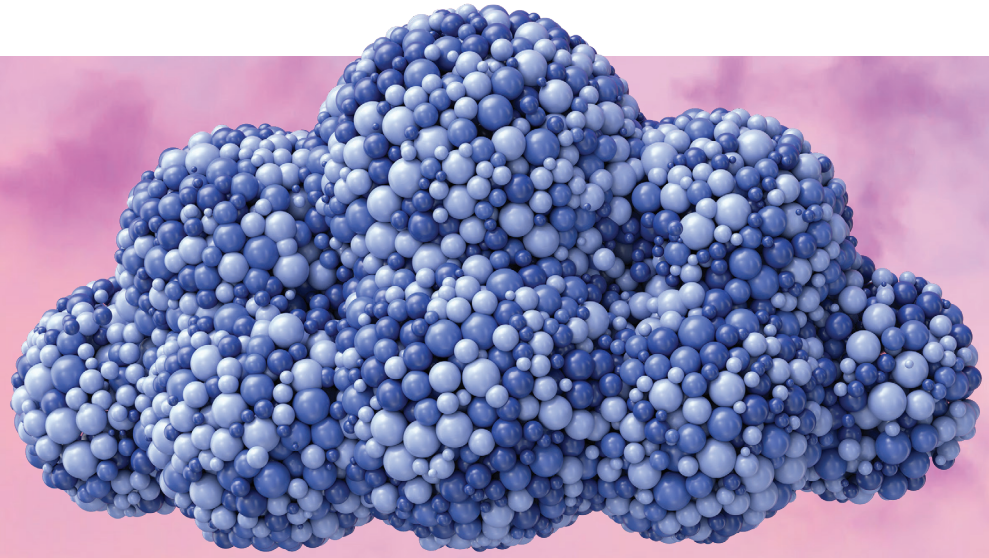


# WHY YOUR CLOUD-BASED DATA NEEDS A BACKUP SOLUTION

PALADIN
BUSINESS CONSULTING

**Perception is not reality. Many organizations that use cloud-based platforms such as Dropbox, Google Drive and Microsoft 365 have a common misconception that it's the vendors' responsibility to protect their data, and cloud backup isn't necessary. Because of these critical knowledge gaps, businesses fall victim to data loss.**

Software-as-a-Service (SaaS) providers have best-in-class security and disaster recovery capabilities to protect against infrastructure threats, including hardware and software failure, power outages and natural disasters. However, they can't protect you from some of the leading causes of SaaS data loss.

# 4 KEY REASONS FOR DATA LOSS

## 1 HUMAN ERROR

Employees can intentionally or unintentionally overwrite important files or delete business-critical information. Suppose an employee inadvertently deletes an important email or account or accidentally downloads a malicious attachment. If this goes unnoticed, it can lead to massive data loss. SaaS providers have no way of determining whether the request was intentional, so they treat it as a legitimate request and handle it accordingly.

## 2 SYNC ERRORS

By using third-party data sync services, you can have multiple users accessing the same file from different devices and locations. Although this is great for collaboration and information sharing, you cannot ignore its downside. If any of your teammates deletes a shared file, the changes will be reflected on all devices, and you may lose access to the file forever. While most sync services offer limited ability to restore changed or deleted versions of files, they are not true backups and are still prone to large amounts of data loss.

## 3 RANSOMWARE

As cloud storage synchronizes with local storage, it is susceptible to ransomware attacks. For example, Dropbox, OneDrive, and other file sync and share solutions allow you to work on your files locally while syncing changes to the cloud. Ransomware not only encrypts your files locally but also syncs this encryption with your cloud storage copy.

## 4 INSIDER THREATS

The biggest threat to your data is probably your workforce, especially when they have malicious intentions. Employees with malevolent intent and access to sensitive data might readily circumvent security measures to erase or delete crucial corporate data.

# DEMYSTIFYING BACKUP MYTHS

**Here are three typical misunderstandings businesses often have regarding "built-in" cloud backups:**

## MY CLOUD PLATFORM ALREADY INCLUDES ROBUST BACKUPS

Your business might be in a vulnerable spot if you are fully dependent on native backup capabilities because it typically comes with limitations. As an additional layer of protection, many vendors like Microsoft and Google recommend you opt for a more robust backup solution to what's included in Microsoft 365 and Google Workspace.

## RANSOMWARE CAN'T INFECT MY DATA IF I HAVE A BACKUP

You may be able to restore encrypted or stolen data using a comprehensive backup and recovery solution, however, the data has still been stolen. The cybercriminal still could use the stolen data to further harm your business, such as making your organization's IP address and sensitive data public or extorting to stop it.

## ALL BACKUPS ARE THE SAME

There are various backup formats starting from entry-level to enterprise-class. While some offer seamless integrations with time-saving productivity solutions, others provide strong security features that enable you to quickly and easily recover any files that were deleted because of a ransomware attack. It is important to consider what matters most to your organization when choosing a backup and recovery solution.

# THE SOLUTION: BACKUP & RECOVERY

Implementing a backup and recovery solution can not only reduce risks but also keep your business operations up and running in the event of an incident. Are you ready to bolster your business's data protection strategy without adding to its internal IT workload?

# WHAT IS CLOUD BACKUP & RECOVERY?

A cloud backup and recovery solution allows you to back up and store data and applications on a remote server, ensuring seamless recovery of files and data in the event of a system failure, cyberattack, outage or natural disaster. Backing up your cloud-based data is no more a choice, it is essential since most, if not all, of your business-critical information is stored in the cloud.

# HOW CAN IT HELP?

## COST-EFFICIENT

The cost of cloud backups is extremely low compared to on-site data centers because you don't need to invest in backup hardware, disks, servers or infrastructure. Additionally, most cloud backup providers operate on a pay-as-you-go model, which means you only pay for what you use.

## SHIELDS YOUR DATA & APPS

Critical applications and data can be stored and maintained off-site, thereby ensuring local weather disturbances and outages do not disrupt them.

## SCALABLE STORAGE

The capacity of cloud-based backup can be scaled up or down quickly, unlike traditional backup techniques that rely on local storage such as hard drives or tapes.

## FASTER DATA RECOVERY

Companies can quickly gain access to files and systems they need by restoring the data they backed up on cloud servers.

# 4 REASONS YOU NEED A SECONDARY BACKUP FOR YOUR CLOUD PLATFORM

**SaaS applications are becoming increasingly popular among companies looking to save money and gain flexibility, but these cloud service providers have multiple bugs that increase the chances of data loss.**

1

## SaaS RETENTION POLICIES

Many SaaS apps contain a data retention policy outlining how long the data will be retained, including Microsoft 365 and Google Workspace. Most companies are unaware of this. Microsoft allows a maximum retention period of 180 days before permanently wiping the data. Google Workspace's trash folder is automatically erased after 30 days. Once data has been removed from the trash, it cannot be recovered or restored.

2

## PROGRAMMATIC ERRORS

This occurs when a program is being executed. The SaaS provider might not always be able to protect your data from programming faults. These kinds of failures might occur while integrating different SaaS apps. This can be brought on by a wide range of other variables, such as an incorrect code setting or unexpected input. Your data could become corrupted or lost forever if such errors happen.

3

## HARDWARE FAILURE

There are thousands of servers and network equipment in data centers that provide SaaS services with speed, redundancy and uptime. Despite the high level of redundancy these items offer, it does not lessen the likelihood of a hardware malfunction that could result in data loss.

4

## CYBERATTACKS

Cyberthreats like malware, phishing and ransomware attacks aren't going away any time soon. Cyberattacks are growing more sophisticated, and cybercriminals are becoming more intelligent. You need additional protection because built-in backups are insufficient to protect your data from these sophisticated threats.

# 4 FEATURES TO LOOK FOR IN YOUR CLOUD BACKUP SOLUTION

**1**

## COMPREHENSIVE PROTECTION

A reliable backup, with unlimited storage space and an unrestricted retention policy, ensures your cloud data is always backed up and protected.

**2**

## COMPLETE AUTOMATION

Aim for a “set and forget” backup that provides daily, automated backup and auto-discovers new or altered content to backup. The backup process must run quietly in the background.

**3**

## EASY AND RAPID RESTORE

The backup must work for you by making it simple to locate and restore lost data.

**4**

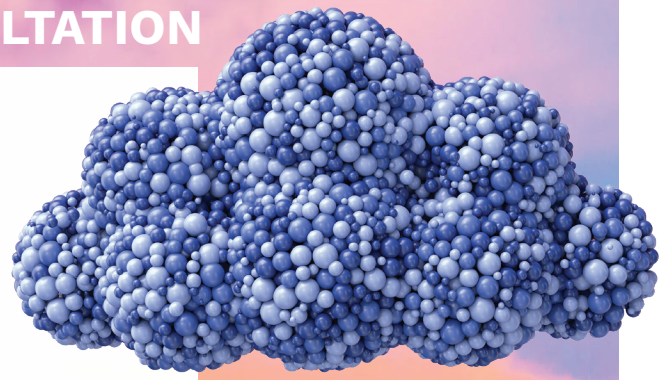
## TRANSPARENT REPORTING

A good solution should include an immutable audit log that provides a transparent, actionable report of every cloud backup as well as daily backup health status reports.

# ENSURE THE CLOUD PLATFORMS & APPS YOUR ORGANIZATION USES ARE CORRECTLY BACKED UP AND FULLY RESTORABLE

**CONTACT US TODAY FOR A NO-OBLIGATION CONSULTATION**

PALADIN
BUSINESS CONSULTING




**828-322-2074**

**REX@PALADINBC.NET**


**We look forward to hearing from you!**