Veritas NetBackup

Advanced data protection with integrated cyber resilience.

Veritas 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.

With our latest release (NetBackup 10.5), Veritas is taking data protection even further with new cyber resilience capabilities, more advanced automation, and expanded control and flexibility — all of which strengthen protection while reducing cost and resource demands.

Cyber Resiliency

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

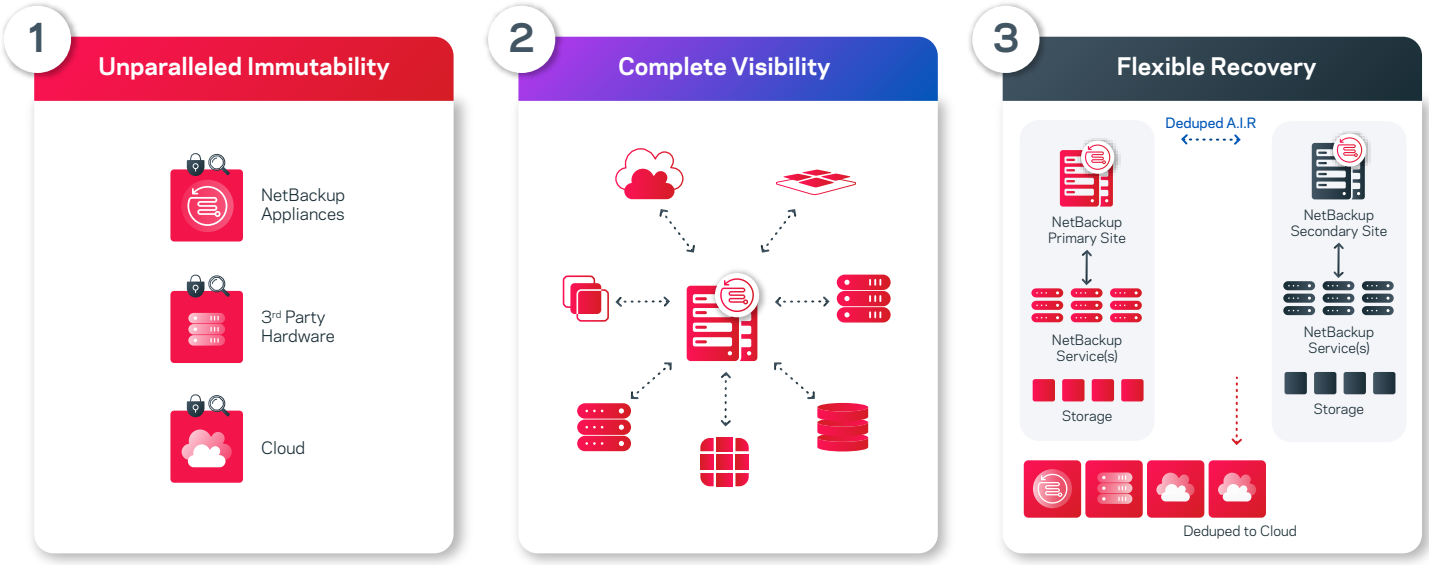

Figure 1. The three steps NetBackup takes to ensure cyber-resiliency

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
- Automated recovery point recommendations with suggested recovery points that optimize recovery time and minimize data loss based on in-depth analysis

Version 10.5 of NetBackup adds the following new capabilities:

- 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.

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.

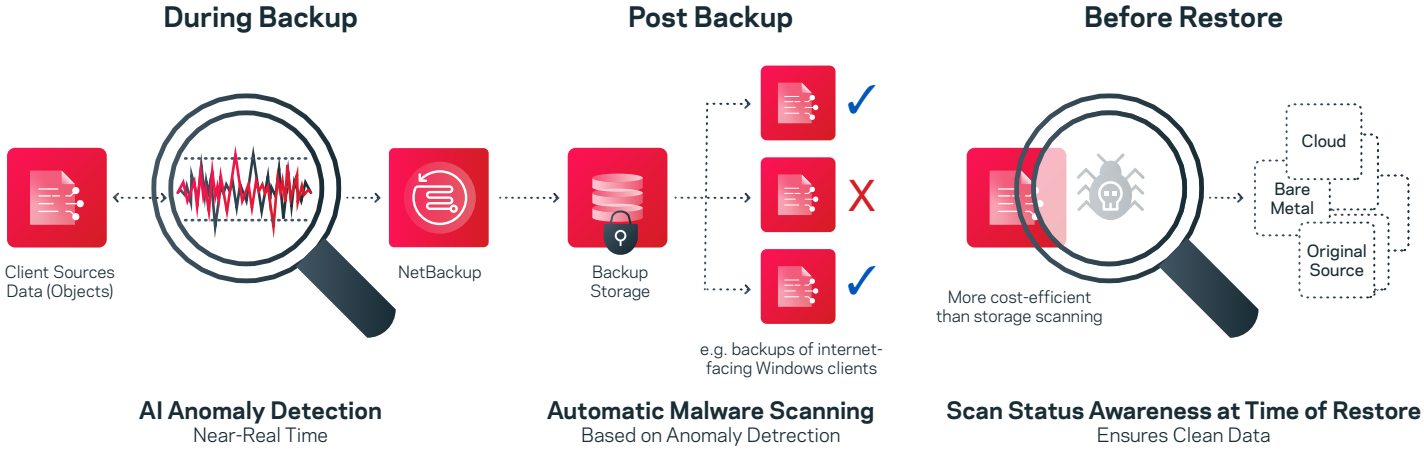

Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

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 in Veritas Alta™ View that provide the best optimization of RPO and RTO while also ensuring a clean, malware-free restore.

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 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
- Twenty platform as a service (PaaS) workloads

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

Version 10.5 adds the following new capabilities:

- Multi-stream cloud object storage protection — offering dramatically higher throughput with multi-stream backups of cloud object storage targets, ensuring protection needs are met for the most demanding hybrid cloud enterprises.
- Cross-cloud recovery — with the added flexibility to recover VMs from Azure to AWS or AWS to Azure. Also now enables the replication of DBPaaS backups to other NetBackup domains for recovery.
- Enhanced Cloud Elasticity — eliminates the requirement in Cloud Scale Technology for dedicated load balancers, reducing fixed costs and providing improved efficiency and scalability.

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 10.5 adds the following new capabilities for enhanced automation:

- MSDP Volume Groups — creates a single, light-weight MSDP server that acts as a front-end storage target on top of multiple MSDP storage targets to simplify management and improve scalability.
- Policy Management for Cloud and Kubernetes — standardizes protection across all major workloads by adding policy management and support for Storage Lifecycle Policies to cloud and Kubernetes environments.
- Granular RBAC for VMware vSphere — provides more granular support for RBAC in VMware environments by allowing permissions to be configured in alignment with the VMware hierarchy, at the datacenter or group level.

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).

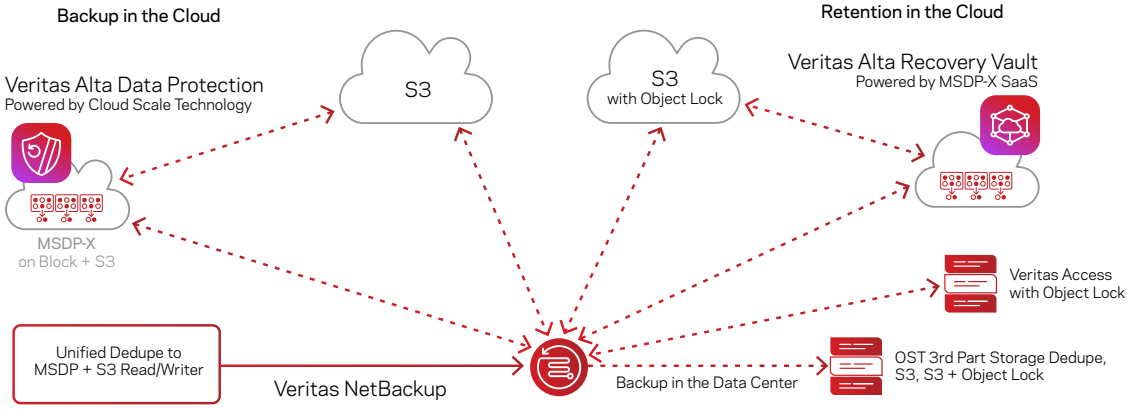

Figure 3. Overview of Veritas NetBackup cloud workload support

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).

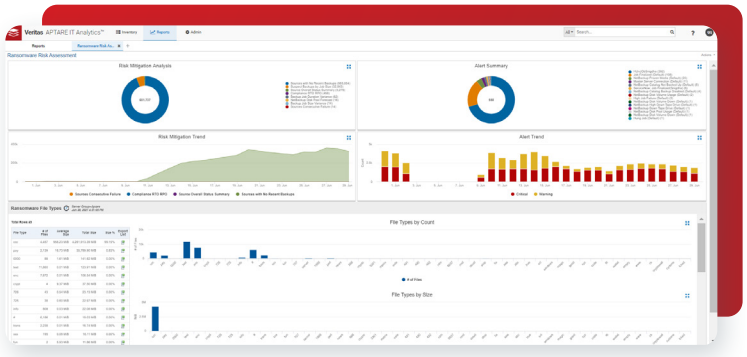

Figure 4. Example of NetBackup IT Analytics Foundation's single-source report bringing together cloud and information insights

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.

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 10.5 extends its protection policy functionality to include Kubernetes environments. With the ability to create backup policies, 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
- 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
- Dell EMC
- Dell EMC Data Domain
- FalconStor
- Fujitsu
- H3C
- HPE
- Hitachi Vantara
- Huawei
- IBM
- Infinidat
- NEC
- Oracle
- Overland
- Qualstar
- Quantum
- Quest
- Spectra Logic
- Tandberg

Fibre Transport Media Servers

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

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. Follow us on X at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V0891 09/24