Veritas NetBackup 10.3

Advanced data protection with integrated cyber resiliency.

Veritas NetBackup 10.3 builds on the existing foundations of NetBackup's secure by default architecture. The latest version expands intelligent, automated threat-detection support and integrates resiliency in recovery operations. The updates minimize attack surface and provide the most powerful and secure architecture to date. NetBackup continues to radically simplify data protection with the benefit of new resiliency features, advanced automation, and expanded workload support, all strengthening 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, amount of 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 resiliency strategy reinforces your data and infrastructure defense against malicious data-damaging threats. Use it to confidently defend against ransomware for multi- and hybrid cloud using a three-step approach (Figure 1):

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

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

Step 3—Recover: Automate and orchestrate complete cross-system restoration with clean copies and non-disruptive

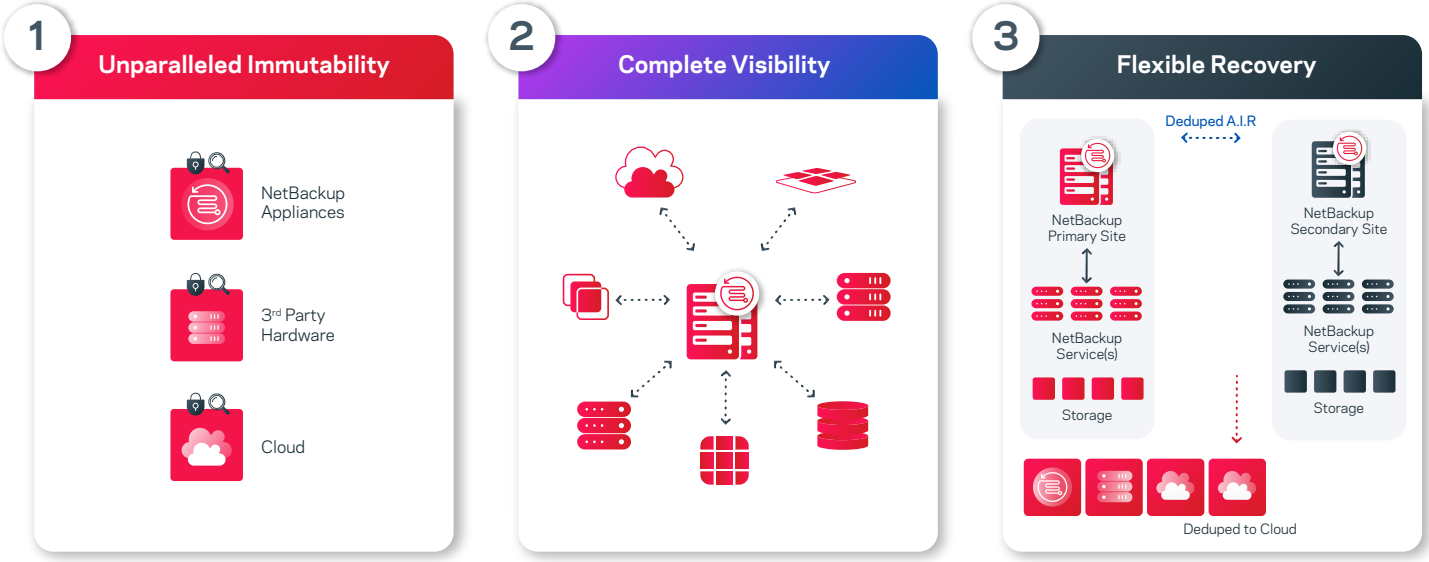

Figure 1. The three steps NetBackup takes to ensure cyber-resiliency

Enhancements for security, ransomware, and resiliency in Release 10.3 include:

- Multifactor authentication across all product interfaces, including GUI, CLI, and SSH
- Multi-person authorization for critical operations to prevent unauthorized data deletions and other malicious actions, along with a new internal tracking and ticketing system
- ML-based anomaly detection enhancements, which add user-behavior analysis and image-level entropy
- Integrated inline malware scanning during a restore including configurable options for handling of infected files
- FIPS compliance for Kubernetes workloads

AI-driven Anomaly Detection and Automated Malware Scanning

NetBackup augments its AI-driven anomaly detection capabilities with automated malware scanning. It checks for anomalies in near-real time during backup operations. If it suspects anomalies, it automatically initiates malware scanning of backups. In the case of a positive malware scan, it can automatically pause data protection, replication, and expiry of infected targets to contain the spread and prevent expiration of uninfected backups.

Release 10.3 leverages ML to further extend anomaly detection and audit trails to identify system-level or user behavior anomalies. It also adds the ability to analyze image-level entropy to aid the selection of recovery points using Veritas Alta™ View.

NetBackup 10.3 also uses malware scanning to identify the last-known good backup before restoring. Now early warning systems such as SIEM platforms can easily ingest anomaly and malware scan alerts stored within system logs. 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 enhancements allow NetBackup to pause data-protection activities including backups, duplication, and expiration automatically 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 these activities based on security or maintenance events.

Fast recovery of critical business operations relies on the ability to identify and recover the most recent malware-free backup. When recovering, it is also imperative to ensure any infected files are omitted. Excluding these files prevents the possibility of reinfection, enables recovery of the most current backups, and gets your business back to the closest point prior to the attack (Figure 2).

NetBackup 10.3 extends integrated malware scanning support with the ability to use inline malware scanning during recovery. This ensures a clean, automated recovery without additional steps from the user. And malware scanning support now includes cloud VMs and Universal Shares.

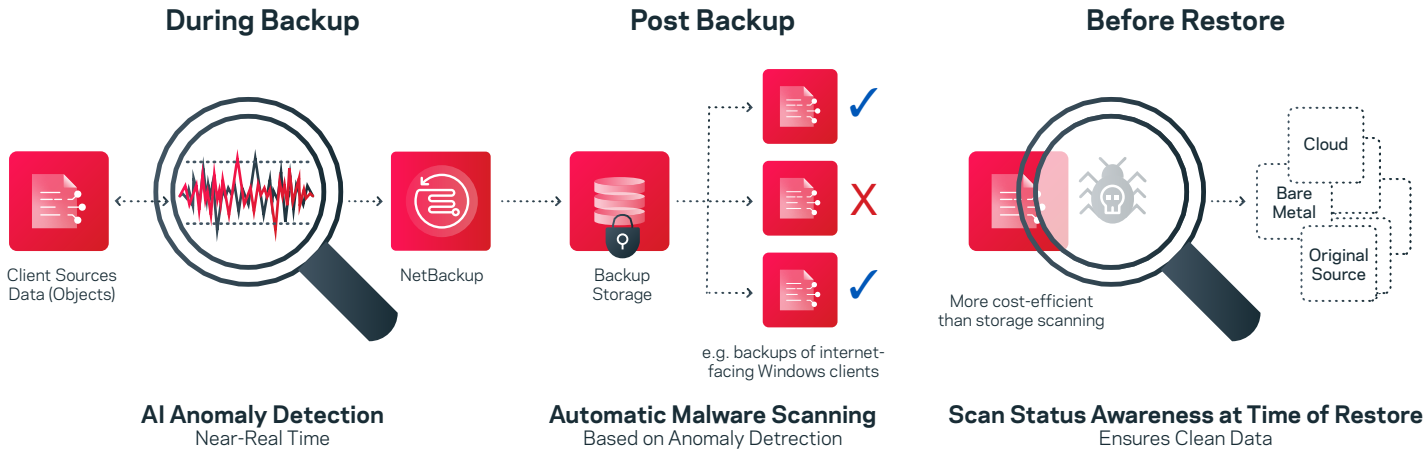

Figure 2. An overview of NetBackup's anomaly detection and malware scanning capabilities.

Multi-Cloud Optimized with Veritas Alta Data Protection

Veritas Alta™ Data Protection is the NetBackup component that provides coverage for cloud workloads. NetBackup 10.1 and 10.2 greatly expanded support for platform-as-a-service (PaaS) workloads, adding protection for 15 new workloads across three cloud providers. Veritas Alta Data Protection fully supports highly flexible cloud workloads, empowering you to transport workloads from providers into the MSDP storage pools, optimizing and deduplicating data, and using efficient object storage to simplify recovery. Cloud data is now available directly from backup storage so users can view compressed, encrypted, and deduplicated data.

NetBackup 10.3 further expands functionality with support for more PaaS workloads, including:

- AWS Amazon Relational Database Service — Oracle
- Google Cloud Platform Cloud SQL for SQL Server
- Microsoft Azure Cosmos DB – Mongo and SQL API
- Microsoft Azure Data Lake

This brings the total to 20, with more to come in future updates. Incremental backup support is available for Azure SQL and Azure SQL MI, protecting Azure SQL workloads with minimal overhead, compute, and storage requirements.

Veritas Alta Data Protection is powered by Cloud Scale Technology, which delivers enhanced protection and simplified operations across expanded workloads, including Kubernetes and software-as-a-service–based (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 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 enhances protection and simplifies operations for 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. Reduce data-protection gaps by minimizing human error and time-consuming administrative tasks with new capabilities, including:

- Integration with cloud-based SIEM/SOAR for Azure Sentinel
- Integrated SaaS application data protection
- Integrated multi-cloud analytics and insights
- Kubernetes multi-cloud recovery
- Enhanced media server elasticity and intelligence
- Expanded Amazon S3 immutability support

NetBackup 10.3 also introduces 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 10.3 expands support to include the market's widest range of certified S3 and integrated object-level lock targets, providing full deduplication and optimization from any workload to any target (Figure 3).

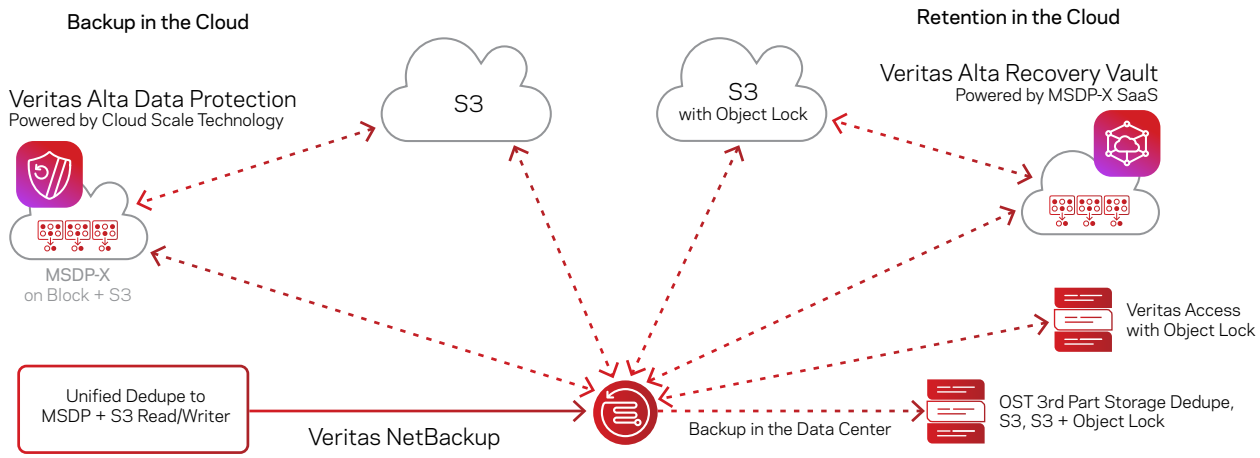

Figure 3. Overview of Veritas NetBackup cloud workload support

Veritas Alta SaaS Protection

Veritas Alta SaaS Protection enables you to back up and recover SaaS application data from any major SaaS offering. This includes Box, Google Workspace, Microsoft 365, Salesforce, and Slack—more than any other vendor (Figure 4).

Veritas Alta SaaS Protection provides fully managed, automated backups that run according to the policies you configure. Unlike other vendors' products, its built on a single-tenant architecture, giving your organization its own dedicated instance. Your data remains completely isolated, and you receive a dedicated set of cloud resources, ensuring high performance. This provides short recovery point objectives (RPOs), minimizing the data that can be lost through deletion—accidental or malicious—or to a ransomware attack.

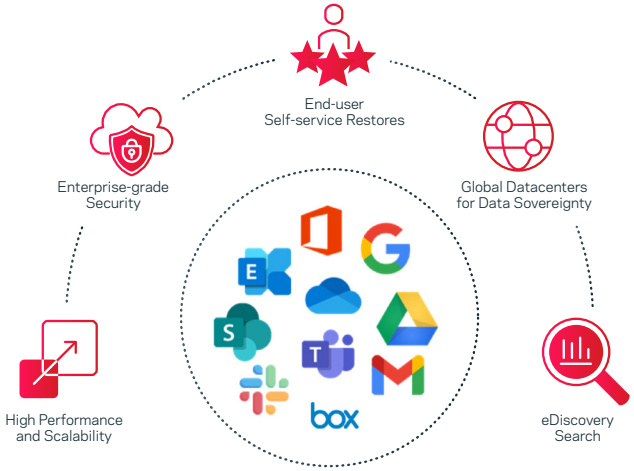

Figure 4. NetBackup protects data across a variety of SaaS applications and environments.

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

Veritas Alta Recovery Vault

Veritas Alta Recovery Vault is a cloud-based data-retention service that provides a seamless, fully managed secondary storage option for NetBackup users (Figure 5).

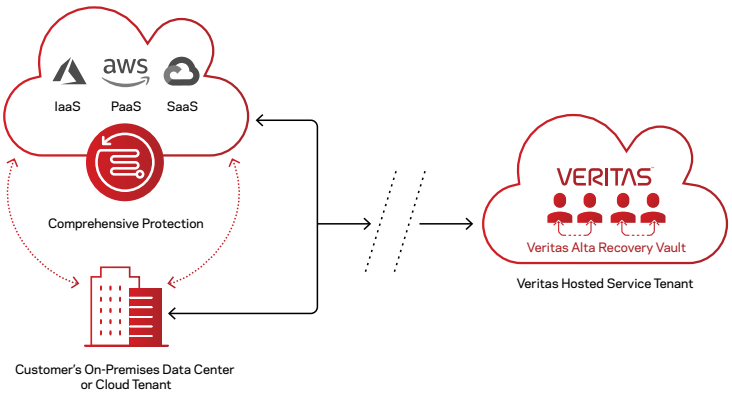

Figure 5. Veritas Alta Recovery Vault provides storage for data across on-premises and cloud

Veritas Alta Recovery Vault and the Intelligent Cloud Policy Engine ensure that no data is left behind. Multi-cloud isolation provides complete protection from ransomware and other threats. All this is accomplished through a simplified process within the familiar NetBackup UI.

Use Veritas Alta Recovery Vault to safely store anything that you protect with NetBackup or Veritas Alta Data Protection. With Veritas Alta Recovery Vault, you can plan for disaster recovery, meet compliance and governance requirements, and prevent data loss from ransomware.

Veritas Alta Recovery Vault also offers a token-based authentication feature that maintains a cloud-based air gap in Azure or AWS to ensure complete security of your data from external threats.

Integrated NetBackup IT Analytics Foundation

Introduced in NetBackup 10, the Integrated NetBackup IT Analytics Foundation delivers capabilities to connect cloud and information for data insights and provide intelligence across hybrid and multi-cloud environments. NetBackup 10.1 added the ability to use information to optimize performance and mitigate risk. By pinpointing operational inefficiencies, identifying threshold-based backup inconsistencies, and compiling a single-source report, NetBackup can easily identify necessary changes to make (Figure 6).

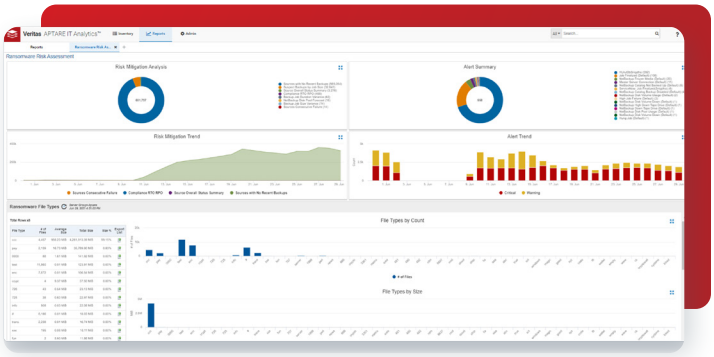

Figure 6. Example of NetBackup IT Analytics Foundation's single-source report bringing together cloud and information insights

Using these analytics reduces overall cloud costs through rightsizing and optimizing cloud infrastructure. Unifying insights from multiple cloud service providers helps you identify exact costs and consolidate public-cloud expenditures for further analysis and action.

Kubernetes Multi-Cloud, Multi-Distribution Recovery

NetBackup provides the industry's broadest support for Kubernetes with the consistency and portability you need to protect any Kubernetes distribution, on-premises or in the cloud. Veritas designed NetBackup for Kubernetes to offer operational simplicity and enterprise-grade resiliency with choice and flexibility for workload protection.

Back up Kubernetes workloads to any available storage target in the NetBackup web UI. For cloud, Kubernetes data protection operations are effectively managed with NetBackup's elastic cloud autoscaling, dynamically provisioning and removing cloud instances as needed to maximize cost and efficiency. In addition, it includes built-in features for:

- Instant rollback from snapshots
- Application-consistent Kubernetes cluster backup
- Deduplication
- Image duplication for tiering backup storage service lifecycle policies (SLPs)
- Auto image replication (AIR)

NetBackup 10.3 extends CSI-based snapshot support for block-based and file-based storage in the same namespace. This allows for parallel stream recovery and up to a 218% performance gain in restore speeds. These Kubernetes capabilities are fully integrated with all NetBackup ransomware resiliency functionality to ensure 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, plus use customer-defined parameters to add namespaces to the protection plan. This ensures automatic protection, reduces risk of data loss, and gives you much greater control in defining how you protect your applications, providing the ability to easily include and exclude specific resources.

More than 50% of organizations using Kubernetes run more than one distribution. Portability is one of the biggest drivers of Kubernetes adoption, specifically the ability to move between on-premises and different clouds. NetBackup provides the freedom to run as many distributions of Kubernetes as you need, 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. The solution uniquely integrates SaaS, analytics, and automated on-demand services, protecting data while improving operational agility and control across any cloud.

Today's environments require you to manage data as a key asset and ensure rapid recovery of critical data during catastrophic events such as lost files, security attacks, or unexpected business disruptions.

Learn more about **NetBackup** and **Alta Data Protection**.

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 Twitter 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

V1512 10/23