

Datenblatt



ActiveProtect Appliance

DP5200

Synology

ActiveProtect Appliance

DP5200



Leistungsstarke Datenschutzlösung für schnell wachsende Unternehmen

Das Synology ActiveProtect DP5200 ist ein speziell entwickeltes Datensicherungsgerät für mittelständische Unternehmen mit starkem Wachstum, Unternehmen, die flexible Bereitstellungsoptionen benötigen, sowie Managed Service Provider (MSPs). Das ActiveProtect DP5200 ist eine leistungsstarke Lösung für Datensicherung und Wiederherstellung mit vorkonfigurierter Hardware und Software namens ActiveProtect Manager. Es wurde entwickelt, um Sicherungen und Sicherungskopien zu schützen und Daten vor Ransomware zu bewahren. Das 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**
Stellen Sie
Datensicherungsgeräte bereit
und beginnen Sie innerhalb
weniger Minuten mit dem
Schutz Ihrer Daten
- **Alle Workloads schützen**
Schützen Sie SaaS, IaaS, VMs,
physische Geräte und
Datenbanken über eine einzige
Konsole
- **Datentransparenz schaffen**
Verwalten und überwachen Sie
bis zu 1.000 Server oder
120.000 Workloads. Stellen Sie
die Lösung in
mittelständischen
Unternehmen bereit, um lokale
Sicherungen oder
Sicherungskopien zu speichern
- **Effizienz von Datensicherung
und Speicher maximieren**
Optimieren Sie die Effizienz der
Datensicherung mit CBT-
Technologie und deduplizieren
Sie Daten mithilfe der
quellseitigen und
serverseitigen Deduplizierung
- **Schutz vor Ransomware**
Implementieren Sie die 3-2-1-
1-0-Richtlinie für
unveränderlichen Datenschutz,
automatische
Sicherungsüberprüfung,
externe Sicherungen und DR-
Tests in einer Sandbox
- **Flexible Wiederherstellung
jederzeit und überall**
Stellen Sie Daten
plattformübergreifend aus der

Cloud oder von lokalen
Plattformen mit P2V-, P2C-,
V2V-, V2C- und C2V-
Datenwiederherstellung wieder
her

- **Jederzeit skalieren**

Verschieben Sie Daten in die
Cloud oder auf lokale
Lösungen, um Speicherplatz
freizugeben



Vereinfachtes Einrichten

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



Workload-Schutz konsolidieren

Schützen Sie eine Vielzahl lokaler, virtueller und cloudbasierter Workloads, einschließlich Windows-PCs, Macs, Linux, VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, NetApp ONTAP, Nutanix Files, Synology NAS, Microsoft 365-Diensten, Google Workspace-Diensten, 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. Mit der Changed Block Tracking (CBT)-Technologie werden nur geänderte Datenblöcke gesichert, um die Datenübertragung zu minimieren und die Sicherungseffizienz zu optimieren. Die quellseitige Deduplizierung entfernt Daten vor der Datenübertragung, während die serverseitige Deduplizierung redundante Daten auf mehreren Sicherungsgeräten entfernt.

Mit Datensicherheit als zentralem Prinzip entwickelt

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 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 Zugriffskontrollen:** Setzen Sie den Zugriff mit geringstmöglichen Berechtigungen durch 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 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. Außerdem erhalten Sie regelmäßig eine Zusammenfassung der Sicherungs- und Wiederherstellungsaktivitäten per E-Mail. Richten Sie für Echtzeittransparenz SNMP-Traps, SMTP-Benachrichtigungen oder syslog-Weiterleitung ein, um vorhandene Monitoring-Plattformen zu integrieren und Warnmeldungen sofort 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-Abwehr:** Setzen Sie die 3-2-1-1-0-Sicherungsstrategie um und gewährleisten Sie die Datenresilienz. Überprüfen Sie Daten während der Sicherungen automatisch, um sicherzustellen, dass fehlerfreie Kopien Ihrer Daten gespeichert werden können. Erkennen und reparieren Sie Datenfehler mithilfe von Selbstreparaturfunktionen. Führen Sie DR-Übungen über die integrierte Sandbox von ActiveProtect durch. Sichern Sie Sicherungen mit der WORM-Technologie (Write Once Read Many), sodass Ihre Daten weder geändert noch gelöscht werden können. Schützen Sie fehlerfreie Kopien Ihrer Sicherungen extern in einer Air-Gap-Umgebung durch logische oder physische Isolierung.



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 dateibasierte Wiederherstellungen 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.

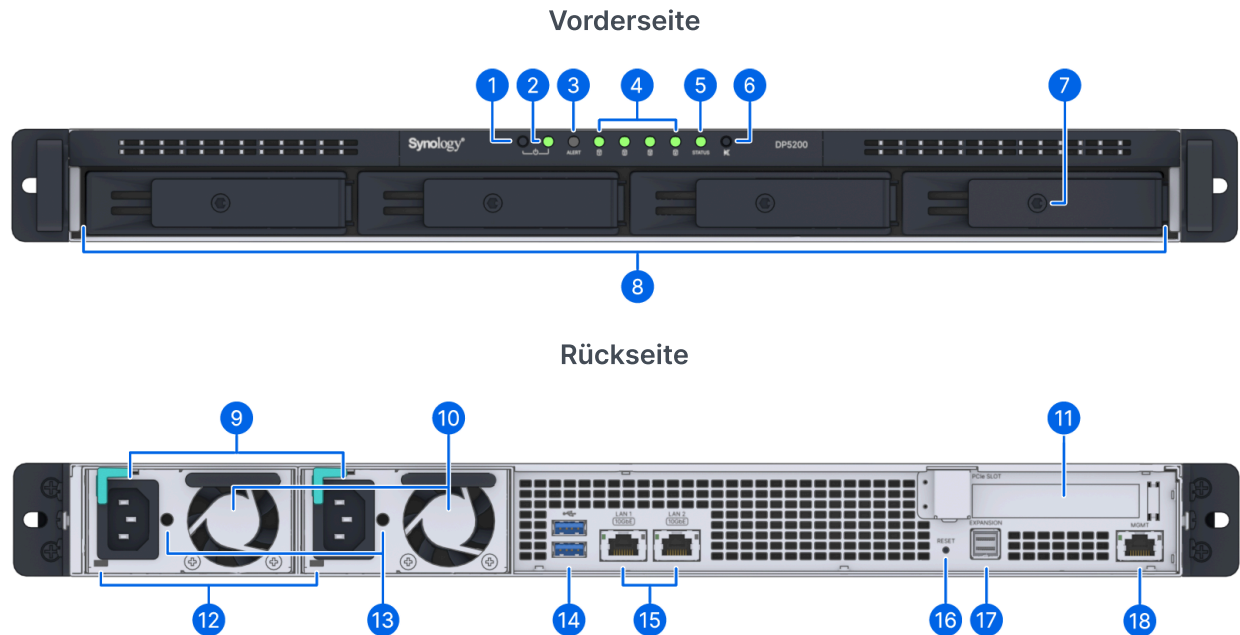


Bedarfsgerecht skalieren

Verwenden Sie Version-Tiering, um Daten auf 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 Sicherungsgeräte hinzu und verwalten Sie sie alle über die zentrale Konsole von ActiveProtect Manager.

Hardwareübersicht



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

Technische Daten

Allgemein	
Empfohlene Sicherungsquelle	21,5 TB ¹
Empfohlene wiederhergestellte integrierte VM	2 ²
Clusterverwaltungskapazität	Unterstützt bis zu 1.000 Server oder 120.000 Workloads ³
Notizen	1. Diese Werte sind Schätzungen auf Grundlage von Telemetriedaten und können je nach Nutzungsbedingungen im Unternehmen variieren. 2. Bei Ausstattung mit 64 GB Arbeitsspeicher (zusätzliche Speichermodule erforderlich) kann die maximale Anzahl virtueller Maschinen auf 10 erweitert werden. 3. Eine ActiveProtect-Lizenz ist erforderlich.

Hardware	
Formfaktor	1U (RU)
CPU	Intel Xeon D-1726 (6 Kerne)
Speicher	16 GB (max. 64 GB)
Speicherkonfiguration	• 4 × 12 TB 3,5" 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
British Thermal Unit	332,78 BTU/h
Betriebsumgebung	• Temperatur: 0 °C bis 35 °C (32 °F bis 95 °F) • Relative Luftfeuchtigkeit: 8 % bis 80 % RH
Speicherumgebung	• 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 DP5200 Hauptgerät • 4 × 3,5" SATA HDD • 2 x C13-zu-C14-Netzkabel • 1 x Frontabdeckung • 1 x Zubehörpaket • 1 x Kurzanleitung zur Installation
Garantie	5 Jahre
Hinweise	Der Garantiezeitraum beginnt ab 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.