

# Veritas NetBackup 10.4

Advanced data protection with integrated cyber resilience.

Veritas NetBackup 10.4 builds on the existing foundation of NetBackup's secure-by-default architecture. It expands threat detection with self-defending capabilities based on user-centric analytics, providing the most powerful and secure architecture to date.

With the latest release, Veritas continues to simplify data protection with intelligent cyber resilience, advanced automation, and expanded control and flexibility — all of which strengthen protection while reducing cost and resource demands.

## 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

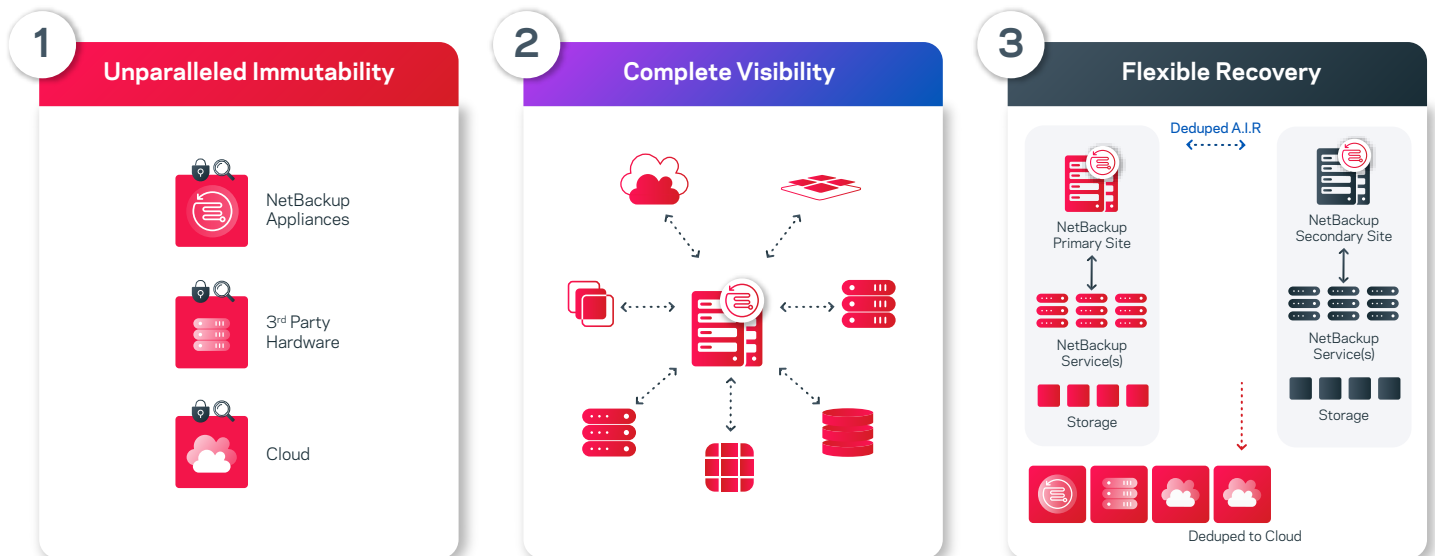


Figure 1. The three steps NetBackup takes to ensure cyber-resilience

NetBackup 10.4 adds ML-based user behavior analytics to ensure security at all times — not just at login. The latest release utilizes self-defending intelligence to monitor user behavior, and it enhances your cyber resilience posture with new capabilities:

- A new 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 uses the new adaptive risk engine to identify high-risk user actions and subject them to additional authentication
- Adaptive multi-person authorization (MPA) that uses the new adaptive risk engine to defend against insider threats by monitoring changes to security and other settings
- Automated recovery point recommendations with suggested recovery points that optimize recovery time and minimize data loss based on in-depth analysis
- New support for the Open Cybersecurity Schema Framework (OCSF) for security event logs, accelerating security incident analytics

### 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 10.4 leverages its ML to further extend anomaly detection with its new adaptive risk engine. With built-in user behavior analytics, it monitors and learns 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 10.4 also adds inline entropy analysis to NetBackup's anomaly detection capabilities, which computes entropy levels as the backups occur. This new 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 in Veritas Alta™ View that provide the best optimization of RPO and RTO while also ensuring a clean, malware-free restore.

Malware scanning is used to identify the last known good backup before restoring. 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.

These enhancements allow NetBackup to automatically pause data protection activities for the protected asset when a malware scan detects an infection in a backup image. The API also enables SOAR/XDR platforms to pause or resume data protection activities based on security or maintenance events. 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.



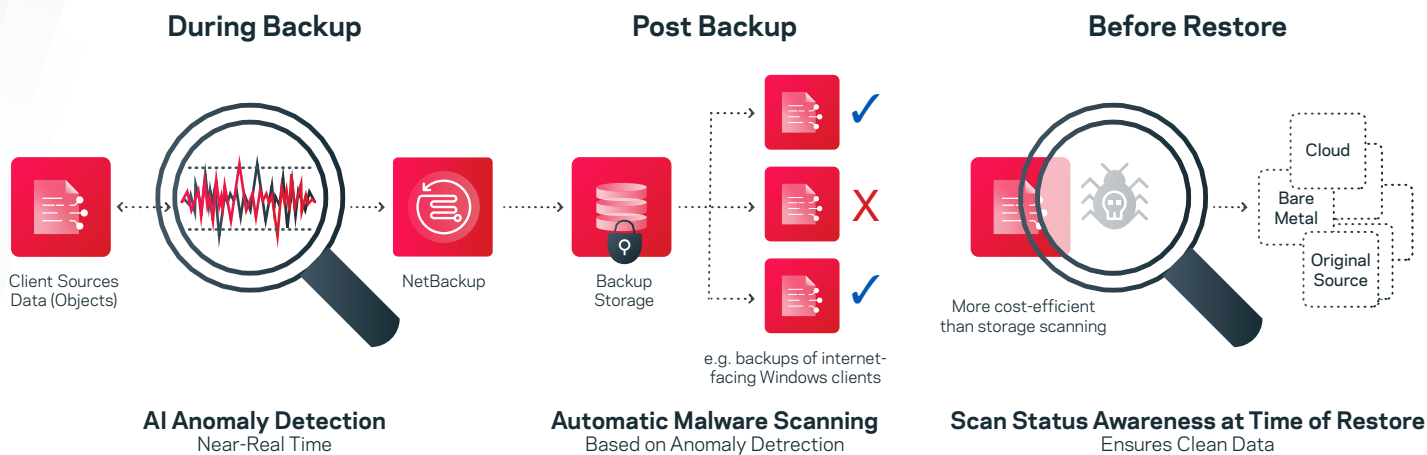


Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

## Multi-Cloud Optimized with Veritas Alta Data Protection

Veritas Alta™ Data Protection is an extension of NetBackup that runs in cloud environments. It 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 10.x and Veritas Alta Data Protection, our support for cloud workloads, cloud targets, and cloud storage has grown dramatically and is unmatched in the industry:

- Five cloud service providers
- Seventeen cloud object storage targets
- Eight cloud storage options
- Ten software as a service (SaaS) applications
- Nineteen platform as a service (PaaS) workloads

Version 10.4 also adds the following new capabilities:

- Intelligent Groups for PaaS workloads, providing expanded cloud workload discovery capabilities and eliminating the need for ongoing manual addition of new workloads
- Cloud to on-premises VMware recovery delivers new support for the recovery of VM backup images in AWS and Azure to on-premises VMware environments
- A new Universal Shares integration for OpenStack, greatly expanding the protection capabilities and functionality for OpenStack environments
- Direct support for VMware vSAN Express Storage Architecture (ESA) workloads, increasing scalability and performance

Veritas Alta Data Protection 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
- Elastic cloud deduplication services

## 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 10.4 adds the following new capabilities for enhanced automation:

- New point-in-time recovery capabilities for PostgreSQL databases and MS SQL databases within VMware environments, providing increased control and granularity for recoveries
- Agentless snapshot protection of the Oracle Cloud Infrastructure (OCI) platform now provides protection equivalent to that of AWS and Azure environments
- Oracle Pluggable Database support within Instant Access, allowing you to create a mount point in the same manner as other Oracle backups and further facilitating recovery
- Full support for Oracle RBAC which enables DBA credentialing and management from directly within the NetBackup UI
- New multi-stream recovery support for Hadoop, providing optimal performance for backup and recovery

NetBackup 10.4 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).

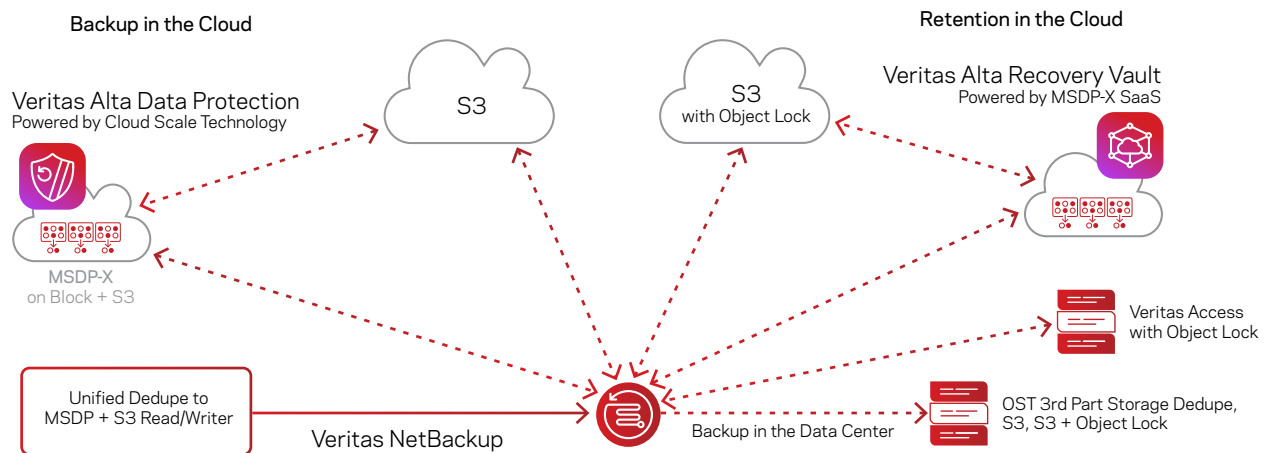


Figure 3. Overview of Veritas NetBackup cloud workload support

## Integrated NetBackup IT Analytics Foundation

Integrated NetBackup IT Analytics Foundation delivers capabilities to bring together cloud and information with insights on the data and provide intelligence across hybrid and multi-cloud environments. By pinpointing operational inefficiencies, identifying threshold-based backup inconsistencies, and compiling a single-source report of information, NetBackup 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.

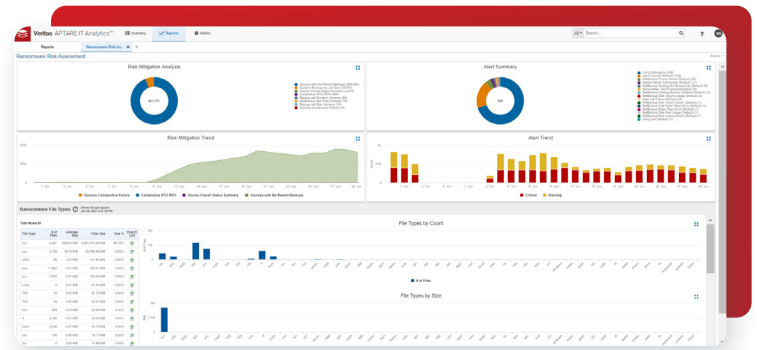


Figure 4. Example of NetBackup IT Analytics Foundation's single-source report bringing together cloud and information insights

## 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 Veritas designed NetBackup for Kubernetes 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.

NetBackup 10.4 extends malware scanning support for one or more persistent volume (PV) filesystem resources in Kubernetes namespaces. Forensic recovery of infected files is protected via role-based access controls (RBAC). With integrated anomaly detection and malware scanning for Kubernetes namespaces, data is always protected and recoverable.

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 Veritas?

Veritas NetBackup and Veritas Alta Data Protection provide 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 vendor in data protection with the most exabytes under management, Veritas can protect any size workload at scale at petabyte-level capacity, eliminating the need for point products. Veritas 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.

Learn more about [NetBackup](#) and [Veritas Alta Data Protection](#).

## Specifications

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

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

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

Protected Workloads: File Systems		
BTRFS	Lustre	VxFS
Ext2/3/4	NTFS	XFS
GPFS	REFS	ZFS
HFS/HFS+	ReiserFS	
JFS/JFS2	UFS	

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

## Protected Workloads: Cloud-Native Databases

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

## Storage Platforms

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

## Cloud Storage Targets

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

## NAS Protection

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

## 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	

### About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 91 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at [www.veritas.com](http://www.veritas.com). Follow us on X at [@veritastechllc](https://twitter.com/veritastechllc).

# VERITAS™

2625 Augustine Drive  
Santa Clara, CA 95054  
+1 (866) 837 4827  
[veritas.com](http://veritas.com)

For global contact  
information visit:  
[veritas.com/company/contact](http://veritas.com/company/contact)