SaaS Protection

datto
A Kaseya COMPANY

Remote Data Backups, Inc.
25 Years of Support & Service
www.remotedatabacups.com
email: sales@rdbu.com
phone: 1.866.722.2587

Overview

Datto SaaS Protection Buyer's Guide

Datto SaaS Defense for Microsoft 365

Datto SaaS Protection for Microsoft 365

Datto SaaS Protection for Google Workspace

Microsoft 365

Google Workspace

SaaS Protection Buyer's Guide

datto
A Kaseya COMPANY

Introduction

SaaS application adoption has spiked with the increase in remote work due to the global health pandemic. These tools have become essential in today's remote work world. Even before work-from-home became the norm for many, the benefits of easy access to documents from any device and improved collaboration are obvious.

Unfortunately, many organizations still believe that these tools make backup obsolete. This simply isn't true. Backup is just as important for data in SaaS apps as it is for data hosted on-premises.

In this eBook, you'll learn some common myths and misconceptions about SaaS, talking points for discussing SaaS data loss and downtime with clients, what to look for when selecting a SaaS backup solution, and how you can use SaaS backup to build margin and grow your business.

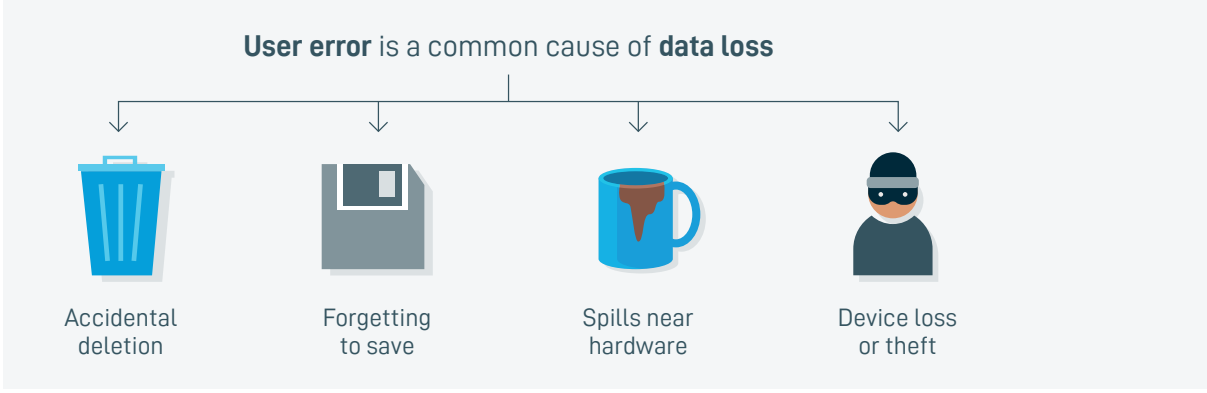
Microsoft 365

Google Workspace

Common SaaS myths and misconceptions

SaaS applications do not require backup

While SaaS applications have built-in redundancy that protects against data loss in their cloud servers, this doesn't protect against user error, accidental and malicious deletion, or ransomware attacks. While accidental deletion of files is by far the most common form of data loss in SaaS apps, ransomware can be the most damaging. That's because ransomware is designed to spread across networks and into SaaS applications, impacting many users.



Ransomware isn't only an on-premises problem. It can and does spread into SaaS applications, especially Microsoft 365. Businesses need a way to quickly revert files, folders, settings, and permissions in the event of an attack.

File sync is a replacement for backup

While file sync tools like Microsoft OneDrive or Google Drive do create a second copy of files and folders, they are not a replacement for backup. File sync automatically copies changes to synchronized files. So, if a file or folder is infected with ransomware, the malware will automatically be copied to all synced versions of that file.

File sync services do offer some restore capabilities via versioning, but they fall short of a true SaaS backup solution. Here's why:

- **Versions are not immutable recovery points.** So, if a file is deleted, older versions of the file are deleted as well.
- **Versioning doesn't enable centralized management of user data.** In other words, you don't have control over backup and recovery—it's left in the hands of end users.
- **Versioning doesn't maintain recovery points across files, folders, settings and users.** If you only need to restore a couple of files, no big deal. But, large restores are a time-consuming, manual process.

Beyond simply lacking the restore capabilities of a backup solution, file sync can actually introduce ransomware to SaaS applications. File sync and backup are not competitive solutions, rather they can and should be used side-by-side. Remember: file sync and share is for productivity and backup is for data protection and fast restore.

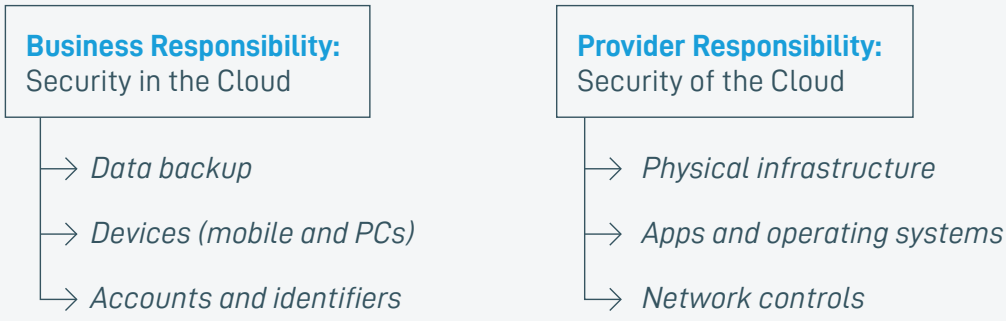
SaaS applications are always available

While SaaS apps are highly reliable, outages do occur. In October 2020 alone, Microsoft 365 had three significant outages that impacted businesses worldwide. Last year, a massive Google outage affected nearly one billion Gmail, G Suite, and YouTube users.

Outages and slow restore times aren't just an inconvenience. When businesses can't access important business data, productivity falls and revenue is impacted. Creating backups that are independent of a SaaS provider's cloud servers is the only way to ensure access to essential files in the event of an outage.

Microsoft and Google are responsible for backup

SaaS providers ensure they won't lose your cloud data with built-in redundancy and other high availability measures. However, they do not take responsibility for restoring data if you lose it. Microsoft calls this the Shared Responsibility Model for data protection. That's why Microsoft recommends third-party SaaS backup in its user agreement. In the Shared Responsibility Model:



The Shared Responsibility Model places the onus of data protection squarely on businesses that rely on SaaS services. SaaS providers are responsible for keeping their infrastructure up and running, but businesses are responsible for the preservation and security of their data.

Evaluating SaaS Backup Solutions

There are a variety of SaaS backup solutions at competitive price points on the market today. However, there is disparity in exactly what these products protect. So, when evaluating products that can be a good place to start.

Comprehensive Protection

Some SaaS backup solutions only protect email, files, and folders. However, there are solutions available today that offer more comprehensive coverage. When selecting a SaaS backup product, look for solutions that offer protection for things like contacts, shared drives, collaboration and chat tools, and calendars. SaaS protection solutions that offer this type of coverage are far more effective at maintaining business continuity than less robust offerings (more on that below).

RPO/RTO

Recovery point objective (RPO) and recovery time objective (RTO) are also critical considerations. These metrics refer to the point in time you can restore to and how fast you can perform a restore, respectively. When it comes to SaaS backup these are largely dictated by the frequency of backups and what specifically is being protected. Solutions that offer frequent backups address RPO since they enable you to restore to a recent point in time, minimizing data loss. As noted above, these make restores faster and easier by reducing the amount of manual effort to perform restores. Plus, they enable users to access data in the event of a SaaS outage.

Ease of Use/Management

Ease of use is critical for MSPs. Increasing efficiency can expand margins on services delivered, so finding a product that is easy to deploy and manage should be considered essential. Look for SaaS backup products that are designed specifically for MSPs. That might mean streamlined onboarding, native reporting capabilities, intuitive seat management, and flexible retention

policies. Consider partnering with vendors that offer not for resale programs, sales-based discounts, and 24x7x365 tech support. Finally, products that integrate with other tools you also increase your ability to deliver SaaS backup services efficiently.

Security/Compliance

Many MSPs serve clients in verticals with significant security and compliance requirements. So, choosing a SaaS protection solution that can address these needs is essential. Look for products that back up data in compliance with Service Organization Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards that can meet clients' HIPAA and GDPR compliance needs. Solutions that enable automated retention management to meet compliance standards can reduce the need for manual intervention—streamlining management and ensuring client data is stored for the right length of time.

Business Growth

No discussion of product evaluation for MSPs is complete without considering profitability. Look for products that have the features and functionality you need at a price point that allows you to build margins on your services. Consider products that offer pricing benefits for MSPs such as sales-based discounting and flexible 'pay for what you use' licensing. As noted above, products that increase efficiency can also grow margin and increase revenue, since they require less manual intervention. You may also want to bundle SaaS protection on top of SaaS services you already deliver—this has proven effective for some MSPs. This isn't necessarily part of the product evaluation process, but it's worth noting when discussing business growth.

Datto SaaS Protection

Datto SaaS Protection is a cloud-to-cloud backup solution that offers comprehensive backup and recovery for critical cloud data in Microsoft 365 and Google Workspace. It is designed specifically for MSPs to protect their clients' SaaS data efficiently and manage client data retention, licenses, and cost.

SaaS Protection protects against permanent data loss and allows MSPs to easily recover clients' data following a ransomware attack with 3x daily, point-in-time backups. Backups are stored securely in the Datto Cloud with files, folders, settings, and permissions intact for fast restores whether you need to restore a single item or an entire user account.

SaaS Protection delivers backup, search, restore, and export for:

Microsoft 365	Google Workspace
• Exchange • Tasks • OneDrive • SharePoint • Teams	• Gmail • Google Drive • Calendar • Contacts • Shared Drives

As you know, delivering profitable managed services is all about increasing efficiency and maximizing return on services. Datto SaaS Protection improves MSP efficiency with streamlined onboarding that gets new clients up and running fast. Single pane of glass management gives you complete visibility into client backups, further increasing efficiency.

Datto SaaS Protection also offers:

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.
- **Margin building opportunities:** Build margin and add multi-layer protection for your Microsoft 365 clients by bundling Microsoft 365 and Datto SaaS Protection.
- **Unlimited NFR Program:** Pilot the Datto SaaS Protection product with your clients and add a new NFR client in minutes with our streamlined onboarding process.
- **SaaS Protection marketing and sales campaigns:** Launch pre-built SaaS Protection campaigns, access a library of co-branded content, and manage your leads from prospect to sale.

Datto SaaS Protection By The Numbers:

Billions of Backups

Tens of Thousands of Recoveries

Hundreds of Thousands of Teams Protected

datto | UNIFIED CONTINUITY

Datto SaaS Defense for Microsoft 365

Datto SaaS Defense is a comprehensive threat protection solution for Microsoft 365 applications. SaaS Defense ensures that managed service providers (MSPs) can proactively identify and protect against zero-day threats across the Microsoft 365 suite, including Exchange, OneDrive, SharePoint, and Teams.

Limitations of ATP solutions

While MSPs leveraging an Advanced Threat Protection (ATP) solution have taken the necessary step to go beyond essential threat protection, they are still leaving themselves open to attacks, given the inadequate threat detection rates amongst most ATP vendors on the market.

Zero-day threats are evolving every day, and hackers are sophisticated enough to penetrate attack vectors beyond email. Unfortunately, many solutions fall short in protecting the entire Microsoft suite.

Datto SaaS Defense

SaaS Defense is an ATP and spam filtering solution that detects unknown malware threats at first encounter across the Microsoft 365 collaboration suite, shortening the time to detection and helping to close the threat protection gap.

SaaS Defense's data-independent technology was developed by security experts to stop zero-day threats and proactively defend against malware, phishing, and business email compromise (BEC) attacks that target Microsoft Exchange, OneDrive, SharePoint, and Teams.

Detection against the unknown

Traditional email security solutions depend on data of previously known cyber threats and their penetration modes, thereby leaving protection gaps for new, unknown threats. With Datto SaaS Defense, MSPs can feel confident that cyber threats–even zero-day threats–are stopped as soon as they are encountered and time to detect is minimized.

- **Identify unknown threats:** SaaS Defense's data-independent technology detects unknown threats that other solutions miss by analyzing the composition of a safe email, chat, or document rather than scanning for already known security threats.
- **Minimize time to detection:** Datto SaaS Defense does not rely on third-party software and is built from the ground up to prevent zero-day threats as soon as they are encountered, minimizing the time needed to detect an intrusion.
- **Superior Microsoft 365 protection:** When tested by Miercom*, SaaS Defense detected 96% of the malware threats delivered by Microsoft 365 applications, even catching threats that were missed by native Microsoft security.

Comprehensive threat protection

SaaS Defense provides MSPs with advanced threat protection and spam filtering for critical business data in Microsoft 365.

- **Protection beyond email:** Cyber threats are not limited to just phishing emails–proactively protect your clients' Microsoft 365 suite, including OneDrive, SharePoint, and Teams, from ransomware, malware, phishing, and BEC.
- **Spam filtering:** Configure customizable spam filtering with a single click and add another level of protection to your clients' inbox.
- **Impressive Business Email Compromise (BEC) detection:** In a Miercom test, SaaS Defense proved 91% detection efficacy for business email compromise threats, outperforming competition by at least 29%.

*Miercom is a global leader in independent product testing, publishing hundreds of comprehensive testing and product comparison analyses over the years.

Detailed monitoring and reporting

Traditional ATP solutions are built for large enterprises, with complex scoring models and confusing reporting metrics, it's difficult to understand why a threat was flagged. MSPs need detailed, simple explanations as to what threats were identified and why.

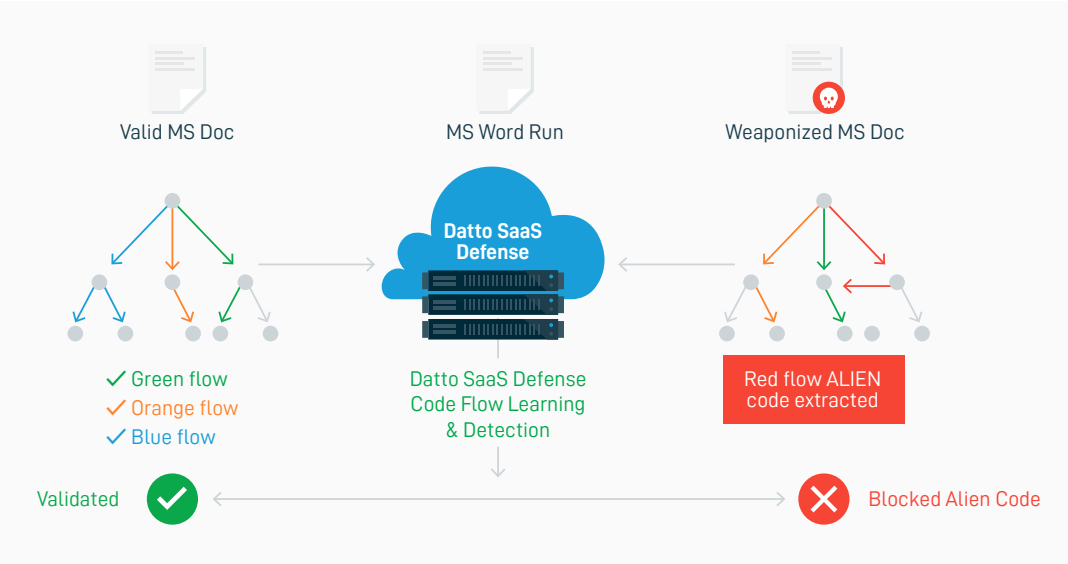
- **Silent detection:** Proactively monitor and eliminate cyber threats as soon as they are encountered without manual interference or end-client disruption.
- **Robust reporting:** Demonstrate product value with simple, detailed reporting that articulates why a threat was identified as malicious.

Enterprise-grade security packaged for MSPs

Expand your addressable market and offer clients a simple and robust threat protection solution that goes beyond just email security.

- Seamless deployment and management: Get new clients up and running in minutes with two-click onboarding and multi-tenant management from a single dashboard. Meircom reports SaaS Defense time value benefit is far superior as compared to the competition.
- Designed for MSP growth: Built exclusively for MSPs, Datto SaaS Defense helps MSPs attract new clients and expand market share with an enterprise-grade security solution without the need for additional headcount or confusing security training.
- Direct access to Datto technical experts: Eliminate multi-vendor confusion and new product fatigue while providing an extra confidence level when deploying new technology.
- API-Based solution: Traditional, SEG-based solutions require a change to the DNS MX record which slows down deployment and allows threat actors clear visibility into which email security solution is being used and gives the information needed to evade the solution and launch targeted attacks.

How Datto SaaS Defense works



A fully integrated cloud security solution

Protect and defend your clients' critical cloud data against unknown cyber threats and common data loss scenarios with comprehensive detection, protection, and recovery from a single, channel-focused vendor.

Datto offers a completely integrated solution built exclusively for MSPs that scans Microsoft 365 for malicious cyber threats and ensures complete protection with 3x daily backups and flexible, fast recovery.

Miercom CERTIFIED SECURE™

datto | UNIFIED CONTINUITY

Datto SaaS Protection for Microsoft 365

Datto SaaS Protection ensures that MSPs can access, control, and most importantly protect their clients' Microsoft 365 data. As the leading cloud-to-cloud backup solution, SaaS Protection for Microsoft 365 offers an all-in-one backup, search, restore, and export solution for Exchange, OneDrive, SharePoint and Teams.

Microsoft 365 is Not Automatically Protected

As organizations increasingly move data into cloud-based applications, many believe that traditional best practices such as data backup are outdated. After all, SaaS applications are always available, accessible from anywhere, and highly redundant, so why is backup necessary?

An astonishing 1 in 3 companies report losing data stored in cloud-based applications. The single leading cause of this data loss? End-user error. Other common culprits include:

- Malware or ransomware attacks
- Malicious end-user activity
- Accidental data overwrites
- Canceled account subscriptions

With more and more companies depending on Microsoft 365 for collaboration and business operations, these risks are impossible to ignore. Backup is just as important in the cloud as in traditional on-premises IT systems. An independent, third-party, SaaS backup solution is the best way to protect organizations against the most common data loss pitfalls.

Protecting Your End Clients in the Cloud —A Shared Responsibility

Many organizations mistakenly believe that Microsoft 365 data is automatically protected. But, that's only partially true. Microsoft does ensure that it won't lose your data, but it does not make any guarantees about restoring data if you do. In other words, Microsoft 365 data is as vulnerable to accidental or malicious deletion, ransomware and other types of data loss as on-premises applications.

SaaS vendors like Microsoft promote a "shared responsibility" model. They are clear in recommending providers and end-users pursue third-party solutions to ensure they meet data protection, business continuity, compliance, and security requirements beyond Microsoft 365's limited native recovery capabilities.

Why SaaS Protection for Microsoft 365?

Trusted Backup

MSPs need complete confidence that clients' Microsoft 365 data is protected with a reliable, robust solution designed to reduce risk and time needed to manage backups.

- **Automated, continuous backups:** Protect Exchange, Tasks, OneDrive, SharePoint, and Teams with 3x daily backups or perform additional backups as needed at any time.
- **Streamlined client onboarding:** Get your clients' critical cloud data protected in a matter of minutes with a simplified setup and an easy click-through onboarding process.
- **Flexible retention:** Not all client environments are the same. That's why SaaS Protection offers different data retention options to meet clients' individual needs.
- **Intuitive, user-friendly management portal:** Quickly and easily determine the number of licenses in use, gauge profitability, and view clients' backup status all from a single pane of glass.

Fast & Effortless Restore

- **Point-in-time restore and export:** Quickly restore or export data from a specific point-in-time before a data loss event occurred.
- **Non-destructive restore process:** Quickly identify and recover individual objects or entire accounts with related records and folder structure intact.
- **Cross-user restore:** Restore data from one Microsoft 365 user account into another.
- **Retain user data:** Save money and effort by preserving inactive Microsoft 365 user data with SaaS Protection for as long as you need it.
- **Easy export:** Export entire accounts or specific items in standard file formats.

Effective Monitoring and Management

Have complete administrative control and proactively monitor your backup activities. Be confident in the status of all backup and recovery operations with detailed, actionable reports.

- **Backup monitoring:** Enables on-demand retrieval of events such as backup, export, or restore. Here you can see all of your successful and failed backup runs at the seat-level with error messaging around the root cause.
- **Admin audit log:** Maintain a detailed record of all administrator and user actions from your admin dashboard.
- **Multi-Admin roles:** Manage your accounts using roles such as Super Admin and multiple General Admin roles.

Predict Profitability

Build margin with bundled solutions that include protection for clients' Microsoft 365 data.

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.
- **Increase margins:** Build margin and add multi-layer protection for your Microsoft 365 clients by bundling Microsoft 365 and Datto SaaS Protection.

Data Protection and Compliance

Balance security and transparency with powerful controls and robust user lifecycle management. Protect valuable business data from accidental or malicious acts.

- **Security and compliance:** SaaS Protection backs up data in compliance with Service Organization Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards and supports your HIPAA and GDPR compliance needs.
- **Ransomware protection:** Roll-back data to a point-in-time before ransomware attacks.
- **Custom data retention:** Keep data indefinitely or adjust retention settings to meet compliance standards.

datto | UNIFIED CONTINUITY

Datto SaaS Protection for G Suite

Datto SaaS Protection ensures that MSPs can access, control, and most importantly protect their clients' Google G Suite data. As the leading G Suite backup solution for MSPs, Datto SaaS Protection offers all-in-one backup, search, restore, and export for Gmail, Calendar, Contacts, and Shared Drives.

G Suite is Not Automatically Protected

As organizations increasingly move data into cloud-based applications, many believe that traditional best practices such as data backup are outdated. After all, SaaS applications are always available, accessible from anywhere, and highly redundant, so why is backup necessary?

An astonishing 1 in 3 companies report losing data stored in cloud-based applications. The single leading cause of this data loss? End-user error.

Other common culprits include:

- Malware or ransomware attacks
- Malicious end-user activity
- Accidental data overwrites
- Canceled account subscriptions

With more and more companies depending on G Suite for collaboration and business operations, these risks are impossible to ignore. Backup is just as important in the cloud as in traditional on-premises IT systems. An independent, third-party, SaaS backup solution is the best way to protect organizations against the most common data loss pitfalls.

Why Google Vault Is Not Backup

While Google Vault does include some primitive recovery capabilities, it does not protect against:

- **Data loss due to permanent deletion:** If an admin or end user permanently deletes data, files are only recoverable for a short period of time. Plus, it doesn't provide admins the granular control they need—only a restore of all deleted items in a 25 day window.
- **Data loss due to a ransomware attack:** If your business suffers a ransomware attack, Google doesn't allow you to roll-back your data to a point-in-time before the corruption occurred. If you cannot restore your data to the point before the attack happened, you end up losing not only your valuable business data, but also a hefty sum of money to criminals—without any guarantee your files will be unlocked, or any future protection from the same attack.
- **Time lost in recovering files:** The time it takes to recover data from the cloud might take longer than what your business can afford. It can take anywhere from minutes to weeks or longer to restore lost data.
- **Data loss due to inactive licenses:** As one would expect, an active G Suite license is required to access G Suite data. Unfortunately, inactive or deprovisioned user data is permanently deleted, and there is no rollback option.

Why SaaS Protection for G Suite?

Trusted Backup

MSPs need complete confidence that clients' G Suite data is protected with a reliable, robust solution designed to reduce risk and time needed to manage backups.

- **Automated, continuous backups:** Protect Gmail, Calendar, Contacts, and Shared Drives with 3x daily backups or perform additional backups as needed at any time.
- **Streamlined client onboarding:** Setup is fast and easy with a straightforward click-through onboarding process.
- **Flexible retention:** Not all client environments are the same. That's why SaaS Protection offers different data retention options to meet clients' individual needs.
- **Intuitive, user-friendly management portal:** Quickly and easily determine the number of licenses in use, gauge profitability, and view clients' backup status all from a single pane of glass.

Fast & Effortless Restore

- **Point-in-time restore and export:** Quickly restore or export data from a specific point-in-time before a data loss event occurred.
- **Non-destructive restore process:** Quickly identify and recover individual objects or entire accounts with related records and folder structure intact.
- **Cross-user restore:** Restore data from one G Suite user account into another.
- **Retain user data:** Save money and effort by preserving inactive G Suite user data with SaaS Protection for as long as you need it.
- **Easy export:** Export entire accounts or specific items in standard file formats.

Effective Monitoring and Management

Have complete administrative control and proactively monitor your backup activities. Be confident in the status of all backup and recovery operations with detailed, actionable reports.

- **Backup monitoring:** Enables on-demand retrieval of events such as backup, export, or restore. Here you can see all of your successful and failed backup runs at the seat-level with error messaging around the root cause.
- **Admin audit log:** Maintain a detailed record of all administrator and user actions from your admin dashboard.
- **Multi-Admin roles:** Manage your accounts using roles such as Super Admin and multiple General Admin roles.

Predict Profitability

Build margin with bundled solutions that include protection for clients' G Suite data.

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.

Data Protection and Compliance

Balance security and transparency with powerful controls and robust user lifecycle management. Protect valuable business data from accidental or malicious acts.

- **Security and compliance:** SaaS Protection backs up data in compliance with Service Organization Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards and supports your HIPAA and GDPR compliance needs.
- **Ransomware protection:** Roll-back data to a point-in-time before ransomware attacks.
- **Custom data retention:** Keep data indefinitely or adjust retention settings to meet compliance standards.