VERITAS

Preparing to Protect the Future

STAY AHEAD OF THE GAME

Data protection and recovery isn't a race, but a journey along an often-winding path.

Threats to your data are increasing and evolving, with bad actors developing new ways to attack and gain access to the lifeblood of your operations.

Data protection has evolved from a line item to an evolving aspect of business culture with multiple moving pieces. The variety and location of workloads and the criticality of each application and its data are vital components in assessing the levels of protection you need and how you handle recovery.

Factors including high availability, governance, and compliance all play a role and affect recovery-time objective (RTOs) and recovery-point objective (RPOs).

Shadow IT and tech debt have exploded. Teams create overwhelming volumes of data and mistakenly leave mission-critical data vulnerable. Organizations lack full visibility of what is essential, making it hard to prioritize to mitigate risk.

With forward thinking and diligence you can stay ahead of the curve and remain prepared for potential challenges along the way.

Identify the Data You Have

How can you adequately protect what you don't know you have?

Vast numbers of apps and platforms promise to improve efficiency and deliver more effective data. Your employees start using these tools in silos, feeding customer information and company data into platforms that are likely located in the cloud. The result? A data sprawl dilemma and a multi-cloud coverage problem.

Bad actors can infiltrate this data because it is not properly covered by the company. Suspicious behavior can go unnoticed because the IT team is unaware they should be watching it — or even that it exists. If disaster occurs, you may learn that critical information hasn't been backed up properly and isn't recoverable.

Additionally, there is the problem that if disaster occurs the information is critical and it may not be backed up properly and may not be recoverable.

Data sprawl is a governance challenge that requires more structure and employee training in addition to improved visibility into the company infrastructure.

To create more successful outcomes, put context around data and gauge risk around complex procedures to decide how to execute the backup and recovery strategies of the edge, core, and cloud.

Key Questions:

- What data do you have and where does it live?
- How does it improve visibility into our data?

Veritas Solutions

Veritas Data Protection Solutions deliver data protection at scale. The AI-powered anomaly detection engine helps mine enormous amounts of data, automate monitoring and reporting, identify actionable insights, and establish early warning of potential attacks.

Veritas Analytics Solutions help cross-reference servers and storage with all your backup vendors to ensure nothing falls through the cracks and is left vulnerable. It can scan and monitor all systems including third-party products to help eliminate blind spots.

Veritas Data Insight can help you discover the potential of reporting while enabling detection of potentially harmful data, revoke access to delicate data, and collaborate with data owners for better decision making and adherence to compliance standards. Spotlight risks, unearth dark data, and record user activity for numerous activities to uncover activity patterns to identify and detect anomalies.

Keep the Bad Actors Out

Cyber criminals know that people are the weakest points of your network.

Most cyberattacks and data breaches are a result of human interaction and lack of attention. That's why phishing is so effective.

How do you prevent an attack? Elements including identity and access management and encryption are vital protection measures. You can reduce the chances of a successful attack by implementing multi-factor authentication and role-based access control. Encrypting data at rest and in motion reduces the usability of your data and helps protect against data exfiltration. Things like smart-card authentication, single sign-on, and privileged access management help reinforce the "least privilege" principle of Zero Trust.

Layered prevention and protection strategies use multiple solutions implemented at multiple levels. You can (and should) issue digital certificates to devices for further authentication. Use dual authorization for access to backups as one more layer.

Managing secure access and protecting your data against misconfiguration is of the utmost importance. Identifying and understanding the resources, actions, and identities in your environment is crucial to manage privileges and enforce appropriate permissions whether you are on-premises or in the cloud. Tracking and monitoring attempts and the progression of changes helps you enhance your security posture and make real-time improvements.

Key Questions

- What are we currently doing to prevent breaches from phishing and malware?
- Are there ways we can improve upon our current protection measures?

Veritas Solutions

Veritas Data Protection Solutions are vendor-agnostic and built on the foundations of Zero Trust. It helps secure your network, protect data in transit and at rest with AES 256-bit encryption, meet FIPS 140-2 certification, limit user access, and enable role-based access control and multi-factor authentication.

Veritas Data Insight offers near real-time visibility into production data to help identify ransomware based on anomalous user behavior and known ransomware extensions. It can also discover over-exposed data to limit and reduce attack surfaces.

Veritas Analytics Solutions offer a single, unified dashboard with operational insights and intelligence to help identify ransomware, unprotected systems, and backup anomalies. Use them to optimize storage, decrease costs, and stay on top of compliance and regulatory requirements.

Veritas Alta™ Classification removes obstacles preventing you from achieving data security and compliance. Gather meta data attributes and user-behavior forensics for actionable intelligence; identify data ownership, usage, and access controls; and mitigate data privacy and security risks.

Identify Your Critical and Vulnerable Data

Your data isn't static, your strategy and solutions shouldn't be either.

Make sure you implement products and services that are scalable and ready to adapt. Flexibility is crucial to delivering performance under pressure with multiple integrations across multiple clouds.

It doesn't make sense to assume that a company will purchase every solution from a single vendor on a single invoice. Business development doesn't function that way: It's messy and involves combinations of older, legacy software and technology with newer, more sophisticated solutions.

Prioritize the data and identify what level of compliance and regulations you need to meet. Decide how to manage backups and ultimately how to handle the scaling and size of backups that ultimately influences recovery time. Understand how your bandwidth capacity affects your backup and recovery so you can shape how to most efficiently back up and recover critical workflows.

Key Questions

- What data is most important to "keeping the lights on"?
- How do we prioritize our data backups?

Veritas Solutions

Veritas Data Protection Solutions are vendor agnostic and offer a solid retention and protection workflow that is cost-effective and easy to deploy and manage. Simplify and organize into a single platform across multi-cloud and hybrid cloud environments.

Veritas Alta™ Shared Storage is designed to power your business-critical applications and deliver enterprise-grade shared storage with superior performance and resilience while keeping costs down. It enables application and infrastructure admins to secure sensitive data. And it offers encryption; write-once, read-any capabilities (WORM); consistent snapshots; and database acceleration.

Veritas Alta™ SaaS Protection allows you to retain access to data stored in Microsoft 365 accounts after employee departure without having to maintain—and pay for—the extra license. Restore folders, mailboxes, or sites with granular, multi-level recovery to a preferred location, whether cloud or on-prem. Maximize performance and flexibility by scaling backup storage up to petabytes and billions of objects. Perform incremental backups more regularly to minimize RPO and RTO while implementing continuous data protection for site collections.

Make Data and Backups Available and Efficient

You've backed up your data. Why is it so hard to restore it when disaster hits?

Migrating large amounts of data (such as moving it to secondary storage), takes a significant amount of both time and computing resources. And you're not only doing it once, but if you're using the 3-2-1 backup rule, you're doing it three times to two different types of storage with at least one off-site for extra guarding.

Many things can derail a complete backup during migration, which is why high availability and failover are important. It's like pouring water from a pitcher into a glass; as one glass overflows, a secondary glass can catch the excess. Load balancing distributes a workload by assessing which system can handle your request. You can cluster multiple servers to ensure high availability and enable failover. If one server fails, another can take its place—and nothing skips a beat.

Key Questions

- Where do we have opportunities to improve our backup efficiency?
- How do we know if our backups are clean, free from malware, and uncorrupted?

Veritas Solutions

Veritas Data Protection Solutions cover the 3-2-1+1 backup strategy easily and add an additional layer of security with a built-in intrusion prevention system and an air-gapped isolated recovery environment for indelible storage and a built-in isolated, immutable data vault.

Veritas InfoScale helps reduce the attack surface for production data and isolates production data from I/O with snapshots and data mirroring. It also optimizes recovery for low RTO and RPO. Using automated scripting, you can run malware scans on the isolated volume to ensure it is malware free.

Veritas NetBackup Flex and Flex Scale applies an additional layer of security by eliminating multiple points of failure in hardware. They use clustering components to remain continuously available.

Veritas Analytics Solutions create a baseline of known successful backups, using it to compare future backups and help you spot anomalies. You can also classify backups by application to view restorability of all your apps from a single dashboard.

Protect Data with an Air Gap and Immutable Data Vault

How do you ensure that backup data is invulnerable to encryption?

Even if your company is diligent about backing up data, there is still the risk of human error and equipment failure. The risk of accidental deletion or modification is high.

Backups must be made in a way that ensures that the data can't be changed. Files stored in immutable storage can help you avoid the stress of corruption and cyber attacks.

Immutable backups offer the highest level of data protection for your business. Data permanence is an integral part of immutable storage, ensuring that files are not altered by accident or on purpose. This creates a more efficient and effective process within your cybersecurity and disaster recovery strategy and can help you avoid financial loss and downtime.

The additional layer of an air-gap solution ensures that your immutable backup data is isolated and uncorrupted so you can move forward with a clean restore of the data.

Key Questions

- How do we currently protect backups from corruption?
- Are there any compliance standards that require you to have an air gap and isolation for your data?

Veritas Solutions

Veritas aligns to the NIST principles to offer unparalleled immutability, visibility, fast recovery, and indelibility. It supports multiple methods for both onsite and offsite solutions including tape-based backups, cloud-based locked object storage, and efficient data storage in AWS S3 Object Lock.

Veritas Data Protection Solutions proactively block unwanted resource access behaviors before the operating system can act on them.

Veritas Flex allows you to implement an isolated recovery environment (IRE) with an immutable data vault and provide a secure copy of critical backup data from an isolated, immutable environment. The IRE architecture protects your important backups and provides a safe space that you can use to orchestrate a clean recovery or rehearse your cyber resiliency recovery plan. The Veritas infrastructure-agnostic virtual air gap offers an additional layer of protection and isolation to help thwart rogue attacks.

Define a Disaster Recovery Process

The ideal recovery solution supports every workload.

Create a process that incorporates easy integration, meets your desired RPO and RTO, supports all storage, and offers a consolidated dashboard of everything under protection. As you define your process, consider factors including the following:

- Orchestrated recovery (deciding in what order to recover)
- Intelligent deduplication
- Snapshot integration
- Storage tiering
- Automated replication of images, catalogs, and snapshots to on-premises and cloud storage
- Container support
- Data insight and analytics
- Security and compliance for both on-premises and flexibility in the cloud
- Ensure that your data and backup systems are protected with encryption

Harness the power of Zero Trust, multi-layered data security, and intelligent automation to ensure business operations stay resilient. Unlock multi-cloud intelligence and upgrade cyber defenses while cutting costs and utilizing integrated solutions. Minimize your costs and stay compliant with evolving regulations by consolidating backup and recovery for cloud-based workloads, automating workload migration, and implementing hassle-free disaster recovery with single-click recovery, custom scripting, and rehearsals.

Key Questions

- How long will it take me to recover?
- What is the priority of recovery?

Veritas Solutions

You can choose between bare metal recovery or granular file recovery if only a portion of your files have been compromised. We also offer instant rollback for VMs to recover and concurrently roll back hundreds of VMs in minutes.

Enhanced data resiliency and Veritas Resiliency Platform allow you to assign different recovery priorities across applications and to recover multi-tier apps in a sequence according to business criticality. Continuous data protection checkpoints enable low RPO recovery.

Veritas NetBackup Flex and Flex Scale have a hardened operating system, Zero Trust architecture, and immutable and indelible storage. The IRE and immutable data vault offer an isolated, air-gapped solution that is not discoverable from the outside. Malware and anomaly scanning provide confidence that your backup data is clean so you can recover instantly regardless of environment, on-site or in the cloud.

Rehearse Your Resiliency

Rehearsing isn't about restoration; it's about avoiding downtime.

Cybercriminals hope that your organization, like most, is not optimized for recovery. They want maximum damage and downtime to ensure payment of ransoms. If you are ready and rehearsed for recovery, then you're already a huge step ahead. To get to rapid recovery, you must have a cybersecurity response plan for your entire environment that includes testing early and often. Regular rehearsal and exercise of your recovery help limit downtime and disruptions and reduce the impact of an attack.

As the demand for hybrid and multi-cloud systems rise, you need the ability to manage multiple frameworks as well as coordinate multiple clouds and storage systems. Teams are tasked to manage and scale multiple servers and applications.

Take advantage of automation to manage the complexity of your environments, identify potential threats, and manage rehearsals proactively to ensure continual readiness and minimize downtime.

Key Questions

- How do I reduce downtime?
- How do I speed up remediation?

Veritas Solutions

Veritas NetBackup Flex and Flex Scale maximizes the potential of data protection with easily expandable architecture. With multiple layers of immutability, automated provisioning, and load balancing, you can deploy a complete turnkey data protection solution.

Veritas InfoScale and Veritas Alta™ Application Resiliency address not only whether your setup is working, but if it's working well enough. It is a comprehensive infrastructure solution designed to maximize availability and disaster recovery through tight integration with critical business applications to ensure maximum uptime and failover. An all-encompassing platform, it provides flexibility to customize protection levels depending on industry demand with features including:

- Data-integrity compliance
- Automated runbooks for multi-tier applications to reduce manual efforts
- Mobility that allows workloads to move between platforms effortlessly
- Seamless integration with traditional systems and environments

Optimize Your Backup and Recovery

Ease the challenge of managing data protection across the organization.

Data orchestration is the answer for identifying bottlenecks and understanding where your most time-consuming processes are. Orchestration can help save time by automating processes including server provision, database management, and applications. Use it to handle tasks including scanning for vulnerabilities, searching for logs, and even helping connect security tools and integrate systems so teams can avoid becoming overwhelmed with tasks.

Choosing the right solution can make managing data easier, but it's an ongoing challenge.

Access to the right analytics provides visibility into the essential elements of your environment. Dig deeper and you can also identify what is underutilized, mis-configured, or un-indexed, helping IT address issues and identify resources to re-purpose to achieve cost savings.

Uncover actionable insights to improve your utilization, performance, and resiliency while predicting failures and identifying proactive recommendations to mitigate risks to service level agreements (SLAs).

Intelligent automation can help you eliminate the inefficiencies of manual processes and unlock endless possibilities.

Implement and deploy agile, secure backup and recovery for complete data protection and optimization.

Streamline resources, reduce costs, and monitor your entire network from edge, to core, to cloud through one comprehensive console view.

Veritas Solutions

Veritas Data Insight enables you to analyze activity and provide in-depth analysis of usage and collaborative activity. It can help classify users and better understand activity patterns; identify data that is duplicated, stale, or orphaned; and leverage risk scores to assess potential threats and prioritize high-risk data. Create detailed audit trails and leverage integrated file analysis, data loss prevention, and archiving with Veritas compliance solutions.

Veritas Analytics Solutions help quickly identify applications and services at risk. Recover more quickly by gaining the ability to monitor and optimize backups across all environments and efficiently locate affected hosts by location, environment, or application.

Key Questions

- Is your data optimized for quick recovery?
- Do you understand your SLAs?

Close the Gaps in Your Cybersecurity Strategy. Learn more >

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 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

V1812 06/23