VERITAS

Building a Hybrid and Multi-Cloud Data Protection Solution

White Paper | October 2023

VERITAS ALTA™

Executive Summary

Data center architectures have evolved from traditional on-premises designs to a combination of on-premises and public cloud services. In fact, the 2022 Technology Spending Intentions report by ESG shows 94 percent of large enterprises adopting a multi-cloud strategy, and 23 percent of all applications and workloads will remain on-premises. Even organizations with a cloud-first strategy have data that must stay on-prem due to regulatory, security, or performance reasons. Organizations often use multiple cloud providers for additional resiliency and operational flexibility, making the new standard data center a hybrid and multi-cloud model.

Protecting data on-premises and in multiple clouds is very complex. Each cloud service provider and on-premises data protection platform has its own specific interface and operating procedures, none of which are compatible with each other. Although some on-premises data protection platforms connect to the cloud, and in some cases leverage cloud capabilities, they still must be managed to meet on-premises infrastructure requirements. What you are left with is silo sprawl—two or more sets of requirements for architecture, strategy, and operations—which increases costs, risk, and exposure to cyber threats including ransomware.

Cloud service providers also operate in a shared responsibility model, leaving data protection squarely as the customer's responsibility. As such, they offer only rudimentary tools for data protection that are:

- Proprietary and not compatible with other platforms
- Snapshot-based, which limits your recovery options
- Not typically suitable for application-aware data protection

Some key challenges facing organizations include:

- Training multiple administrators operating procedures for various cloud and on-premises data protection solutions
- Managing multiple support contracts and service organizations
- Acquiring and retaining the expertise needed to deliver a vendor-specific solution that is cost-efficient, secure, and resilient to ransomware
- Unexpected egress costs for routine backup operations

To easily manage a hybrid and multi-cloud solution, you need a comprehensive data protection solution that provides enterprise-level protection and operates the same way, regardless of where the data resides. This is where Veritas' hybrid and multi-cloud data protection can help eliminate risk and complexity. It is based on NetBackup, which is a proven data protection software solution used by 87 percent of Fortune Global 500 companies, and protects more than 100 exabytes of data globally.

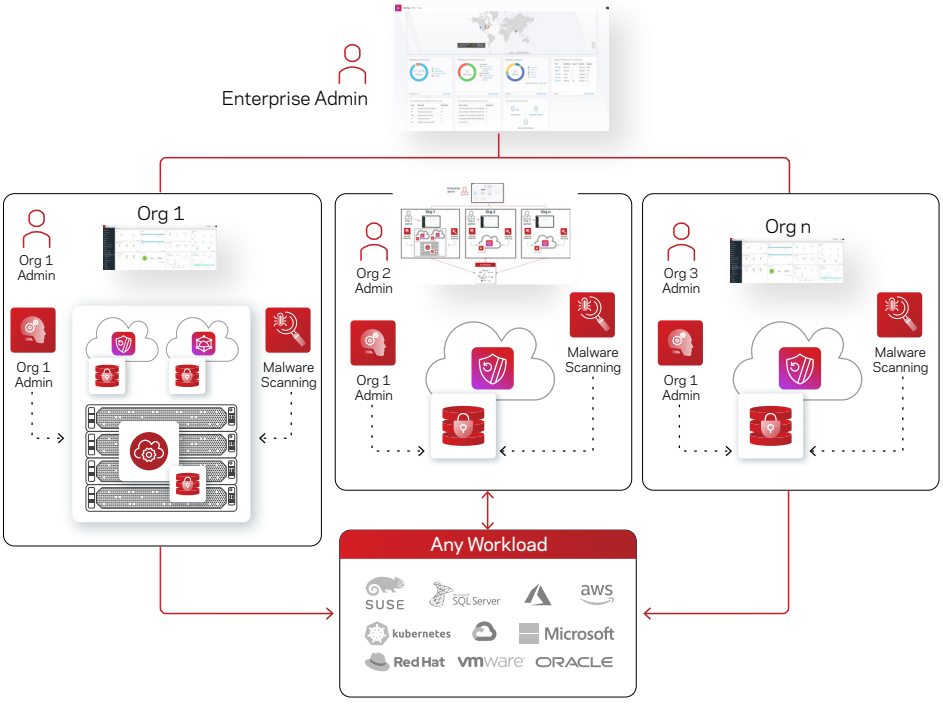


Figure 1. Veritas' hybrid and multi-cloud data protection solution

Veritas provides a single data protection solution powered by NetBackup that can manage your entire hybrid and multi-cloud data center footprint with the flexibility to run and store your backups in the public and private cloud. The Veritas hybrid and multi-cloud protection solution includes Veritas Alta™ Recovery Vault—a cloud-based storage-as-a-service offering that provides a fully managed secondary storage option for NetBackup users. Anything NetBackup can protect can be stored in Veritas Alta Recovery Vault, regardless of your data sources—on-premises and public cloud workloads. Seamless integration into NetBackup simplifies cloud storage, delivering limitless scale without compromising security or compliance policies.

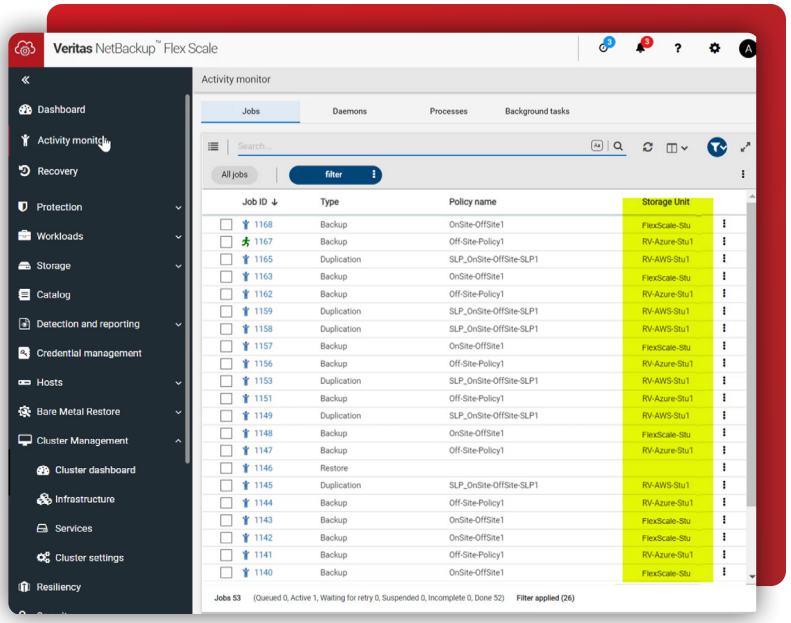


Figure 2. Single UI to manage you entire data protection landscape

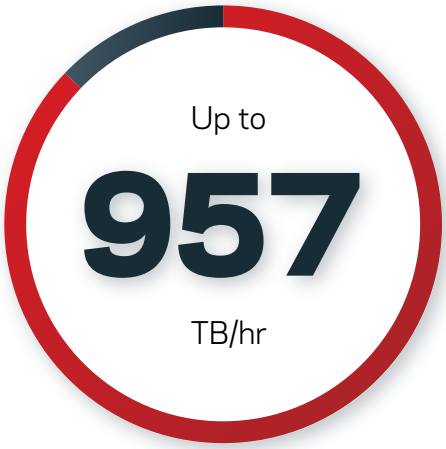
This hybrid and multi-cloud optimized solution provides a secure, cyber-resilient solution that is simple to manage with a single UI, all while reducing hidden costs and overall carbon footprint. This same UI provides clear visibility into where all your data copies are located at any point in time, so that you can protect and recover easily. It also gives you the flexibility to maintain the same data protection strategy, whether you shift your applications between storage tiers, cloud service providers, or repatriate them back to on-premises systems.

The Veritas hybrid and multi-cloud data protection solution is made up of:

- Veritas Alta™ Data Protection: NetBackup software with optimized cloud integrations and automated cloud recovery
- NetBackup Flex Scale: The fastest way to deliver ransomware resilient private cloud data protection
- Veritas Alta Recovery Vault: Cloud-based storage-as-a-service—the easiest way to add immutable public cloud-based storage to NetBackup using Microsoft Azure or AWS
- Veritas Alta™ View: A secure management console - delivered as a service- that aggregates data across your organizations into a single aggregated view providing enhanced visibility and control for all your Veritas-managed domains.

Lower Costs and Carbon Footprint

Cloud providers charge for what you use and do not offer any deduplication tools to reduce the amount of stored data. Snapshots are space efficient, but without deduplication, they are potentially a significant cost increase when using cloud provider backup tools. Frequent snapshots and the need for long-term data retention significantly reduces space efficiency and makes reconstructing the data time-consuming, requiring you to merge a long chain of snapshots taken over time. Plus, these costs are carried forward in all your copies if you are replicating data for site protection, additional recovery options, and ransomware immutability.



Since backups are highly redundant, the best way to lower costs is to use an advanced deduplication technology on your backup data. Veritas is a leader in advanced deduplication technology, with years of engineering and more than 80 patents specifically for data deduplication. Veritas technology enables deduplication and compression of backup data, with savings of up to 98 percent.

NetBackup lets you choose where to perform deduplication—on the NetBackup server to centralize data processing, or on the client to further decrease your network throughput and increase your backup performance. NetBackup Flex Scale has seen backup performance of up to 957 TB/hr with client-side deduplication.

NetBackup also provides direct and secure access to the deduplicated storage via Network File System (NFS) and Common Internet File System (CIFS) protocols using Universal Shares. Any new data stored in a universal share will gain the same deduplication savings as data previously ingested by NetBackup.

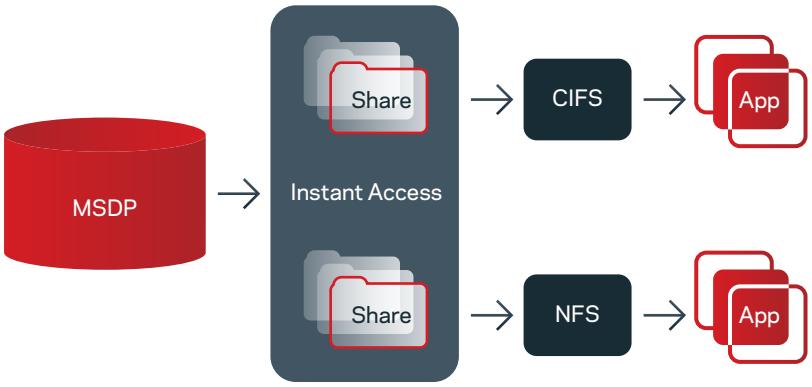


Figure 3. Gain instant access to your application data

NetBackup Flex Scale is optimized for the recovery speed and parallelism you need to get your business back up and running quickly in the event of an outage. It allows you to run multiple parallel recovery operations, and gives you instant access to your most critical data stored in virtual machines (VMs) and applications, such as Oracle and MSSQL. It works by presenting a read-only copy of the backup image that can be mounted for immediate access to the data, without affecting the backup image or the recoverability of the data.

In our internal NetBackup Flex Scale testing, we were able to mount thousands of VMs from backup images, allowing users to instantly gain access to their data.

In addition, replicating or duplicating your data to another site is also highly optimized to reduce the network and storage costs. This is because the deduplication savings are retained, and only the unique segment data is sent from the source location.

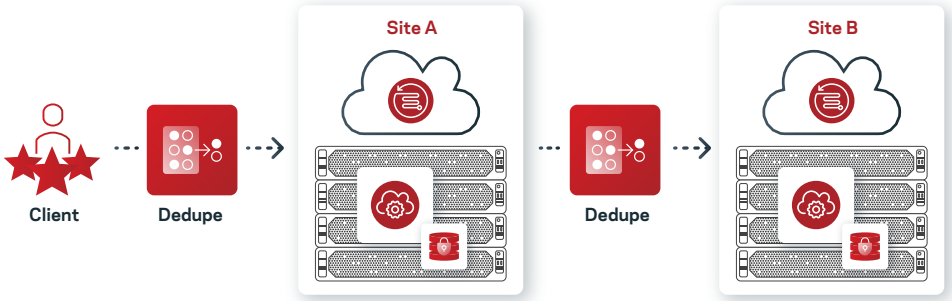


Figure 4. Dedupe savings retained—Only unique blocks are sent from clients and between private and public sites

Data written to NetBackup Flex Scale is further optimized by a clustered file system that uses erasure coding 8:4 on 2MB chunks of deduplicated data. This provides the lowest licensing costs, best space efficiency, performance, and resiliency for NetBackup data stored in a private cloud.

Data sent to and stored in the cloud utilizes the same NetBackup Deduplication Engine which has been optimized with improved efficiency—compressing more data, and utilizing less network and memory than ever before—allowing your cloud resources to go further. You also avoid hidden fees, with pricing based on a fixed back-end terabyte basis.

Whether you write data locally or to the cloud, NetBackup reduces your on-premises data footprint and the amount of data moved to—and stored in—the cloud. This global deduplication leads to significant savings by:

- Decreasing your infrastructure and licensing costs
- Reducing the amount of network bandwidth consumed by backup operations
- Lowering your recovery point objective (RPO) with faster and more frequent backups, and shorter backup windows

98% Reduction in Carbon Footprint

From 3.5 to 0.08 metric tons of CO_2, based on storing one petabyte of un-optimized data in the cloud.

Together, unified data protection management, elastic backup from snapshots, and the optimized deduplication engine can reduce your storage and carbon footprint by 98 percent.

Simplified Management

Veritas' hybrid and multi-cloud solution provides a common interface to display various views of data in all locations at any point in time. Depending on your administrative level, you have the capability to view and manage:

- an entire enterprise from a single UI that aggregates data across all organizations
- an entire organization from a single UI that can be used to manage NetBackup, cloud-based storage, and the on-premises private cloud infrastructure.

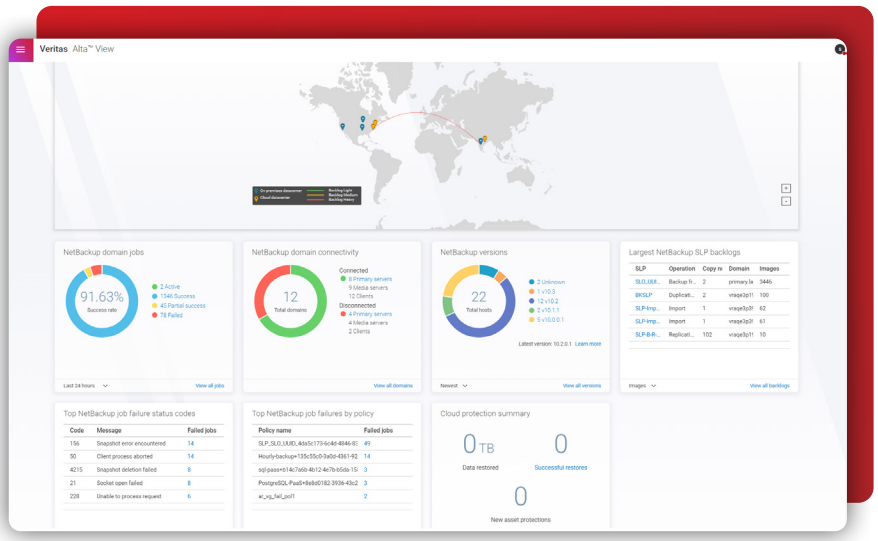


Figure 5. Enterprise Management from a single UI

Using Veritas Alta Recovery Vault, configuring cloud-based storage is simple and does not require unique skills or deployment strategies to leverage multiple cloud storage provider offerings. Instead of working directly with each of the different cloud storage providers, you can now provision, manage, and monitor the cloud storage resources and retention policies directly from NetBackup using the same intuitive interface as the rest of the hybrid and multi-cloud data protection solution. Also, data stored in Veritas Alta Recovery Vault can be restored to the primary domain, or to an alternate site in a different domain or cloud environment, using image sharing.

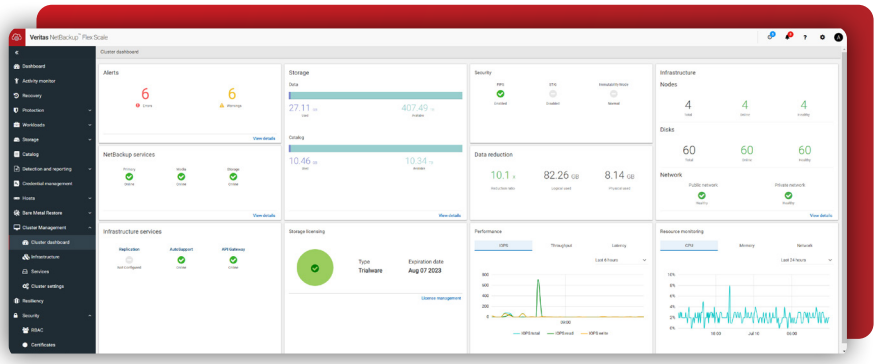


Figure 6. Organization Management from a single UI

Operational simplicity is also prevalent throughout the management lifecycle.

- Storage lifecycle policies allow you to control where your data is stored and for how long. There is no limit on the maximum time to live, even in the cloud. For example, you may store backups from your applications running within your data center in the NetBackup Flex Scale private cloud for 30 days, then move them to cloud-based storage in Veritas Alta Recovery Vault for longer-term retention.
- New workloads can be detected and have protection policies applied automatically.

Similar to public clouds, NetBackup Flex Scale is designed to provide simplified management with several automated processes, including:

- **Deployment**: Simply provide configuration details, and an automated process configures the cluster and NetBackup for you.
- **Node replacement**: Whether you are replacing a failed node or doing a technology refresh, you can easily replace nodes with one click, without having to migrate data—even if you replace the node running the primary service.
- **Recovery operations**: The containerized services and management software is deployed using a resilient storage and server configuration that allows automatic detection and recovery from hardware and site failures.
- **Rolling or parallel upgrade**: Upgrades are packaged together for the OS, drivers and NetBackup software. With one click you can initiate a safe rolling or parallel (admin's choice) upgrade that runs simultaneously on all nodes in the cluster (at both sites if configured in a dual site, single domain configuration). In the event of an upgrade error, a rollback operation is run automatically.

- **Provides a simple automated process to configure an active/active dual site configuration.** Further in the event of a site failure an administrator can with one click initiate a recovery process that can get your backup and recovery jobs up and running again in ~10 minutes.

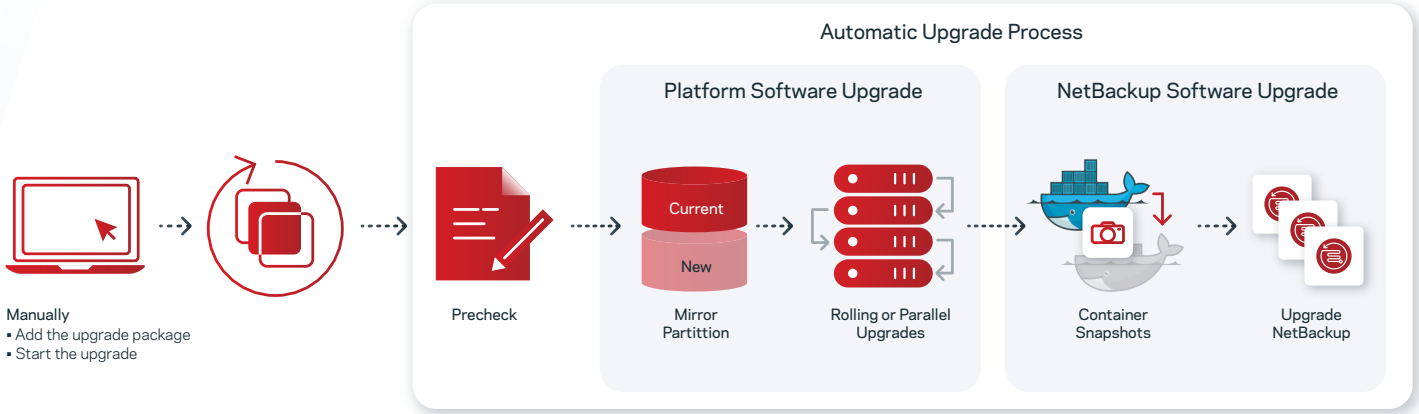


Figure 7. Automated rolling or parallel upgrade process

Private Cloud Scaling

NetBackup Flex Scale includes Cloud Scale Technology, making it easy to add more capacity and run more concurrent jobs. Simply power up a new node, provide network details, and the non-disruptive background process will automatically:

- Balance data across the cluster
- Start new NetBackup services
- Use intelligence derived from backup history and current system load to optimally distribute the backup and recovery jobs across the nodes in the cluster, including the new node, without making any client-side or policy changes

Cyber Resiliency

No matter where your data exists, you will always face challenges related to protecting against cyber and ransomware attacks, making it equally important to protect your cloud environment with the same strategy as your on-premises environment.

The **attack surface** open to a hacker increases with the size of the silo sprawl. And the complexity of managing the sprawl offers opportunities for bad actors to sneak into your environment and wreak havoc. The NetBackup hybrid and multi-cloud solution reduces the attack surface by:

- Protecting all data within a single platform
- Ensuring complete visibility of data stored locally and in the cloud
- Enabling rapid recovery of affected data

In addition to reducing the attack surface, many factors are involved in protecting your backup data from an attack. The first thing people typically think of is immutable write-once, read many (WORM) storage, which stores data as read-only and prevents deletion for a set retention period. But this is only part of the solution. The NetBackup hybrid and multi-cloud solution supports immutable WORM storage for your public and private cloud infrastructures. It includes:

- AI/ML-based anomaly detection: Identifies and flags unexpected changes to backup data, which may indicate an attack
- Policy-based image retention: Defines a time period in which a backup image cannot be deleted
- KMS encryption: Encrypts data in flight
- Integrated malware scanning: Can be triggered automatically based on a high anomaly score, or run on-demand to ensure only uninfected files are recovered

- Isolated Recovery Environment (IRE) options: For an air gapped solution
- Non-disruptive ransomware recovery rehearsals

To ensure that security and compliance policies are in check, Veritas Alta Recovery Vault allows you to provision and manage all public cloud storage-as-a-service resources from within NetBackup's locked-down security and role-based authentication policies. This eliminates the need for separate accounts and user interfaces across cloud providers.

The private cloud solution—NetBackup Flex Scale—enhances your ransomware resilience, with multiple infrastructure layer security enhancements that further protect your backup data. It was purposely designed to be secure by default, using a zero trust architecture that helps protect data with an immutable and indelible infrastructure that includes:

- System hardening
- Immutable and indelible storage with an integrated secure compliance clock/timer
- Encryption at rest
- Containers providing service isolation and network segregation

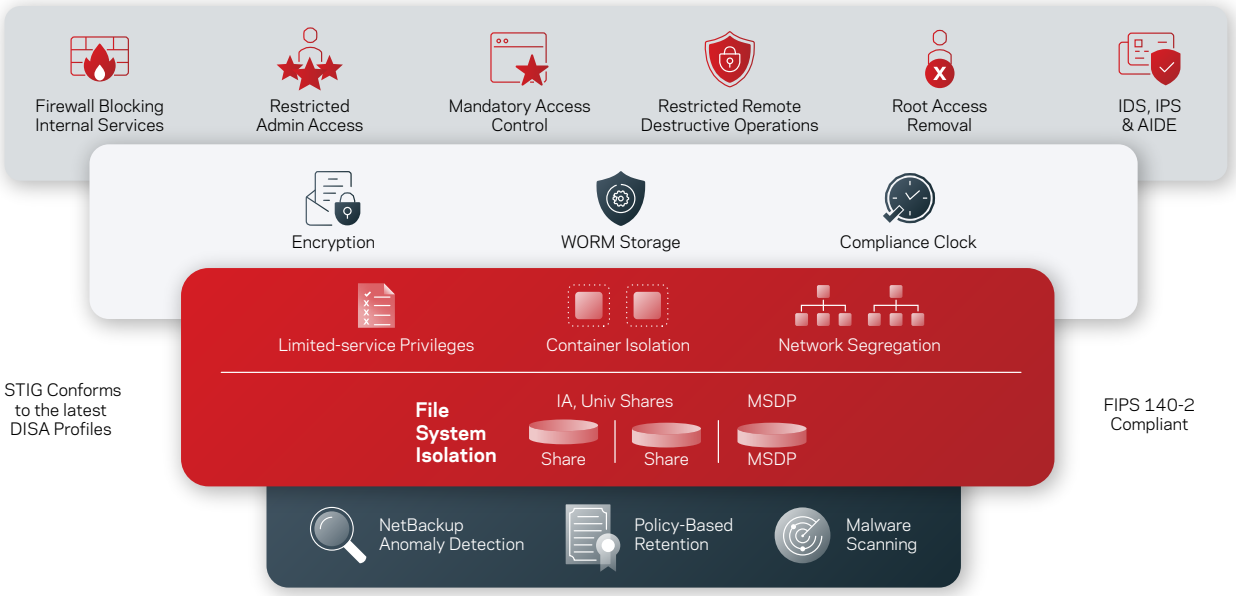


Figure 6: Multiple layers of security built-in.

Comparing Against Cloud Native Tools

A comparison of backup protection available for cloud service providers and Veritas Alta Data Protection is shown below.

Functionality	Cloud Service Provider	Veritas Alta Data Protection
Snapshots	Limited integration with advanced application features	▪ Application aware for all supported workloads using API hooks or native vendor integrations ▪ Integrates with cloud provider snapshots, automating these activities and providing more advanced recovery options ▪ Integrates directly with application APIs providing additional streaming backup options
New Application Support	Low priority	▪ More than 800 workloads currently supported ▪ Prioritized support for new workloads
Deployment Options	Cloud-specific	Anywhere: ▪ On-premises ▪ In any single cloud or hybrid and multi-cloud environment ▪ Virtualized or containerized (via Kubernetes, OpenStack, etc.)

Protect Databases or Other Workloads Where No Agent or Backup API Exists	Limited	▪ Deduplicated storage on a NetBackup server can be provisioned as secure shares using Universal Shares. ▪ Universal Shares can also be used as network attached storage (NAS) to store data using compression and deduplication, with full API support and centralized management of shares
Replication	▪ Cloud specific ▪ Limited site replication ▪ No lifecycle management	▪ Automated replication with lifecycle management to any location (within/across regions and cloud providers)
Recovery	▪ Limited restore options ▪ Lack of orchestration with cloud providers requires manual recovery	▪ Multiple restore options including Granular restore ▪ Recovery orchestration with application integration
Disaster Recovery	▪ Protects against hardware failure ▪ Data management is customer responsibility ▪ Data Recovery limited to same cloud.	▪ Manages the lifecycle of multiple copies in separate geographic locations away from possible ransomware attacks ▪ Enables you to maintain the continuity of your data in the event of a disaster ▪ Includes replicating data across regions, availability zones, between on-premises and the cloud and between cloud service providers, for better disaster recovery planning options ▪ Allows for data portability in the event you want to move your data between cloud service providers or repatriate your data onsite
Auto-Discovery	NA	New VMs are auto discovered, added to existing policies, and protected without manual intervention using Cloud Intelligent Policies
Self-Service	NA	Robust role-based access controls (RBACs), allowing application owners to perform their own restores
Global View of Data	Partial view only, limited to snapshots under management of single cloud	Global view of data, regardless of backup storage location, at any point in time for all applications and file systems

Summary

The Veritas hybrid and multi-cloud data protection solution, made up of Veritas Alta Data Protection, NetBackup Flex Scale, Veritas Alta View, and Veritas Alta Recovery Vault, removes the complexity associated with providing enterprise-class data protection for hybrid and multi-cloud environments. Regardless of where your clients or data reside, you can use a single interface and the same NetBackup software to manage it all.

Whether you write data locally or to the cloud, NetBackup uses the same deduplication technology, allowing you to reduce your on-premises data, as well as the amount of data transported and stored in the cloud. This global deduplication leads to significant savings by:

- Decreasing your infrastructure and licensing costs
- Lowering your carbon footprint
- Reducing the amount of network backup bandwidth
- Decreasing your RPO with faster, more frequent backups; and shorter backup windows

With multiple layers of integrated security and ransomware resiliency, the Veritas hybrid and multi-cloud data protection solution provides confidence in the ability to quickly recover your data, ensuring that your data is always available when needed.

Additional Resources

NetBackup Flex Scale - Mass Recovery and Backup Performance

NetBackup Flex Scale – Secure by Default

Enterprise Data Protection for the Cloud with Veritas NetBackup

Veritas Alta Recovery Vault Deployment Guide

Moving Towards a Sustainable Future

Veritas Alta Recovery Vault Deployment Demo Azure

Veritas NetBackup Recovery Vault: Creating Storage Buckets on AWS

Veritas Hybrid and Multi-Cloud Data Protection Solution

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

V1612 10/23