Hoja de datos

ActiveProtect Appliance

DP340

Última actualización: Oct 15,2026

ActiveProtect Appliance

DP340



Potente solución de protección de datos para oficinas periféricas y sucursales

Synology ActiveProtect DP340 es un dispositivo de copia de seguridad diseñado específicamente para sucursales, oficinas remotas, establecimientos comerciales o proveedores de servicios administrados (MSP). DP340 se puede implementar como servidor periférico mientras se administra mediante dispositivos ActiveProtect, como DP7400, DP7200 o DP5200. Como unidad de escritorio compacta, permite a las empresas almacenar copias de seguridad locales o copias de respaldo y restaurar datos rápidamente incluso con recursos mínimos. DP340 incluye hardware y software preconfigurados, denominados ActiveProtect Manager. Synology ActiveProtect es una potente solución de protección de datos diseñada para simplificar las copias de seguridad y la recuperación, así como para proteger contra el ransomware, independientemente de dónde se encuentren sus datos.

- **Implementación rápida**
  Configure sus dispositivos de copia de seguridad y comience a proteger sus datos en cuestión de minutos
- **Proteja todas las cargas de trabajo**

Proteja SaaS, IaaS, máquinas virtuales, dispositivos físicos y bases de datos desde una única consola

- **Visibilidad completa**
  Implemente torres en las sucursales para almacenar copias de respaldo y copias externas, administradas mediante dispositivos 1U o 2U
- **Maximice la eficiencia de las copias de seguridad y el almacenamiento**
  Optimice la eficiencia de las copias de seguridad con la tecnología CBT y elimine datos duplicados mediante la deduplicación en el origen y en el servidor
- **Defensa contra el ransomware**
  Implemente la política 3-2-1-1-0 para la protección de datos inmutables, la verificación automática de copias de seguridad, las copias de seguridad externas y las pruebas de DR en un entorno aislado
- **Restaure datos entre plataformas**
  Recupere datos entre plataformas en la nube o locales mediante la

recuperación de datos P2V, P2C, V2V, V2C y C2V

- **Escale en cualquier momento**
  Traslade los datos a soluciones en la nube o locales para liberar espacio

Acelere su implementación

Comience a realizar copias de seguridad de sus cargas de trabajo en cuestión de minutos. Las configuraciones esenciales, como la partición de discos y la configuración de RAID, se completan automáticamente durante la configuración inicial de Synology ActiveProtect. El DP340 viene como un dispositivo de copia de seguridad preconfigurado que incluye todos los componentes de hardware necesarios.

Protección de cargas de trabajo en todos los entornos

Consolide sus cargas de trabajo locales, en la nube y virtuales en una sola plataforma. Proteja PC con Windows, Mac, Linux, VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, NetApp ONTAP, Nutanix Files, Synology NAS, servicios de Microsoft 365, servicios de Google Workspace, Oracle Database, Microsoft SQL Server, Azure VM y Amazon EC2.

Garantice una visibilidad total de los datos

Gestione y supervise todas sus copias de seguridad, copias de seguridad adicionales y datos almacenados por niveles mediante una consola unificada. Implemente políticas de protección de cargas de trabajo para proteger automáticamente las cargas de trabajo nuevas o existentes. Diseñado para implementaciones periféricas y ROBO, el DP340 proporciona protección de copias de seguridad locales o protege copias de seguridad adicionales en ubicaciones distribuidas.

Mejore el rendimiento de sus copias de seguridad y el almacenamiento

Con la tecnología SURE (Synology Unified Reduction Engine) de Synology ActiveProtect, optimice la eficiencia de las copias de seguridad y maximice la capacidad de almacenamiento. Con el seguimiento de bloques cambiados (CBT), solo se realizan copias de seguridad de los bloques de datos modificados. Esto minimiza la transferencia de datos y optimiza la eficiencia de las copias de seguridad. La deduplicación en el origen elimina los datos antes de la transmisión, mientras que la deduplicación en el servidor elimina los datos redundantes entre los dispositivos de copia de seguridad.

Protección avanzada para sus datos

El mecanismo de seguridad del DP340 se basa en el principio de autenticación con privilegios mínimos y protección de red, lo que garantiza que los datos estén protegidos en cada etapa, desde el acceso a los datos hasta las copias de seguridad, el almacenamiento y la restauración.

- **Arquitectura de red:** Configure los ajustes del firewall para permitir únicamente el acceso desde dispositivos dentro de rangos de IP y subredes especificados, y asegúrese de que solo los dispositivos de copia de seguridad autorizados puedan realizar transmisiones de datos. El puerto de administración integrado es una interfaz aislada dedicada a tareas de administración, independiente del flujo de datos, para reducir los riesgos de seguridad.
- **Controles de identidad y acceso:** Aplique el acceso con privilegios mínimos mediante roles de admin, de modo que cada usuario solo tenga los permisos que necesita. Integre Active Directory, LDAP o SAML 2.0 para utilizar su SSO existente con MFA y bloquee automáticamente las IP sospechosas para evitar intentos de inicio de sesión no autorizados.
- **Cifrado:** Evite que los datos confidenciales queden expuestos aunque le roben el dispositivo mediante el cifrado a nivel de volumen, con el fin de mantener la confidencialidad de los datos y cumplir los requisitos de conformidad.
- **Registro y supervisión:** Conserve, consulte y exporte registros para auditorías periódicas, y reciba por correo electrónico un resumen periódico de las actividades de copia de seguridad y recuperación. Para obtener visibilidad en tiempo real, configure traps de SNMP, notificaciones SMTP o el reenvío de syslog para integrarse con las plataformas de supervisión existentes y recibir alertas cuando se produzcan, de modo que el personal de TI pueda rastrear la actividad de los usuarios y mantenerse al tanto.
- **Actualizaciones y mantenimiento:** ActiveProtect Manager se actualiza automáticamente a la última versión, manteniendo su sistema seguro y reduciendo el riesgo de filtraciones de datos. Si se detectan vulnerabilidades, Synology está preparado para validar los problemas de seguridad y publicar los parches o correcciones pertinentes.
- **Defensa contra el ransomware:** Cumpla la estrategia de copia de seguridad 3-2-1-1-0 para garantizar la resiliencia de los datos. Verifique los datos automáticamente durante las copias de seguridad para garantizar que se puedan almacenar copias limpias de sus datos. Detecte y repare cualquier error de datos mediante funciones de recuperación automática. Realice simulacros de DR mediante el sandbox integrado de ActiveProtect. Proteja las copias de seguridad con la tecnología WORM (Write Once Read Many) para impedir que se realicen cambios o eliminaciones en sus datos. Proteja copias limpias de sus copias de seguridad en una ubicación externa dentro de un entorno aislado mediante aislamiento lógico o físico.

Migre y restaure datos con flexibilidad

Mueva datos sin problemas entre plataformas en la nube y locales. Restaure datos con flexibilidad en entornos de nube, virtuales y físicos como Azure VM, Amazon EC2, VMware vSphere, Microsoft Hyper-V y otros. Cumpla los objetivos de tiempo de recuperación (RTO) para la recuperación ante desastres y garantice un acceso rápido a los datos para cumplir los requisitos de continuidad empresarial. Realice recuperaciones de bajo nivel y restauraciones a nivel de archivo, y descargue sus copias de seguridad para restaurar los datos cuando sea necesario.

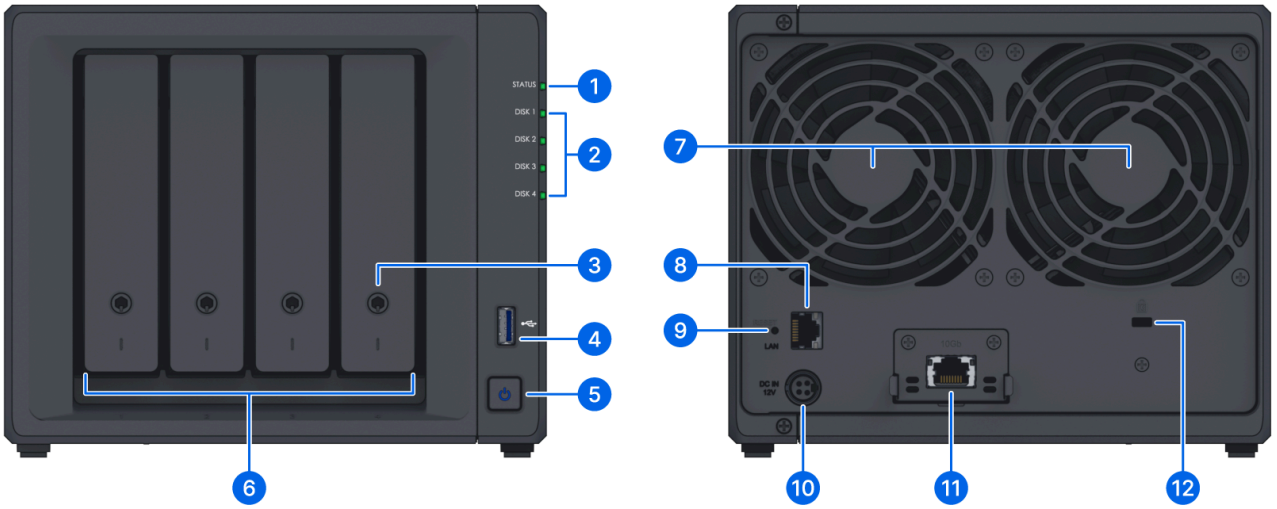
Realice simulacros de recuperación ante desastres periódicamente en un entorno sandbox sin ningún impacto en su sitio de producción. Verifique sus copias de seguridad y genere automáticamente vídeos de recuperación para fines de auditoría.

Escalabilidad bajo demanda

Utilice el almacenamiento por niveles de versiones para mover datos a un almacenamiento remoto como Synology NAS, C2 Object Storage, Wasabi Cloud Storage, Azure Blob Storage o AWS S3, con el fin de ampliar fácilmente el almacenamiento y conservar los datos a largo plazo.

A medida que crezca su empresa, añada nuevas torres DP340 y gestiónelas de forma centralizada mediante un dispositivo ActiveProtect de 1U o 2U que ejecute ActiveProtect Manager.

Descripción general del hardware



N.º	Nombre	N.º	Nombre
1.	Indicador de estado	7.	Ventilador
2.	Indicador del estado de la unidad	8.	Puerto de gestión
3.	Bloqueo de la bandeja de la unidad	9.	Botón RESET
4.	Puerto USB 3.2 Gen 1	10.	Puerto de alimentación
5.	Botón de encendido	11.	Puerto LAN 10GBase-T
6.	Bandeja de la unidad	12.	Ranura de seguridad Kensington

Especificaciones técnicas

General	
Capacidad bruta[1]	24 TB
Capacidad con clasificación por niveles[2]	Hasta 770 TB
Capacidad de administración del clúster[3]	Admite hasta 30 servidores o 1.500 cargas de trabajo
Máquina virtual restaurada integrada sugerida[4]	2
Notas	1. Estos valores son estimaciones basadas en datos de telemetría y pueden variar según las condiciones de uso empresarial. 2. Los datos archivados a largo plazo se pueden clasificar por niveles en un almacenamiento remoto, conservando únicamente el índice localmente para reducir el uso de espacio local. El límite de Capacidad con clasificación por niveles depende del uso de datos del dispositivo y del número de cargas de trabajo y versiones clasificadas por niveles. Póngase en contacto con el equipo de Synology para obtener una evaluación. 3. Se requiere una licencia de ActiveProtect. 4. Número máximo de máquinas virtuales de restauración integradas sugeridas

Hardware	
Factor de forma	Escritorio
CPU	AMD Ryzen R1600 (2 núcleos)
Memoria	16 GB
Configuración de almacenamiento	• 4 × 8 TB HDD de 3,5" (RAID 5) • 2 × 400 GB SSD M.2 (RAID 1)
Interfaz de red	• 1 × 10GbE RJ-45 (Transferencia de datos) • 1 × 1GbE RJ-45 (Administración)
Dimensiones del producto (AlxAnxPr)	166 × 199 × 223 mm
Peso	5,2 kg
Tensión de entrada de CA	De 100 V a 240 V CA
Frecuencia de alimentación	50 / 60 Hz, monofásica
Consumo de energía	35,51 W
Unidad térmica británica	121,09 BTU/h
Entorno operativo	• Temperatura: de 32 °F a 104 °F (de 0 °C a 45 °C) • Humedad relativa: del 8 % al 80 % de HR
Entorno de almacenamiento	• Temperatura: de -5 °F a 140 °F (de -20 °C a 60 °C) • Humedad relativa: del 5 % al 95 % de HR

Entorno y embalaje	
Certificación	FCC, CE, BSMI, VCCI, RCM, UKCA, EAC, KC, UL, BIS
Seguridad medioambiental	Conforme con RoHS
Contenido de la caja	• 1 x unidad principal DP340 • 4 x HDD SATA de 3,5” • 1 x paquete de accesorios • 1 x guía de instalación rápida
Garantía	3 años
Notas	El periodo de garantía comienza en la fecha de compra indicada en el recibo. Obtenga más información sobre la garantía limitada del producto.

SYNOLOGY INC. © 2026, Synology Inc. Todos los derechos reservados. Synology y el logotipo de Synology son marcas comerciales o marcas registradas de Synology Inc. Los demás nombres de productos y empresas aquí mencionados pueden ser marcas comerciales de sus respectivas empresas. Synology puede realizar cambios en las especificaciones y descripciones del producto en cualquier momento y sin previo aviso.