

Veritas NetBackup 10.2

Advanced data protection with heightened efficiency and resiliency.

Veritas NetBackup™ 10.2 delivers the industry’s most advanced, cloud-optimized, scalable data protection solution, with enhancements to cyber resiliency and operational efficiency that strengthen data protection, while reducing cost and resource demands. With the latest release, NetBackup continues to radically simplify data protection, with the benefit of new resiliency and automation features and expanded workload support.

Cyber Resiliency

More than 96 percent of business leaders identify ransomware as a critical threat and their primary concern. Ransomware continues to grow—the rising number of attacks, the costs of ransoms paid, and the cost of downtime from attacks are increasing exponentially. Securing your environment and your data, as well as ensuring you can recover, are key requirements of any enterprise data protection solution.

NetBackup’s comprehensive data protection solution reduces risks, eliminates uncertainty, and helps maintain control of your environment. NetBackup’s resiliency strategy reinforces your data and infrastructure defense against malicious data-damaging threats—and confidently defends against ransomware—for the multi- and hybrid cloud, using a three-step approach (see Figure 1):

1. **Protect:** Safeguarding data integrity with system hardening, immutability, and air gap
2. **Detect:** Monitoring and reporting on system activity, leveraging AI/ML to mitigate threats and vulnerabilities
3. **Recover:** Automating and orchestrating complete cross-system restoration with clean copies and non-disruptive rehearsals

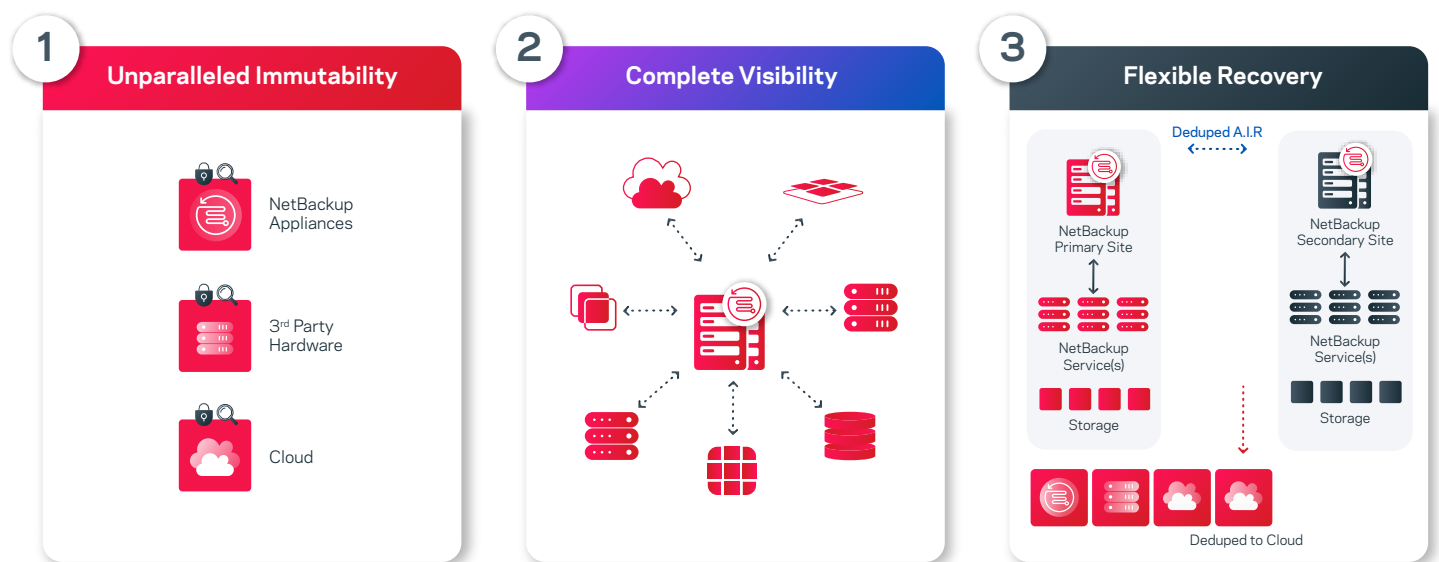


Figure 1. The three steps NetBackup takes to ensure cyber-resiliency.

NetBackup 10.2 enhancements for security, ransomware, and resiliency include:

- Configurable malware scanning for concurrent scans, and real-time progress tracking
- Malware scanning support for DNAS workloads
- NAS parallel recovery from DNAS backup
- Credential management system support for MSSQL workloads

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 10.2 extends integrated malware scanning to support DNAS workloads, and expands malware scanning configuration to allow concurrent jobs to run with the ability to monitor each job in progress individually.

Malware scanning is also used to identify the last known good before restoring. Now 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 also allow NetBackup to automatically pause data protection activities for the protected asset when a malware scan detects an infection in a backup image. These include backups, duplication, and expiration activities. 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 also 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).

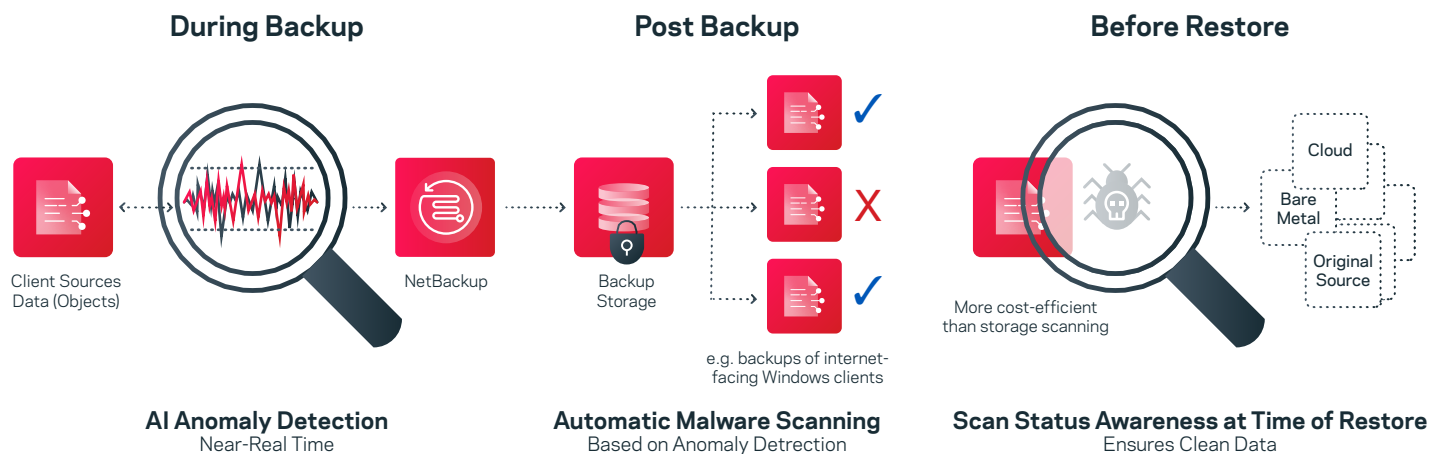


Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

Parallel Recovery support for DNAS Backup Sets

New recovery support introduced in NetBackup 10.2 provides for simultaneous recovery streams to significantly reduce the time required to complete a backup task. By coordinating backup activities in parallel, DNAS protection can multiply the throughput of the backup. This functionality accelerates recovery while maintaining recovery performance, ensuring that data remains available and secure.

Multi-Cloud Optimized with Veritas Alta Data Protection

Veritas Alta™ Data Protection is a component of NetBackup that provides broad coverage for a variety of cloud workloads. With NetBackup 10.1, support for PaaS workloads was greatly expanded, bringing full backup and recovery to nine new PaaS workloads across three cloud providers. Cloud workloads are highly flexible and fully supported by Veritas Alta Data Protection and NetBackup, empowering organizations to transport workloads from cloud providers into the 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.

NetBackup 10.2 further expands this functionality, providing customers with incremental backup support for PaaS workloads. This allows for the extraction of data from workloads referencing against the point in time of the previous full backup.

NetBackup 10.2 also delivers improvements to Oracle Instant Access, providing customers with the ability to use Multiple Universal Shares Protection to protect large Oracle databases across universal shares and MSDP storage pools of data that are larger than the capacity of one node in the MSDP cluster. This will, in turn, provide for the full backup support of large Oracle databases, overcoming any limits of NetBackup deduplicated storage, and improving the recovery time objective (RTO).

With automated and intelligent policies and elastic services, NetBackup brings enhanced protection and simplified operations to the broadest collection of workloads to date, including traditional, platform as a service (PaaS), software as a service (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.

- Incremental backup support for PaaS workloads
- Integration with cloud-based SIEM/SOAR for Azure Sentinel
- Oracle Instant Access using Multiple Universal Shares Protection
- Integrated SaaS application data protection
- Integrated multi-cloud analytics and insights
- Kubernetes multi-cloud recovery
- Enhanced cyber resiliency

Automated Operations

NetBackup powered by Cloud Scale Technology hosts a variety of capabilities that contribute to its ease of use and highly simplified and automated operation. Cloud Scale Technology is a new generation of the proven NetBackup architecture, modernized to operate at web-scale and provide a foundation for our vision to deliver autonomous data management.

Cloud Scale Technology 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
- NetBackup Elastic Cloud Dedupe Services

Agentless backup from snapshots provides efficient, cloud-optimized, application-consistent, multi-cloud data protection. NetBackup 10.2, powered by Cloud Scale Technology, expands this functionality in the following ways:



- New ability to configure NetBackup Snapshot Manager service in the NetBackup web user interface (UI) and manage Backup from Replica with the array's replication Data Mover to streamline replication
- New single file restore capability, allowing administrators to quickly recover individual files from backups without having to recover an entire snapshot, providing easier and faster granular recovery, and reducing snapshot/storage costs

NetBackup 10.2 also introduces automated recovery of PostgreSQL and MySQL databases. This additional support simplifies the management of databases and instances to PostgreSQL and MySQL when performing a recovery task by eliminating the manual lift of extracting, updating, and attaching associated databases.

NetBackup's Intelligent Cloud Policy Engine automatically discovers workloads and directs cloud-based snapshot protection in Azure and AWS.

Data optimization at the source and directly storing data in the most cost-effective cloud tier provide cost-effective, long-term retention in the cloud.

NetBackup's multi-tier replication, the ability to restore to anywhere—on-premises or in the cloud—and the application of NetBackup's full cyber resiliency capabilities ensure that data is always available and recoverable.

Veritas Alta SaaS Protection

Veritas Alta™ SaaS Protection (formerly known as NetBackup SaaS Protection) enables organizations to backup and recover software as a service (SaaS) application data from any of the major SaaS offerings. This includes Salesforce, Microsoft 365, Slack, Google Workspace, and Box—more applications than any other vendor.

Veritas Alta SaaS Protection provides customers with fully-managed, automated backups that run according to the policies they configure. Unlike other vendors' products, Veritas Alta SaaS Protection is built on a single-tenant architecture, giving each customer their own dedicated instance of the solution, ensuring that their data remains completely isolated, and that they receive their own dedicated set of cloud resources, enabling high performance. This, in turn, provides short recovery point objectives (RPOs), minimizing the amount of data that can be lost through deletion—accidental or malicious—or to a ransomware attack.

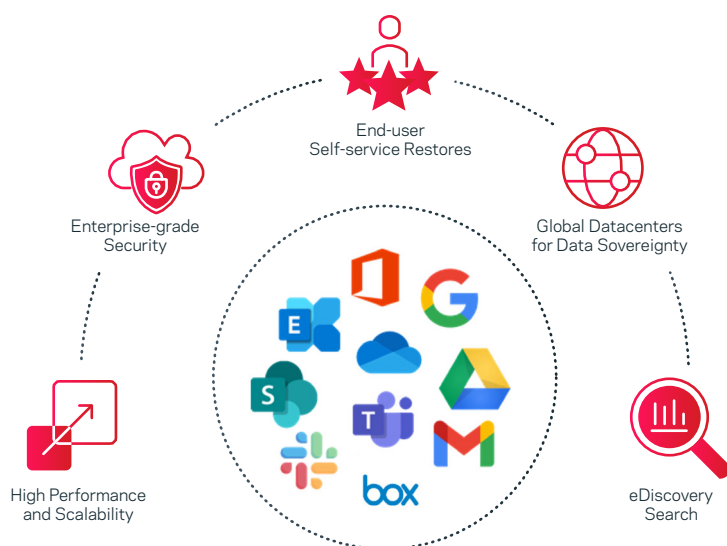


Figure 3. NetBackup protects data across a variety of SaaS applications and environments.

Veritas Alta SaaS Protection provides automatic compliance enforcement by allowing you to set policies for data retention and data location controls. Veritas Alta SaaS Protection offers flexible recovery options, from bulk to single-item restores. Veritas Alta SaaS Protection integrates with NetBackup, allowing customers to monitor the status of its backup jobs from the NetBackup web UI console.

Veritas Alta Recovery Vault

Veritas Alta™ Recovery Vault (formerly known as NetBackup Recovery Vault) is a cloud-based data retention service that provides a seamless, fully managed secondary storage option for NetBackup users (see Figure 4).

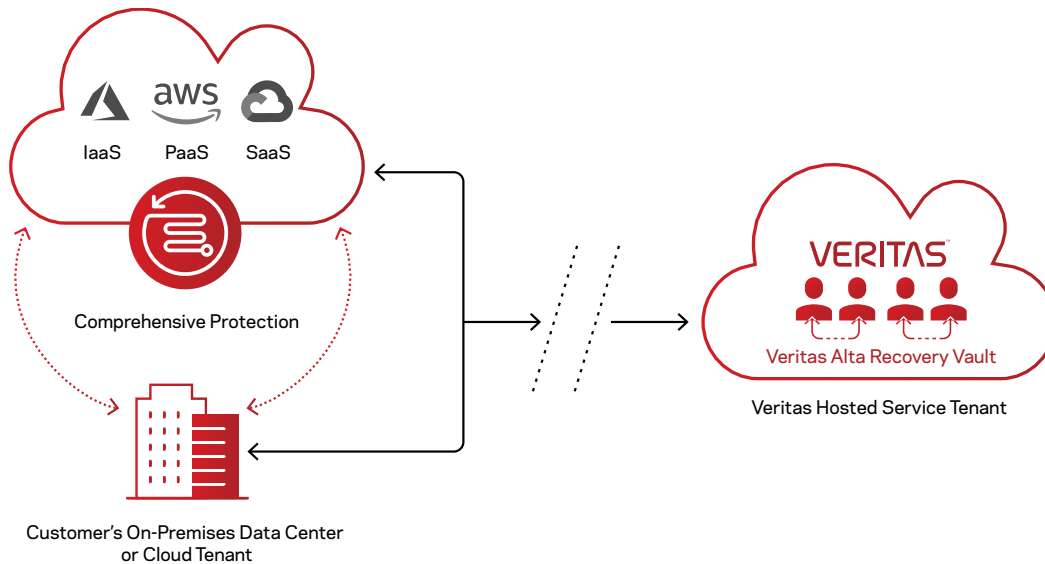


Figure 4. Veritas Alta Recovery Vault provides storage for data across on-premises and cloud

Veritas Alta Recovery Vault and the Intelligent Cloud Policy Engine ensure that no data gets left behind, and multi-cloud isolation provides complete protection from ransomware and other threats—all through a simplified process presented within the familiar NetBackupUI.

Anything that can be protected by NetBackup can be safely stored in Veritas Alta Recovery Vault. With Veritas Alta Recovery Vault, an organization can plan for disaster recovery, meet compliance and governance requirements, and prevent data loss from ransomware.

And with NetBackup 10.2, Veritas Alta Recovery Vault now offers a token-based authentication feature that maintains a cloud-based air gap in Microsoft Azure—ensuring that data is completely secure from external threats.

Integrated NetBackup IT Analytics Foundation

Integrated NetBackup IT Analytics Foundation, introduced in NetBackup 10, delivered capabilities to bring together cloud and information with insights on the data, and provide intelligence across hybrid and multi-cloud environments. NetBackup 10.1 built on these accomplishments using information to optimize performance and mitigate risk. By pinpointing operational inefficiencies, identifying threshold-based backup inconsistencies, and compiling a single-source report of information, NetBackup can easily identify necessary changes so you can take action (see Figure 5).

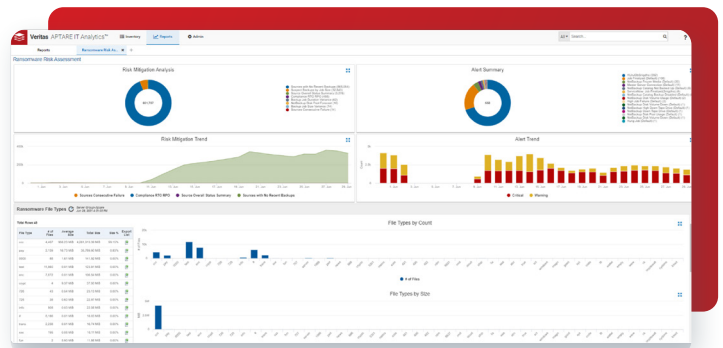


Figure 5. Example of NetBackup IT Analytics Foundation's single-source report bringing together cloud and information insights.

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. These Kubernetes capabilities are also fully integrated with all NetBackup ransomware resiliency functionality, ensuring data is always recoverable.

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 percent 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.

NetBackup 10.2 can support all Cloud Native Computing Foundation (CNCF)-certified Kubernetes distributions. It unifies backup for all Kubernetes environments, on-premises or in the cloud. It also allows for multi-cloud cross-distribution restores, significantly increasing disaster recovery (DR) capabilities. This data mobility provides Kubernetes users with the most efficient and comprehensive choices for backup and recovery, plus the freedom to choose and change their Kubernetes environments as necessary.

Why Veritas?

Veritas is trusted today to provide enterprise data management to organizations of all sizes, including 95 percent of Fortune 100 companies. Veritas NetBackup powered by Cloud Scale Technology provides cost-effective and secure sustainability to your enterprise's cloud experience. It uniquely integrates SaaS, analytics, and automated on-demand services, protecting data while improving operational agility and control across any cloud. Organizations today need to manage data as a critical asset, and ensure rapid recovery of critical data during catastrophic events such as lost files, security attacks, or unexpected business disruptions.

In today's data-intensive world, every enterprise faces the same issues and challenges with data protection and management. As the #1 vendor in data protection 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.

For more information, visit veritas.com/netbackup.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 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 Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

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

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