VERITAS

Secure cloud data and ensure your applications are resilient

THREE MUST-HAVES FOR ENSURING YOUR SAAS APPS AND DATA ARE SECURE.

Contents

With businesses like yours increasingly aiming to deliver more agile, flexible workplaces, software-as-a-service (SaaS) applications have quickly become the norm. A cloud-first approach to digital transformation means organizations are using a wide range of workloads across public and private cloud infrastructures.

But while SaaS providers safeguard their platforms, the Shared Responsibility Model puts you in charge of protecting and backing up the data you've stored within the applications. Fail to do so, and you could be exposed to anything from accidental deletion and malicious attacks to data corruption and insider threats.

Inadequate cyber resiliency means you won't be able to respond or recover quickly from cyber incidents, putting you at risk of prolonged downtime, financial losses, legal implications, decreased productivity, and damage your reputation and customer trust.

In this guide, we'll explore three of the must-haves of SaaS security—backup and restore, regulatory compliance, and minimizing downtime and data loss.

17.7%

SaaS spending is projected to grow 17.7% from 2023 estimates to $232 billion by 2024.[1]

Must-have 1

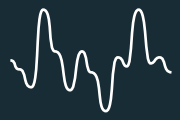
Build an effective SaaS backup and recovery strategy

Under the Shared Responsibility Model, it falls on you to protect the data you store within SaaS apps. So, your data isn't immune to risks, and without proper backup and recovery mechanisms, you face potential loss of critical data. This can lead to operational disruption, compliance issues, and reputational damage.

75%

of organizationswill adopt a digital transformation model predicated on the cloud as the fundamental underlying platform by 2026, according to Gartner predictions.[2]

Here are some of the things you must consider in your SaaS data backup to ensure data integrity and minimize the risk of data loss:



Regular Frequency

Determine the appropriate backup frequency based on the volume and rate of data changes. Strive for a balance between data protection and operational efficiency.

Redundant Storage

Use backup storage options that ensure redundancy and geographical diversity. These reducethe risk of data loss due to hardware failures, natural disasters, or cyber incidents.

Automated Process

Leverage the automation capabilities of the backup solution to streamline the process. Automated backups reduce dependency on manual intervention and minimize the chance of error.

Secure Data Encryption

Secure your critical assets and minimize your exposure to unauthorized access. Encrypt your data, both in transit and at rest.

Multi-Factor Authentication (MFA)

MFA adds an extra layer of protection to accounts by requiring users to provide verification beyond a password. This prevents unauthorized access and reduces the risk of account compromise.

Prevent data loss with reliable backup and flexible recovery

With Veritas Alta SaaS Protection you can scale across regions and domains, back up continuously, and deliver the performance that ensures your backup never falls behind.

Seamless integration with SaaS and PaaS APIs easily maintains a synthetic full backup of your data. It enables you to perform backup of entire data stores and restore data at granular and bulk levels to the original or alternate locations.

In addition to backing up all data objects, Veritas Alta SaaS Protection also captures—and can restore—important metadata including permissions.

Learn more

Case study

A UK health organization protects itself against data loss and ransomware

Microsoft is not responsible for protecting data in Microsoft 365, so when Oxford Health NHS Foundation Trust—along with the rest of Britain's National Health Service (NHS)—was transitioning key data and workloads to Microsoft 365, the network management team needed a robust and proven data protection solution.

The organization chose Veritas's NetBackup™ SaaS Protection (NSP) solution, which manages backups and data restores to deliver the ability to recover from all data-loss scenarios and eliminate threats from ransomware and accidental or malicious deletion of data.

Read case study

- Data backups of all Microsoft 365 apps are available for recovery in the event of disaster, ransomware, or data corruption.
- Responses to GDPR subject access requests (SARs) and other legal and regulatory requests are now streamlined.
- There has been a 100% success rate for data restores.

> **NSP [NetBackup SaaS Protection] enables us to keep backups of cloud-based data in the cloud. Our Microsoft 365 traffic is not impacted by our LAN traffic or any throttling of links. We can keep our backups running 24/7, safe in the knowledge that we always have the most up-to-date copies.**
>
> Darren Rodgers, IT Infrastructure Manager, Oxford Health NHS Foundation Trust

Must-have 2

Comply with data privacy regulations

A growing number of regulations means the pressure on you to protect information and maintain compliance is ever-growing. Fail to meet the stringent requirements for data protection and privacy practices—such as the General Data Protection Regulation (GDPR)—and you could face severe financial penalties, not to mention reputational damage.

Effective SaaS data protection measures are essential to safeguard sensitive information, and to demonstrate a commitment to data privacy and adherence to regulatory obligations.

22%

of enterprise businesses buy new hardware/software because of changes to regulations/compliance standards.[3]

You need to consider elements including:

Data Retention and Deletion

SaaS backup solutions provide the capability to set retention policies and securely delete data when it is no longer required. This aligns with GDPR's "right to be forgotten" principle, and allows you to manage data according to regulatory guidelines.

Auditing and Monitoring

SaaS backup solutions often provide features to track and analyze data activities. This visibility helps you proactively identify suspicious or non-compliant actions, facilitating timely response and mitigating potential breaches.

Vendor Due Diligence

Assess your SaaS provider's data protection measures. Conduct a thorough evaluation of their security protocols, certifications, and adherence to regulations. Review your agreement to ensure they align with your obligations.

Incident Response and Disaster Recovery

A comprehensive SaaS backup and recovery strategy includes robust plans for incident response and disaster recovery. These plans outline the steps to mitigate the impact of a data breach or system failure, ensuring business continuity and minimizing downtime.

Ensure compliance through intelligent automation

With Veritas Alta SaaS Protection, all backup data from your SaaS applications is stored on immutable storage (which prevents modification or deletion) on a platform and in data centers that are SOC 2 Type II-compliant.

Automated data residency controls make it simple to comply with data sovereignty regulations, while the ability to search across multiple data sources simultaneously enables you to apply legal holds quickly and easily.

Flexible retention policies, based on numerous customizable criteria, ensure preservation of data throughout the required timeframe.

Learn more

Case study

An investment firm finds and implements a compliance solution in just 4 months

In order to close an acquisition by a large global bank, a boutique Asia-Pacific (APAC) investment firm needed to quickly find a solution for securing and surveilling trade communications across its disparate communications channels. It had only around four months to find and implement a solution to complete the deal before the end of the year.

The investment firm deployed Veritas Enterprise Vault™ and Discovery Accelerator to archive employee communications, while Merge1 was used to ensure capture of all communication content into Enterprise Vault. Now, its communication data is being collected, surveilled, and stored in an easily searchable repository, and content is sampled to ensure compliance.

Read case study

- The Veritas solution samples content from places like emails and attachments, instant messages, and trading platform communications.
- Content rules are designed to identify messages that suggest compliance violations such as price collusion or anti-competitive behaviors.
- A high level of support and ease of integration within the Veritas solution ensured the firm met its deadline.

Veritas provided one unified approach for surveillance that has allowed us to move forward with a multibillion-dollar acquisition.

Compliance and Technology Director, Large Global Financial Institution

Must-have 3

Minimize downtime and data loss

Today's employees rely on SaaS apps to perform their jobs well, wherever they are, while customers rely on them to access your services. So, any downtime or data loss can have significant consequences for your business.

45%

of businesses say learning curve or downtime is their biggest worry while implementing new technology.[4]

Here are some of the actions you can take to avoid productivity impacts, lost revenue, and damaged customer trust by minimizing downtime and data loss:

3-2-1 Backup Strategy

Regularly back up critical data and store backups securely in an immutable, separate location. Consider the frequency of backups. Periodically test restoration processes to verify the integrity and availability of backed-up data.

Disaster Recovery Planning

Develop a robust plan tailored to SaaS environments. Identify potential risks and scenarios that could lead to service disruptions or loss. Establish recovery time objectives (RTOs) and recovery point objectives (RPOs) to identify your limits. Define clear steps and responsibilities, including communication protocols for activating the plan.

Redundancy and Failover Mechanisms

Lessen the impact of hardware failures or service interruptions. Use infrastructure components such as load balancers, redundant servers, and backup power supplies, to ensure continuous service availability. Set up failover mechanisms to automatically redirect traffic or switch to backup systems in the event of disruption.

Process Testing and Validation

Conduct simulations and drills of your recovery strategy. Testing helps identify gaps, weaknesses, or dependencies that could hinder a smooth recovery. Adjust based on the outcomes to improve efficiency and reliability.

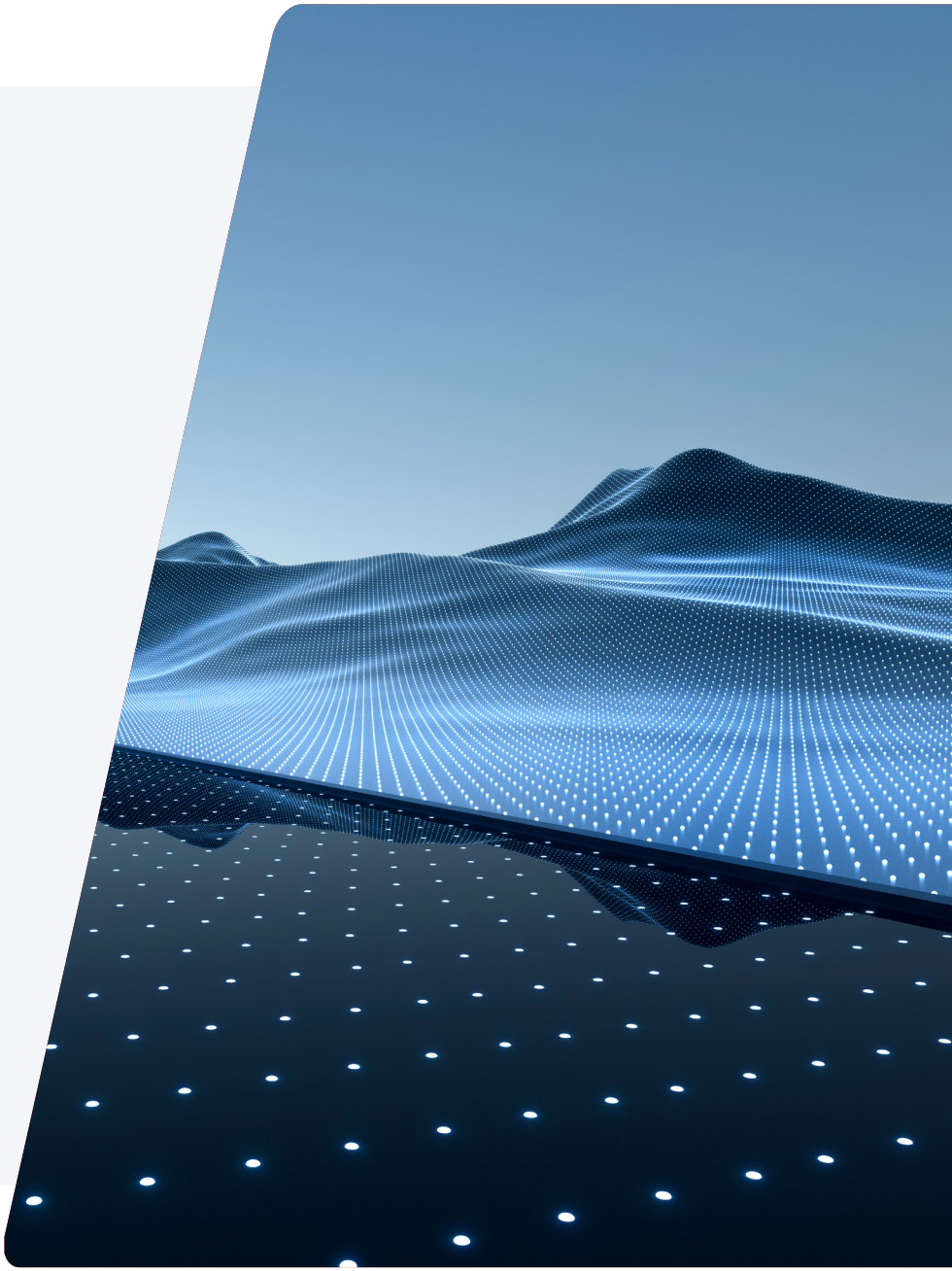
Strengthen your cyber resilience with multi-level recovery

Veritas Alta™ SaaS Protection helps you keep your apps up and running, enabling you to restore items, folders, mailboxes, or sites with granular, multi-level recovery. You can recover data to a preferred location—its original location, another cloud location, or on-premises.

Point-in-time restores or air gap copy options help you avoid falling victim to ransomware and data loss. And to further protect your data, you can write all backup data to immutable WORM storage that's separate from the data in the SaaS application itself.

You can capture data from SaaS applications at rates of multiple terabytes per day, with backup storage scaling to multiple petabytes of data and billions of objects.

Learn more



Case study

A financial data provider securely migrates its data backups to the cloud.

With regulatory bodies requiring financial data provider MSCI to keep certain data for at least five years, any data loss could mean significant legal and compliance implications. But having transitioned many core business activities to the public cloud, it wanted to move 7PB of related on-premises backups to long-term retention in the cloud. However, the firm's current data protection solution did not enable direct migration.

MSCI turned to Veritas Support, which worked alongside Veritas partner Insight, to streamline the data migration processes, using Veritas NetBackup™ to securely complete the migration from legacy storage to the cloud.

Read case study

- 7PB of data securely moved from legacy storage to the cloud.
- The cost of storing backups for long-term retention was minimized.
- Compression increased from 40-50% to 70% thanks to Veritas NetBackup, reducing the cloud data footprint of backups.

The migration has been 100% successful to date. We met the regulatory compliance requirements throughout the transition of our first three data centers, and we expect that to continue as we finish migration of the fourth data center.

Sandesh D'Souza, Executive Director, IT, MSCI

Secure your SaaS apps and data with Veritas Alta™ SaaS Protection

SaaS applications promise many benefits for businesses aiming to give employees more agile, flexible workplaces, and customers better experiences—from cost-effectiveness and accessibility to scalability and faster, simpler updates. But SaaS comes with its own set of challenges. The Shared Responsibility Model means it's on you to ensure your data is secure and backed up.

Veritas Alta™ SaaS Protection helps you reduce risk, eliminate uncertainty, and take control of your SaaS applications. It's a powerful data management and protection solution that delivers fully managed, cost-effective, automated backup as a service (BaaS) for the leading SaaS business applications—including Microsoft 365, Microsoft Entra ID, Google Workplace, Box, and Slack—through a single, intuitive interface.

The platform can also help you reduce the cost of your SaaS applications by automatically archiving inactive data to lower-cost cloud storage, make it easy to reclaim extra user licenses and preserve data from former employees, and accelerate and automate your migration to the cloud while reducing its cost.

Learn more about Veritas Alta™ SaaS Protection

1, 2 "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023," Gartner, April 2023.
3 "The 2023 State of IT," Spiceworks Ziff Davis," 2023.
4 "2023 Global Software Buying Trends, Fourth Edition," Gartner Digital Markets, 2023.

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% 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 and 1,400+ storage targets 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 X 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

V1949 01/24