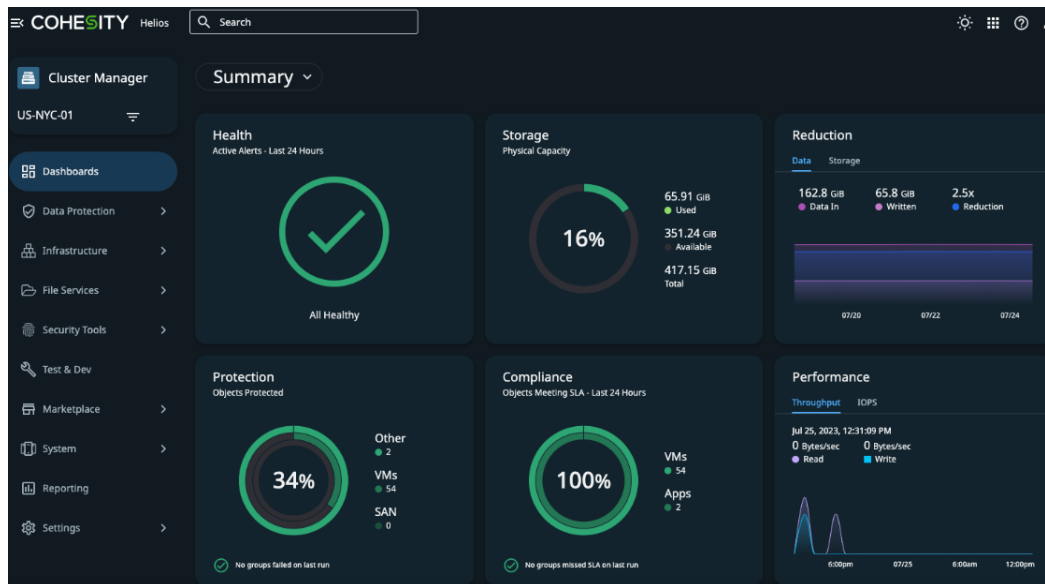# COHESITY

Cohesity DataProtect

Available as a Service or Self-managed Software

Cohesity DataProtect is a high-performance, secure data protection solution. Designed to safeguard your data against sophisticated cyber threats, it offers the most comprehensive policy-based protection for your cloud-native, SaaS, and traditional data sources.

DataProtect converges multiple-point products into a single software that can be deployed on-premises or consumed as a service (BaaS).

Multi-layered Protection for Enterprise Applications

Designed on zero-trust principles, Cohesity DataProtect secures your enterprise data across a broad set of sources - virtual and physical servers, traditional and containerized applications, databases, NAS, and SaaS workloads.

A combination of immutability, WORM, data encryption framework, multifactor authentication, and granular role-based access control helps to stop unauthorized applications and bad actors from modifying or deleting your data.

Lightning Fast Recovery

The solution features near-zero recovery point objectives (RPOs) and near-instant recovery time objectives (RTOs) to meet business service-level agreements (SLAs). With Cohesity Helios' unified control plane quickly search and recover data on any Cohesity cluster, located anywhere[1]. DataProtect in self-managed deployment uniquely reduces downtime by instantly mass restoring any number of virtual machines (VMs), large volume of unstructured data, and any size Oracle database, to any point in time[1], and reduces data protection costs by 70% or more.

Freedom of Backup as a Service (BaaS)

Take advantage of the public cloud's elasticity and economics with DataProtect delivered as a service. Choose an OpEx spend model and eliminate the need for on-premises hardware. The SaaS option allows you to easily configure your backup jobs and, within minutes, start protecting your mission-critical data and applications without needing any hardware on-premises.

Hosted in AWS and Microsoft Azure, Cohesity BaaS offers flexibility and choice to meet your business requirements.

Specifications		
Protected Workloads	**Self-managed** • Hypervisors: VMware vSphere (6.5 and later), Microsoft Hyper-V (2022, 2019, 2016, 2012 R2), Nutanix AHV and RHeV • Kubernetes: Vanilla, Red Hat Open Shift, VMware Tanzu Grid and Grid Service • Cloud: AWS EC2, Azure VM, and Google Compute • Physical: Windows, Linux (RHEL, CentOS, OEL, Debian, Ubuntu), AIX (7.x), and Solaris • Enterprise Databases: Oracle (11g R2, 12c), Oracle RAC and Microsoft SQL (2008 or later), SAP Oracle, SAP HANA, SAP Sybase ASE, SAP MS SQL, Sybase IQ, IBM DB2 LUW, Sybase ASE • Modern Databases: MongoDB with CDP, Hive, Hbase, Cassandra, CouchbaseDB, MySQL Enterprise Commercial Edition, PostgreSQL, Datastax Enteprise, Hortonworks Hadoop Distribution • Cloud-native Databases: AWS RDS, AWS Aurora, CockroachDB • Applications: MS Exchange (2019, 2016), MSFT Active Directory, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive, Teams, Groups), SalesForce (SFDC), and SAP HANA • Primary storage: Pure FlashArray, HPE Nimble and Cisco Hyperflex • NAS: Pure FlashBlade, NetApp, Isilon, IBM GPFS, Elastifile, and generic solutions	**Cohesity-managed BaaS** • Hypervisors: VMware vSphere (6.5 and later) and Microsoft Hyper-V (2019, 2016, 2012 R2) • Cloud: AWS EC2, Azure VM • Physical: Windows and Linux (RHEL, CentOS, OEL, Debian, Ubuntu) • Enterprise Databases: Oracle (11g R2, 12c) and Microsoft SQL (2008 or later) • Cloud-native Databases: AWS RDS, Azure SQL • SaaS Applications: Microsoft 365 (Exchange Online, SharePoint Online, OneDrive and Teams) and Salesforce • Primary storage: AWS S3 • NAS: NetApp, Isilon and generic solutions
Recovery Level	• Instant mass restore • Granular recovery of files, folders, and objects • Volume recovery • VMDK recovery • Instant volume mounts • Instant restores of VMs • Cyber recovery	• 12 hour RPO
Ransomware Protection	• Immutable backups, DataLock (WORM), encryption, and RBAC, Cyber vaulting • Machine learning-based anomaly detection • Rapid recovery at scale	
Long-Term Archival	• Public cloud infrastructure, S3 and NFS compatible devices • Tape support using QStar archive manager	
Global Search	• Global actionable search • Automated global indexing • Wildcard searches for any VM, file, or object on the platform	

Specifications		
Flexible Deployment	• Software-defined solution for on-premises, public cloud, hybrid cloud, backup as a service, and edge sites	
Public Cloud Integration	• Multiple cloud solutions including long-term retention, disaster recovery, dev/test and native cloud backup • Cohesity CloudSpin	• Cohesity Cloud Snapshot Manager • Cohesity CloudArchive (unlimited) • Cohesity CloudArchive Direct
Global Management and Access Control	• Cohesity Helios control plane • Multi-cluster single sign-on • Role-based access control	• Multi-factor authentication • Multi-cluster dashboard
Machine-Drive Recommendation	• Clean recovery point • Proactive system wellness • Capacity prediction	• What-if analysis • Performance balancing • Support automation
Capacity Optimization	• Storage efficiency (EC, small file efficiency) • Global variable-length sliding-widow deduplication • Compression	
Integration and Automation	• API-first architecture • Python SDK • OpenAPI standard • PowerShell Module • RESTful API • VMware vRealize (vRA/vRO)	• VMware vCloud Director (vCD) • ServiceNow • Ansible
Security	• Software-defined AES-256, FIPS 140-2 compliant encryption of data in flight and at rest • TOTP, Restricted Shell Access	

[1]Not supported on backup as a service.

Simplify and modernize your backup and recovery infrastructure with Cohesity DataProtect. Learn more at Cohesity.com/products/dataprotect.

1000008-030-EN 2-2025