VERITAS

Six Fundamentals of Business Resilience

Build the foundation for reliable data protection

Reimagine Your Backup Strategy to Ensure Reliable Data Protection

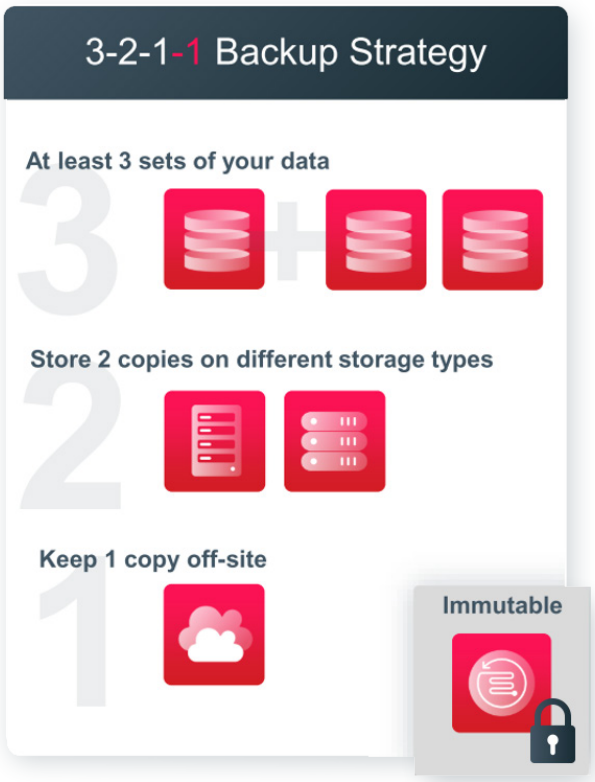
No matter the size of your organization, eliminating silos, controlling data, and protecting against IT threats and cyberattacks requires continuous data protection. Manage risk and reinforce data protection by setting up a backup and data management strategy.

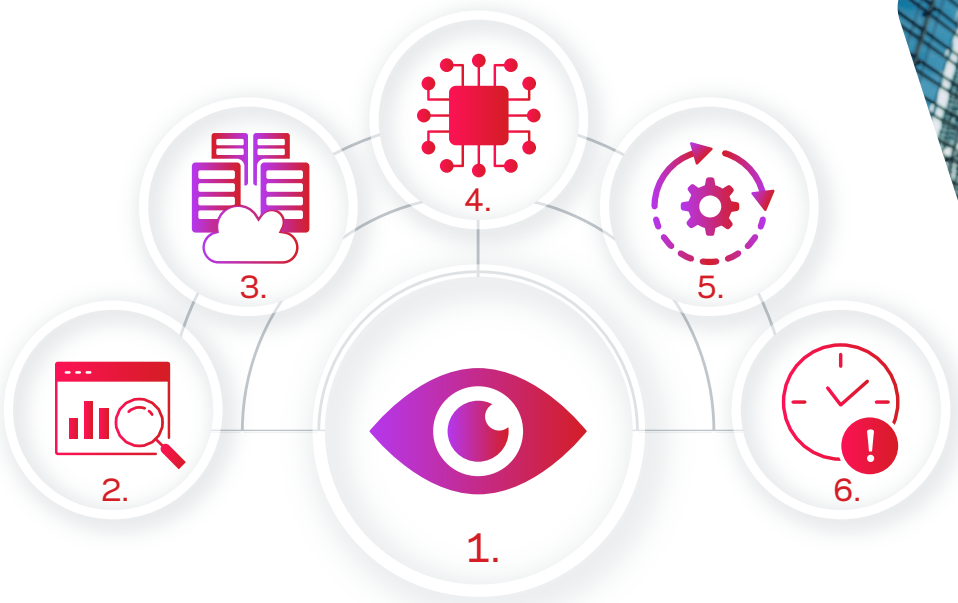
The 3-2-1 backup rule is a commonly referenced data protection strategy. It recommends three backups, saved to two different storage types, with one stored off-site.

While 3-2-1 simplifies explanation, the approach is more than a decade old and isn't enough for business resiliency in today's ever-evolving environment. Likewise, most organizations have hybrid data-storage approaches, so they already have different storage types, including off-site to at least one cloud service provider (CSP).

Ensuring data protection is now more about management than redundancy.

Complete business resiliency requires going beyond backup to ensure comprehensive coverage with automated policies. A proactive approach allows you control data-related risks through visibility into your data, storage, and backup infrastructure. To do this, establish a data resiliency strategy based on six fundamental actions.





FUNDAMENTAL 1:

Assess Your Data Footprint and Recovery Needs

How much data do you need to protect?

Chances are that your IT team and business units want to protect every bit of the data they collect and generate. And they want it available on demand. It comes down to economics. A good plan considers budget while optimizing data protection with the flexibility to adjust individual application protection levels as needed.

The rise in remote work has complicated infrastructure visibility. You may struggle to uncover and monitor dark data across new channels, including messaging and collaboration apps, file-sharing tools, and social media. Automate processes to capture, classify, and monitor all company data sources to maintain visibility so you can ensure compliance and governance over your data environments.

The compliance factor.

IT needs to create a careful balance. On one side is the need for business units to access data and work collaboratively. On the other are corporate and government requirements for customer data privacy as well as multi-regional and geographical access regulations.

Explore how to prevent your organization from obtaining and exposing sensitive data at veritas.com/solution/compliance.

FUNDAMENTAL 2:

Evaluate Critical Data and Applications

Once you have assessed your data footprint, define a plan that addresses your priorities and recovery objectives. In an ideal world, you are up 24x7, protecting all data from all sources.

Every application is important, but your operations can withstand longer outages for some applications without potentially catastrophic consequences. Prioritize each application's criticality according to tolerance for data loss and time to recovery.

- Recovery point objectives (RPOs) refer to how much data you can bear to lose.
- Recovery time objectives (RTOs) refer to how long an outage you can tolerate.

Table 1 shows standard service level agreements (SLAs) with their corresponding periods of acceptable downtime or unavailability, including planned maintenance and unplanned (disasters).

Implementing a single availability solution across your IT infrastructure allows you to increase application uptime and optimize performance by orchestrating mission-critical services across all physical, virtual (including containers), cloud, and on-premises environments.

Table 1. Standard SLA Goals and Corresponding Downtime

Uptime/Availability Percentage	Downtime per Year	Downtime per Month
99.9% (three nines)	8.76 hours	43.2 minutes
99.99% (four nines)	53.6 minutes	4.32 minutes
99.999% (five nines)	5.26 minutes	25.9 seconds

Reliable uptime and availability of critical data and applications are essential to operational resilience. They're also vital for compliance with global regulations such as GDPR, NIST, and DORA.

Once you know where your data and your sources are, you can safeguard them with multiple layers of protection to reduce the attack surface and limit access.

What is DORA?

The Digital Operational Resilience Act includes rules and standards focused on operation resilience to mitigate information and communications technology (ICT) risks for financial entities. It includes frameworks for risk management, resiliency testing, sharing threat intelligence, incident reporting, and audit access. Published in late 2022, the new European Commission regulation is set to take effect January 17, 2025.

Learn more about proactive approaches to ensure predictable availability, application resilience, and storage efficiency across multi-cloud, virtual, and physical environments at veritas.com/solution/high-availability.

FUNDAMENTAL 3:

Implement Immutable, Indelible, and Isolated Storage

With oversight of your infrastructure and defined goals for availability, you can identify where to store protected datasets. The traditional 3-2-1 backup strategy suggests you need three sets of data in two storage types, but those storage types should depend on the workload you want to protect.

Tape: While tape has its place—very low-cost media, off-site storage—many organizations are choosing other options due to operational challenges. Disk-based, on-premises, long-term retention, and archival storage often have a similar total cost of ownership and greatly improve RTO and operational efficiencies.

Backup Appliances: Purpose-built backup appliances alleviate many deployment burdens and can perform deduplication in the device itself.

Long-Term Retention and Archival Appliances: You likely must address regulatory constraints that mandate long-term data retention (LTR) and may require on-premises storage. Purpose-built LTR appliances have similar performance characteristics to primary storage yet are cost-optimized to compete with the economics of tape and cloud.

Cloud Storage: With the increase of virtualized workloads hosted at cloud providers such as AWS, Azure, and Google, organizations look to cloud storage to protect those workloads. And cloud storage can meet your needs if you don't have an off-site location for protecting on-premises workloads.

In addition to traditional storage types, new services are becoming available. Veritas Alta™ Recovery Vault, a fully managed, cloud-based data retention service, removes the complexity of cloud data retention and data management in the cloud.

Optimizing and managing backup storage methodologies is an ongoing challenge. Choosing a recovery solution that is secure by default can ease the burden.

Beyond storage types, consider the security of the options. Safeguard your data from tampering by implementing immutable and indelible storage to ensure that no one can change, encrypt, or delete data for a determined length of time—or at all.

- Immutable backup or storage refers to fixed, unchangeable, and undeletable data, which is impervious to ransomware infections. Available options include optical technology, purpose-built backup appliances, enterprise disk arrays, and the cloud.
- Indelible backup or storage refers to data that cannot be removed or exfiltrated through unauthorized data transfer, export, or copy. For example, Veritas write-once, read-many (WORM) storage includes a timestamp with the image metadata to indicate when the retention period expires, meaning users cannot overwrite or delete the data.
- An air-gapped isolated recovery environment enables secure backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators with a clean set of files on demand to neutralize the impact of a ransomware attack.
- Zero Trust principles describe a "never trust, always verify" approach. In selecting a storage target with zero-trust practice, consider identity and access management (IAM) for users and machines, encrypting data both in-flight and at-rest to reduce exfiltration, limiting access to backups, and implementing security analytics to monitor for—and mitigate—malicious activity.

The Veritas data protection platform will encrypt data, in-flight and at-rest, along with the newly introduced encryption crawler. Since more recent backups may reference older unencrypted data, the crawler scans storage and secures older data with encryption.

Another best practice for securing your storage target is to address how to limit excessive or expired data your organization may have forgotten. Even if you're not actively using the data, it can still be an attack vector, leak personal identifiable information (PII), or result in an unnecessary increase in cloud storage costs and compute resources. Now is the time to implement storage options with source and target deduplication and data lifecycle management.

Explore how data protection services can help you ensure your data is always secure at veritas.com/solution/data-protection.

FUNDAMENTAL 4:

Adopt Activity Detection and Malware Scanning

Next, implement tools that detect abnormal data and user behaviors or activities. Establish concrete and automated measures to alert you if anything out of the ordinary happens anywhere in your environment. It is vital to know immediately of anomalies in your data environment. For example:

- Unusual file-write activity that could indicate infiltration
- Known ransomware file extensions
- Abnormal file access or traffic patterns
- Code downloads
- Access requests
- Capacity surges or activity spikes
- External traffic paths

Combining the storage target recommendations with detection and scanning tools will provide greater control of your infrastructure. Coupled with Veritas Analytics and Insights solutions, you can monitor for data exfiltration, unauthorized data transfer, export, or copies taken from a device. Scan and assess primary data sets, backup, and any unstructured files to identify your data liabilities and risks—all the way to user behavior and exactly which account read the data. Then take the necessary steps to investigate using a pre-built remediation workflow.

78%

increase in ransomware attacks in the past year[1]

FUNDAMENTAL 5:

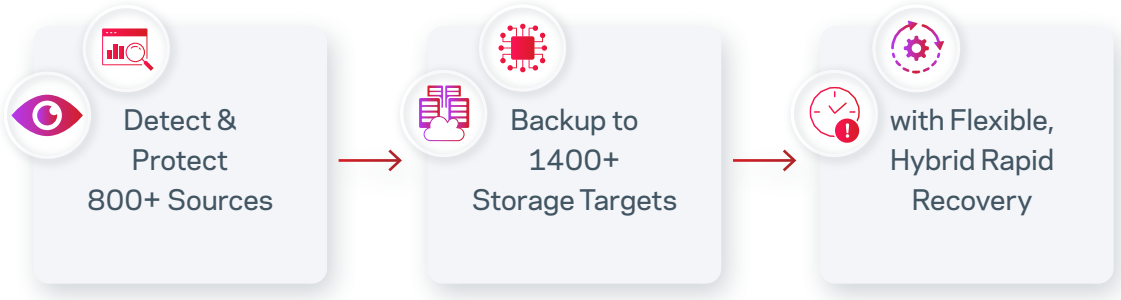
Optimize for Flexible Recovery at Scale

Data protection is about more than a restore point, a single backup copy, or multiple copies. Resiliency and rapid data recovery are the goal. You must architect an optimized and simplified recovery experience that will help you restore operations quickly, even at scale.

Optimizing recovery requires careful planning, orchestration, options to recover to alternative locations, cross-functional alignment and training, storage deduplication efficiencies, plus global visibility and oversight. Veritas solutions provide backup recovery and options that offer flexibility and choice in the event of a cyberattack or disaster.

Why are these elements important? Sometimes everything is impacted and you may need to recover an entire data center in the cloud, on-demand. If only part of your environment is affected, granular file recovery lets you select individual databases and files to recover quickly. If entire servers are encrypted, or you need to recover a large amount of VMs back to production, bare-metal recovery will enable you to recover the entire server quickly. With the flexibility of cloud object storage, many applications are built to run specifically in cloud object stores.

Veritas Alta Data Protection includes the ability for backup and recovery in cloud object stores in Azure, AWS, GCS, HCP, IBM, COS, Ceph, and others.



Without the right technology to surface such intelligence and optimize operations, you have to rely on manual oversight. Unfortunately, people are often your weakest link, especially in environments where swift and data-driven decision-making is critical to achieve business and operational goals.

Autonomous Data Management

Veritas is designing data management for the modern, digital enterprise that self-provisions, self-optimizes, and self-heals in multi-cloud environments.

- **Self-provisioning** assigns appropriate protection policies and deploy data-management applications and services without human involvement.
- **Self-optimizing** adapts and adjust protection policies and data-management services based on the environment, using AI and machine learning.
- **Self-healing** identifies, predicting, and repairing data-management service faults or performance issues.

Autonomous operation creates a more performant, secure environment by eliminating the manual steps and protecting the application without additional actions from the app developer or the data protection team.

Data Insights and Compliance

In addition to optimizing for disaster recovery, be sure to consider how to optimize for compliance with cloud-native agility. Capture corporate data across communication and collaboration platforms for seamless migration, archiving, and automated identification of key content to meet data governance requirements efficiently.

Learn more about synthesizing intelligence across unstructured data sources to minimize business risk at **veritas.com/solution/compliance**.

$812,360

average ransom paid by mid-size organizations[1]

FUNDAMENTAL 6:

Orchestrate Non-Disruptive Rehearsals and Recovery

Cybercriminals hope that your organization is, like most, missing a backup recovery plan. They want to exact maximum damage and downtime to ensure you pay their ransoms. You're a huge step ahead if you've rehearsed for recovery.

Rapid recovery requires a cybersecurity response plan for your entire environment that includes testing early and often. Regular plan rehearsals help to limit downtime, minimize disruptions, and reduce the impact of an attack. Veritas simplifies and makes it more efficient to execute non-disruptive tests with automated and assured rehearsals, while leveraging non-production resources such as network-fenced and sandbox environments.

We suggest that you rehearse recovering everything—not just a subset of applications. Include elements such as your name service, authentication, system time, and other infrastructure services. In a real situation, you'll most likely need to recover most—or all—of your production environment.

Regular rehearsals and validations are vital for success: When you are in crisis mode, the plan just needs to work.

$1.4M average cost to remediate an attack[1]

Create a Cycle

Complete business resiliency requires vigilance. Set a schedule or triggers for reevaluation to ensure that your plan continues to meet your visibility, protection, availability, recovery, and compliance requirements.

No matter the size of your organization, we're uniquely equipped to help you conquer the complexity of managing and protecting your business-critical data with the most comprehensive data-management platform available.

Veritas Alta

Take control of enterprise data resiliency. Veritas Alta brings together a robust offering that will scale with your data-protection needs and provide flexibility to control your workloads across any cloud, at any scale. Purpose-built for modern applications and workloads, and engineered to achieve optimal security and performance at scale across any environment, including multicloud, hybrid, public, private, edge, or on-premises. No other solution enables you to take such complete control of your enterprise data and applications in the cloud.

Reduce risk, eliminate uncertainty, and maintain control. Connect with our Veritas team to learn more about how our solutions can ensure your entire enterprise data resiliency cycle.

Close the Gaps in Your Enterprise Resiliency Strategy. Learn more >

1 The State of Ransomware 2022, Sophos, April 2022

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

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

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

V1796 04/23