Synology

Urządzenie ActiveProtect

# DP340

## Odporne na cyfrowe zagrożenia rozwiązanie do ochrony danych dla punktów końcowych

Urządzenie Synology ActiveProtect DP340 to rozwiązanie do ochrony danych wstępnie skonfigurowane ze sprzętem obsługującym ActiveProtect Manager, system operacyjny zaprojektowany specjalnie do tworzenia kopii zapasowych. Dzięki możliwości wykonywania kopii zapasowych, przywracania, deduplikowania, replikacji i zarządzania przy jednoczesnym zapewnieniu bezpieczeństwa, serwer DP340 jest idealnym serwerem kopii zapasowych dla małych i średnich punktów końcowych. Bezproblemowo integruje wszystkie bieżące i przyszłe obciążenia w wielu lokalizacjach w klastry, umożliwiając scentralizowane zarządzanie za pośrednictwem jednej platformy. Dzięki niezmienności, fizycznie izolowanym kopiom zapasowym i kontroli dostępu, DP340 chroni przed atakami ransomware i chroni wszystkie dane.

## Najważniejsze cechy

- **Szybkie wdrożenie**
  Konfiguracja serwera w kilka minut
- **Zabezpieczenie wszystkich obciążeń**
  Ochrona maszyn wirtualnych, SaaS, baz danych, serwerów fizycznych i innych
- **Widoczność**
  Monitorowanie stanu serwerów i kopii zapasowych na scentralizowanej platformie
- **Niezawodne tworzenie kopii zapasowych**
  Sprawdzanie kopii zapasowych i testowanie planu odzyskiwania po awarii w środowisku piaskownicy
- **Elastyczne odzyskiwanie**
  Odzyskiwanie na poziomie plików lub natychmiastowe przywracanie P2V/V2V w celu osiągnięcia potrzebnego docelowego RTO
- **Ochrona przed oprogramowaniem ransomware**
  Zintegruj niezmienność danych oraz kopie zapasowe typu 'air-gap' z pamięcią masową WORM w celu ochrony przed ransomware.
- **Zoptymalizowana wydajność tworzenia kopii zapasowych**
  Wykorzystywanie globalnej deduplikacji po stronie źródła i specjalistyczny silnik tworzenia kopii zapasowych
- **Zabezpieczenie danych**
  Implementowanie najniższych uprawnień dzięki kontroli dostępu, zaporze i izolacji w celu osiągnięcia solidnej architektury

## Szybkie i bezproblemowe wdrażanie

Podstawowa konfiguracja, taka jak partycjonowanie dysków i konfiguracja macierzy RAID, jest przeprowadzana automatycznie, dzięki czemu wdrożenie jest szybkie i łatwe, a ochronę danych można rozpocząć natychmiast.

## Ochrona obciążeń za pomocą określonych zasad

Chroń wszystkie obciążenia, w tym VMware vSphere, Microsoft Hyper-V, Windows, macOS, Linux, NetApp ONTAP, Pliki Nutanix, usługi Microsoft 365, Oracle Database, i Microsoft SQL Server. Ustal zasady dla firm w celu spełnienia wymagań SLA i zautomatyzuj ochronę danych poprzez wykrywanie istniejących i przyszłych obciążeń, zapewniając, że zostaną zabezpieczone zgodnie z odpowiednimi zasadami. W prosty sposób przeglądaj i modyfikuj zasady oraz zarządzaj nimi.

## Niezawodne tworzenie kopii zapasowych i elastyczne odzyskiwanie danych

Urządzenie DP340 obsługuje funkcję automatycznej naprawy z ciągłym wykrywaniem cichego uszkodzenia danych za pomocą sumy kontrolnej Btrfs. Zapewnia brak błędów poprzez naprawę uszkodzonych danych za pomocą technologii RAID. Aby zweryfikować możliwość odzyskania danych z kopii zapasowych, można regularnie przeprowadzać testowe odzyskiwanie po awarii w środowisku piaskownicy, bez wpływu na główne miejsce produkcji. Dostępna jest również weryfikacja kopii zapasowej, która automatycznie generuje testowe pliki wideo z odzyskiwania dla celów audytu. W przypadku awarii dane mogą być elastycznie przywracane w oparciu o cele czasu odzyskiwania (RTO) za pomocą przywracania całego urządzenia, odzyskiwania na poziomie plików, metod przywracania danych fizycznych do wirtualnych (P2V) lub wirtualnych do wirtualnych (V2V) do wyznaczonej lokalizacji.

## Bezkompromisowa ochrona przed oprogramowaniem ransomware

Aby zapobiec atakom ransomware, DP340 chroni kopie zapasowe danych i kopie zapasowe z niezmiennością i pamięcią WORM (Write-Once-Read-Many), aby zapewnić, że nikt nie będzie mógł zmodyfikować danych, które zostały utworzone w określonym okresie przechowywania. Ponadto integruje funkcje szyfrowania, umożliwiając szyfrowanie danych lokalnie przed utworzeniem kopii zapasowej w zdalnych miejscach docelowych. Aby jeszcze bardziej zwiększyć bezpieczeństwo, można również fizycznie odizolować zdalne środowisko.

## Zoptymalizowana wydajność tworzenia kopii zapasowych

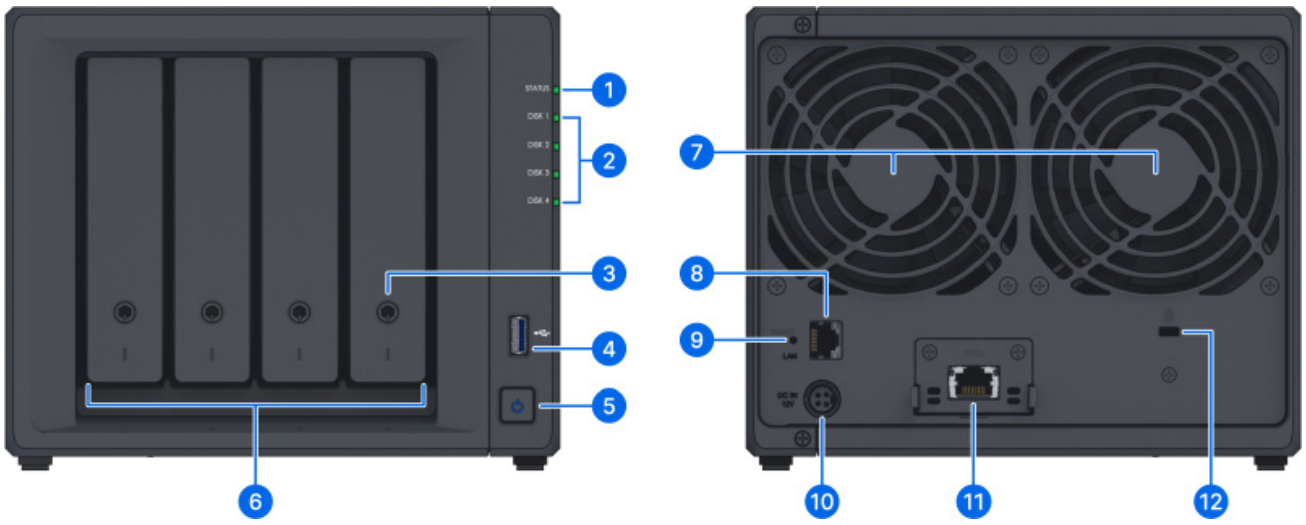
Serwer DP340 optymalizuje alokację miejsca na dysku poprzez integrację sprzętu i oprogramowania.  Dzięki wykorzystaniu pamięci podręcznej SSD do przechowywania metadanych związanych z kopiami zapasowymi, optymalizacji organizacji danych i konsolidacji wielu plików w jeden obraz, przyspiesza przetwarzanie danych. Zarówno kopie zapasowe i ich kopie wykorzystują globalną deduplikację po stronie źródła, ponieważ porównuje dane u źródła i przesyła tylko niezduplikowane dane, aby zaoszczędzić przepustowość i przestrzeń dyskową.

## Bezpieczeństwo danych u podstaw

Mechanizm bezpieczeństwa urządzenia DP340 opiera się na zasadzie uwierzytelniania na najniższym poziomie uprawnień i architekturze ochrony sieci. Mechanizm ten umożliwia dostęp do danych tylko upoważnionemu personelowi, ogranicza dostęp do określonych urządzeń oraz dostęp do infrastruktury kopii zapasowych w wyznaczonych godzinach, aby zapewnić bezpieczeństwo danych.

- **W przypadku upoważnionego personelu:** Integracja z usługą Active Directory, LDAP i SAML 2.0 umożliwia przedsiębiorstwom korzystanie z istniejącego SSO z uprawnieniami MFA i granulowanymi w celu zwiększenia kontroli dostępu.
- **W przypadku urządzeń:** Ustawienia zapory można skonfigurować tak, aby zezwalały na dostęp tylko z urządzeń w określonych zakresach IP i podsieciach. Wbudowany port zarządzania jest izolowanym interfejsem przeznaczonym do celów zarządzania. Jest on oddzielony od przepływu danych w celu zmniejszenia zagrożeń bezpieczeństwa.
- **Zwiększona izolacja:** Zabezpiecz zdalną infrastrukturę kopii zapasowych za pomocą rozwiązań umożliwiających osiągnięcie izolacji sieciowej lub fizycznej. Ogranicz dostęp do sieci do określonych godzin lub ustaw włączanie i wyłączanie urządzeń.

# Przegląd sprzętu




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | Wskaźnik STATUS | 2 | Wskaźnik stanu dysku | 3 | Zamek kieszeni dysku | 4 | Port USB 3.2 1. generacji |
| 5 | Przycisk i wskaźnik zasilania | 6 | Kieszenie dysków | 7 | Wentylator | 8 | Port zarządzania |
| 9 | Przycisk RESET | 10 | Gniazdo zasilania | 11 | Port 10GbE RJ-45 | 12 | Uchwyt linki zabezpieczającej Kensington |

# Specyfikacja techniczna

## Specyfikacje ogólne

| | |
|---|---|
| **Polecane źródło kopii zapasowych** | 14,5 TB[1] |
| **Polecana wbudowana przywrócona maszyna wirtualna** | 2 |
| **Zdolność zarządzania klastrami** | Obsługa do 30 serwerów lub 1,500 obciążeń[2] |

## Specyfikacje sprzętu

| | |
|---|---|
| **Obudowa** | Komputer stacjonarny |
| **CPU** | AMD R1600 (2 rdzenie) |
| **Pamięć** | 16 GB |
| **Konfiguracja pamięci masowej** | • 4 dyski HDD 8 TB (RAID 5)<br>• 2 dyski SSD 400G (RAID 1) |
| **Interfejs sieciowy** | • 1 port 1GbE RJ-45 (zarządzanie)<br>• 1 port 10GbE RJ-45 (przesyłanie danych) |
| **Wymiary (wys. × szer. × gł.)** | 166 × 199 × 223 mm |
| **Waga** | 5,2 kg |
| **Środowisko pracy** | • Temperatura: od 0°C do 45°C (od 32°F do 104°F)<br>• Wilgotność względna: od 8% do 80% |
| **Środowisko przechowywania** | • Temperatura: od -20°C do 60°C (od -5°F do 140°F)<br>• Wilgotność względna: od 5% do 95% |

## Ochrona środowiska i opakowanie

| | |
|---|---|
| **Certyfikaty** | FCC, CE, UKCA, BSMI, RCM, NCC, VCCI |
| **Ochrona środowiska** | Zgodność z dyrektywą RoHS |
| **Zawartość opakowania** | • 1 jednostka główna DP340<br>• 4 dysków 3,5″ SATA HDD<br>• 1 zasilacz<br>• 1 kabel zasilający<br>• 2 przewody RJ-45 LAN<br>• 1 pakiet akcesoriów<br>• 1 przewodnik szybkiej instalacji |
| **Gwarancja** | 3 lata[3] |

Uwaga: Dane techniczne produktu mogą zostać zmienione bez wcześniejszego powiadomienia. Najnowsze informacje można znaleźć na **stronie danych technicznych** urządzenia.

1. Wartości są oparte na szacunkowych danych telemetrycznych i mogą się różnić w zależności od warunków używania rozwiązania przez firmę.
2. Wymagana jest **licencja ActiveProtect**.
3. Okres gwarancyjny rozpoczyna się od daty zakupu podanej na paragonie. **Dowiedz się więcej** o ograniczonej gwarancji produktu.

**SYNOLOGY INC.**

© 2024, Synology Inc. Wszelkie prawa zastrzeżone. Synology i logo Synology są zarejestrowanymi znakami towarowymi lub znakami towarowymi firmy Synology Inc. Inne nazwy produktów i firm zawarte w niniejszymi dokumencie mogą być znakami towarowymi odpowiednich podmiotów. Firma Synology zastrzega sobie prawo do wprowadzania zmian w danych technicznych i opisach produktów w dowolnej chwili i bez wcześniejszego powiadomienia.

DP340-2024-PLK-REV001