Best Practices and Strategies for Secure Cloud Data Management

With most companies prioritizing a multi-cloud strategy, and with 85 percent being cloud first by 2025[1], it is vital that every cloud leader prioritize best practices and implement a unified data management and protection strategy across their cloud data landscape. Cloud service providers are first a business and therefore motivated to improve revenue. As they regularly update and change their support and coverage of the shared responsibility model, confusion can create gaps in security, and prevent you from staying in control of your company data.

Proper data security requires the right tools. Veritas cloud solutions provide a multi-layered cyber security strategy that extends into cloud technologies to safeguard data, keeping your business resilient and your teams in control, with 99.999 percent uptime.

Veritas puts you in control of your cloud and helps you meet your end of the shared responsibility model by:

- **Reducing risk**, by safeguarding all data, regardless of where it is—edge, core, or cloud. Veritas protects data and reduces attack surface with added layers of security such as system hardening and immutability. Veritas gives you the power of choice and flexibility with intelligent, automated, orchestrated, non-disruptive, cost-effective recovery rehearsals. All while keeping you compliant.
- **Eliminating uncertainty**, with complete visibility, intelligent anomaly detection, and malware scanning. So you can confidently know where all your data is, while reducing operational complexity and optimizing cost management.
- **Maintaining control**. Veritas puts you in control of your multi-cloud, ensuring performance, application availability, and cross-cloud mobility.

Reduce Risk

The cloud may offer incredible simplicity, availability, and performance, but not without securty risks. The first step to reduce risk is to ensure that your most important assets—your data and your IT infrastructure—are protected from the unknown. Veritas provides a vast amount of solutions to protect and safeguard your data, optimize your ecosystem for rapid recovery, and keep your data compliant.

Figure 1: Protection safeguards for cloud

Protect

Veritas safeguards data integrity by protecting all data from all sources in the six areas. (See Figure 1)

Identity and Access Management

- **Role-based access**: Granular access controls you can tailor to meet specific persona needs, specifying who can access data, and defining what actions they can or cannot perform.
- **Single sign-on**: Support for Active Directory and LDAP as well as SAML 2.0. Organizations can use their authentication provider to achieve two-factor authentication.
- **Customizable authentication**: NetBackup Flex Appliances support configurable authentication strength.

Data Encryption

- **In-transit**: Ensures your data is sent to authenticated environments and is protected while in transit. This solution leverages Veritas or customer-provided TLS 1.2 certificates, with 2048-bit+ key support to ensure data transport encryption during transit.
- **At-rest**: If attackers are successful in getting to your data, having it encrypted protects it from being exploited. Veritas offers AES 256-bit, FIPS 140-2 certified cryptography with our own key management, while allowing you to leverage your preferred key management using the Key Management Interoperability Protocol (KMIP).

Immutable/Indelible Storage

Veritas provides extra safeguards with immutable and indelible storage, with flexible, storage-agnostic options including BYO, appliance, cloud, and software as a service (SaaS). Immutability keeps your data secure and compliant, regardless of location.

- OpenStorage Technology (OST) API lets you manage immutable backup images with Veritas or third-party storage solutions.
- Supports primary, secondary (duplication), and cross-domain replication (with AIR), giving you unlimited configuration options across any backup storage tier.
- Uses cloud immutable storage with Amazon Web Services (AWS) S3 Object Lock to ensure your cloud data is secure and unable to be compromised. To learn more about NetBackup's cloud immutable storage, see the Object Lock support for AWS technical brief[2].
- Immutable and indelible storage with NetBackup Flex Appliance deployment.
- Images are stored in write once, read many (WORM) storage
  - NetBackup Flex Appliance includes a WORM storage server that offers a secure, container-based multicast source discovery protocol (MSDP) solution.
  - NetBackup Flex Appliance offers Enterprise and Compliance lock-down modes, so you can choose the right immutability strength.

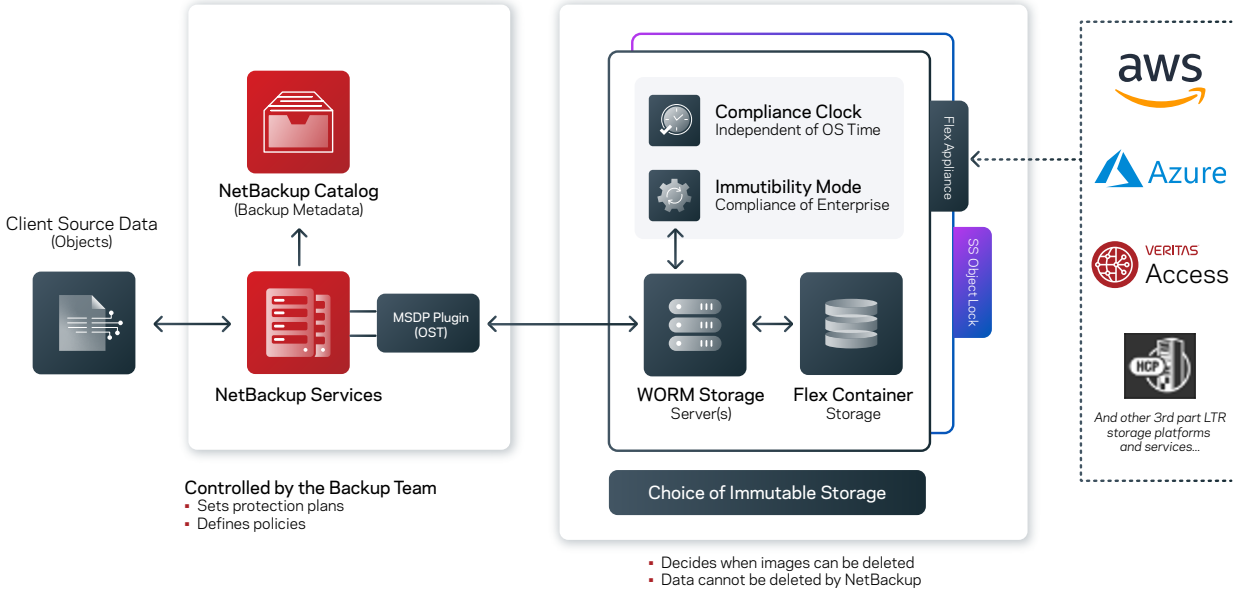

Figure 2: Example of integrated security and data immutability

- Compliance mode enables immutable storage, in which no user—including the root user—can delete data during a predefined retention period.
- Enterprise mode protects data from being deleted during a predefined retention period, but only users with special permissions can alter the retention settings or delete the data using dual authorization. Two individuals with different RBAC levels must agree to make any changes to the retention time, or modify or delete data.
- NetBackup Flex Appliance has completed a third-party Immutability Assessment from Cohasset Associates[3], an industry-recognized assessor of immutability controls, specifically SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles of the Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1 31(c)-(d).

Solution Hardening

- NetBackup Flex Appliance and NetBackup Flex Scale have been hardened from a software and hardware perspective to offer a complete secure solution that supports immutable and indelible storage. The solution offers a secure WORM storage server and hardware security features.
- Throughout the development cycle, Veritas analyzes NetBackup Flex Appliance and NetBackup Flex Scale code for vulnerabilities using recognized third-party detection tools that perform:
  - Static code analysis
  - Runtime vulnerability checks
  - Penetration testing
- NetBackup Flex Appliance and NetBackup Flex Scale come with a wide variety of security features that include:
  - OS security hardening, including Security-Enhanced Linux (SELinux)
  - Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
  - Robust role-based authentication
  - Locked-down storage
  - A secure, robust, and hardened Veritas File System

SaaS Data Protection

NetBackup SaaS Protection provides a unified data management and protection solution, delivering a single, fully managed, and cost-effective platform for SaaS workloads, including 365. Software-as-a-Service vendors have adopted a shared responsibility model, which means it's up to businesses to protect and secure their own cloud-based data. Our solutions consist of a cloud-native backbone that runs in Microsoft Azure data centers as a fully-managed SaaS deployment. NetBackup SaaS Protection is a storage platform for enterprise organizations to centrally protect, analyze, archive, search, tier, recover, and manage all types of SaaS application data—at any scale.

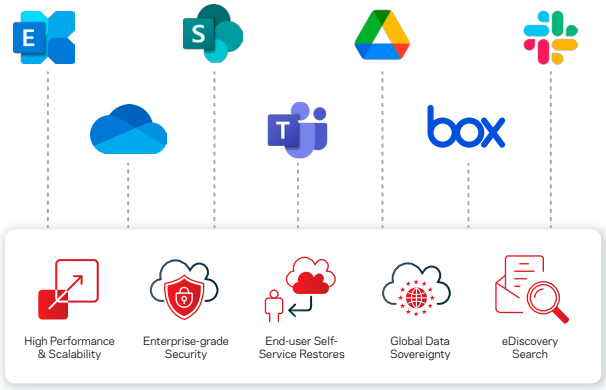

Figure 3: Unified data management and protection solution

Key benefits include:

- High performance and scalability
- Enterprise-grade security
- End-user self-service restores
- Global sovereignty
- eDiscovery search

Network Isolation Using Air Gap Solutions

What is an Isolated Recovery Environment?

For enhanced ransomware resiliency, it is important to secure your backup data for clean recovery. This can be achieved with an environment purposely built and designated as an isolated recovery environment. An IRE may also be a disaster recovery (DR) environment, a sandbox, or a test environment—which means you can use your existing infrastructure. Whichever the environment, it should employ methods to perform test restores of production data; scan for malware ensuring that any discovered infections cannot spread; and in some cases, perform data forensics. This provides administrators a clean set of files on demand to neutralize the impact from a ransomware attack. Such an environment can also benefit from data isolation techniques, such as an air gap, where the physical and logical connections are blocked unless specifically allowed through implementation of the NetBackup IRE solution. Implementing a zero trust architecture, along with immutable and indelible storage and malware scanning techniques within the IRE, further secures backup data from the spread of malware and ransomware.

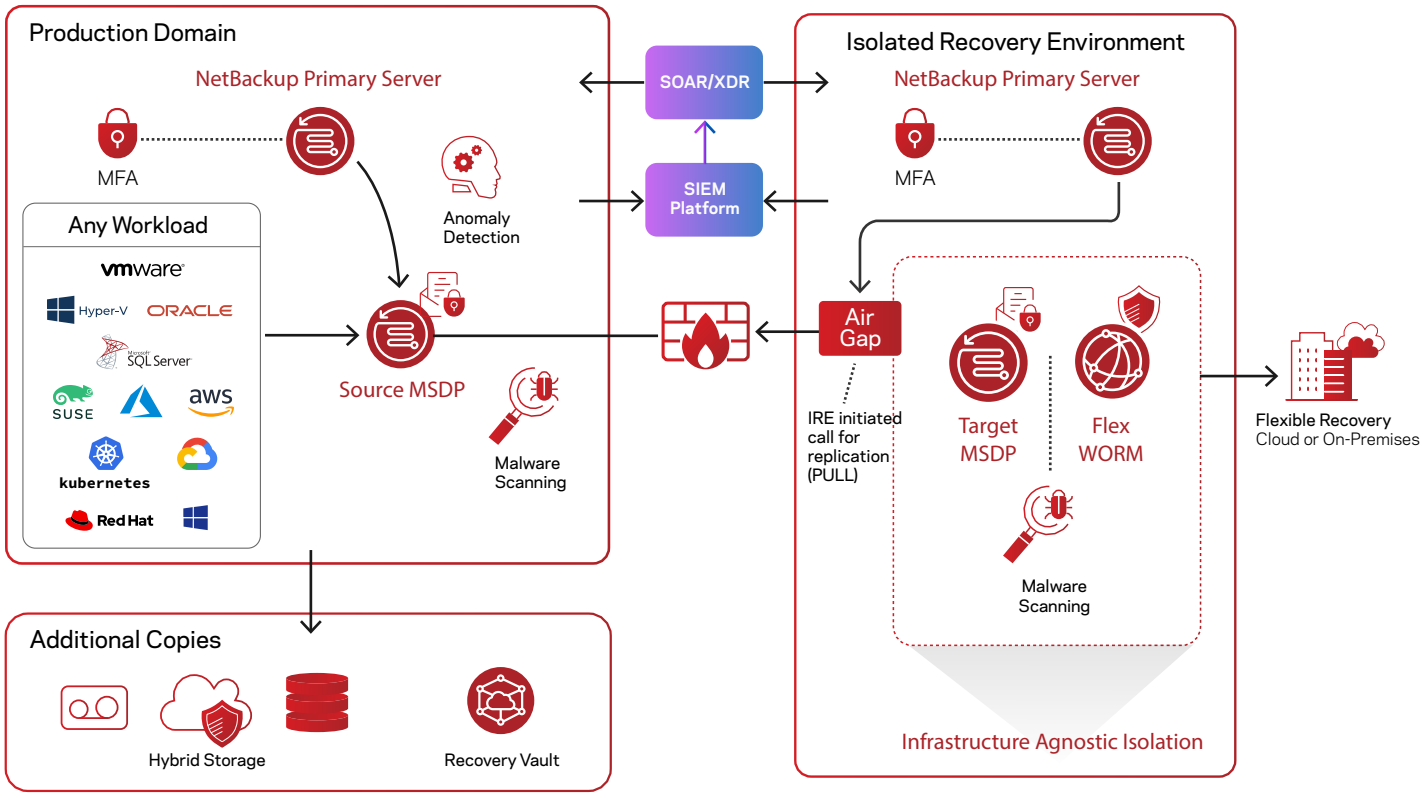

Figure 4: Isolated recovery environment from Veritas

NetBackup's Isolated Recovery Environment Solution

Traditional network isolation solutions physically or logically break connectivity between secure locations, making all communication in or out impossible. This limits data transfer to the isolated environment and endangers recovery time objectives (RTOs) and recovery point objectives (RPOs) if the tertiary copy is needed. Commonly referred to as the pushing of replication data from the source to the target, the source domain independently processes and submits a replication job to a target domain. This traditional approach limits the time available to replicate critical data into a secure environment when the connection is down or blocked.

By contrast, the Pull replication model initiates the replication request from the target. As of version 10.1, NetBackup's IRE solution optimizes data movement by offering a Pull replication model whereby the request to send data comes from the IRE's MSDP, and the reverse connection offers better control of the data flow to further secure the environment logically and physically. Replications to the IRE are now able to be fully controlled from within the IRE, including support of a specific window as defined in the IRE air gap schedule.

IRE functionality should be combined with 3-2-1-1 best practices for your data: at least 3 copies of critical backup images, on at least 2 different types of storage media (disk, tape, cloud), with at least 1 image offsite from production, and at least 1 image written to some form of immutable storage. MSDP-C with immutable cloud storage, Flex Appliances WORM instances, and NetBackup Recovery Vault are excellent ways to implement or augment this solution. Business needs may further require additional copies of backup images on different media in different locations in order to meet continuity goals and compliance requirements.

An IRE will commonly be the last stop, or one of the last SLP operations for the backup image. This allows integration with multi-domain SLP strategies, where several domains act as a DR for a counterpart domain, as well as the inverse, allowing two production domains to protect each other. The IRE can be an extra destination to further isolate the critical data outside of any production domain. Conversely, an existing DR environment can implement IRE on any NetBackup 10.1 MSDP or Flex Appliance WORM version 17 instance.

Recovery

At Veritas, our resiliency solutions are optimized for flexible, hybrid, and rapid recovery, with the ability to automate and orchestrate complete cross-site or cloud restoration with the click of a button. And we do it at scale.

Why is flexibility important? Sometimes everything is impacted, and you may need to recover an entire data center in the cloud and on demand, other times you may just need recovery from the object level, and other times you may need to recover a portion of your virtual machines (VMs) back to production. The flexibility to recover everything—from data to application to an entire data center—without restriction, is key in the event of an attack.

In today's ever-evolving threat landscape where no cyber attack is the same as the next, it is vital to architect an optimized and simplified recovery experience to get you up and running in minutes versus hours or days, regardless of scale.

Additionally, Veritas makes it easy and efficient to automate non-disruptive DR tests with rehearsals for all tiers of business, leveraging non-production resources such as network fencing and sandbox environments.

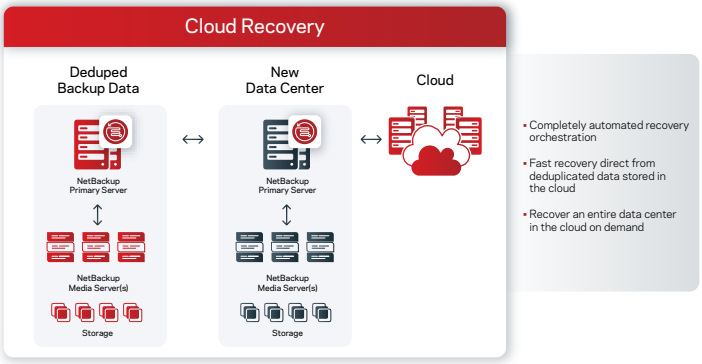

Figure 5: Flexible Cloud Recovery

Veritas offers a number of recovery solutions, including granular file recovery, bulk/instant recovery, instant rollback of VMs, continuous data protection, and bare metal recovery, to name a few.

Eliminate Uncertainty

Data Visibility

Veritas provides tools for complete visibility of your entire environment. This includes physical, virtual, and cloud workloads ranging from storage, to compute, to every major data protection solution. Cross-reporting ensures no system falls through the cracks. This is especially crucial in today's threat landscape, as cyber criminals are hoping that you are not keeping an accurate inventory of all your applications and data, or that there may be areas where you have limited security or oversight.

In addition to shining a light on the dark areas of your environment, Veritas solutions provide comprehensive insights, alerting and reporting across on-prem, cloud, data protection, and storage. You'll have the insights needed to make informed decisions in the face of a cyber attack, with reporting options that help you gain visibility into your backup environment, enabling your organization to:

- Discover all hosts or VMs in your infrastructure, and compare them with the VMs protected by NetBackup
- Flag hosts that are missing from the backups or have no recent backups as potential risks
- Detect the potential ransomware-affected files, along with their size and where they reside in the environment
- Use interactive graphs that provide a historical view of the risks generated

NetBackup IT Analytics also identifies potential false positives by comparing historical backups against the new backup and identifying anomalies such as significant changes in job durations, image size variations, and policy configuration changes.

Anomaly Detection

Veritas provides AI-powered anomaly detection that recognizes out-of-the-ordinary data and user activity across your entire environment, and alerts you to suspicious anomalies, in near-real-time. The technology is able to mine an enormous amount of data, automate monitoring and reporting, and provide actionable insights into what is happening in your environment. Alerts could be triggered by unusual file write activity, which could indicate an infiltration, known ransomware file extensions, file access patterns, traffic patterns, code downloads, access requests, storage capacity surges, external traffic paths, and even an unexpected jump in activity compared to typical patterns—can all be detected.

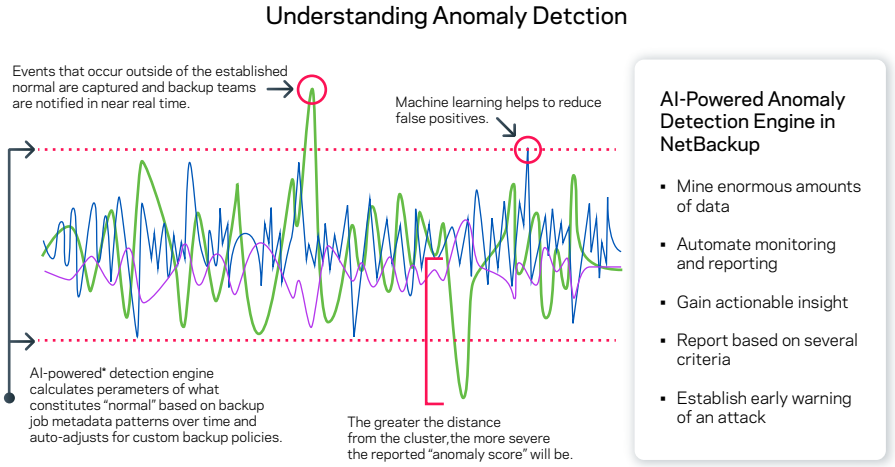

Figure 6: Understanding anomaly detection

These solutions can help you recognize indicators that an attack is underway or about to begin, which enables you to take immediate action and limit the impact.

Administrators have the ability to view data and provide recommendations associated with anomalies at any time by monitoring all devices and establishing early warning of any attacks, to can stay on top of issues as they arise. For example, NetBackup's AI-powered anomaly detection seamlessly integrates into the NetBackup primary server, enabling it to detect anomalous forms of observations—considering those that do not fall into the cluster as anomalies or outliers. This capability lets an administrator see anomalies and drill down to identify any concerns. It offers the ability to mine large amounts of data and provide actionable intelligence to address ransomware events or simply changes in the environment that an administrator should be aware of.

Malware Detection

Veritas can help you detect multiple types of malware, including encrypting exfiltration, and providing automated and on-demand scans. The automated feature will remove human dependencies and allow artificial intelligence/machine learning (AI/ML) technology to scan for malware, and is triggered by a high anomaly score. Scanning includes unstructured data, Windows, Linux, and VMware. This inclusion is vital because malware often enters your environment in locations where large sets of unstructured data exist, such as a home directory.

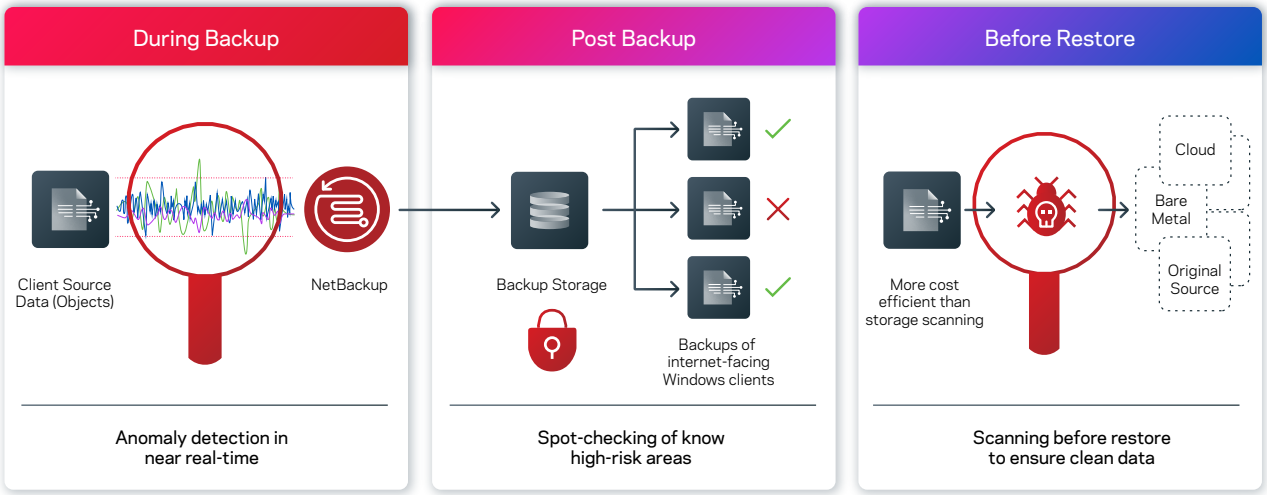

Figure 7: Malware scanning overview

Additionally, when recovery is necessary, the backup data can be scanned, ensuring the latest malware signatures are leveraged. Clear visuals and warning prompts provide awareness of infected backups, ensuring all data restored is clean and unimpacted. This practice is often referred to as restoring to the last known good copy.

SIEM/SOAR Integration

Take Full Advantage of NetBackup and Syslog Messaging

According to the State of Security 2022 survey conducted by Splunk, up to 67 percent of organizations are investing in security information and event management, (SIEM) (and up to 88 percent are investing in security orchestration automation and response (SOAR)) platforms, sometimes also including extended detection and response (XDR)) platforms. NetBackup can integrate with these tools in a simple universal method. NetBackup audit messages are consistently formatted to be consumed by third-party tools from the server platform system logs, including several new audit categories. Ensure that you have selected to export the audit messages to the system logs. This is easily enabled under the Security > Security Events area of the NetBackup WebUI (see Figure 8). By default, this is not enabled. Once enabled, there are no default messages until the next audit event.

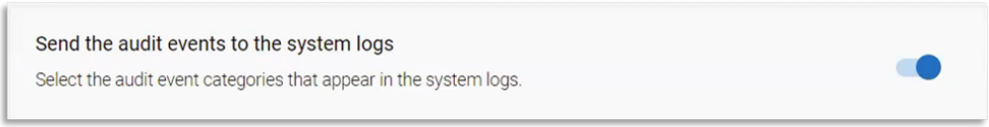

Figure 8: Enabling audit events exported to the system log of the primary server

NetBackup can always manually export the audit events using the `nbauditreport` command on the primary server, but leveraging the export allows for automation. NetBackup audit messages are categorized. The audit messages that are exported can further be customized by category, opening up a wide array of possibilities for integrations with SIEM and SOAR platforms, with different triggers for each category, as well as removing categories that you do not wish to export. The primary consumer of this data would normally be a SIEM platform, in order to perform analytics, generate alerts, and often provide further analysis in the form of reports. SOAR actions can follow triggers from the SIEM platform, or in some cases trigger directly from certain event patterns, according to your level of customization in the SIEM and SOAR platforms.

Disaster Recovery for Storage as a Service

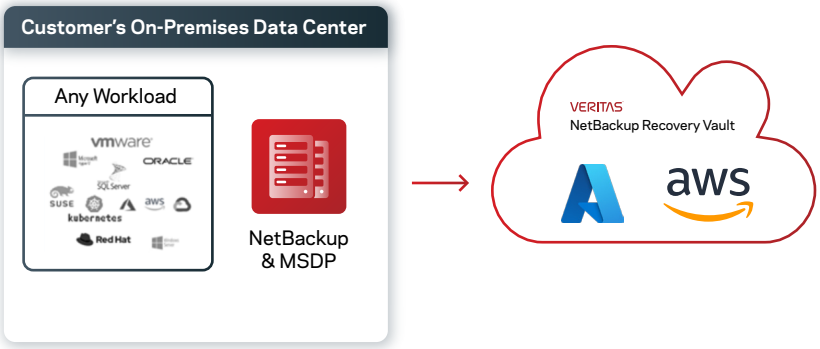

Figure 9: NetBackup Recovery Vault

NetBackup Recovery Vault is a cloud-based storage-as-a-service offering that provides a seamless, fully managed secondary storage option. Seamlessly integrated with NetBackup, it provides an easy-to-use UI that simplifies provisioning, management, and monitoring of cloud storage resources and retention policies. Most NetBackup Recovery Vault customers use Image Sharing, a feature in NetBackup that packages a minimal set of metadata with all backup data to make it self-describing. This allows backup data to be restored from a primary location onto a NetBackup primary server in an alternate domain or cloud environment to meet data compliance and governance requirements.

NetBackup Recovery Vault provides a fully managed cloud data protection tier, seamlessly integrated with NetBackup to scale protection across any cloud model while controlling costs. NetBackup Recovery Vault can use NetBackup Image Sharing to copy data from a primary site to an alternate site in a different domain or in the cloud. With NetBackup Recovery Vault and Image Sharing, you can copy your mission-critical data and restore it using a completely autonomous primary server located off-site. In the event the primary server is compromised, your mission-critical data can be converted to the alternate site to continue to meet data compliance and governance requirements.

Maintain Control

Performance

Cloud infrastructure often has system level limitations that minimize overall application performance. Veritas provides intelligent caching where application reads can be served from faster volumes using cloud SSD storage, while writes can be served from a less costly storage tier. This can significantly improve application performance, with minimal additional expense.

Cross-Cloud Mobility

Veritas helps you to easily move your applications within public cloud and hybrid cloud architectures, and can also provide automated cloud migration from on-premises systems as well as between different cloud providers. This helps avoid cloud service provider lock-in, and it gives you better resiliency and protection against cloud provider outages.

Application Availability

While cloud infrastructure is designed to provide excellent availability and durability for compute and storage systems, Veritas is focused on the applications that run on top of this infrastructure. With customized integrations developed specifically for cloud services, Veritas can manage cloud compute, network, and storage resources required for your infrastructure and application to be online in the cloud.

Resiliency

It is important to highlight that no cloud service is invulnerable. Whether a network outage disrupts a business-critical app, or malicious code locks out the users from their storage, resiliency must be maintained at all cost, or customer confidence will be lost. Veritas ensures that any uptime service level agreement (SLA) is achievable; and not just region to region, but cloud to cloud, or even cloud to on-prem. The figure below showcases how Veritas resiliency solutions can orchestrate the failover of apps, infrastructure, and data from an IaaS infrastructure operating in AWS to Azure.

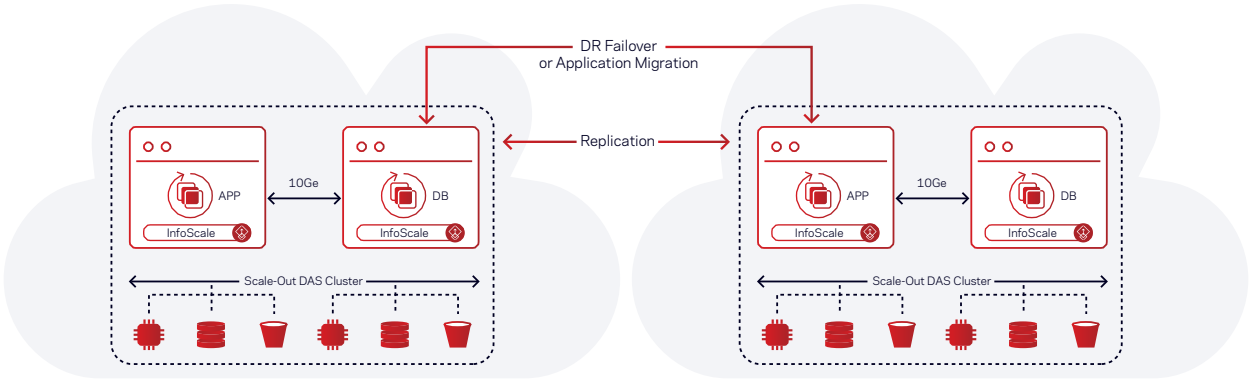

Figure 10: Veritas resiliency solutions orchestrating the failover of apps, infrastructure, and data from an IaaS infrastructure operating in AWS to Azure

Enterprise-Wide Availability and Resiliency in the Cloud

Veritas offers a holistic cloud solution that delivers resiliency, protection, and management for AWS, Azure, and GCP alongside the traditional data center. The figure below showcases how Veritas can orchestrate the failover of apps, infrastructure, and data from an IaaS infrastructure operating in AWS to Azure.

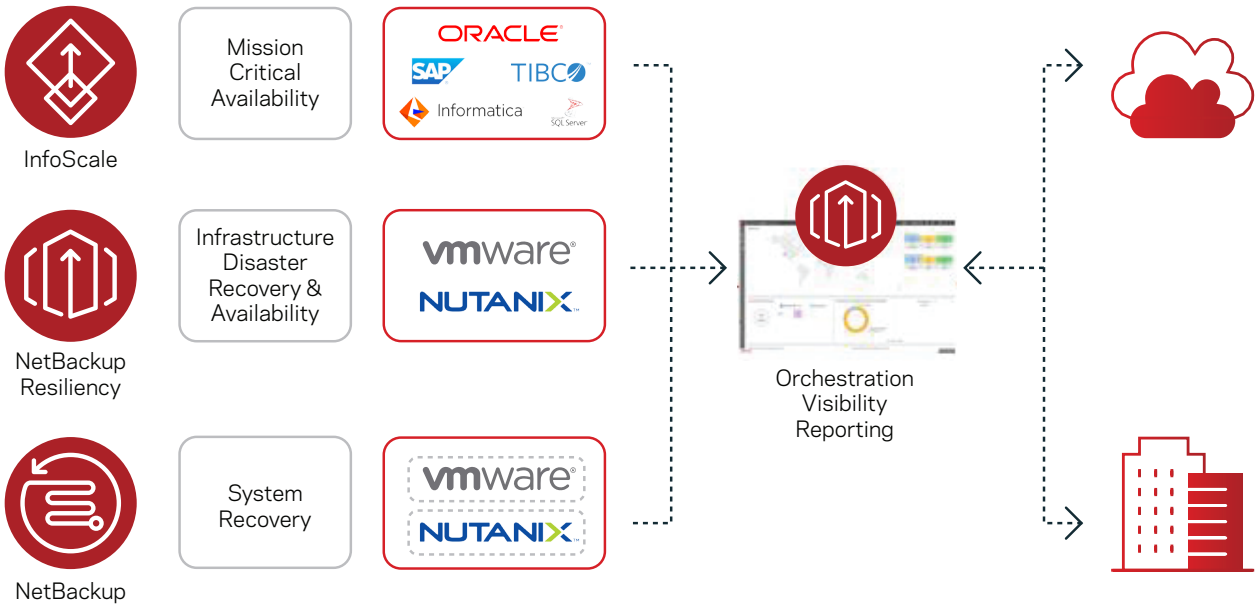

Figure 11: An overview of the Veritas enterprise resiliency strategy.

Veritas Unified Data Management and Protection Across Every Cloud

Veritas Solutions

Workloads customers need. Architectures they want. Simplicity they demand.

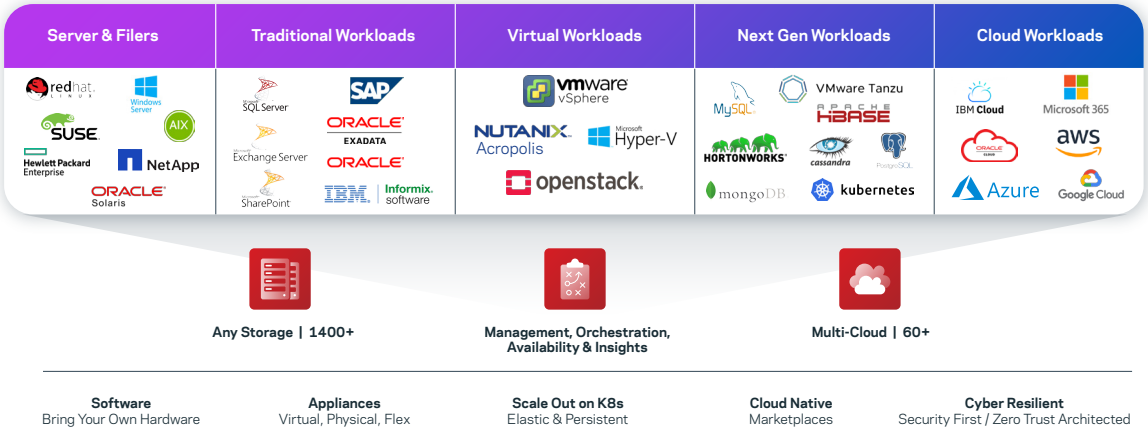

Figure 12: Unified data management and security.

Veritas helps you think beyond cloud-native utilities with products that enable you to architect a unified strategy for data management, with cyber security and data safeguards at the forefront.

Veritas provides you with cloud control.

Visit https://www.veritas.com/solution/cloud-data-security to learn more.

1. https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences
2. https://www.veritas.com/content/dam/Veritas/docs/briefs/V1350_GA_ENT_SB_Object-Lock_EN.pdf
3. https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95% of the Fortune 100 –rely on us 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 Veritas' ability 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 our 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

V1622 08/22