VERITAS

VERITAS ALTA™

Protect Your Critical SaaS Data

Your SaaS solution providers aren't doing it for you.

Introduction

We've all seen a meteoric rise in the enterprise adoption of software-as-a-service (SaaS) applications and solutions during the past few years. SaaS tends to be less expensive and easier to manage, while making it easier for people to work together despite the geographic distance between them.

Like all technology, SaaS is not a magical fix for companies—it comes with its own set of challenges and problems. In this document, we'll explain the most glaring challenge—ensuring data protection for SaaS applications—why it's a challenge, the importance of addressing this challenge, and how to address the challenge simply and thoroughly.

The Problem

SaaS solution providers **do not** provide data protection for the data that their customers have stored in the platform. SaaS solution providers **are not** running backups on your data.

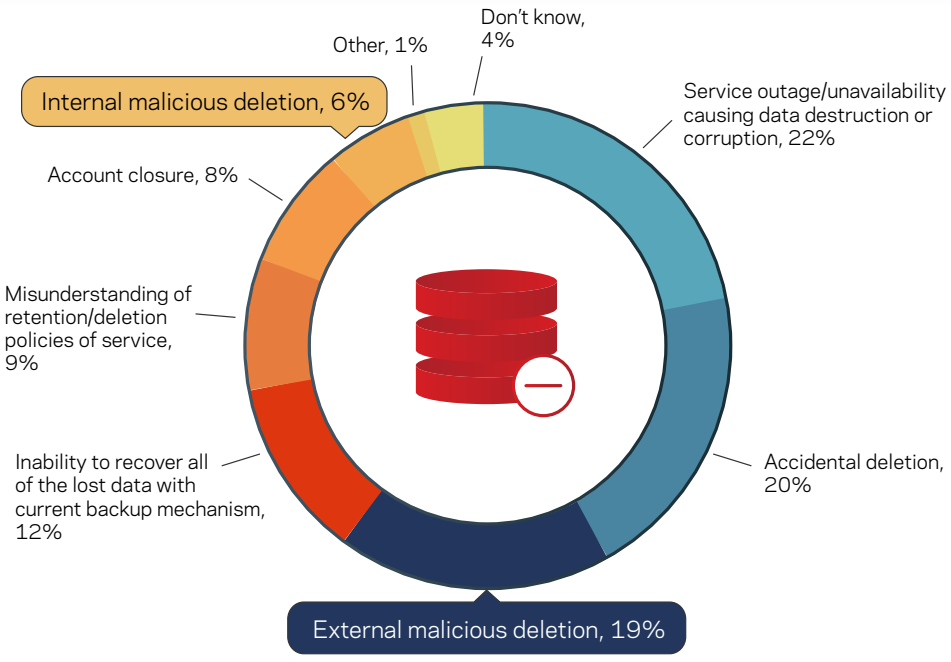
The biggest threat to SaaS application data—outside of ransomware—is simple deletion. Regardless of whether the deletion was accidental or malicious. Analyst firm ESG's research report titled *The SaaS Data Protection Disconnect* identifies deletion as being the cause of 45 percent of all SaaS data loss.

Malicious and Accidental Deletion

Top Cause of SaaS Data Loss

45%

of SaaS data loss is caused by malicious and accidental data deletion.



ESG Research Report: The Evolution of Data Protection Cloud Strategies

> *Too many IT organizations still incorrectly believe that their requirement to preserve previous versions of data is inherently built into—and subsequently satisfied by—cloud application services."*
>
> *[Office 365] data is always the organization's responsibility—whether it resides in an on-premises data center or in the cloud—and it must have a backup and recovery solution in place."*

Source: ESG Research Report: The SaaS Data Protection Disconnect

SaaS Solutions' Native Tools are not Enough

Most SaaS solution providers create several synchronized replicas of customers' data, but they do this to help ensure high-availability of the data, not to protect it. Replicas are not backups. If you delete an object from your SaaS solution, that deletion is replicated to all copies of the data. Likewise, if an object were to become corrupted—perhaps by ransomware—that corruption will also be replicated to all copies of the data.

Microsoft 365 provides the Recycle Bin, and many consider it sufficient data protection. It is not. Relying on the Recycle Bin has the following limitations:

- Unless you're checking the Recycle Bin regularly, it only helps if you're aware that something has been deleted
- The Recycle Bin only keeps data for a limited time
- Any data deleted from the Recycle Bin is gone forever
- The Recycle Bin is not suitable for a bulk recovery for a large number of objects

Advanced options such as Microsoft 365 Enterprise Plans (E3/E5) provide additional features such as Legal Hold, that help with in-line threats, security of the data, and digital compliance. None of these features are data backups.

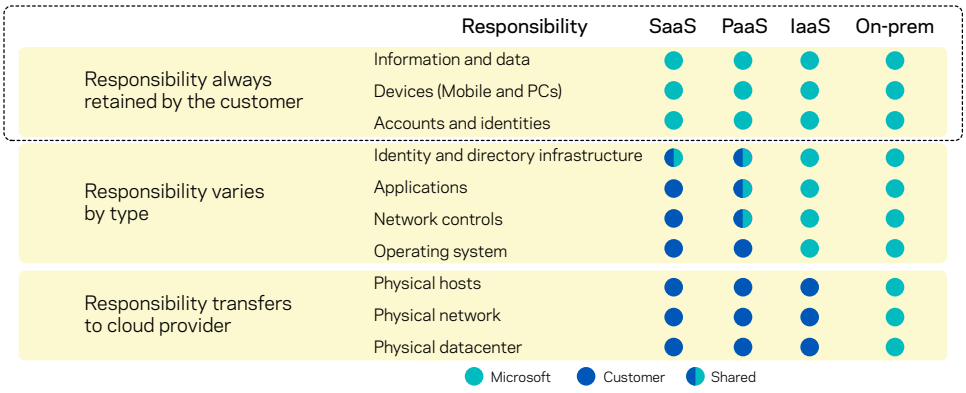
Don't Expect Backup and Recovery From Your SaaS Solution Provider

Microsoft has adopted a *shared responsibility model,* and all of the other major SaaS providers have followed suit. In this model, Microsoft details the division of responsibilities between itself and its customer.

Did you know?

You (*the customer*) bear responsibility for protecting your M365 SaaS Information and data, **not Microsoft**.

Microsoft Shared Responsibility in the Cloud—Azure



As you can see in the table above, from Microsoft's own documentation of the shared responsibility model, Microsoft does not provide backups of SaaS data, and takes no responsibility whatsoever for any loss of data.

The truth of SaaS solutions is that you, and you alone, are responsible for protecting your own data. You need a backup and recovery solution for your SaaS applications

The Consequences

We see it in the headlines more often now—organizations that suffered the loss of SaaS data and were powerless to recover it.

Here are just a few of the many real-world examples of SaaS data loss.

Microsoft 365

A terminated employee deleted 1,200 (out of a total of 1,500) Microsoft 365 user accounts. The accounts and the data in them were unrecoverable.

> *In my 30-plus years as an IT pro, I have never been a part of a more difficult work situation."*

Intentional deletion of 1,200 Microsoft user accounts

Google Workspace

A startup developer of interior design tools accidentally deleted the company's Google account, losing all of its data.

> *All efforts failed. We received a one-line email that stated our data was lost and couldn't be returned to us."*

Moss accidentally deletes Google G Suite account

MS Teams

At KPMG, a configuration error in a data retention policy deleted the chat histories of 145,000 employees rather than the one account intended.

> *KPMG went to Microsoft for help, but Microsoft replied that the Teams chat data is not recoverable."*

Major IT disaster at KPMG

None of the organizations above had been using a SaaS application data backup and recovery solution—something that wouldn't have prevented the initial deletions but would have made it possible to recover the data.

The Solution

The solution to the risk of data loss in your SaaS applications is the industry-leading Veritas Alta™ SaaS Protection (formerly known as NetBackup SaaS Protection) solution that provides unparalleled data protection for SaaS applications.

Broad SaaS Environment Support
Protect popular SaaS environments such as Microsoft 365, Google Workspace, Box, Slack, and more with native connectors—at any scale

Operational Efficiency
Simple controls and a modern UI make deployment, compliance, and recovery easy

Cyber Resilience
Ensure recovery of business-critical SaaS data with near-zero recovery point objectives (RPOs) and recovery time objectives (RTOs) after a ransomware attack

Enterprise-Grade Security

Single-tenant architecture enables enterprise-grade performance, security, and data privacy

Recovery from Data Removal

Easily recover SaaS data after it has been intentionally or accidentally deleted, including bulk recovery after a mass deletion event

Comprehensive Recovery

Powerful, enterprise-grade SaaS recovery capabilities.

- Restore items, folders, mailboxes, or sites with granular, multi-level recovery
- Reinstate multiple mailboxes in a single operation
- Recover data to a preferred location—its original location, another cloud location, or on-premises
- Retain access to Microsoft 365 account data after an employee departs without maintaining an extra active license
- Avoid falling victim to ransomware or data loss with point-in-time restores and an air-gapped copy option

Learn more about Veritas Alta SaaS Protection

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

V1629 01/23