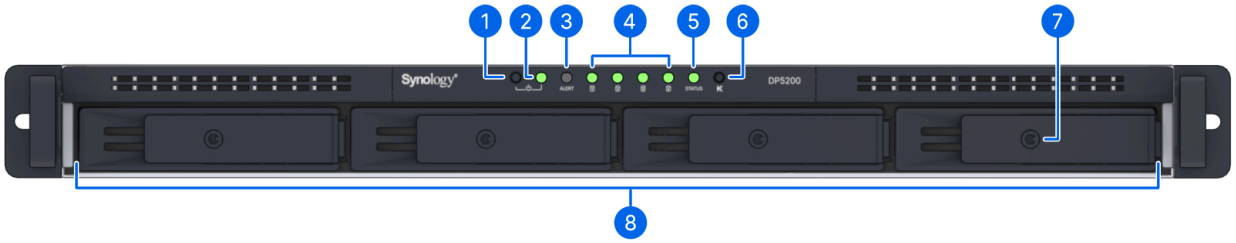
Nach Bedarf skalieren

Verwenden Sie Version-Tiering, um Daten zur einfachen Erweiterung des Speichers und zur langfristigen Datenaufbewahrung in Remote-Speicher wie Synology NAS, C2 Object Storage, Wasabi Cloud Storage, Azure Blob Storage oder AWS S3 zu verschieben.

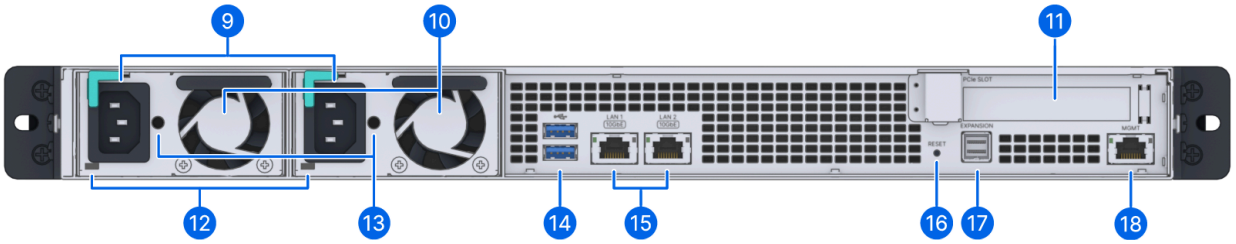
Wenn Ihr Unternehmen wächst, fügen Sie neue Sicherungsgeräte hinzu und verwalten Sie sie alle über die zentrale Konsole von ActiveProtect Manager.

Hardwareübersicht

Vorderseite



Rückseite



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

Technische Daten

Allgemein	
Rohkapazität[1]	36 TB
Kapazität mit Tiering[2]	Bis zu 1,15 PB
Cluster-Management-Funktionen[3]	Unterstützt bis zu 1.000 Server oder 120.000 Workloads
Empfohlene integrierte wiederhergestellte VM[4]	2
Notizen	1. Diese Werte sind Schätzungen auf Grundlage von Telemetriedaten und können je nach Nutzungsbedingungen im Unternehmen variieren. 2. Langfristig archivierte Daten können auf Remote-Speicher getiert werden, wobei nur der Index lokal gespeichert wird, um den lokalen Speicherplatzbedarf zu reduzieren. Die Grenze für die Kapazität mit Tiering hängt von der Datennutzung des Geräts sowie der Anzahl der getierten Workloads und Versionen ab. Wenden Sie sich zur Evaluierung an das Synology-Team. 3. Eine ActiveProtect-Lizenz ist erforderlich. 4. Bei Ausstattung mit 128 GB Speicher (zusätzliche Speichermodule erforderlich) kann die maximale Anzahl virtueller Maschinen auf 17 erweitert werden.

Hardware	
Formfaktor	1U (RU)
CPU	Intel Xeon D-1726 (6 Kerne)
Speicher	16 GB (max. 64 GB)
Speicherkonfiguration	• 4 × 12 TB 3,5-Zoll-HDD (RAID 5) • 2 × 800 GB M.2-SSD (RAID 1)
Netzwerk-Interface	• 1 × 1GbE RJ-45 (Verwaltung) • 2 × 10GbE RJ-45 (Datenübertragung) • (Optional) 2 × 10GbE RJ-45 / SFP+ oder 2 × 25GbE SFP28 (Datenübertragung)
Produktabmessungen (HxBxT)	44 × 437,5 × 634,5 mm
Gewicht	12,2 kg
AC-Eingangsspannung	100 V bis 240 V AC
Stromfrequenz	50 / 60 Hz, einphasig
Stromverbrauch	97,59 W
Britische Wärmeeinheit	332,78 BTU/h
Betriebsumgebung	• Temperatur: 32 °F bis 95 °F (0 °C bis 35 °C) • Relative Luftfeuchtigkeit: 8 % bis 80 % RH
Speicherumgebung	• Temperatur: -5 °F bis 140 °F (-20 °C bis 60 °C) • Relative Luftfeuchtigkeit: 5 % bis 95 % RH

Umwelt und Verpackung	
Zertifizierung	FCC, CE, BSMI, VCCI, RCM, UKCA, EAC, KC, UL, BIS
Umweltsicherheit	RoHS-konform
Packungsinhalt	• 1 x DP5200 Hauptgerät • 4 × 3.5” SATA HDD • 2 x C13-auf-C14-Netzkabel • 1 x Frontabdeckung • 1 x Zubehörpaket • 1 x Kurzanleitung zur Installation
Garantie	5 Jahre
Notizen	Der Garantiezeitraum beginnt am auf dem Kaufbeleg angegebenen Kaufdatum. Weitere Informationen zur eingeschränkten 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.