VERITAS

Top Reasons Veritas NetBackup 10.1 Beats the Competition

Key Vendor Considerations

Industry Leadership

Veritas is a consistent leader, recognized by numerous industry analysts for successfully enabling robust data protection solutions for enterprises worldwide. These solutions provide a vast array of ransomware cyber resiliency offerings, compliance, lower TCO, multi-cloud, Kubernetes, and support across a comprehensive workload matrix.

> *Virtualization is a way of life in our business. We're excited about introducing virtualized servers, and there's no doubt the complete, easy-to-use NetBackup virtualization functionality will have a major role to play here."*
>
> Ziv Oren, Vice President Technologies
> 888 Holdings

A testament to our continued leadership is industry analyst recognition. In 2022, Gartner named Veritas as a leader in its Magic Quadrant for Enterprise Backup and Recovery Software Solutions for the seventeenth year. This leadership continues with NetBackup 10.1, delivering the industry's first cloud-optimized, at-scale data protection solution that protects and manages data on premises, in and across multiple cloud offerings, and in cloud-native software as a service (SaaS) applications. NetBackup protects more than 100 EB of critical data within 80,000 global enterprises from 87 percent of the Fortune 500. With more than 2,200 patents, Veritas is a true innovator in the data protection space. In the words of one of our large financial banking customers, "Veritas is the trusted partner as a gold standard for data protection."

Unlike many vendor solutions, NetBackup™ 10.1 is available in multiple deployment models: cloud, build your own (BYO), scale-up appliance, scale-out appliance, virtual appliance, native Kubernetes, and multi-tenant. This gives enterprise customers and service providers maximum choice and flexibility as their needs evolve.

Comprehensive Data Management

Veritas Alta™ combines all Veritas cloud services and solutions, creating the most comprehensive cloud data management platform built for any environment—allowing enterprises to deliver their part of the shared responsibility model and beyond. Veritas Alta helps elevate business to new heights by enabling business agility and reducing costs, while ensuring data and applications are protected, highly available, and compliant.

Multi-Cloud Optimization

NetBackup 10.1 with Cloud Scale Architecture is a cloud-optimized solution that expands data management insights and intelligence operations in cloud and multi-cloud environments. This consists of delivering containerized, composable micro services; and integrated SaaS protection with valuable analytics and insights. This is accomplished with automated policies and provisioning with elastic dynamically-allocated services for integrated multi-cloud solutions. This includes traditional platform as a service (PaaS), SaaS, and containerized applications. Unlike some vendor solutions, NetBackup 10.1 Recovery Vault offers a single, flexible repository for comprehensive and simple backup and recovery, with enhanced elastic cloud autoscaling for AWS and Azure cloud platforms—without compromising security or compliance.

Comprehensive Cyber Defense

By design, NetBackup 10.1 delivers a zero trust ransomware resiliency model across the entire infrastructure, from edge to core to cloud and multi-cloud. This provides active cyber defenses, allowing quick data recovery without incurring a ransom. Active cyber defenses encompass three main functions:

1. Data protection with multi-cloud and data center immutability
2. AI scanning for anomaly and malware detection
3. Recover quickly with an air-gapped immutable disaster recovery (DR) copy from an on-premises or cloud instance

Environmental Sustainability

Sustainability is essential to our mission, technologies, and community. Veritas promotes corporate sustainability for internal operations, partners, and our supply chain. Combined with Cloud Scale Technology, elastic backup from snapshots, and a superior deduplication engine, NetBackup 10.1 can reduce the storage footprint by up to 98 percent. Based on one petabyte of unoptimized data in the cloud, Veritas was able to reduce CO2 emissions from 3.5 to .08 metric tons, for a 98 percent reduction in carbon footprint. Unlike some vendor solutions, Cloud Scale Technology avoids launching temporary instances for various backup and recovery operations, to further reduce energy use. On-premises appliances can match or exceed performance using much less power and cooling than most vendors—sometimes up to 50 percent less.

Top Reasons NetBackup 10.1 Beats the Competition

1. Unified Cloud Data Management

Veritas Alta™ offers a comprehensive platform of essential cloud data services in a single, powerful platform for maximum enterprise usability. Veritas Alta™ delivers on 3 main pillars of data management: Data protection, application resiliency, and data compliance & governance. NetBackup Cloud Scale enables the data protection pillar.

The data protection combines automation, artificial intelligence, and an elastic architecture to deliver the most secure, autonomous, and cost-effective cloud data protection available. Enterprises can protect and control their data across any environment, on premise, in the cloud, and across multiple clouds, all through a single pane of glass. Other vendors do provide some level of capability in this area but cannot match the data protection capabilities of NetBackup and Veritas Alta™, especially in the areas of data availability and data observability & accountability.

Veritas Alta™ minimizes risk by offering all advanced features with zero lock in for critical resources, such as compute/ infrastructure, storage, operating systems, and platforms. Other vendors cannot the same level of freedom and flexibility and can result fewer supplier options for customers.

2. Multi-Cloud and Kubernetes (K8)

NetBackup 10.1 provides multiple competitive advantages for comprehensive data protection and critical application disaster recovery orchestration, covering all tiers of businesses across the hybrid cloud, cloud, and multiple clouds.

- Provides an application-centric native Kubernetes solution that discovers, protects, and recovers all application components.
- Maintains Certified Kubernetes Conformance. NetBackup is certified by the Cloud Native Computing Foundation (CNCF) to support any CNCF distribution for Container Storage Interface (CSI) storage supporting snapshot and block-based backup from snapshots. This provides a mature multi-distribution support platform (including AWS and Azure) with optimized backup replication across multiple Kubernetes distributions (Red Hat OpenShift, Google Kubernetes Engine, VMware Tanzu, AWS, Azure) on-premises and in the cloud. All workloads are quickly recoverable and always compliant.

- Offers an analyst-acclaimed cloud-native architecture with multi-cloud consistency.
- Delivers cost-optimized easy-to-use data protection for cloud-native workloads.
- Expanded orchestrated multi-cloud recovery capabilities offering extensive cloud mobility. This consists of numerous source and target data replication scenarios:
    1. Hybrid cloud, including physical, VMware, and Hyper-V to AWS; Azure; and Google Cloud Platform (GCP), including AWS/Azure and Gov Cloud
    2. Cross-platform portability for VMware/Hyper-V, object storage, and Kubernetes
    3. Third-party, including Oracle Data Guard; storage array replication for VMware
- Cloud and on-premises object storage protection with cross-cloud portability.
- Provides built-in DR with NetBackup Resiliency Platform, including fully cloud-native Kubernetes (components deployed as Kubernetes containers) support with multi-distribution mobility, auto-scaling, and flexibility to roll back instantly from local snapshot and/or perform a recovery from backup. Users can recover or migrate data across multiple clouds and different Kubernetes distributions, with an on-premises recovery option.
- Kubernetes native and DEVSECOPS friendly. Unlike some vendors, NetBackup protection for Kubernetes is not charged separately and is not a bolt-on solution. This capability offers unmatched extensive portability and flexibility in transitioning from physical to virtual, for cloud and multi-cloud deployments.

NetBackup 10.1 offers major flexibility and efficiencies that other vendor solutions can't match. Some vendors have limited physical to virtual to cloud portability, while others rely on proxies and access nodes for cloud workloads, thus increasing overhead through a larger backup footprint and increased storage costs. Additionally, some vendors have limited capability for AWS S3 and OpenStack, and for customers requiring net-zero recovery point objective (RPO) DR access across the major cloud vendors such as AWS, Azure, and GCP. In some cases, fragmented cloud support requires specific products for each cloud instance. For example, an entirely separate product may be required for cloud backups in K8 environments, increasing cost and complexity. In addition, not all vendors can roll back from snapshots in K8 environments.

3. Cyber Resiliency

NetBackup 10.1 offers multiple unique cyber resiliency competitive advantages.

- Proven on-premises, cloud, and SaaS multi-petabyte scale with a continuous 4-year 100 percent ransomware recovery rate delivers better ransomware recovery reliability.
- Anomaly detection capabilities for primary data, backup, and infrastructure.
- Malware scans pause backups while preventing, containing, and isolating malware infected files.
- The isolated recovery environment (IRE) solution provides malware-free restores using a secure by default approach, where default configuration settings are the most secure possible. Existing and new Flex Appliances offer IRE with a pull model, which provides complete control on the target side for added security assurance with 24-hour replication support in heavily active environments.
- Veritas™ Alta Recovery Vault (formerly known as NetBackup Recovery Vault) offers immutability for all backup tiers, and is hosted on AWS and Azure cloud platforms.
- Coupled with NetBackup IT Analytics and NetBackup Resiliency Platform, offers a comprehensive, orchestrated, and resilient solution for multiple tiers of business service aligned with the NIST cyber security framework (protect, detect, recover).
- Protects backups of all workloads and limits the attack surface for added security. Data Insight helps mitigate exfiltration ransomware with a need-to-know basis for unstructured data access and real-time monitoring.
- Allows for the automation of rehearsals to non-disruptively simulate non-recovery procedures across entire data center(s), applications, or physical and virtual machines.

- Delivers a multi-layer security architecture that is built with security as its primary objective. Containerization provides service isolation, a hardened OS, and a zero trust security model, making NetBackup secure by default. NetBackup's resiliency and air gap approach is more economical and practical than solutions from other vendors that may have more complex deployment models, subsequently increasing costs as well as risk to recovery time objective (RTO) and RPO requirements.
- NetBackup Flex, Flex Scale, and Access Appliances create an integrated resilient solution for primary and long-term backups, which can be a convenient alternative to the traditional BYO approach. These solutions are aligned with zero trust principles and offer a layered security solution, including OS hardening, built-in ransomware prevention and detection, and indelible/immutable write once, read many (WORM) storage for edge and core deployments. NetBackup is also validated by Cohasset Associates. Here, the NetBackup integrated appliance choice helps customers align ransomware resiliency to fit the criticality of backups, rather than forcing a one-size-fits-all costly appliance solution.

Veritas offers a comprehensive, automated, orchestrated solution that is unmatched by the competition. Many vendors have released support for anomaly detection and malware scanning in isolation. NetBackup gives customers the rare ability to automatically trigger malware scans when anomalies are detected, which in turn pauses backup, replication, and expiration of backup images. Additionally, some vendors have third-party dependencies requiring dedicated windows servers, which increases management complexity, exposed attack surface, expanded blast radius, and detection time. Instant rollback and integrated malware scanning are limited, while there is a lack of automation when identifying and restoring the last known clean copy. Lack of built-in air gap operations decreases the ability for reliable restores, and some of these customers have had increased ransomware attacks where hackers exploited their exposed vulnerabilities. Additionally, some vendors increase attack surface by asking customers to deploy attack-prone operating systems based on third-party solutions for granular recovery and air-gapping. NetBackup provides zero trust ransomware resiliency without increasing attack surface, risk, complexity, cost, or using external or vulnerable retention clocks.

4. Cost and Total Cost of Ownership (TCO)

NetBackup 10.1 offers very competitive cost and TCO savings:

- Savings of 50 percent or more by implementing an all-in-one hyper-automated data protection solution, including DR, Continuous Data Protection, and IT Analytics included in a single license. Some vendors lack immutability for all workloads, or have a 100-day immutability period, which can manifest into a delayed ransomware attack for weeks or even months. Some vendors have openly documented how the immutability can be disabled. Ideally, once enabled initially, backups should stay immutable and indelible without exception.
- NetBackup integrated cloud dedupe engine reduces storage costs with built-in global deduplication for up to 95 percent reduction in long-term cloud data storage. NetBackup Elastic Cloud Autoscaling for AWS and Azure can reduce instance use by up to 40 percent.
- Multi-tier backup copies can provide reduced cloud costs through NetBackup storage lifecycle policies (SLPs).
- Snapshot deduplication can result in a 50–90 percent cost savings. For example, one PB of capacity in a cloud with a two-week snapshot retention replication to a second site resulted in a 90 percent savings on data transfer costs, 90 percent savings on storage deduped from a snapshot, 80 percent savings on server storage and networking resources, and 50 percent savings on licensing. Compared to the competition, a major retailer saved 36 percent in overall cloud costs with Veritas.
- NetBackup Resiliency Platform integrates with array and database technologies for DR, yielding potentially higher return on investment (ROI).
- Recent deduplication ratio enhancements and object-based deduplication pool data retirement show tremendous cost savings for short-term retention of primary backup images in the cloud.
- Offers direct-to-cloud deduplication for efficiency and cost savings.
- Autoscaling allows enterprises to improve cost management by implementing and paying only for resources that are being used.

- Front-end terabyte (FETB) licensing can be implemented for more accurate cost predictability, while back-end terabyte (BETB) licensing can be applied for cost savings that can be greater than 50 percent. This can be achieved by licensing capacity for data after it has been de-duplicated and compressed. Some vendors charge based on BETB licensing, which is more expensive. The subscription license model offers unmatched TCO, while proactively ensuring that the customer is always up to date with the latest release.

Competitive offerings are typically more complex, require additional access nodes and proxies, and cannot provide direct backups for all major cloud platforms. Additionally, some vendors heavily rely on third parties for deduplication, granular recovery, tape backup, and SaaS workload protection. This can significantly increase the overall TCO via required license, management, and hardware costs. NetBackup's single platform solution saved a large medical company 36 percent over another vendor. What is typically observed with almost all competitors is that their cloud storage requirement increases by as much as three times, just by enabling WORM or immutability locks. NetBackup's cloud storage capacity requirement is totally independent of immutability. Another observation of several competitors is their limitation to rely on block storage only for primary backup copies. Block storage, especially in the cloud, is much more expensive than object storage. NetBackup leverages object storage for maximum cost savings.

5. Compliance

NetBackup 10.1 delivers a proven competitive compliance solution:

- Supported customers with hundreds of thousands of virtual machines and multiple PBs of data—all of which are required to meet backup service level agreements, recovery point objectives, and recovery time objectives.
- A proven track record for many workloads, supporting immutability across all deployment options, including BYO, appliance, cloud, and multi-cloud object storage.
- Provides WORM support for primary and long-term backup appliances.
- Delivers FINRA (Sec-17a-4f), STIG, DISA, and FIPS 140-2 compliance
- Nondisruptive rehearsals further meet audit compliance and prove the value of the solution to the business, without impacting critical operations.

Many vendors cannot match this total infrastructure compliance capability. Additionally, not all vendors can match NetBackup's data immutability capability for data stored in Azure, NAS, and Oracle backups. There is also some inconsistency with multi-factor authentication (MFA) for restore consoles, command-line interface (CLI), or API. Some vendors rely on an external Network Time Protocol (NTP) clock, which increases vulnerability and risk for on-premises backups and potentially compromises required retention periods.

6. Simplicity

NetBackup 10.1 deployment simplicity can significantly contribute to competitively lower TCO:

- Can reduce administrative costs by 50 percent or more compared to offerings from other vendors. Agentless deployment and auto-discovery for key dynamic workloads result in less administration required to handle growing workloads.
- NetBackup Flex and Flex Scale are deployed as containerized architectures that easily scale up (Flex) and scale out (Flex Scale) in terms of performance and capacity as demands increase.
- TCO is reduced with optimized integration and complete lifecycle support.
- No dependencies on third-party management platforms such as SQL Server, Windows-only CDP access nodes, or third-party deduplication appliances.

- Provides fully native instant access for Oracle, SQL, NAS, and VMware; in BYO, appliances, on-premises, and in cloud deployments.
- Simplifies service level agreement (SLA) monitoring through full integration with Veritas™ Alta SaaS Protection (formerly known as NetBackup SaaS protection).
- Differentiated from other vendors with a complete and proven solution that scales to multiple petabytes across on-premises data center, cloud, and SaaS.
- Can save costs with smaller footprint appliances in two ways, versus competitive offerings:
    1. High density architecture can save up to five times on rack space, 22 times on power usage, and nine times on networking costs.
    2. Superior deduplication can save up to 90 percent on data center storage. A managed service provider (MSP) saved 44 percent over another vendor due to this superior scaling and density.

Customers can face complex deployment options with other vendor solutions, which also leads to risk and increased costs. These complex deployment options often involve third-party software and hardware integration. Simple tasks such as full virtual machine (VM) restores may also require additional access nodes. In some cases, significant space pre-allocation involving complex calculations is required. Other shortcomings include snapshot dependency for Oracle Instant clone and the requirement of dedicated proxies in the large environment for scale out appliance. NetBackup 10.1 has none of these limitations.

7. Environmental Sustainability

Veritas extends its environmental sustainability commitment throughout the entire organization. Autonomous data management technology in NetBackup 10.1 reduces cloud footprint, carbon emissions, and total cost. Other initiatives include:

- Twenty-seven percent reduction in greenhouse gas emissions from fiscal year (FY) 2020 to FY 2021 (ClimatePartner scope 1, 2, and 3) , driven by the procurement of Renewable Energy Certificates.
- Target goal of 25 percent reduction in greenhouse gas emissions by FY 2025 (from FY 2019 base year).
- The implementation of recycling servers and storage devices. In FY 2021, Veritas sent 57 tons of material to our vendor, which resold 61 percent of available material after processing.

NetBackup Flex Scale has been shown to reduce operational expenditures and carbon footprint by percent or more, versus other vendors.

8. Selecting the Best Data Protection Solution

Selecting the right data protection vendor for your unique needs is critical for organizational success. It's important, however, that customers know what key questions to ask before making any solution decision. Key questions that customers should ask all data protection vendors include:

- Which discreet components does your solution require in order to enable customers to operate and optimize data protection, at scale, across any environment, such as multi, hybrid, public, edge, private, and on-premises?
- How do your products scale as my data requirements grow in terms of required products, maintenance, support, and TCO?
- Describe your product's level of automation for maintaining simplicity, while balancing the RPO/RTO needs with the cost of storage on-premises and in the cloud. How can I take advantage of less expensive object storage in the cloud?
- How do you handle backup and restore of cloud object stores?
- Is your Kubernetes solution entirely Kubernetes-native? Are all CNCF-certified Kubernetes distributions supported?

- Describe how you ensure cyber resiliency through immutability, malware scanning, anomaly detection, and air gap capabilities at the core data center, edge, and cloud locations. Is your malware scanning done on isolated backup copies?
- Describe your automated recovery, non-disruptive recovery rehearsals, isolated recovery, and response to ransomware attacks.
- How long does it take for your solution to detect the attack and recover with the most recent clean copy of data?
- How does your licensing model help with financial planning, including planning for overall TCO? What third-party licenses or additional costs are required for a complete solution?
- What are your various deployment options?
- What is your environmental sustainability plan and how does your solution reduce scope 2 emissions?

Comparison Chart

Feature	Veritas	Traditional Data Protection Vendors	Cloud Vendors Backup Products
Comprehensive multi cloud support	Yes	Limited	No
Elastic backup and recovery for all major cloud platforms	Yes	Limited	No
Non-disruptive orchestrated recovery both on-premises and in cloud	Yes	Limited	No
Malware scanning on isolated backup copies, avoiding stress on primary backup infrastructure	Yes	No	No
Automatic pause and resume of backups when malware detected	Yes	No	No
Cloud and on-premises object storage protection with deduplication, immutability, and anomaly detection	Yes	No	No
Parallel streaming across and within buckets for faster cloud object storage protection	Yes	No	No
Instant access on object storage for cost savings	Yes	Limited	Limited
Kubernetes multi-cloud multi-distribution recovery	Yes	No	No
Multi-cloud resource auto-scaling	Yes	Limited	No
Immutable storage support for on-premises, cloud, and SasS, without cost overheads	Yes	Limited	No
Logical air gap support for on-prem, cloud, and SaaS	Yes	Limited	No

Pull-based iIsolated recovery environment (IRE) for BYO and appliances without additional software/hardware components	Yes	No	No
Near real-time initiative-taking anomaly detection across all data platforms	Yes	No	No
Application-aware adaptive deduplication for optimal cost savings at source and target	Yes	Limited	No
Up to eight flexible deployment options	Yes	Limited	No

Disclaimer Notice

Document content is subject to change based on rapidly changing industry developments. Consult the Competitive Marketing Team for any potential changes between content updates or other details. Please use this content at your discretion and preference.

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.

VERITAS

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

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

V1589 02/23