

Availability and Resiliency for the Modern Enterprise

Solution Overview



Contents

- Executive Summary 3
- Solution Value 3
 - Solution Overview 3
- Integrated Resiliency 5
 - Data Corruption and Ransomware Protection 6
 - Flexibility 8
- Automation 9
 - Service Level Management.10
- Visibility.11
 - Reporting11
- Summary11

Executive Summary

Managing enterprise-wide IT resiliency has historically been a complex problem. Businesses planning for disruptions caused by nature, operator error, malware, ransomware and under-provisioned systems require a unified availability and resiliency strategy that spans all business applications. Historically, that strategy has been to deploy multiple independent solutions, leading to high costs and increased exposure to service disruptions.

Veritas provides enterprise data services focused on application availability, protection and insights. As a market leader in application availability, Veritas has a long-standing history of providing innovative solutions for managing IT availability and resiliency. The integration of Veritas data protection, resiliency, high availability and storage management solutions provides organizations with a continuum of availability that enables a unified enterprise-wide resiliency strategy with several key benefits:

- Reduces costs and complexity by eliminating multiple point solutions for application availability and resiliency.
- Provides visibility into availability and resiliency status across all business applications from a single interface.
- Manages availability and resiliency for applications of any type and importance with a single vendor solution.

This solution overview will discuss the Veritas strategy for managing enterprise IT availability and resiliency for any type of application with nearly any uptime requirement. Veritas offers a unique integrated solution that ensures application availability and resiliency for the entire organization while maximizing your investment in new and existing Veritas technologies.

Solution Value

Veritas reduces complexity and simplifies operations by providing a single platform for visibility and control for availability and resiliency operations, with native integrations that operate as a single solution. This approach allows you to minimize the costs associated with making your applications highly available and resilient by allowing you to choose the level of protection required based on your application's business impact. If an application has a less demanding availability requirement and doesn't need to be 'always-on,' you have the flexibility to use a more cost-effective resiliency option to protect the application. This unified approach has several advantages:

- Flexibility to choose how your applications are protected based on their business value.
- Automated availability management for complex, multi-tiered business applications.
- A single solution that can provide any recovery point objective (RPO) and recovery time objective (RTO) you need for any application.
- Visibility and reporting on availability and resiliency status across the entire organization.

The integration of data protection, resiliency and availability management into a single unified solution provides a continuum of availability for all business applications—an attribute that is unique in the marketplace.

Solution Overview

By integrating backup, high availability and replication into a unified resiliency solution, Veritas provides a single source of visibility, automation and control based on advanced integration between the following platforms:



▪ **InfoScale**—A software-defined optimization solution for mission-critical applications that abstracts applications from their underlying hardware and software resources. That abstraction enables enterprise-grade optimizations around business continuity, performance and infrastructure agility across physical, virtual and cloud environments. InfoScale provides advanced software-defined storage and availability management for mission-critical applications that need to be always-on.



▪ **Resiliency Platform**—A software-defined disaster recovery and resiliency orchestration solution for physical and virtual systems that enables automated resiliency and disaster recovery for data centers and both hybrid and multicloud environments. Resiliency Platform provides multiple options for advanced replication management for protected applications, including native data replication capability, integration with storage-level replication and NetBackup replication. Resiliency Platform also acts as the centralized interface when integrated with InfoScale™ and NetBackup™ that provides control and visibility for the overall solution.



▪ **NetBackup**—Provides enterprise-level heterogeneous data protection for nearly any platform and application. It provides cross-platform data protection functionality for a large variety of operating systems and applications. NetBackup uses a centralized management architecture that can be easily scaled to manage data protection for vast enterprise environments. NetBackup has advanced Automatic Image Replication (AIR) capability for replicating backup images between sites to maximize resiliency for backup data and backup services. The Veritas solution discussed here uses NetBackup to provide application resiliency by leveraging advanced integration with Resiliency Platform. As a best practice, it's important to maintain a full NetBackup enterprise data protection solution in parallel that can provide backup and recovery services for all your applications.

Resiliency Platform is directly integrated with both InfoScale and NetBackup to provide a single user interface, making it easy to understand and visualize the state of availability and resiliency within an entire environment from a single console. This integration between Veritas platforms provides a unique way to manage availability and resiliency for applications with any RPO and RTO, which eliminates the need for multiple independent solutions to manage different applications. Instead, Veritas provides a unified solution for managing availability and resiliency for your full spectrum of business applications. Figure 1 shows an overview of how the integrated Veritas solution works.

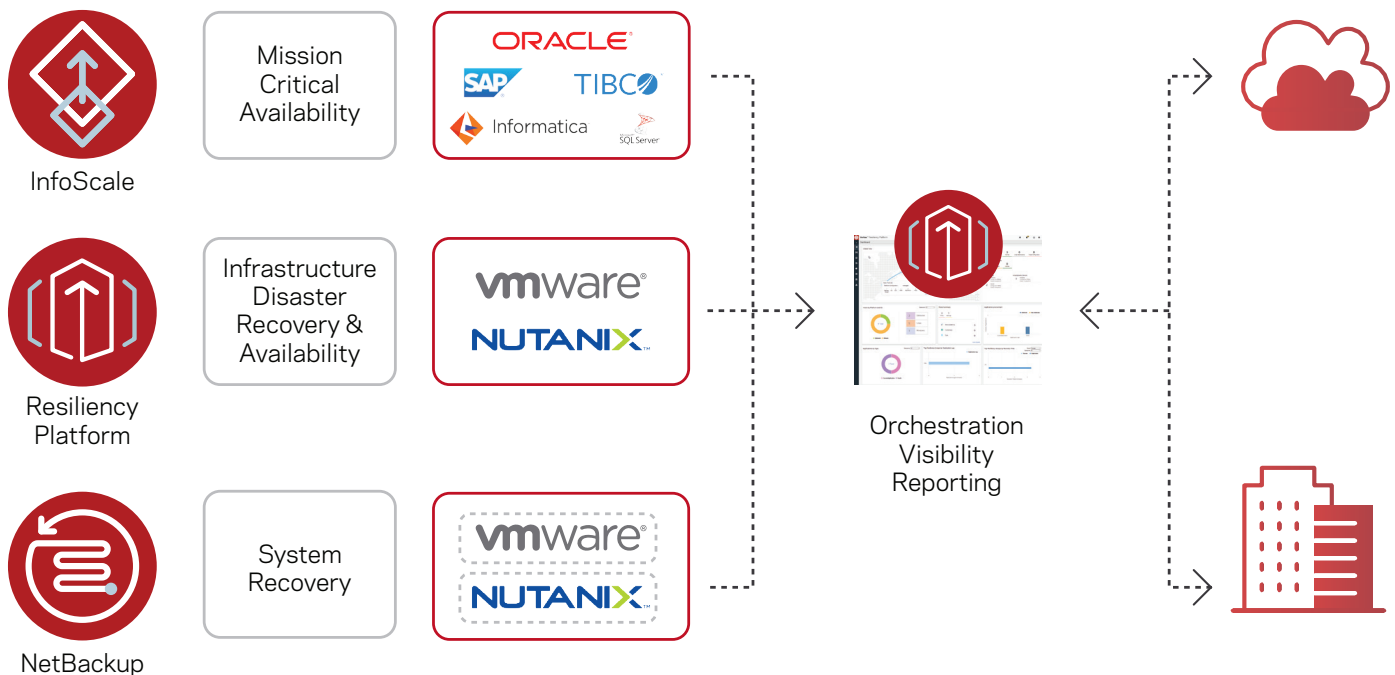


Figure 1. An overview of the Veritas enterprise resiliency strategy.

Integrated Resiliency

Not all applications are created equal. There are several different types of applications that serve different purposes, and they all have service-level agreements (SLAs) you need to manage. By integrating application availability, data replication, infrastructure disaster recovery and system backups, Veritas makes your complete IT environment resilient using an integrated solution that creates a continuum of availability and resiliency for almost any type of application.

- **Mission-critical applications**—InfoScale eliminates planned and unplanned downtime by clustering critical applications and the resources they require. With intelligent kernel-level application monitoring that acts immediately in the event of a system fault, InfoScale can ensure fully automated application high availability and a near-zero RPO and RTO if a failover is needed. InfoScale also dynamically monitors available unused system capacity in terms of CPU, memory and swap space to understand which systems have the most available resources. It can then make dynamic decisions and failover applications to the systems best suited to take over application execution with maximum performance, which helps provide the best user experience.
- **High-and middle-impact applications**—Resiliency Platform can cost-effectively manage applications that don't require always-on capability. The systems that host these non-mission-critical applications can be organized into resiliency groups where Resiliency Platform manages their failover process and data replication between sites. The RPO can be as little as five minutes using Resiliency Platform's integrated replication capability. The failover process that includes DNS updates, managing network mappings between sites and starting entire applications at the recovery site in the event of a failover is entirely automated. When using the cloud as a resiliency target, cloud resources are brought online on demand when needed.
- **Lower-impact applications**—With less demanding RPOs, these applications typically don't require real-time replication and can be made resilient by automating the recovery of their associated backup images. This fully orchestrated process can provide a near-zero RTO with the Instant Access option that can bring a system online almost instantly using a backup image. When several systems or an entire IT service needs to be recovered as a single action, this process can be entirely automated instead of having to manage multiple restore operations, which can be complex and time-consuming.

Resiliency for all applications can be managed as a single integrated solution, regardless of the application tier, RPO and RTO (see Figure 2). This approach provides a continuum of availability for the entire organization that gives you multiple options for availability, resiliency and recovery that can accommodate any SLA. The ability to recover applications almost instantly and to multiple points in time is also supported, giving you additional protection against data corruption and ransomware attacks.

Recover with Confidence

The DR Rehearsal option allows you to test a recovery operation prior to execution with no impact on production services. You can run this process for any application, regardless of how it's protected. You can manage and run a simulated failover test on an isolated, non-production network segment to ensure systems at the secondary site are working properly prior to a full failover event. To do so, the process uses snapshots of production data that are then attached to temporarily provisioned systems used for testing purposes. Clean up of the rehearsal environment when it's no longer needed is fully managed and automated.

The DR Rehearsal feature has flexible configuration options and can be used for a single system or for an entire business service using a feature that provides service-level management. This feature is called Virtual Business Services and is discussed in more detail below. Figure 9 shows an example of how the integrated Veritas solution can orchestrate a DR rehearsal for a multitiered application.

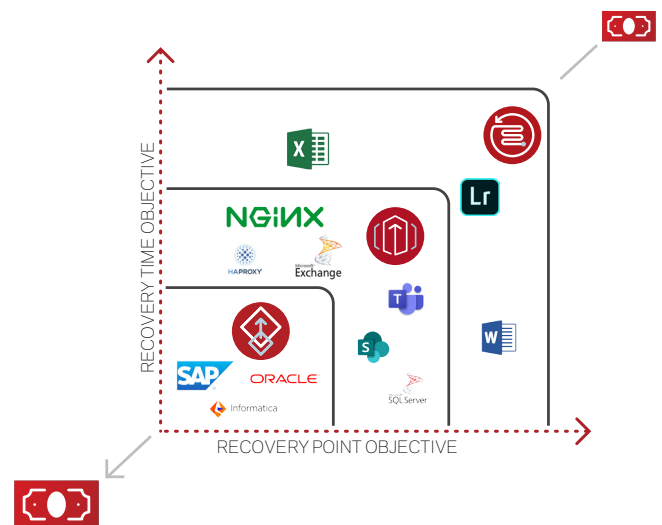


Figure 2. The Veritas integrated solution provides availability and resiliency for all business applications.

Data Corruption and Ransomware Protection

Protecting systems and applications against data corruption and ransomware attacks is a significant concern for businesses today, given the need to ensure application availability and resiliency. IT departments often have inadequate solutions in place to recover applications and systems within their SLAs and with minimum data loss. With applications deployed in multiple locations and on multiple platforms, it's crucial to have a unified solution that protects all your systems and applications across physical, virtual and cloud environments.

Veritas minimizes the disruptive potential of data corruption and ransomware by integrating data replication and recovery into a unified solution that provides multiple options for recovery in the event of a data corruption scenario or ransomware attack, including:

- Continuous data checkpoints derived from real-time data replication.
- Automated recovery for individual systems, applications and multitier business services.

This integration enables maximum availability and resiliency for your applications while providing recovery automation and the frequent recovery checkpoints needed for low RPOs, minimizing the potential for data loss. The integrated Veritas solution gives you the flexibility to recover any application from a ransomware attack based on RPO and business requirements, reducing data protection costs while providing confidence in recovery.

Detection

Veritas Data Insight is a complementary solution that provides the analytics, tracking and reporting necessary to deliver organizational accountability for file use and security. Data Insight software includes anomalous behavior detection, custom query templates and file extension identification that can all be used to detect and alert on ransomware. Data Insight can:

- Detect and alert on anomalous applications or compromised accounts based on data usage. It does so by identifying deviations in read, write, create, delete, security and file counts for each user. It compares historical data it has collected and looks for statistical standard deviations to help detect anomalous behaviour and identify accounts that might be compromised due to ransomware.
- Find ransomware files based on metadata.
- Find the duplicates of the ransomware executables.
- Use built-in ransomware templates to find and review impacted files and compromised accounts. These custom templates can capture counts of activities such as file, folder and extension renames as well as writes performed on the files by each user. If the count is higher than the specified threshold value, then the files on which the activities occurred could be exploited.

When an issue is identified by Data Insight, you then have visibility into the potential threat as well as how the threat is embedded into your environment. At this point, you need a mechanism to correct and resolve the threat. Veritas provides a variety of recovery options that can be used based on the nature of the threat:

- Data Insight can lock down the suspicious account and restore data using custom integrations.
- Restore to a specific point in time using checkpoints.
- Recover systems from backups.
- Run a rehearsal operation in isolation where you can resolve the issue and clean your environment with no impact on production.

Recovery Solution

Robust data replication is key for maintaining application availability and resiliency both locally and across sites; however, replication alone does not protect your applications against data corruption or ransomware attacks. Figure 3 shows the effect of a ransomware attack on data replication.

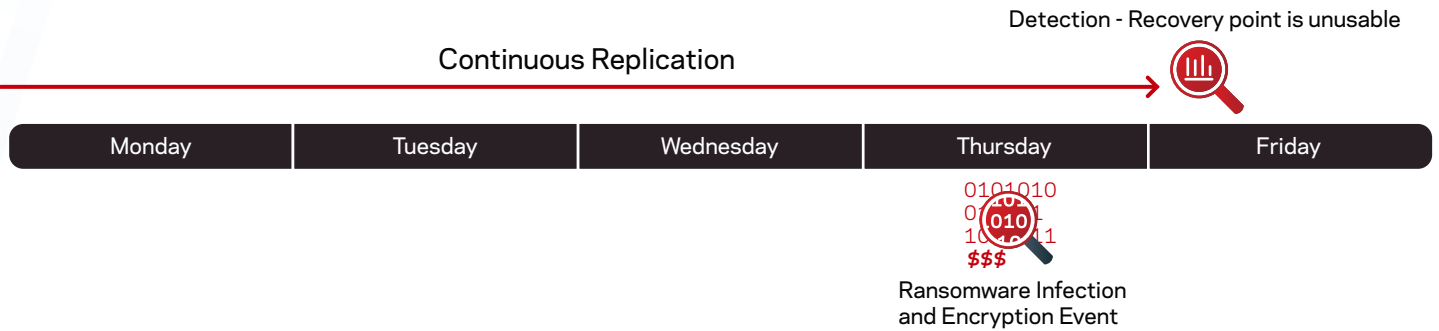


Figure 3. The effect of a ransomware attack on replication.

Data replicated between a source and target location is rendered unusable by the ransomware event and can no longer be used for recovery. You now need to recover your applications using a different recovery solution. One option is to recover your applications from their most recent uninfected backup copy. Figure 4 shows this process.

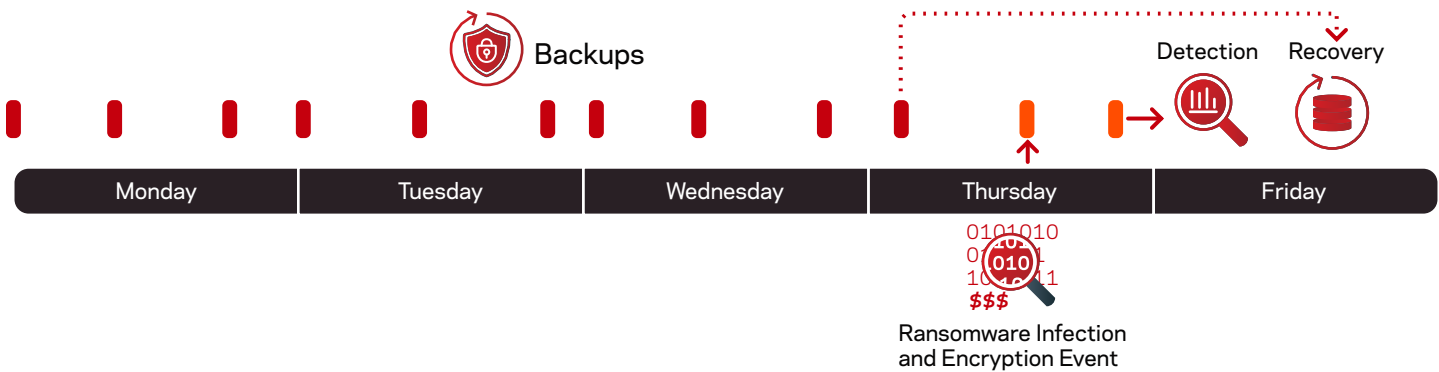


Figure 4. Recovering from a ransomware attack using uninfected backup copies.

Although restoring applications from backup copies can be an effective solution for recovering from corrupted data or a ransomware attack and may be suitable for applications with higher RPOs, it leaves applications with low RPO requirements at risk of data loss, which can be costly and disruptive to your business. Veritas provides an advanced option that creates multiple frequent checkpoints from a live data replication stream that can be used to recover from data corruption or ransomware attacks. When a ransomware threat is detected, you can recover using the latest uninfected checkpoint. If the issue is data corruption, the frequent checkpoints allow you to recover with much better granularity. Having frequent checkpoints significantly reduces the gap between when your data is corrupted or infected and the last good recovery point. Figure 5 shows the continuous stream of checkpoints and reduced gap between recovery points.

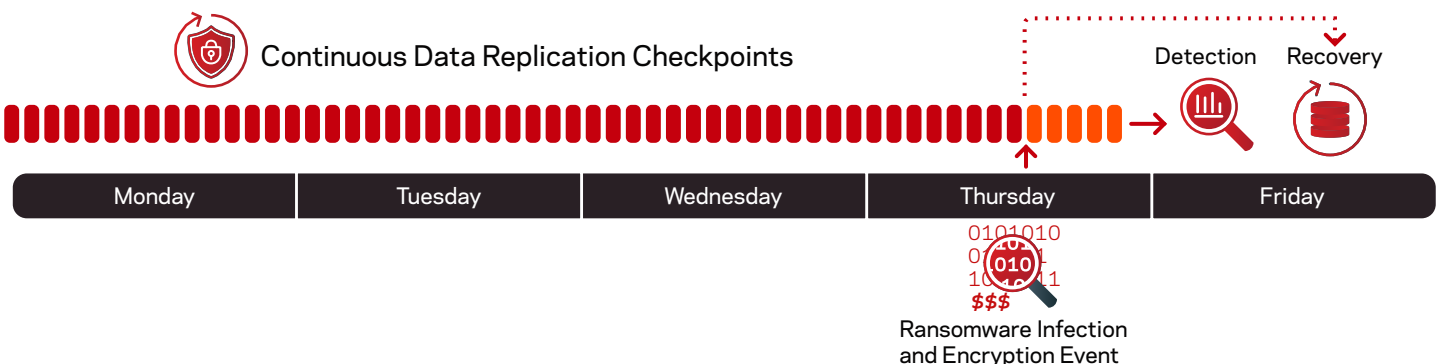


Figure 5. Recovering from a ransomware attack using checkpoints.

By intelligently integrating replication, backup and continuous checkpoints, you have the advanced protection model needed to successfully recover any application with nearly any RPO requirement from a data corruption scenario or a ransomware attack—efficiently and with minimal data loss.

Flexibility

The integrated Veritas solution is compatible with nearly any IT infrastructure. It provides availability and resiliency for the entire suite of business applications, regardless of where and how the applications are deployed. This capability gives organizations the flexibility to run applications on the platforms best suited for their requirements without being locked into specific technologies. You can reduce costs by more efficiently using existing backup data when incorporating backups into the overall resiliency solution.

You can also manage resiliency without having to mirror system configurations across sites. For example, a production site may have different infrastructure and system configurations than a site used for disaster recovery (DR). In this scenario, Veritas ensures your environment is still highly available and resilient while also maximizing resource utilization and reducing overhead.

Platform-Independent Resiliency

Modern IT applications can often benefit from leveraging different platforms to achieve optimal performance and utilization. No matter where or how your applications are deployed, Veritas provides several options for how to make them highly available and resilient (see Figure 6). Whether you're looking for on-premises, hybrid cloud or cloud-only resiliency, Veritas can accommodate nearly any deployment architecture:

- High availability for almost any operating system and platform across local and geographically separated sites.
- Support for bi-directional resiliency for physical and virtual systems on-premises or in the cloud.
- Multiple supported public cloud platforms, including Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform.
- Automated recovery of backup images into live systems in public cloud environments.

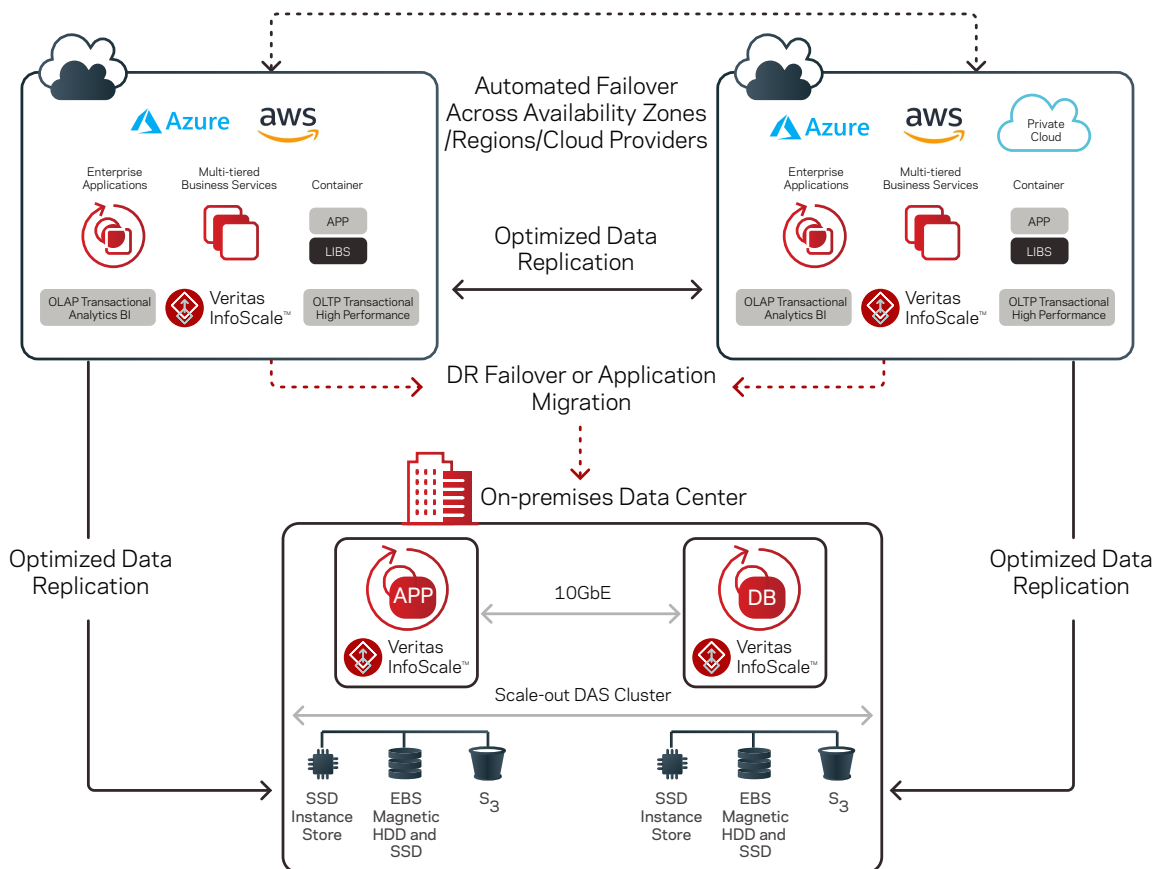


Figure 6. Veritas provides platform-independent resiliency.

With multiple options for how to achieve availability and resiliency with a single solution, you have the flexibility to manage availability and resiliency based on the business value and risk associated with application downtime. This flexibility helps you manage costs and provides a consistent user experience.

Cloud Integration

The cloud has changed both the economics and the approach to IT resiliency. The cloud has effectively eliminated the need to build a second data center dedicated to DR purposes, which allows you to cost-effectively use the cloud as a resiliency and recovery target. Although cloud services offer attractive SLAs, it's important to understand they are not application aware and running your applications in the public cloud doesn't eliminate the risk of downtime or data loss.

Veritas provides automated, application-aware availability and resiliency in the cloud. InfoScale can fully manage mission-critical applications that are orchestrated by the integrated Veritas solution. InfoScale manages high availability in the cloud with customized agents for mission-critical applications. It also provides storage management capability with enterprise storage features and performance using native cloud storage services. You also have advanced application mobility, so you can move applications and data between cloud zones, regions and between different public cloud services.

Both Resiliency Platform and NetBackup can manage cloud resiliency for non-mission-critical applications with advanced functionality that supports a wide variety of RPO and RTO requirements, including:

- Automated near-real-time replication and recovery for physical and virtual systems into a cloud environment.
- Recovery and conversion of NetBackup images into live systems in a cloud environment.

Veritas provides a cloud recovery feature—an innovative option for recovering on-premises system backups in the cloud. It lets you manage the restore of NetBackup images to the cloud without having to deploy or manage NetBackup infrastructure in the cloud environment. This option gives you the flexibility of cloud-based infrastructure that can be provisioned on-demand and used only when it's needed. Cloud recovery of backup images enables a cost-effective hybrid resiliency strategy and is also an excellent option for cloud migration using existing backup images with minimal resources required. Figure 7 shows this process.

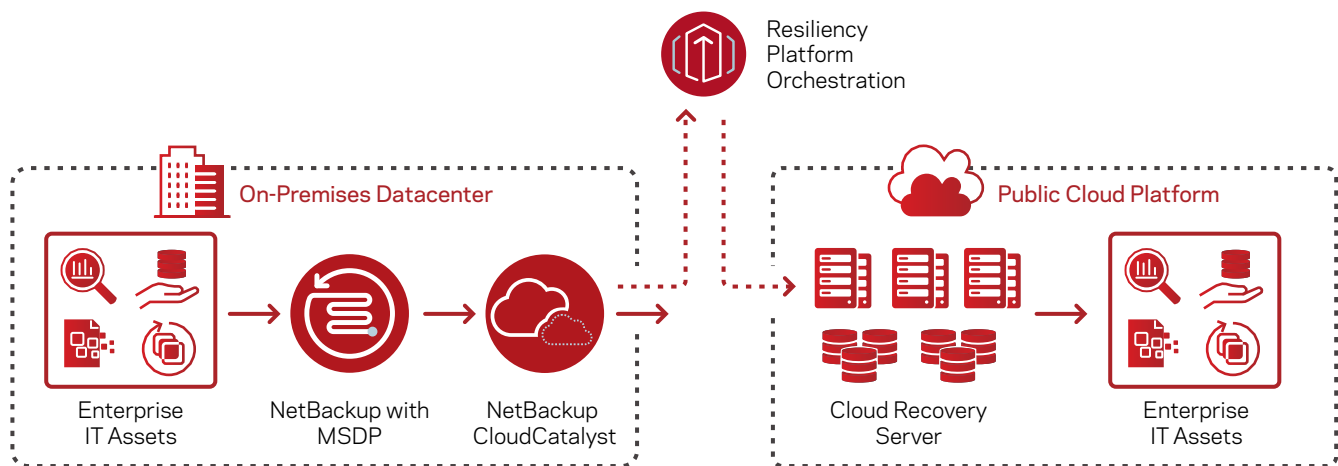


Figure 7. Automated cloud recovery using NetBackup images.

Automation

Enterprise IT resiliency typically involves multiple systems, processes and geographic regions. Without automation, managing resiliency can be time-consuming and error-prone. Veritas helps reduce the need for manual processes and provides several intelligent points of automation for the IT resiliency process that help ensure predictability and reliability, maximizing uptime for your applications. You can even include custom applications that require direct interaction with scripts or other application-specific tools as part of an automated resiliency plan. You can design and build automation plans to manage several resiliency scenarios:

- **Resiliency plans**—Provide the ability to create a customized, automated workflow consisting of a specific set of tasks such as starting, stopping, migrating and taking over application operations and virtual business services. You can also include DR Rehearsals as part of a resiliency plan.
- **Evacuation plans**—Provide the ability to takeover applications, systems or virtual business services for an entire data center and bring them online in a secondary data center (either on-site or in the cloud) in the event of a site loss or evacuation.

You can configure both plans easily and intuitively using the centralized user interface and can include individual systems, applications and virtual business services that manage complex, multitiered applications and all their dependencies as a single business service.

Figure 8 shows an example of a resiliency plan.



Figure 8. An example of the resiliency plan for automated failover of an IT business service.

Service-Level Management

As systems and applications become more complex and interconnected with multiple tiers and dependencies, managing the availability and resiliency of the overall service they provide to users can be difficult.

The Virtual Business Services feature is unique in the market. It allows you to manage high availability and DR for multitiered applications as a single consolidated entity, even when there are different system types, RPOs and RTOs for the individual application tiers. Using Virtual Business Services, you can completely automate the recovery or migration of a complex, multitier application and the business service it provides.

Virtual Business Services manages dependencies between application tiers as well as the order in which the applications and their components are brought online in a start operation and taken offline in a stop operation. The feature is aware of the overall business service provided by the application tiers and can take the appropriate action in the event of a failure to restore the entire service, enabling faster recovery and minimal downtime, with no manual intervention.

Figure 9 shows an example of how Virtual Business Services can manage multitier applications as a single logical business service.

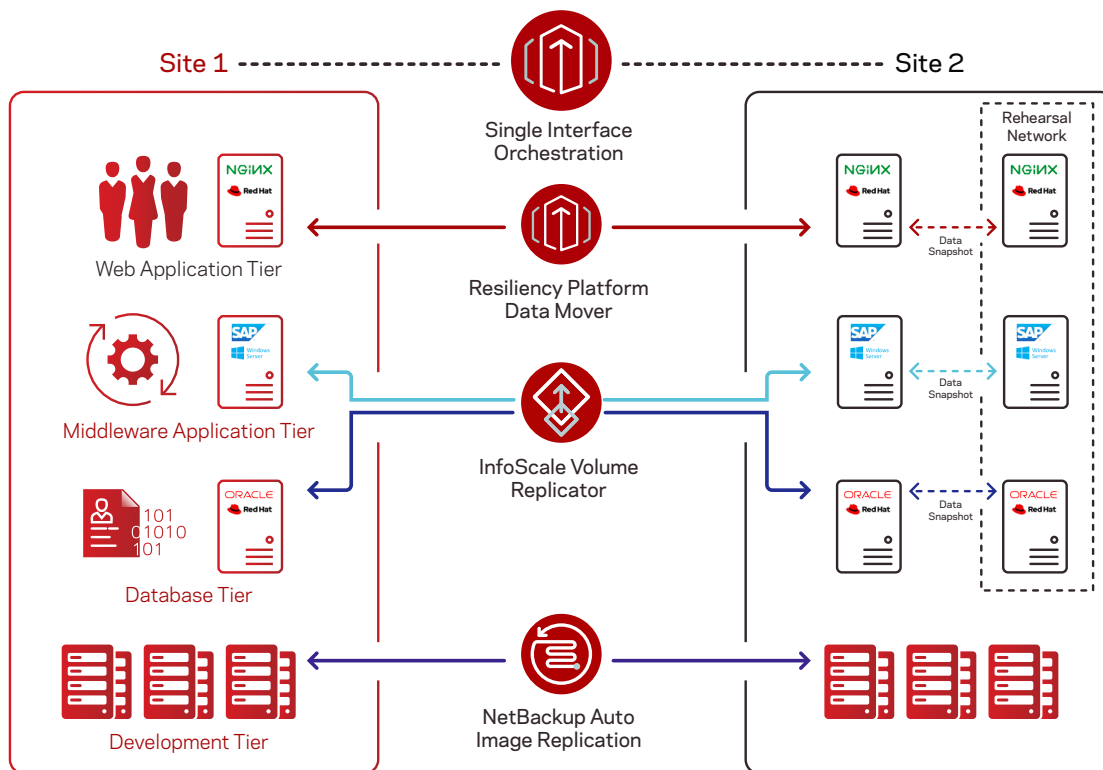


Figure 9. An overview of using the Virtual Business Services feature with a DR rehearsal.

Visibility

A key advantage Veritas delivers is the ability to visualize the resiliency status for all applications in the organization, regardless of how they're protected. The resiliency console is a centralized interface that shows resiliency and availability status and information for all protected applications and systems. The console also provides a map view that shows the physical locations of the protected applications and systems, giving you full insight into multi-site, geographically dispersed resiliency (see Figure 10).

Reporting

Centralized reporting on system information and resiliency status is available in the centralized user interface. You can include all the availability and resiliency information displayed in the user interface in reports that you can download and automatically distribute within the organization. This process helps eliminate operational complexity and increases confidence that your organization is well prepared for often-unpredictable situations. You can schedule and run reports on demand for all protected applications. Business-level reports help prove compliance and service objectives while delivering confidence to business leaders of the resilient state of their business.

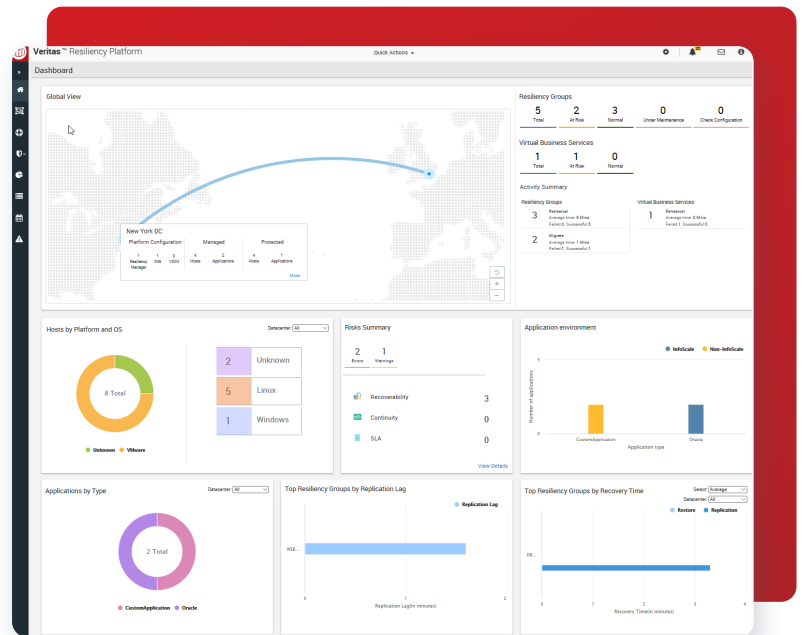


Figure 10. The Veritas resiliency console view of an organization's protected applications and systems.

Summary

Maximizing application availability and resiliency for modern, complex IT environments can be a significant challenge. With multiple applications and systems that have different usage profiles and SLAs, organizations are often burdened with having to use multiple independent products to meet availability and resiliency requirements. Veritas solves this problem by providing a continuum of availability that spans the entire suite of business application within an organization. Having a single point of control and visibility that can integrate with nearly any application within an organization has several key benefits:

- Single solution for overall availability and resiliency across an entire enterprise.
- Full range of availability and resiliency options for all types of applications.
- Intelligent automation that eliminates manual processes and maximizes application uptime.
- Automating full IT service restores from backups provides operational resiliency using existing backup data.
- Minimizes costs by choosing an availability and resiliency option based on your application's business value.

Veritas delivers broad platform support and can be used in nearly any environment with existing infrastructure while providing the flexibility needed to maximize the availability and resiliency of your IT business services. With the cloud becoming an increasingly common platform for delivering IT services, this integrated Veritas solution is available in public cloud marketplaces and is designed to help you with cloud migrations, data protection, high availability and resiliency in cloud environments. Whether on-premises, in the cloud or both, Veritas provides a unique solution that efficiently manages availability and resiliency for your entire organization.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

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

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