Cohesity NetBackup

Advanced data protection with integrated cyber resilience

NetBackup is a powerful and highly scalable data protection solution that supports over 1,000 data sources and over 1,000 storage targets. With built-in threat detection, advanced analytics and integrations, and intelligent automation, NetBackup provides integrated cyber resilience and comprehensive coverage for today's complex hybrid and multi-cloud environments.

Our latest release (NetBackup 11.1) builds on a growing compilation of cyber resilience innovations, cloud workloads, and AI-powered automation capabilities to provide the most powerful and secure architecture to date.

Cyber resilience

More than 96% of business leaders identify ransomware as a critical threat and primary concern. Ransomware continues to grow—the number of attacks, ransoms paid, and cost of related downtime are increasing exponentially.

Securing your environment and data, as well as ensuring the ability to recover, are key requirements of any enterprise data protection strategy.

NetBackup's comprehensive data protection solution reduces risks, eliminates uncertainty, and helps you maintain control of your environment. The resilience strategy reinforces your data and infrastructure defense against malicious data-damaging threats. Use it to confidently defend against ransomware for the multi- and hybrid cloud using a three-step approach (see Figure 1):

Step 1—Protect: Safeguarding data integrity with system hardening, immutability, and air gap

Step 2—Detect: Monitoring and reporting on system activity, leveraging AI/ML to mitigate threats and vulnerabilities

Step 3—Recover: Non-disruptive automating and orchestrating complete cross-system restoration with clean copies

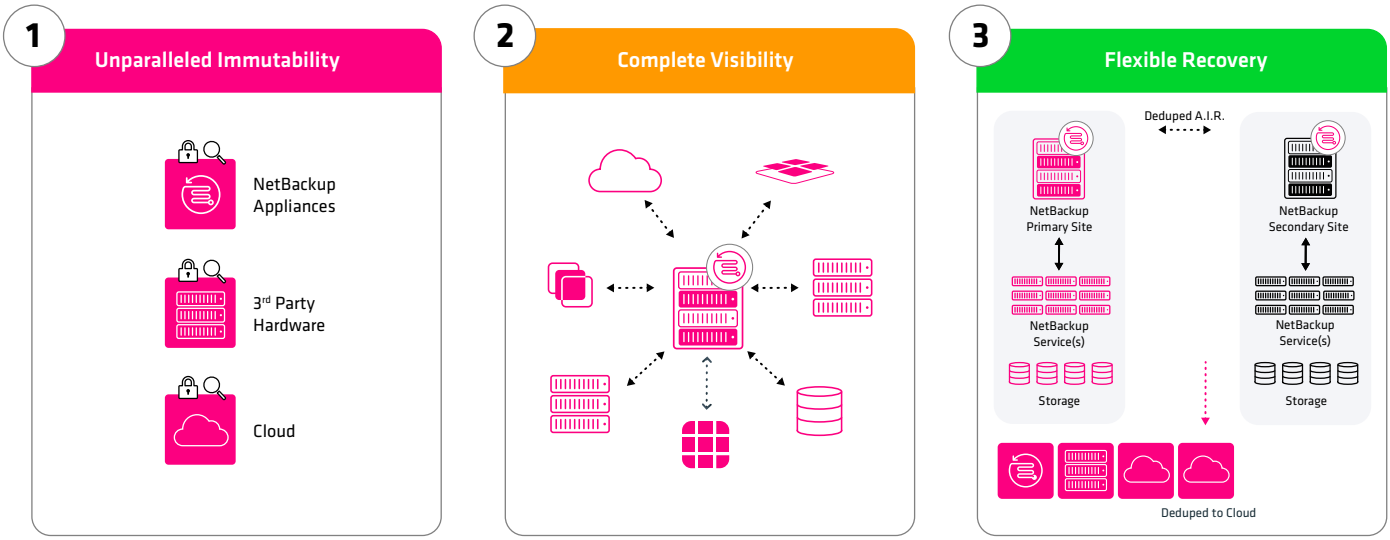

Figure 1. The three steps NetBackup takes to ensure cyber resilience

NetBackup provides ML-based user behavior analytics to ensure security at all times—not just at login. It utilizes self-defending intelligence to monitor user behavior, and it enhances your cyber resilience posture with the following capabilities:

- An ML-based adaptive risk engine that proactively monitors user behavior to guard against internal and external threats and prevent irreversible data destruction
- Inline entropy analysis for rapid detection of encryption events during a backup, and more holistic anomaly detection
- Adaptive multi-factor authentication (MFA) that identifies high-risk user actions and subject them to additional authentication
- Adaptive multi-person authorization (MPA) that defends against insider threats by monitoring changes to security and other settings
- A blast radius analysis that performs searches for malware and other potential indicators of compromise (IOCs) in a highly efficient way that scales across the entire enterprise environment.
- A security risk meter that allows users to set a baseline for their security configuration and track any changes from that selected baseline.
- Version 11.1 of NetBackup adds the following new capabilities:
  - A new **Freeze Mode** acts like a digital "red stop button," allowing administrators to instantly lock down the environment during a cyber event – halting restores, changes, or expirations.
  - A new **Maintenance Mode** enables safer upgrades in a temporary, time-bound state that auto-reverts to lockdown.
  - **YARA rule-based scanning** allows security teams to import external threat feeds and detect malware patterns, using the same tools that security researchers employ worldwide.
  - A new **Stop-on-Infection** workflow halts scans at the first detected threat, flags the image, and moves to the next recovery point – saving compute time and improving RTO.

AI-Driven Anomaly Detection and Automated Malware Scanning

NetBackup augments its artificial intelligence-driven anomaly detection capabilities with automated malware scanning. During backup operations, backups are checked for anomalies in near real-time. If anomalies are suspected, malware scanning is automatically initiated to determine if backups contain malware. If a malware scan is positive, data protection, replication, and expiry can be automatically paused for infected targets to contain the spread and prevent expiration of backups with uninfected data.

NetBackup utilizes an adaptive risk engine to perform built-in user behavior analytics that monitor and learn from user actions as they happen. Once sufficient training data is obtained, high-risk operations will trigger alerts and additional security checks in order to slow down a cyberattacker and prevent irreversible destruction of data.

NetBackup can automatically pause data protection activities for a protected asset when a malware scan detects an infection in a backup image. Malware scanning is also used to identify the last known good backup before restoring. The ability to identify and recover the most recent malware-free backup is crucial for fast recovery of critical business operations. When recovering, it is imperative to ensure any infected files are not included in the restoration.

The ability to exclude these files, preventing the possibility of reinfection, enables the most current backups to be recovered, getting business back to the closest point prior to the attack (see Figure 2). Malware scanning can also be performed inline during recovery, if desired.

Inline entropy analysis is part of NetBackup's anomaly detection capabilities, which computes entropy levels as the backups occur. This patented technology can be performed with no measurable impact to backup performance, and internal testing has shown a 100% success rate in ransomware detection, with an extremely low false positive rate (<0.1%). Based on this data and other heuristics, recommended recovery points are then highlighted that provide the best optimization of RPO and RTO while also ensuring a clean, malware-free restore.

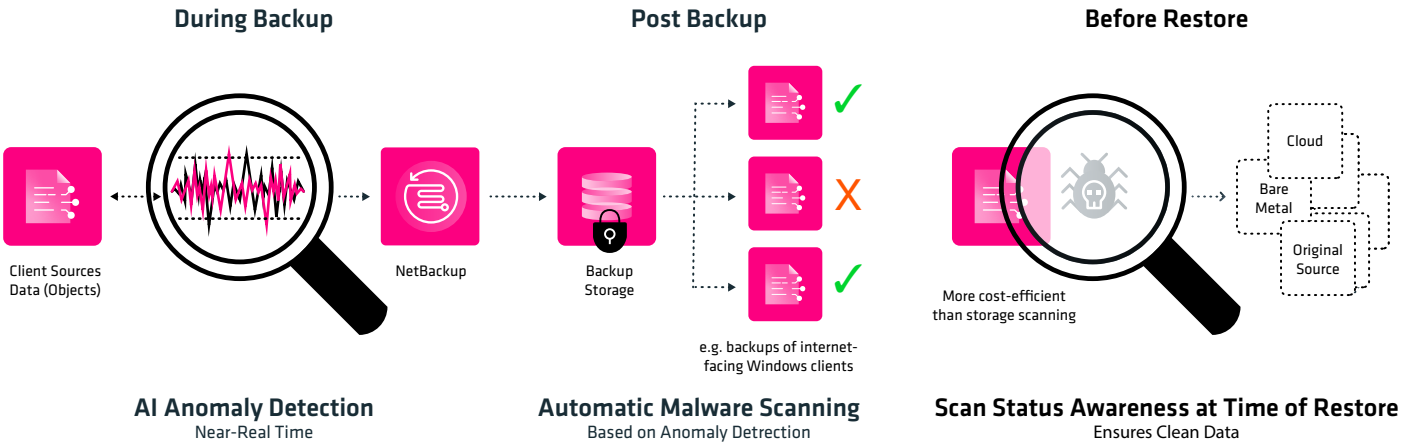

Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

Anomaly and malware scan alerts stored within system logs can be ingested easily by early warning systems such as SIEM platforms.

When combined with security alerts generated by other services, devices, and endpoints within the IT infrastructure, this data provides even greater visibility across an estate, while increasing awareness and response to potential threats. The API also enables SOAR/XDR platforms to pause or resume data protection activities based on security or maintenance events.

Multi-Cloud Optimized

NetBackup provides highly flexible protection of cloud workloads, empowering organizations to transport workloads from cloud providers into MSDP storage pools, optimizing and deduplicating data, and making workloads easily recoverable with efficient object storage. Cloud data is now available directly from backup storage, allowing users to view data that is compressed, encrypted, and deduplicated.

With the past few releases of NetBackup our support for cloud workloads, cloud targets, and cloud storage has grown dramatically and is unmatched in the industry:

- Five cloud service providers
- Twenty-four cloud object storage targets
- Ten cloud storage options
- Ten software as a service (SaaS) applications
- Twenty-nine platform as a service (PaaS) workloads

NetBackup is powered by Cloud Scale Technology, which delivers enhanced protection and simplified operations across expanded workloads, including Kubernetes and SaaS-based applications. It provides secure, automated, and orchestrated workload protection, resulting in a more cost-effective, resilient, and sustainable environment with:

- Elastic backup and recovery services for Amazon Web Services (AWS) and Azure
- Agentless backup from snapshot
- Enhanced elastic cloud autoscaling for AWS and Azure
- Cross-cloud recovery from AWS to Azure or Azure to AWS

Version 11.1 adds the following new capabilities:

- New **unified snapshot management** for consistent snapshots, replication, and restores from a single control plane across both cloud and on-premises workloads.
- **Expanded cloud database protection** with incremental backup support for Amazon DynamoDB, Amazon RDS for SQL Server, and Amazon Aurora PostgreSQL – enabling tighter RPOs and faster recovery.
- New **Oracle Private Cloud Appliance support** allows enterprises running Oracle workloads to protect VMs in private OCI-compatible environments using the same framework as public cloud assets.

Automated Operations

With automated and intelligent policies, NetBackup brings enhanced protection and simplified operations to the broadest collection of workloads to date, including traditional, PaaS, SaaS, and container-based applications. It provides secure, resilient, orchestrated delivery of intelligent, event-driven workload protection at the edge, on-premises, and in the cloud, reducing data protection gaps by minimizing human error and time-consuming administrative tasks with new capabilities.

NetBackup 11.1 adds the following new capabilities for enhanced automation:

- **Native backup and recovery for KVM workloads** directly within the NetBackup Web UI – eliminating the need for third-party tools.
- **Nutanix AHV Instant Access** allows users to restore VMware backups directly to a Nutanix AHV cluster, unlocking seamless data mobility across virtualization platforms.
- **NetBackup DirectIO** allows you to connect to Cohesity SpanFS – the flexible, fast, and distributed file system that powers Cohesity Data Cloud. This new integration turns your NetBackup environment into a modernized, high-performance platform with unprecedented speed and scale.

NetBackup provides enhanced media server elasticity and intelligence to optimize resource utilization and cost savings. NetBackup automatically optimizes spin-up to incrementally improve efficiency by deploying the smallest media server image required for the demand. This reduces total utilization to keep compute costs at the lowest possible level.

NetBackup supports the widest range of certified S3 and Integrated Object Level Lock targets in the market, providing full deduplication and optimization from any workload to any target (see Figure 3).

Integrated Cohesity IT Analytics Foundation

Integrated IT Analytics Foundation delivers capabilities to bring together cloud and information with insights on the data and provide intelligence across hybrid and multicloud environments. By pinpointing operational inefficiencies, identifying threshold-based backup inconsistencies, and compiling a single-source report of information, Cohesity IT Analytics Foundation can easily identify necessary changes so you can take action (see Figure 4).

Using these analytics, overall cloud costs are reduced through right-sizing and optimizing cloud infrastructure. Bringing together insights from multiple cloud service providers helps identify the exact costs, and enables consolidation of public cloud expenditures for further analysis and action.

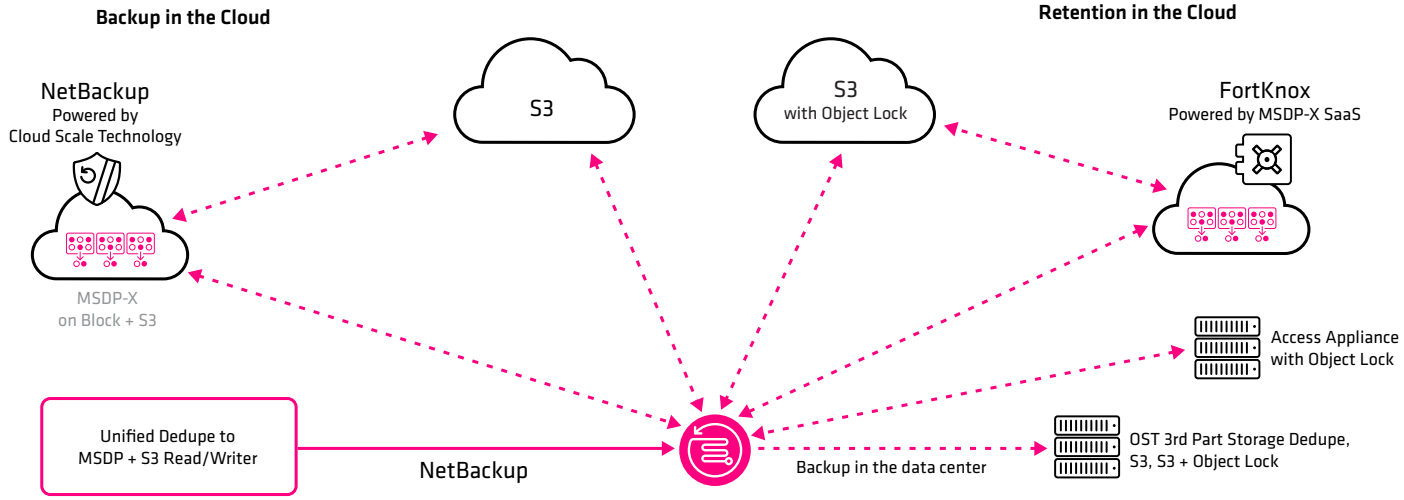

Figure 3. Overview of NetBackup cloud workload support

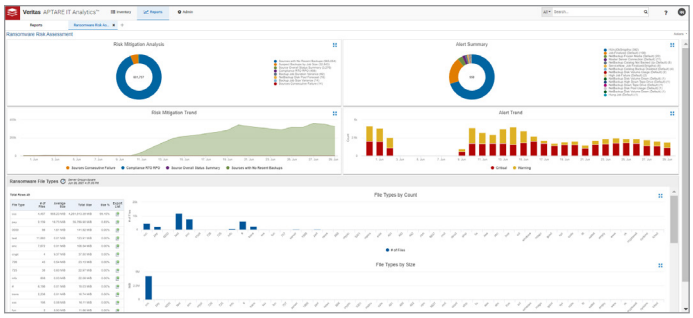

Figure 4. Example of IT Analytics Foundation's single-source report bringing together cloud and information insights

Kubernetes Multi-Cloud, Multi-Distribution Recovery

NetBackup provides the industry's broadest support for Kubernetes by providing the consistency and portability teams need to protect any Kubernetes distribution, regardless of deployment—on-premises or in the cloud. This is because NetBackup for Kubernetes was designed to offer operational simplicity, enterprise-grade resiliency, and choice and flexibility for Kubernetes workload protection.

Kubernetes workloads can be backed up to any storage target available in the NetBackup web UI. When it comes to the cloud, Kubernetes data protection operations are effectively managed with NetBackup's Elastic Cloud Autoscaling, dynamically provisioning and removing cloud instances as needed, maximizing cost and efficiency. In addition, instant rollback from snapshots, application consistent Kubernetes cluster backup, deduplication, image duplication for the tiering of backup storage service lifecycle policies (SLPs), and auto image replication (AIR) are all built-in.

NetBackup for Kubernetes features simplified installation, configuration, and management. Intelligent policies dynamically discover all namespaces and their labels on the Kubernetes cluster and add namespaces to the protection plan based on customer-defined parameters. This process ensures automatic protection, reduces the risk of data loss, and gives users much greater control in defining how their applications are protected, with the ability to easily include and exclude specific resources.

More than 50% of customers using Kubernetes run more than one distribution. One of the biggest drivers of Kubernetes is its portability—the ability to move between on-premises and different clouds. NetBackup provides the freedom to run as many distributions of Kubernetes as needed, without requiring different backup products.

Why NetBackup?

NetBackup provides cost-effective and secure sustainability to your enterprise hybrid cloud. It uniquely integrates SaaS, analytics, and automated on-demand services, protecting data while improving operational agility and control across any cloud.

As the #1 data protection solution with the most exabytes under management, NetBackup can protect any size workload at scale at petabyte-level capacity, eliminating the need for point products. NetBackup helps ensure resiliency and on-demand access from anywhere and reduces the risks and costs of storing ever-increasing amounts of data throughout the globe.

Specifications

(See the NetBackup Compatibility List for additional details and specific versions)

Protected Workloads: Operating Systems

- Alma Linux
- BC-Linux
- BC-Linux-Euler
- Beijing Linux
- Canonical Ubuntu
- CentOS
- Debian GNU
- HP-UX
- IBM AIX
- Kylin Linux
- Microsoft Windows
- Oracle Linux
- Oracle Solaris
- Red Hat Enterprise Linux
- Rocky Linux
- SuSE Linux

Protected Workloads: Databases and Applications

- Apache Cassandra
- Apache Hadoop
- Apache Hbase
- DataStax Cassandra
- Enterprise Vault
- HCL Domino
- IBM DB2
- IBM Informix
- MariaDB
- Microsoft Exchange
- Microsoft Sharepoint
- Microsoft SQL
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP ASE
- SAP HANA
- SAP MaxDB
- SAP Oracle
- SQLite
- Sybase ASE
- XBSA

Protected Workloads: File Systems

- BTRFS
- Ext2/3/4
- GPFS
- HFS/HFS+
- JFS/JFS2
- Lustre
- NTFS
- REFS
- ReiserFS
- UFS
- VxFS
- XFS
- ZFS

Protected Workloads: Cloud/Virtual/HPC

- Alibaba Cloud Object Storage Service
- Amazon GovCloud
- Amazon Simple Storage Service
- AWS S3
- AWS VM (EC2)
- Azure Blob
- Azure Data Lake Storage Gen 2
- Azure File Storage
- Azure VM
- Azure VMware
- Azure Stack
- Azure Storage Service
- Cloudian HyperStore Object Storage
- Dell EMC Elastic Cloud Storage
- Google Cloud Storage
- Hitachi Vantara Content Platforrm - LAN
- Hitachi Vantara Content Platforrm - WAN
- Kubernetes (all CNCF-certified distributions)
- Microsoft
- Microsoft
- Microsoft Hyper-V
- NEC N2
- NetApp ONTAP S3
- NetApp Storage Grid
- Nutanix AHV
- OpenStack
- ONTAP S3
- Oracle Linux VM
- Pure FlashBlade
- Quantum ActiveScale Systems
- Red Hat CEPH Storage
- Red Hat RHV
- Scality RING Storage - LAN
- Scality RING Storage - WAN
- STACKIT Object Storage
- StorageGRID Webscale Object Storage
- VMware
- VMware vRealize

Protected Workloads: Cloud-Native Databases

- Azure MySQL
- Azure SQL DB
- Azure Managed SQL
- Azure MariaDB
- Azure PostgreSQL
- Azure Cosmos NoSQL Database
- Azure Cosmos Mongo Database
- Amazon DynamoDB
- Amazon RDS SQL Server
- Amazon RDS PostgreSQL
- Amazon RDS MySQL
- Amazon RDS MariaDB
- Amazon Aurora
- PostgreSQL
- Amazon Aurora MySQL
- Amazon RedShift
- Amazon RDS Oracle
- Google PostgreSQL
- Google MySQL
- GCP SQL server

Storage Platforms

- Dell EMC
- Dell EMC Data Domain
- Dell EMC Isilon
- ExaGrid
- FalconStor
- Fujitsu
- Hitachi Ventara
- H3C
- HPE
- Huawei
- IBM
- Imation
- Infinidat
- Lenovo
- NEC
- NetApp
- Nexenta
- Oracle
- Pure FlashArray/FlashBlade
- Stratus
- Quantum
- Quest

Cloud Storage Targets

- ACP
- Alibaba
- Amazon
- AT&T
- Backblaze
- Beijing XSKY
- China Mobile
- China Telecom
- Chunghwa Telecom
- Cloudian
- DataCore
- Dell EMC
- Dell EMC Isilon
- Deutsche Telekom
- Fujitsu
- Google
- HPE
- Hitachi Vantara
- IBM
- Impossible Cloud
- Infoniqa
- Iron Mountain
- iTernity
- Microsoft
- NEC
- NetApp
- NooBaa
- Nutanix
- Oracle
- Orange Business Services
- Pure Storage
- Quantum
- Red Hat
- SandStone
- Scality
- Seagate
- Spectra Logic
- STACKIT
- SUSE
- SwiftStack
- Tencent
- VAST Data
- Veritas
- Wasabi

NAS Protection

- Dell EMC
- Dell EMC Data Domain
- Dell EMC Isilon
- Fujitsu
- Hitachi Vantara
- HPE
- Huawei
- IBM
- Imation
- Infinidat
- Lenovo
- NEC
- NetApp
- Nexenta
- Nutanix
- Pure Storage
- Oracle
- Qumulo
- Stratus Technologies

Tape Libraries, Drives, and VTLs

Amazon	Hitachi Vantara	Qualstar
Dell EMC	Huawei	Quantum
Dell EMC Data Domain	IBM	Quest
FalconStor	Infinidat	Spectra Logic
Fujitsu	NEC	Tandberg
H3C	Oracle	
HPE	Overland	

Fibre Transport Media Servers

Broadcom Emulex	Hitachi Vantara	Marvell Qlogic
Dell EMC	IBM	Oracle
HPE	Lenovo	

Learn more about NetBackup

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

1000080-002-EN 11-2025