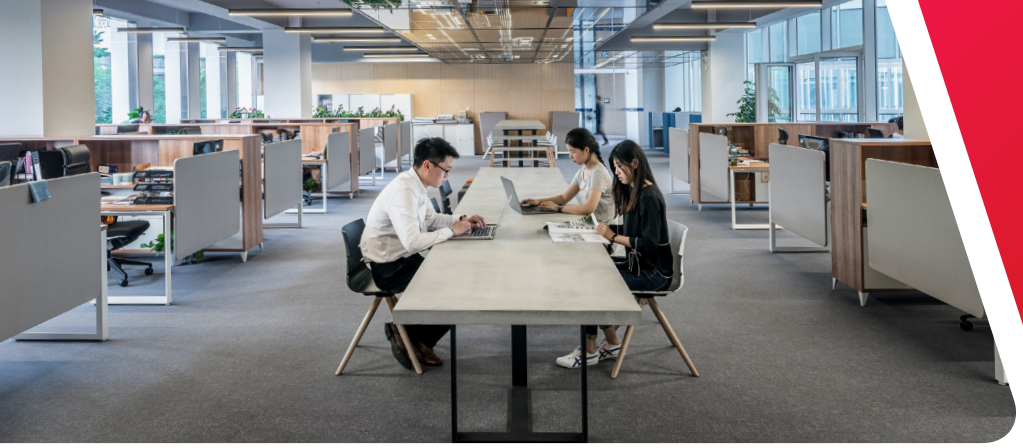
VERITAS

Guard Your Cloud Data Against Threats

STRENGTHEN YOUR SAAS DATA WITH CYBER RESILIENCE.



An increasing number of organizations are adopting a cloud-first strategy to deploy new business applications, utilizing a wide range of workloads across public and private cloud infrastructures. But many are challenged to find suitable data protection solutions for cloud-native, SaaS, and container applications.

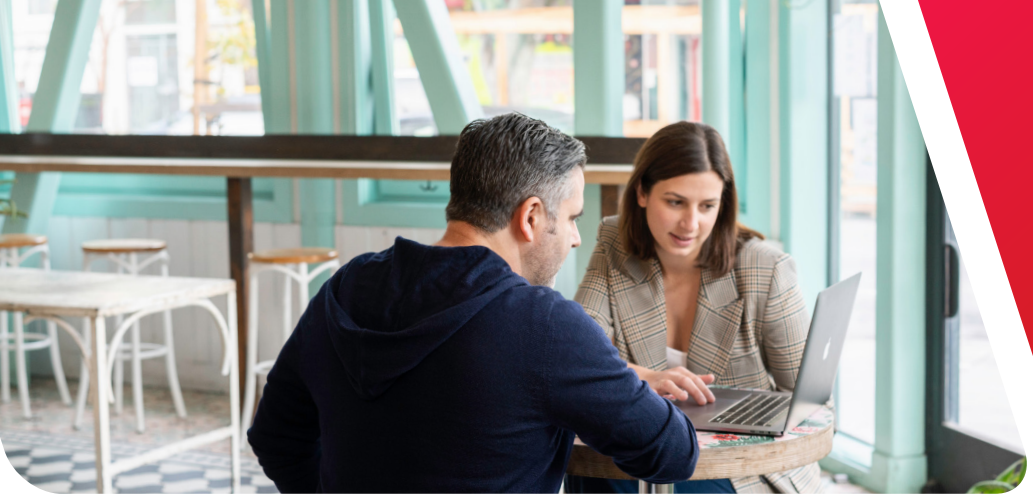
Many organizations rely on cloud service providers for backup tools, or they use the same tools they're using on-prem. When moving data to the cloud, it is crucial to adopt a smart approach. Reliable data protection plays a critical role in deploying multiple clouds to drive digital transformation.

17.9%

SaaS spending is projected to grow 17.9 % to total $197 billion in 2023.[1]

Cyber resilience has become vital to ensure the protection and continuity of businesses. Furthermore, the rise of SaaS applications such as Salesforce and Microsoft 365, has introduced new challenges and vulnerabilities to data security.

A comprehensive understanding of cyber resiliency and the importance of SaaS backup and recovery is vital to mitigate risk.



To achieve more successful outcomes, contextualize data and assess risks associated with complex procedures.

Understanding Cyber Resiliency

Cyber resiliency refers to the ability to prepare for, respond to, and recover from cyber incidents while maintaining essential business functions. It emphasizes a holistic approach that encompasses prevention, detection, response, and continuity.

You must identify and assess potential risks and vulnerabilities—internally and externally. This involves conducting risk assessments and prioritizing risks based on potential impact. From there you can develop mitigation strategies, allocate resources, and prioritize security measures.

Business continuity involves preparing for and responding to incidents to ensure uninterrupted operations and to minimize the impact of disruptions.

Stay One Step Ahead

- Identify vulnerabilities
- Assess the level of risk
- Develop a mitigation strategy
- Allocate resources
- Measure and optimize

The Need for SaaS Backup and Recovery

While SaaS providers safeguard their platforms, the shared-responsibility model puts you in charge of protecting the data you've stored within the applications. Your data isn't immune to risks. Vulnerabilities include accidental deletion, malicious attacks, data corruption, and insider threats. Without proper backup and recovery mechanisms, you face potential loss of critical data. This can lead to operational disruption, compliance issues, and reputational damage.

Native backup capabilities built into SaaS applications have limitations. They might offer basic data retention, but often lack comprehensive backup and recovery. You may assume that your data is automatically backed up by the SaaS provider, only to realize the limitations when faced with disaster. Relying solely on native capabilities can leave you vulnerable to irreversible data loss. And it can hinder your ability to meet regulatory requirements.

Data loss or corruption in SaaS applications can have severe consequences, including:

- Prolonged Downtime
- Financial Losses
- Legal Implications
- Decreased Productivity
- Damage to Customer Trust

Effective SaaS Backup and Recovery Strategy

Your needs vary based on factors such as data sensitivity, compliance requirements, and operational dependencies. For effective SaaS backup and recovery, it is crucial to evaluate these requirements for each application you use.

To ensure data integrity and minimize the risk of data loss, follow best practices for SaaS data backup, including:

75%

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

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 reduce the 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.

Compliance with Data Privacy Regulations

With a growing number of regulations, you face heightened pressure to protect information and maintain compliance. Regulations such as the General Data Protection Regulation (GDPR) have stringent requirements for data protection and privacy practices. Fail to meet these expectations, and you can face financial penalties.

22%

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

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

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.

SaaS-Specific Risks

Mitigating SaaS-specific risks is crucial if your operations rely on cloud-based applications. While SaaS offers many benefits, it also introduces unique security challenges.

Key considerations when implementing data protection specific to SaaS environments include:

Shared Responsibility: Make sure you have a clear understanding of the division of responsibilities to ensure all parties fulfill their obligations.

Access Controls: Strong controls are essential to prevent unauthorized access to SaaS applications and data. Enforce security measures with MFA, role-based access control, and privileged access management.

Regular Data Backup and Recovery: Relying solely on a provider's native backup capabilities may not be enough. Implement an independent data backup and recovery solution to ensure a multi-layered strategy so you can recover quickly in the event of a breach or corruption.

Continuous Monitoring and Auditing: Detect suspicious activities, unauthorized access attempts, and breaches. Regularly review logs and monitor activity to identify potential threats. Use audits to assess the efficacy of your data protection measures and identify areas to improve.

Continuous Improvement

Minimizing downtime and data loss is crucial if you rely on SaaS applications. Take steps to avoid productivity impacts, lost revenue, and damaged customer trust.

Actions you can take to minimize downtime and data loss include:

45%

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

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.

- Regularly review and update strategies to align as risks and industry best practices evolve.
- Keep up to date with the latest advancements in SaaS technologies and security measures.
- Conduct reviews to identify lessons learned, and make improvements to strengthen your overall data protection framework.

You can minimize downtime and reduce the risk of loss in your SaaS environment. Focus on proactive planning, regular testing, and continuous improvement. These efforts contribute to enhancing business continuity, maintaining customer satisfaction, and protecting your reputation in the face of unforeseen events. Investing in robust protection measures is an investment in the long-term stability and resilience of your operations.

Protect what matters most—your data and your business. Learn how to safeguard your SaaS environment with reliable backup and recovery.

Explore **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 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

V1942 08/23