Veritas NetBackup 10.1.X

Delivering a more cost-effective, secure, and sustainable cloud.

Veritas NetBackup™ 10.1.X delivers the industry's most advanced cloud-optimized, at-scale data protection solution, offering protection and data management on-premises, in the cloud, and in cloud-native SaaS applications. With its latest release, NetBackup continues to radically simplify data protection, providing enhanced support for cloud workloads while delivering new resiliency features bolstering protection from edge to core to cloud.

Multi-Cloud Optimized

NetBackup 10.1.X delivers enhanced protection for more workloads than ever before, vastly expanding support for PaaS workloads, and bringing full backup and recovery to 9 new PaaS workloads across 3 cloud providers. Now cloud workloads are highly flexible and fully supported by 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.

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:

- Integrated SaaS application data protection
- Integrated multi-cloud analytics and insights
- Kubernetes multi-cloud recovery
- Subscription licensing
- Cloud scale technology
- Enhanced cyber-resiliency

NetBackup Integrated SaaS Application Data Protection

Cloud-native SaaS application data protection operations are now integrated within the NetBackup family. With Veritas Alta™ SaaS Protection (formerly known as NetBackup™ SaaS Protection) organizations can discover, monitor, protect, and secure data across all applications and environments from a single console, giving you a single view of your entire organization's data protection profile (see Figure 1). Veritas Alta SaaS Protection offers flexible restore options, including the original or alternate locations, in bulk, by object group, a single file, or a Teams chat. With Veritas Alta SaaS Protection you have greater agility, resiliency, and cloud portability.
Veritas Alta SaaS Protection also provides automatic data protection for SaaS workloads, including auto-discovery of new users, mailboxes, and folders without any administrator action. Only data changed since the last backup is copied in each new backup, optimizing both cloud bandwidth savings and reducing backup windows.

**Cyber-Resiliency**

More than 96% 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 all increasing exponentially. Nothing threatens the data and livelihood of businesses around the world more than ransomware. Securing your environment and your data as well as ensuring you can recover are key requirements of any enterprise data protection solution.

Veritas 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 against malicious data-damaging threats—and confidently defends against ransomware—for the multi- and hybrid cloud using a three-step approach (see Figure 2):

1. **Protect** — Safeguarding data integrity with system hardening and immutability
2. **Detect** — Monitoring and reporting on system activity to mitigate threats and vulnerabilities
3. **Recover** — Automating and orchestrating complete cross-system restoration and non-disruptive rehearsals

**NetBackup 10.1.X enhancements for security, ransomware, and resiliency include:**

- Expanded AI-driven anomaly detection, automated malware scanning, and clean recovery
- Support for isolated recovery environments (IRE)
- FIPS/STIG-compliant containers for Flex and Flex Scale appliances (NetBackup 10.1.1 and higher)
- Certificate portability with expiration alerts (NetBackup 10.1.1 and higher)

**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. NetBackup 10.1.X expands integrated malware scanning for unstructured data and VMware workloads, ensuring that the entire environment is protected.
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 3).

A comprehensive plan and tools like those in NetBackup 10.1.X combined with immutable storage provided by the NetBackup Appliances family and NetBackup Object Lock for public clouds along with ransomware recovery rehearsals are all necessary components to provide cyber-resiliency and peace of mind about the security of your enterprise data.

**New Enhancements to Multi-Cloud Cyber-Resiliency**

New Isolated recovery environment capabilities enable organizations to vastly enhance the resiliency strategy without introducing added complexity. NetBackup 10.1.X eliminates the need for additional infrastructure when isolating and protecting data from threats. It also creates an isolation boundary around your existing firewall. And by using the pull method strictly, NetBackup further supports data movement while isolating the stored data from any potential threats. By doing so, NetBackup removes the risk of introducing malicious activity from production to the isolated recovery environment.

![Figure 3. An overview of NetBackup's anomaly detection and malware scanning capabilities.](image-url)

- **During Backup**
  - AI Anomaly Detection
  - Automatic Malware Scanning
  - NetBackup Storage

- **Post Backup**
  - e.g. backups of internet-facing Windows clients
  - Scan Status Awareness at Time of Restore
  - Ensures Clean Data

- **Before Restore**
  - More cost-efficient than storage scanning

- **Figure 3. An overview of NetBackup's anomaly detection and malware scanning capabilities.**

A comprehensive plan and tools like those in NetBackup 10.1.X combined with immutable storage provided by the NetBackup Appliances family and NetBackup Object Lock for public clouds along with ransomware recovery rehearsals are all necessary components to provide cyber-resiliency and peace of mind about the security of your enterprise data.

**New Enhancements to Multi-Cloud Cyber-Resiliency**

New Isolated recovery environment capabilities enable organizations to vastly enhance the resiliency strategy without introducing added complexity. NetBackup 10.1.X eliminates the need for additional infrastructure when isolating and protecting data from threats. It also creates an isolation boundary around your existing firewall. And by using the pull method strictly, NetBackup further supports data movement while isolating the stored data from any potential threats. By doing so, NetBackup removes the risk of introducing malicious activity from production to the isolated recovery environment.

- **Real-time Anomaly Detection and On-Demand Malware Scan**
  - Flexible Recovery to cloud/data center
  - WORM storage and NetBackup instances on FLEX Appliance

- **OPTIONAL - Data Isolation using an operable air gap**
  - Data Integrity with multi-tenant WORM storage

- **Recover at scale to "Last Known Good State"**
  - Encrypted WORM storage

- **Any NetBackup Server**
  - Customer Firewall
  - Air Gap
In addition, NetBackup 10.1.X delivers immutability options – providing the flexibility to move the isolated recovery environment freely. Now the choice can be made between continuing to use the Flex appliance or implementing another while ensuring data remains immutable and indelible in an environment that is isolated and unreachable, built on a platform featuring encryption and aligned to STIG.

Today, protecting SaaS application data from malware is a critical priority for all businesses. Integration with Veritas Alta SaaS Protection provides comprehensive protection, governance, and resilience of your business-critical data across multiple SaaS applications. Moreover, it now offers an air-gapped, immutable copy of your SaaS application data on-premises. Stored in the NetBackup Access LTR Appliance, an on-premises, air-gapped copy of data from Google Workspace, Microsoft 365, and many other SaaS applications provides another layer of ransomware resiliency, enabling fast restoration, and helps meet critical governance compliance requirements that were previously unobtainable.

**New Protection for SAP Workloads**

NetBackup is now a SAP-certified data management integration with SAP HANA. SAP HANA certification enables customers to deploy NetBackup with the confidence of certified compatibility for SAP and NetBackup, assuring that even the largest of your SAP databases are protected and recoverable. For more information, please visit: [https://www.sap.com/dmc/exp/2013_09_adpd/enEN/#/solutions?id=s:474019e7-51b3-4190-9906-b7e1735b2dc5](https://www.sap.com/dmc/exp/2013_09_adpd/enEN/#/solutions?id=s:474019e7-51b3-4190-9906-b7e1735b2dc5).

**Protect Your Cloud Data with Confidence**

Veritas Alta™ Data Protection for NetBackup Cloud Workloads enables NetBackup, powered by Cloud Scale Technology to protect workloads across 60+ different cloud environments. Veritas Alta Data Protection offers flexible disaster recovery options, elastic infrastructure for reduced cloud costs and carbon footprint, native container protection and recovery, advanced storage technologies, and AI-powered automated ransomware protection to deliver the industry's broadest protection for cloud workloads at unlimited scale.

**Integrated NetBackup IT Analytics Foundation**

Integrated NetBackup IT Analytics Foundation introduced in NetBackup 10, delivered capabilities bringing together cloud and information with insights on the data, and providing intelligence across hybrid and multi-cloud environments. NetBackup 10.1.X builds 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 easily identifies 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.

**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. And 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. And 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, and image duplication for the tiering of backup storage (service lifecycle policies, "SLP") and A IR 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.

Over 50 percent of customers running 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 unifies backup for all Kubernetes environments, either 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.

**Cloud Scale Technology**

Ninety percent of enterprises expect cloud usage to exceed their prior plans. As cloud adoption increases, however, so do cloud expenses. Enterprises are often surprised by cloud costs. Fighting wasteful spending on cloud resources and optimizing cloud costs are top priorities. Veritas Alta Data Protection for NetBackup Cloud Workloads provides efficient data management and use of resources, helping executives meet their priority of efficient cloud spending.

Veritas’ cloud scale technology delivers enhanced protection and simplified operations across expanded workloads, including Kubernetes and SaaS-based applications. It provides secure, resilient, automated, and orchestrated delivery of event-driven workload protection, resulting in a more cost-effective, secure, and sustainable cloud with:

- Elastic Backup and Recovery Services for Amazon Web Services (AWS) and Azure
- Enhanced Elastic Cloud Autoscaling for AWS and Azure
- Elastic Cloud Dedupe Services


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 restores to anywhere—on-premises or in the cloud—and the application of NetBackup’s full cyber-resiliency capabilities ensure the data is always available and recoverable.

**New Elastic Backup and Recovery Services for AWS and Azure**

NetBackup’s backup from snapshot capability allows organizations running their workloads on AWS and Azure to lower their storage costs by either moving their snapshot data to lower-cost storage tiers in the cloud, to Veritas’s own storage-as-a-service offering—Veritas Alta™ Recovery Vault (formerly known as NetBackup™ Recovery Vault)—or to their own storage on-premises. When used with Intelligent Cloud Policy Engine, this entire process can be automated based on criteria that is pre-defined by the backup administrator. And for archiving to the cloud, Veritas Alta Recovery Vault now offers a cloud archive storage tier at a much lower cost—delivering the flexibility to choose the recovery time and cost structure that best fits the organizational needs.
Enhancements to Elastic Cloud Autoscaling for AWS and Azure

Cloud costs should be proportionate to cloud adoption. Yet as more workloads are moved to the cloud, companies are overspending by 20–50 percent on the cloud. NetBackup provides significant capabilities to help reduce cloud costs by only using cloud compute resources when required. Event-driven, Elastic Cloud Autoscaling for Azure and AWS automatically deploys and removes cloud instances as needed, providing the optimum cloud resources required by the business, at the right time. With Elastic Cloud Autoscaling for AWS and Azure, cloud compute resources are only in use as they are needed.

New NetBackup Elastic Cloud Dedupe Services

In addition to optimized, application-consistent backups from snapshots in multi-cloud environments, NetBackup Elastic Cloud Deduplication Services reduce the overall cost of long-term cloud data retention by 95 percent. The Cloud Dedupe Engine in NetBackup 10.1.X is a simple, containerized deployment that eliminates the need for static instances, lowering the cost of cloud compute instances while processing more data.

Why Veritas?

Veritas is trusted today to provide enterprise data management to organizations of all sizes, including 87 percent of Global Fortune 500 companies. Veritas NetBackup powered by Cloud Scale Technology provides cost-effective and secure sustainability to your enterprise’s cloud experience. It uniquely integrates SaaS and Analytics and automated on-demand services, protecting data while improving operational agility and control across any cloud. A software-based, vendor-agnostic platform, it uniquely focuses on the value of information rather than the underlying environment. 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 is facing 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 www.veritas.com/netbackup.