VERITAS

# Four Reasons SaaS Data Protection is Vital for Cyber Resiliency

Software as a Service has revolutionized the way organizations operate, helping to streamline operations and enhance productivity. It provides convenient access to a wide range of productivity tools and business-critical applications. From email and customer relationship management (CRM) to project management and file store, SaaS is a convenient way to store and access data.

It is vital to address potential data security risks and vulnerabilities as your organization increasingly relies on SaaS solutions. Prioritizing SaaS data protection is essential to ensure the safety of your data and reinforce a solid foundation for success and sustainable growth.

Data breaches or losses can be devastating, eroding customer trust and confidence. That's why implementing strong data protection and cyber resiliency measures is essential. Proactively implement SaaS data protection measures and effectively communicate your security practices. Differentiate your organization as a trusted custodian of sensitive data, fostering long-term relationships and business growth.

**35%**

of worldwide respondents use more than 50 SaaS applications[1]

## Top Four SaaS Priorities to Strengthen Your Cyber Resiliency

### 1. Safeguard Business-Critical Data

SaaS applications process and store sensitive data such as customer information and financial records. While SaaS providers have security measures to safeguard the platform, data within the applications is not immune to risk. Common vulnerabilities include accidental deletion, malicious attacks, data corruption, and insider threats. Without a proper backup strategy, you risk losing critical data, which can lead to operational disruption, compliance issues, and reputation damage.

By implementing robust SaaS backup and recovery solutions, you can mitigate risks, maintain control over your data, and ensure business continuity to overcome unexpected challenges.

### 2. Comply with Data Privacy Regulations

Data privacy regulations are on the rise, making compliance increasingly critical for businesses. By implementing robust SaaS data protection measures, you can ensure compliance with these regulations and demonstrate your commitment to data privacy. By ensuring compliance, implementing encryption, and deploying multi-factor authentication (MFA), you add additional security layers to reduce unauthorized access and minimize the surface attack area. With plans in place, you can mitigate risks associated with breaches and non-compliance, and protect sensitive data.

### 3. Mitigate SaaS-Specific Risks

SaaS applications introduce unique risks due to their cloud-based nature. Multiple factors can pose security challenges, including the shared-responsibility model, third-party dependencies, ability for teams to purchase outside of IT oversight, and potential vulnerabilities in the SaaS provider's infrastructure.

Safeguarding data and assets in the SaaS environment demands an unwavering commitment to security. Advanced measures such as encryption, access controls, and backup and recovery must be implemented to strengthen cyber resiliency and mitigate the risks that accompany SaaS deployment. Keep your systems secure and build trust with customers by staying ahead of the curve with proactive data protection strategies.

### 4. Minimize Downtime and Data Loss

Natural disasters, cyberattacks, and human error can disrupt SaaS services and result in downtime or data loss. Implementing data protection measures, including regular backups and disaster recovery plans, helps minimize downtime and enables quick restoration of critical data. Deploying robust data protection strategies, such as optimized SaaS recovery, helps to ensure business continuity and reduce the impact of potential disruptions.

Follow best practices such as proactive planning, regular testing, and continuous effort. You can minimize downtime and reduce the risk of data loss in your SaaS environment with regular security audits and assessments of your SaaS applications—important to building your cyber resiliency. Investing in resilient data security and protection measures is a long-term improvement to stabilize business continuity.

In an increasingly interconnected and data-driven world, SaaS data protection plays a vital role in building cyber resiliency. By prioritizing SaaS data protection, you protect your data and provide a solid foundation for sustainable success.

Taking these steps prioritizes your SaaS protection and supports compliance with data protection regulations. It also helps reduce the risk of breaches and other security incidents, while improving customer trust, and increasing operational resiliency.

Protect your most important assets and ensure the long-term success of your business. Read our e-book, "Guard Your Cloud Data Against Threats," for guidance on how to secure your SaaS applications and improve your cyber resiliency.

[1] Thales Data Threat Report, 2022 EMEA

## 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