How and Why to Backup Your Office 365 Tenant

A companion guide to the AvePoint backup calculator

AvePoint®

How And Why To Backup Your Office 365 Tenant

A Companion Guide To The Office 365 Automated Governance Value Calculator

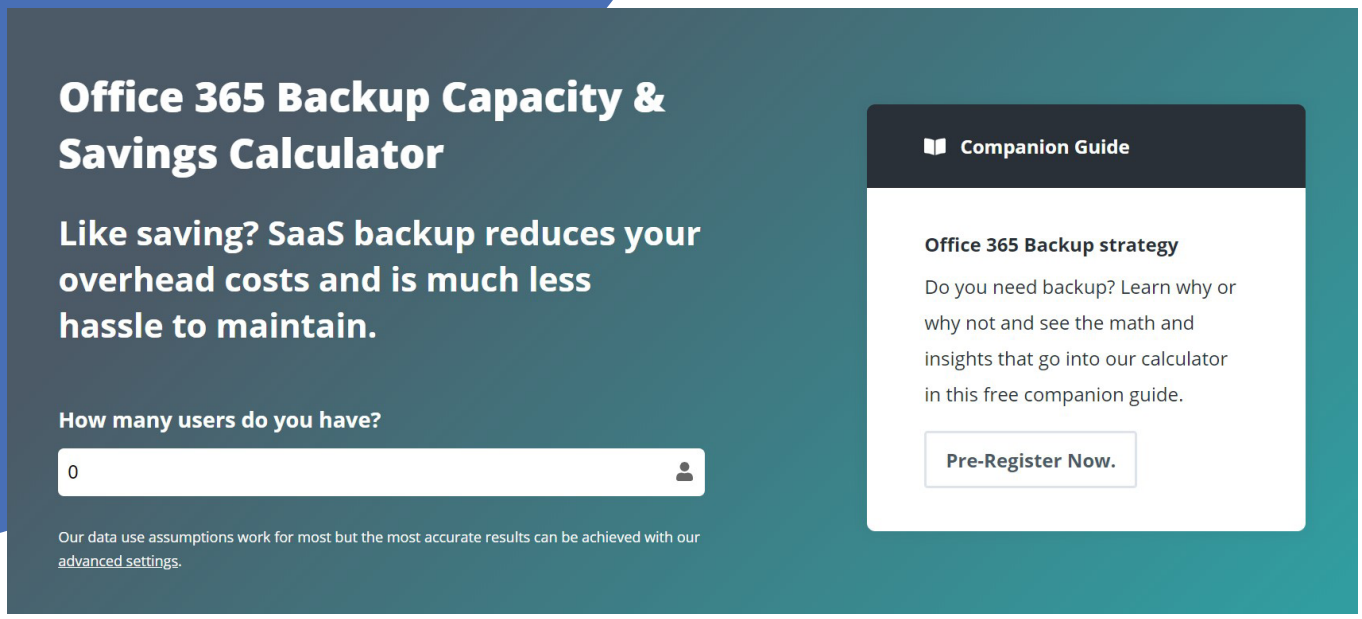
AvePoint®

Introduction

Congratulations on taking the first step in your Office 365 data protection and backup journey!

The surge in remote work has made backing up Office 365 more important than ever. Not only is data growing faster, but the platform is being used more broadly, making it critical to backup advanced workloads and every component of a Microsoft Team.

This guide will help you understand the basics of Office 365 backup, including common data loss scenarios, and how to evaluate the correct strategy for your organization. While IT budgets may be tight, the cost of losing critical business data is much higher, particularly for regulated organizations.



Interpreting Your Results From the Backup Calculator

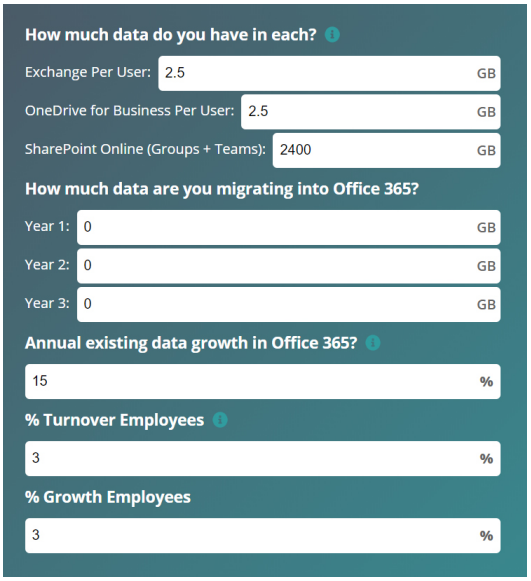
If you haven't accessed the calculator, don't worry! This guide will still be a very helpful and relevant introduction to why you need Office 365 backup and how to evaluate different technologies.

If you want to dive straight into the math, jump ahead to page 16. ▶

If you have accessed the calculator, you know the main input is the number of Office 365 users within your organization. From there, we make estimates on the amount of data you have now and how much you will have in up to four years.

This is based on a combination of industry averages, actual customer examples, and dozens of years of first-hand IT management experience by our own team members.

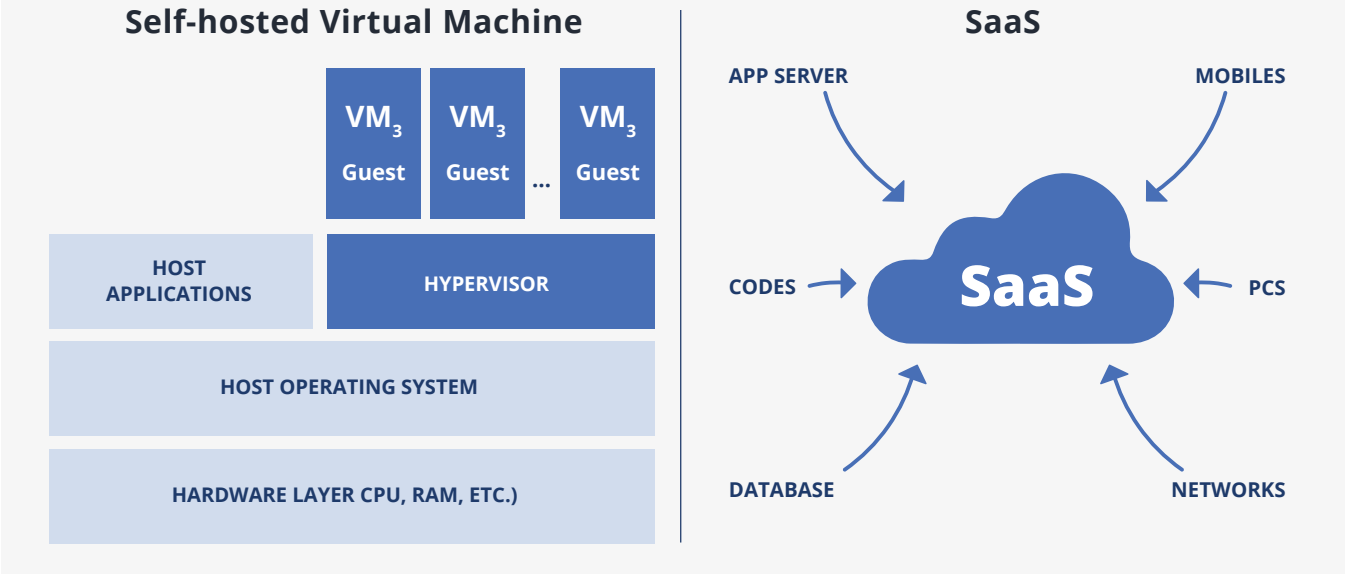
For the Office 365 admins out there, we have also given you some advanced options to customize your calculations. This includes how much data you actually have in each workspace, the amount of data you plan to migrate, your employee turnover, and how much additional headcount you anticipate (especially helpful for fast growing or acquisition-happy organizations).



After determining how much data you will have, we then do a series of calculations to see how much it will cost to store that backup data across a SaaS backup solution versus a self-hosted backup solution from a vendor like Veeam.

For the SaaS solution this involves calculating the licensing cost. For a self-hosted model solution this includes licensing as well as the cost of virtual machines, network, storage, redundancies (we conservatively include one redundancy while many self-hosted vendors suggest having two), and staff time for maintenance.

Self-hosted Virtual Machine vs. SaaS



Even though you are utilizing software that can utilize a cloud virtual machine, it's important to understand this does not mean the software is SaaS. You will still be responsible for the cost of running that machine, data storage, network transfer as well as the manual maintenance of the settings of the virtual machine.

While AvePoint does offer a self-hosted backup solution for just $.60 per month per user (a fraction of Veeam's list price), we generally recommend our SaaS backup solution because you don't have to maintain your own servers or storage.

In short, by running a solution that requires a traditional a self-hosted model to run (even though it's installed in the cloud) you're not able to take advantage of the ROI that cloud SaaS offerings can bring.

Our calculations show that in virtually every circumstance, a SaaS based cloud backup solution is the most cost-effective option. However, even for the limited, edge scenarios where self-hosted backup may be more cost effective—say if an organization had already acquired excess compute resources—SaaS backup may still be a better option.

That's because your IT team has better things to be doing than maintaining backup infrastructure. For example, we conservatively project an organization of 6,000 users with a data growth rate of 15 percent will spend 644 hours on

You've got options when it comes to Office 365 backup...

Lowest Retention

1 YEAR OF DATA RETENTION

73% SAVINGS

OVER 3 YEARS COMPARED TO SELF-HOSTED

Peace of Mind

2 Years of Data Retention

53% SAVINGS

OVER 3 YEARS COMPARED TO SELF-HOSTED

Long-term Savings

3 Years of Data Retention*

37% SAVINGS

OVER 3 YEARS COMPARED TO SELF-HOSTED

45% SAVINGS STARTING YEAR 4

**AvePoint Unlimited savings grow as the plan matures.*

self-hosted backup maintenance over three years. And if a mistake is made, the entire digital workplace gets impacted!

Finally, not all clouds or SaaS backup solutions are created equal. In this eBook, we will lay out some methodologies and considerations you may want to leverage when evaluating solutions. Things like:

- RTO and RPO
- Security credentials
- End user restore capabilities
- And much more!

Don't forget the hassle of self-hosted backup.

Your time spent maintaining application servers, networks and storage...

644 Hours

OVER 3 YEARS

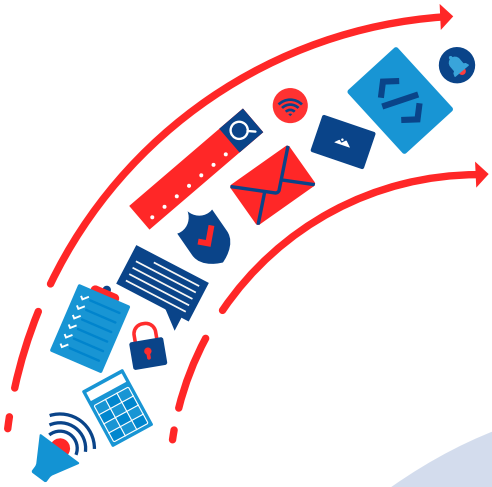
Disclaimer:

It's important to understand the values provided by the Office 365 Backup Calculator are simplified estimates based on limited input data. This was done to make the calculator as accessible as possible for a broad spectrum of audiences.

AvePoint can work with you to discuss and further distill the value of a SaaS Office 365 backup solution for your organization. If downloading this guide was your first step in your data protection and backup journey, consider this the second.

You will also want to supplement the topline number provided by the calculator with a greater understanding of why and how to backup Office 365.

However, if you want to jump to the explanation of how we made these calculations skip to page 16.



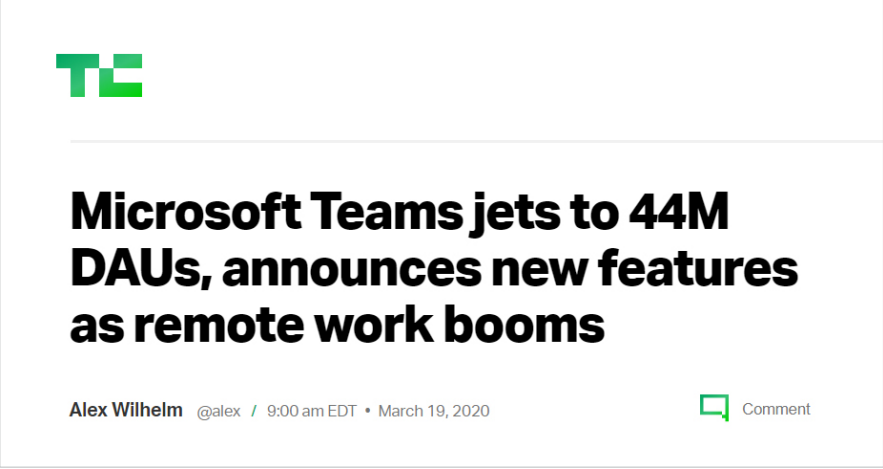
Reasons To Backup Office 365

Data security and recovery in the cloud era

Organizations have shed their servers and gone to the cloud in record numbers. The coronavirus pandemic has only accelerated this trend as organizations need to fully support remote work.

This is particularly true of Office 365, which sees more than 200 million commercial users log in each month.

The excitement and potential for productivity gains can also be seen in the growth of Microsoft Teams, the fastest growing business application in the company's history. And, as people started working from home in record numbers starting in March 2020, Microsoft Teams usage surged more than 110 percent.



TC

Microsoft Teams jets to 44M DAUs, announces new features as remote work booms

Alex Wilhelm @alex / 9:00 am EDT • March 19, 2020 Comment

This move to the cloud and enabling remote work requires organizations to think differently about how they are protecting and backing up their data. In the past, organizations kept physical backup copies of their data in an on-premises data center or rack of servers.

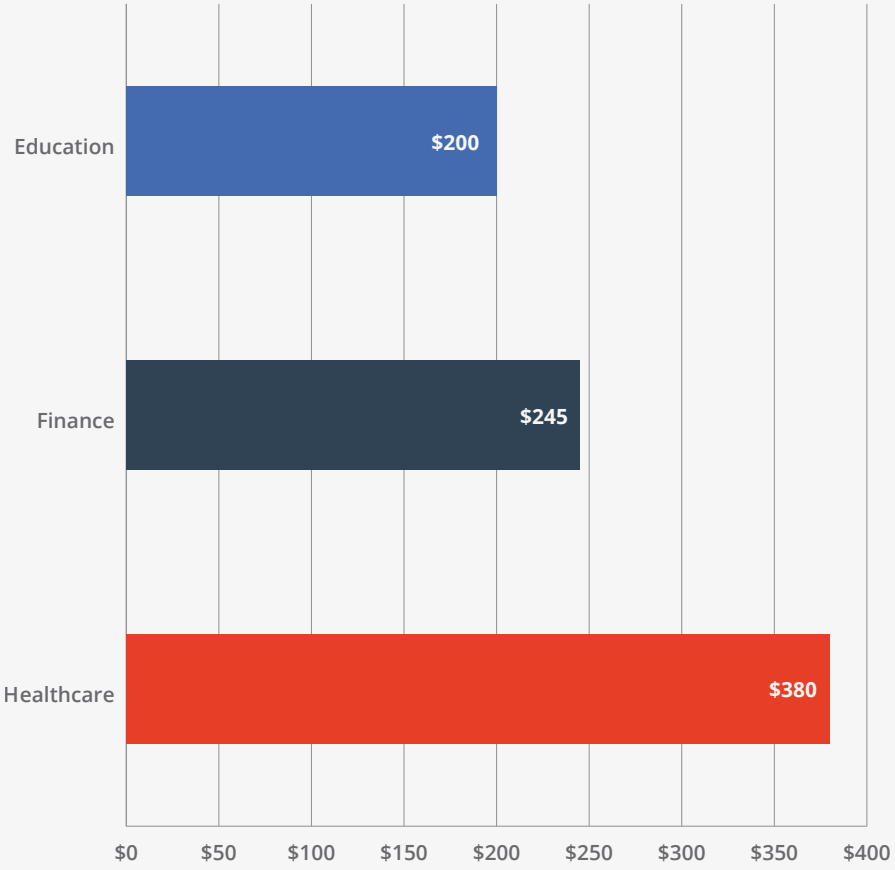
With this infrastructure now virtualized and provided as a service today, organizations should examine relevant regulations as well as the service level agreement (SLA) with their cloud service providers to determine if extending the default protection levels is an appropriate strategy.

Office 365 provides industry-leading data protection and retention mechanisms for organizations (more on that later). However, a recent Forrester report points out that every SaaS provider, including Microsoft, explicitly assert clients are responsible for protecting their own data.

Yet, an IDC study (and several others) have consistently shown only about **40 percent of organizations using Office 365 are leveraging a third-party backup solution to protect their data**.

The cost of data loss

Average Cost Per Industry



- **Education:** $200 per lost or stolen record
- **Finance:** $245 per lost or stolen record
- **Healthcare:** $380 per lost or stolen record

Additional Notes:

60%
of small businesses that lose data will shut down within 6 months

13%
of organizations are prepared to handle data loss and ransom-ware attacks

50,000
compromised records results in a data breach of
$6.3 million

The reality is organizations experience data loss. **One recent survey found 80 percent of companies using SaaS have lost business data.**

This can be costly. A Verizon report found small data loss incidents can cost businesses an average of up to $35 thousand. Large incidents of more than 100 million records can cost up to $15 million.

This doesn't even measure the full impact—what's the cost of your organization not being able to run for a period of time?

As such, most organizations that value their data will consider a third-party backup solution to ensure their data is fully protected and available across all data loss scenarios.

Let's look at some of these scenarios where extended data protection can ensure the availability of information.

Data loss scenarios

User Error

Accidents happen—we're human after all—which is why the most common data loss scenarios involve user error.

Users can accidentally delete documents, emails—and even an entire workspace (Group, Team, or SharePoint site) if they are an Owner. That's why Microsoft has effective out-of-the-box tools such as version control and the recycle bin to address these mistakes.

If a document has been deleted within 93 days, an email has been deleted within 14 days (or up to 30 days depending on your settings), or a workspace has been deleted within 30 days, you can simply restore these items from the recycle bin.

Third-party backup solutions allow you to extend these protections so you can restore Office 365 data even if it has been deleted for longer than 93 days.

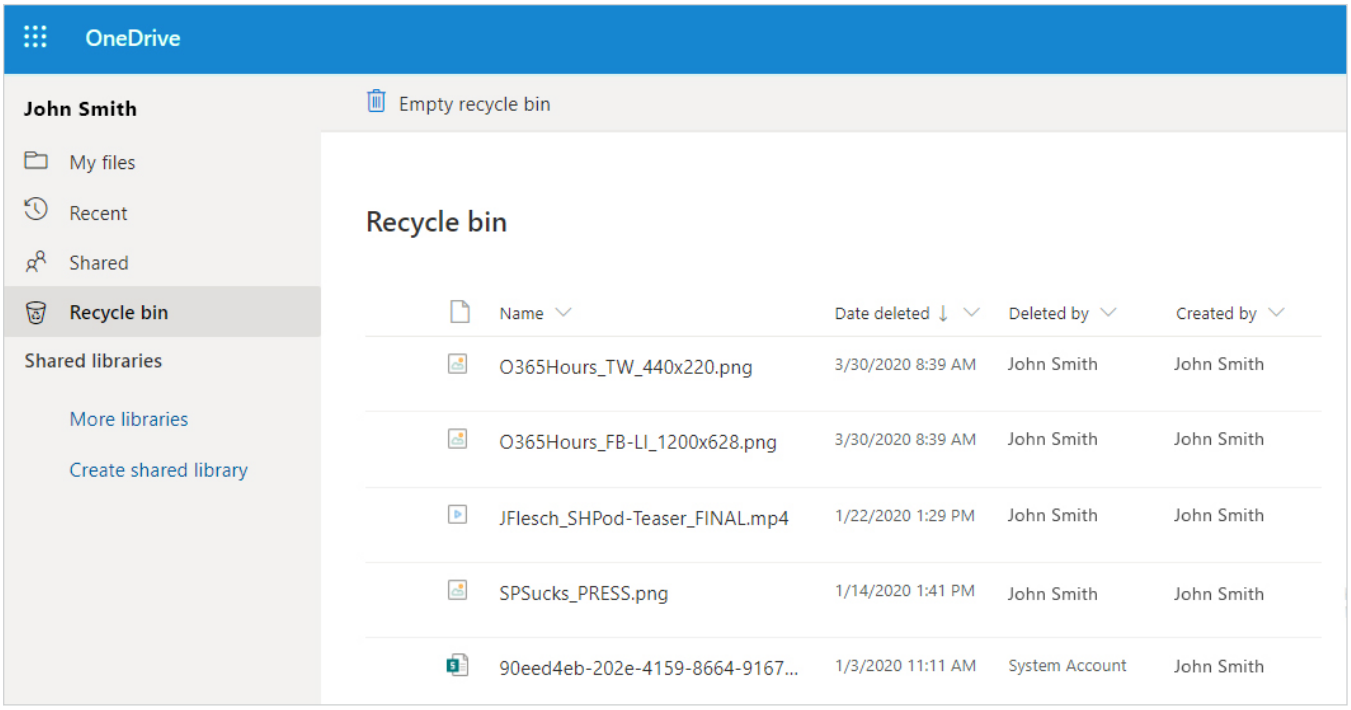
Admin Error

Office 365 administrators and IT professionals are also human, and thus just as capable of making the occasional error.

One scenario could include messing up the permissions to a workspace. A third-party backup solution will be needed to quickly restore those permissions.

Another scenario would be forgetting or failing to set the proper retention setting—for example not properly retaining a mailbox of an employee who has departed the organization.

After the 30-day window (and its almost always after), if a user needed to access that mailbox, or that data was needed for record/compliance purposes, a third-party backup solution would be required.



File Versioning / Recycle Bin

Malicious Insiders

On occasion a disgruntled user or administrator may attempt to delete, corrupt or otherwise remove access to important data within Office 365. In most scenarios, the data can be easily restored using native tools.

However, if that malicious insider—either a user that is an Owner of a workspace or an administrator— "rolls back" or restores a SharePoint site from a previous point in time, a third-party backup solution is required to "move forward" and restore the data that has been created since that restore point.

Malicious Outsiders

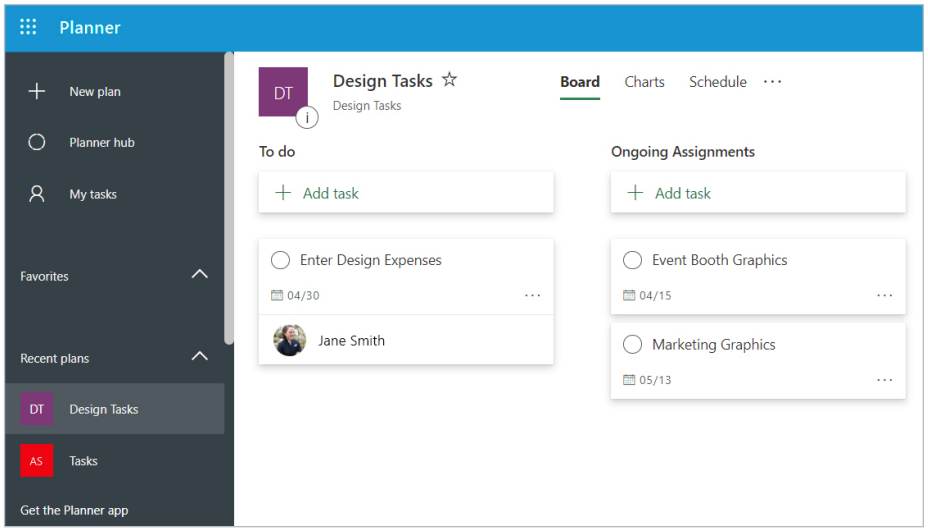
Ransomware attacks are a rising type of cyber attack typically involve an outside threat compromising a system to block access to its data until they are provided with a ransom (often in Bitcoin).

In 2018 for example, the City of Atlanta spent $2.6 million to respond to a ransomware attack that had impacted their municipal operations.

In these scenarios, having a backup copy of your data can enable agencies to quickly restore the compromised data and resume operations.

Project or Planner Data

For organizations using the Project or Planner services within Office 365, a third-party backup tool can help backup critical granular items such as Planner tasks or sites.



Change how long permanently deleted items are kept for an Exchange Online mailbox

02/07/2020 • 3 minutes to read • +4

If you've *permanently* deleted an item in Microsoft Outlook or Outlook on the web (formerly known as Outlook Web App), the item is moved to a folder (**Recoverable Items** > **Deletions**) and kept there for 14 days, by default. You can change how long items are kept, up to a maximum of 30 days.

> ⓘ Note
>
> You must use Exchange Online PowerShell to make the change. Unfortunately, you can't currently do this directly in the Outlook or Outlook on the web.

How To Backup Office 365

Which backup approach is right for your organization

There are two main approches to Office 365 backup: either leveraging self-hosted software or a Software-as-a-Service (SaaS) solution.

As concluded in the Forrester report, cloud-to-cloud (SaaS) backup is the only practical option. That's because self-hosted backup software does not easily scale as your data grows and it requires much more manual work to manage.

With a self-hosted backup solution, the organization is responsible for all the **infrastructure** behind it, including:

- Installation and configuration of the platform
- Scaling and deployment of the necessary servers to support this software
- Network bandwidth and monitoring for connections to Office 365
- Storage for all Office 365 backups, including redundant storage locations to protect against disk-failures or corruption

In addition, the organization is responsible for the **configuration** of the software, including:

- Maintaining server solution service accounts and authentication for connections
- Deciding on the best backup scope / schedule between full vs. incremental backups (often monthly full backups of all Office 365 content)
- Configuring storage locations and capacity planning to match backup schedules

And let's not forget the **ongoing maintenance** of the software, including:

- Constant monitoring for Office 365 throttling errors due to service account activity
- Monitoring network consumption to prevent interference with user-traffic on the organization's network
- Monitoring security logs for the platform to ensure no unauthorized actions are taken by the administrators
- Support and troubleshooting are on the shoulders of the organization's IT Team

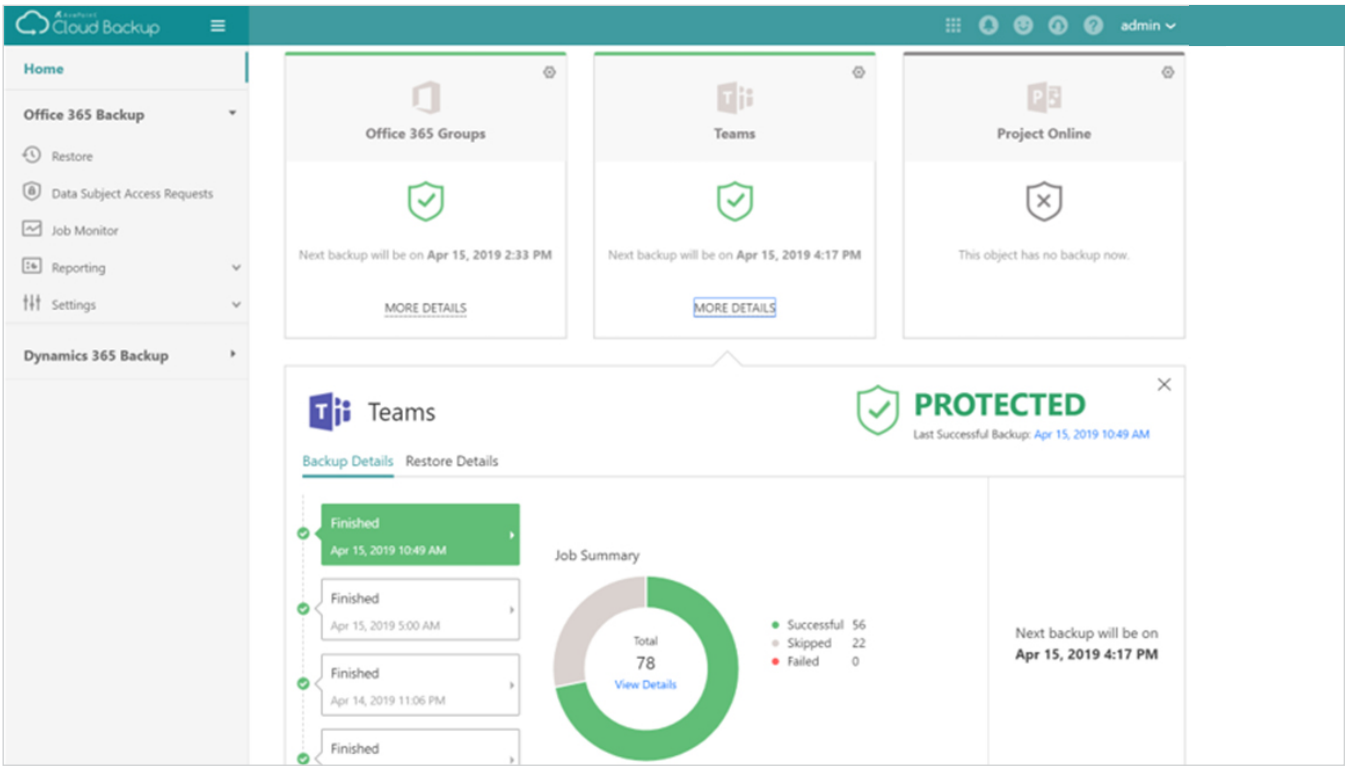
Not only could a self-hosted software impede your IT team from providing reliable business continuity, the time spent on these items can be better spent on higher value tasks.

In short, simply backing-up your data on a server does not equate to an effective data protection program.

How to evaluate SaaS backup providers

The trend in digital workplace solutions is away from rigid self-hosted systems, and towards subscription models and cloud-based SaaS providers.

However not all clouds are created equal. There are four critical components to evaluate when developing your data protection and Office 365 backup strategy.



1. RPO and RTO

Anytime you discuss Office 365 data protection, you need to approach the problem with two primary goals in mind: Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

RPO, the maximum targeted timeframe in which data can be restored from a backup, includes the plan for the frequency of backups as well as your ability to recover individual components.

Consider, how recent does the backup need to be? In other words, how many times a day is your data backed up?

Also, how granular do you need to be able to restore content? Is it at the item level? Is it Team channel conversations? Does the solution backup and restore files and folders in Groups, Teams and SharePoint?

RTO, or the amount of time in which content must be restored, helps you refine your recovery points as well as classify the data you are backing up. Consider, how quickly will business users need their content restored? Also, how much content can I restore inside of a specific time frame?

If you are not able to restore user content quickly enough, your organization can grind to a halt and all eyes will be on you as the administrator. Ensuring that you can restore content on-demand as quickly as possible is the first step in protecting not only your organization's content but also yourself.

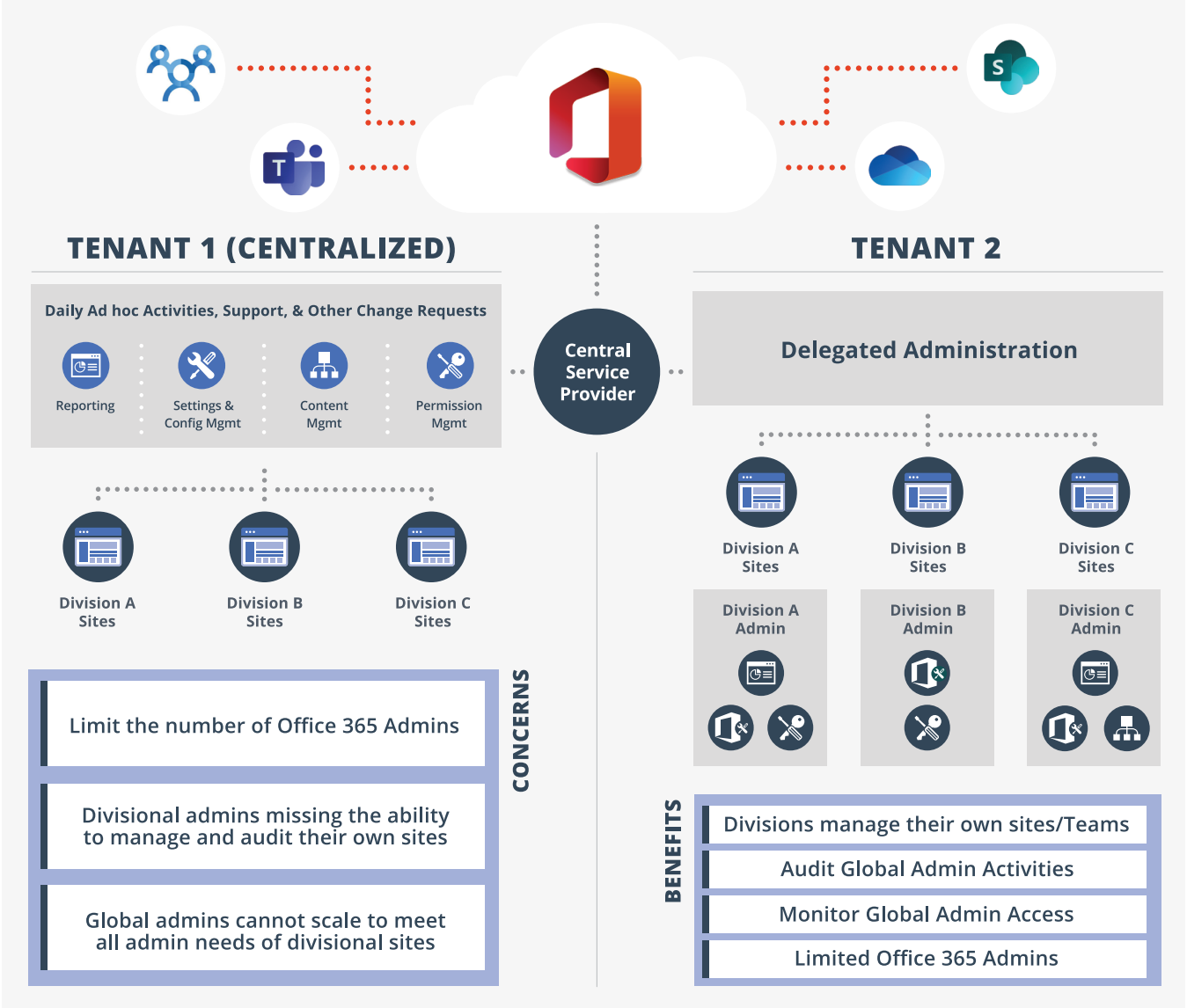
2. Ease of Use

One of the benefits of SaaS backup solutions is they are typically quick to install and maintain. You will want to make sure the user interface is intuitive for restores.

Evaluating the ease of use is not just about the installation and user interface, however. Larger businesses, for example, often must deal with large complex tenants that span across departments and even countries.

This helps collaboration and prevents data silos. However, by softening the traditional barriers that existed from maintaining separate SharePoint servers on-premises, administration has now become an all-or-nothing proposition. There are no smaller containers within the tenant that can have their own administrators.

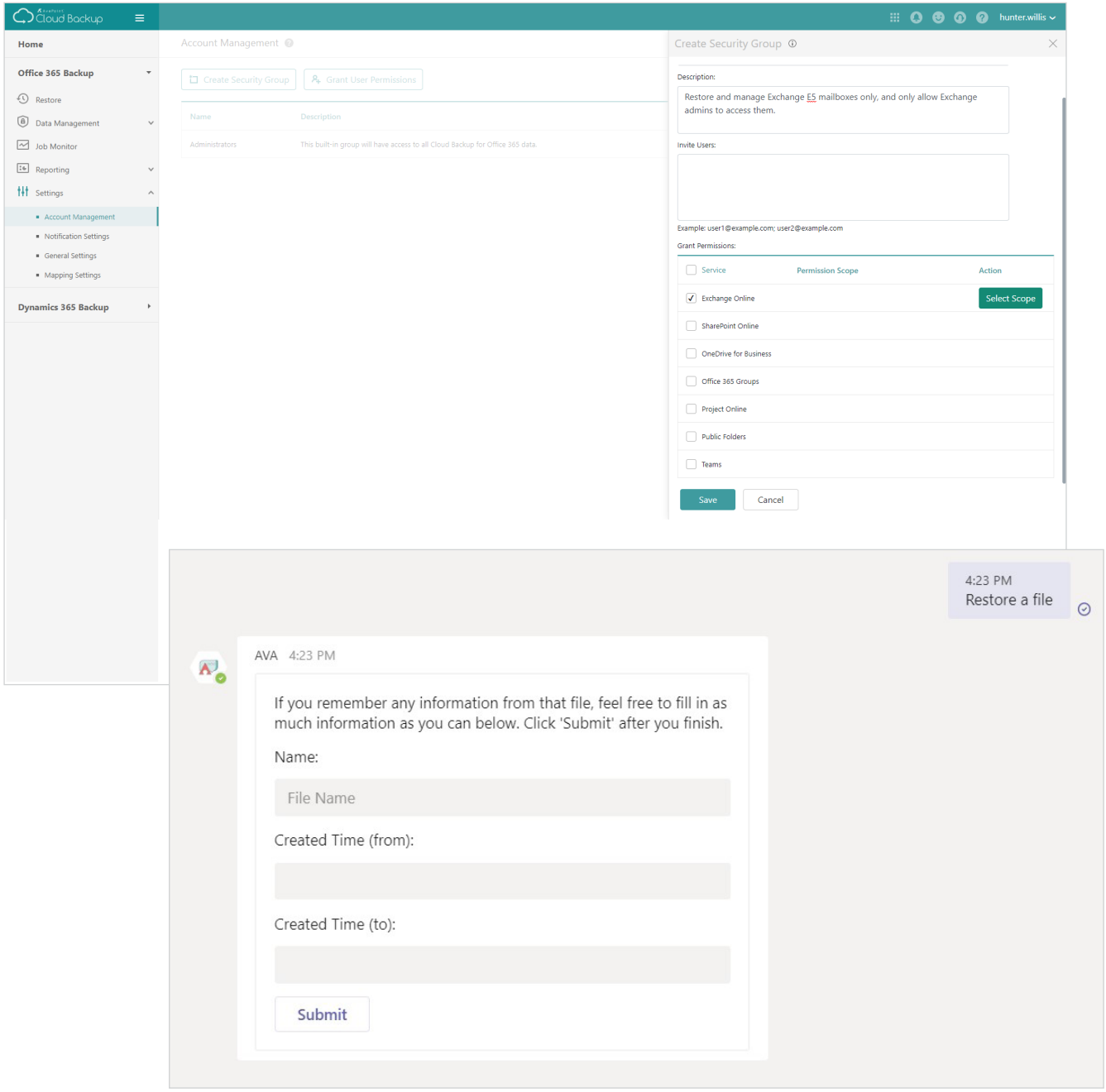
Centralized Tenant vs. Tenant with Delegated Administration



Imagine being able to take your central Office 365 tenant and carve it up into separate, more manageable containers with that can be administered at the division level without giving up access to the entire tenant.

So, for example, while Contoso may be under a single Office 365 tenant, they could then create Office 365 admins in the North America marketing department who just have access to those workspaces and data when managing backup and restore tasks.

Finally, giving users the access to find and restore their own lost data, and only their data, can free IT teams from routine restore tasks. Evaluate if a cloud backup solution has self-service options for your users.



3. Security and Credibility

When you are leveraging the SaaS solutions of a vendor, you are inheriting their level of commitment to organizational security. Certifications and standards like ISO 27001 are important indicators that a SaaS vendor is fully committed to the security of their solutions.

Engineering Security into Managing Office 365

- RBAC to All Environments
- Secure credentials & MFA
- Azure-Based Security
- Auditing & Alerting

Security Event Response

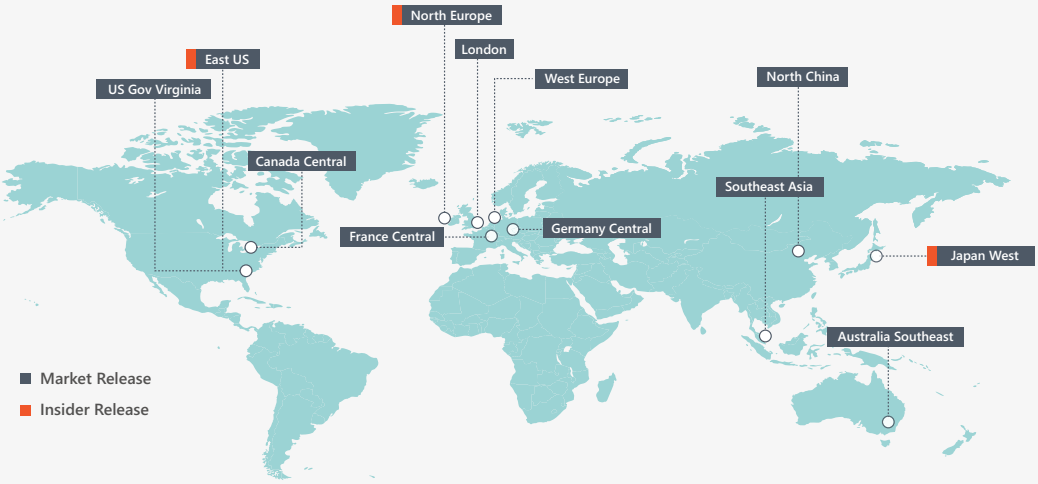
- Monitoring/Auditing for all activity
- Alerting for potential risks
- SIEM integration for AOS platform
- 7*24 hour for security event response

Another helpful question to ascertain your SaaS vendor's dedication to security is what level of access they have to your data. For example, AvePoint leverages Azure Key Vault to provide unique encryption keys for each tenant that is owned by each customer to prevent unauthorized access.

Another consideration is if your data must reside in a certain geographic area or data center, your backup data may need to as well.

Can your backup vendor support multi-geo capability? This is the ability to provision and store data at rest in the geo locations that you've chosen to meet data residency requirements.

Global Cloud Footprint



4. Licensing

Does the backup SaaS provider have multiple licensing options to make their solutions easy to buy?

There should be options to have access to the level of functionality you need, flexible user adoption ramp up schedules, and contract plan options. Most vendors will offer pricing per user, but for some organizations, licensing per amount of backup needed may be a better option.

Backup Math:
Our Calculator Explained

And now the moment you have been waiting for! Here are the assumptions that drive our formulas.

Input Field	Default Assumption
Exchange Online	2.5 GB per user
One Drive for Business	2.5 GB per user
SharePoint Online (Groups and Teams)	We determine the number of workspaces by dividing the number of users by 50. We then assume about 20 GB per workspace.
Migrated from Legacy Sources	0
Annual Growth of data in Office 365	15%
% Turnover in Employees	3%
% Employee growth	3%
Versions	20% of the data has 5 incremental copies

Assumption Explanations

These assumptions are based on a combination of numerous market studies, our own market research, and compiled statistics from industries across nearly every vertical. If anything, with the recent surge in remote work, these assumptions are overly conservative.

Exchange Online

At Ignite in 2018, Microsoft revealed telling statistics related to their Exchange Online infrastructure as covered by Tony Redmond. By dividing 1.1 exabytes of data by 5.5 billion mailboxes you get about 200 megabytes per mailbox. When you account for the nearly 30 percent growth in Office 365 commercial users since then, and discount the millions of inboxes from service accounts and inactive Office 365 Groups and Teams, our 2.5 GB is a very safe assumption.

OneDrive for Business

By default, each user at an organization gets up to 1TB of OneDrive For Business storage space. In 2015, Microsoft walked back their unlimited storage offer for paid Office 365 Home and Personal subscribers saying that some extreme users had 75 TB of storage or more than 14,000 times the average.

That means at the time the average user had 5.5 GB. Assuming the average business user, has less than half that amount is a safe, conservative number considering they should have more data needs than personal accounts.

SharePoint Online (Groups and Teams)

File data for Groups and Teams is actually stored in SharePoint so we don't break these virtual workspaces out separately for the purposes of the backup calculator (but it's important to be sure your backup solution is backing up more than just inboxes and files in Teams).

We determine the number of virtual workspaces by dividing the user count by 50. This is the average ratio we have seen across our 16,000 wide customer base, however we have seen some organizations with ratios as high as one workspace for every user. We have even seen an organization with 1,500 users and more than 2,000 workspaces. We then assume each workspace has an average of 20 GB of data.

Exchange Online Scale

Footprint

- **175k** Physical Servers
- **47** Datacenters
- **70** Network POPs

Storage

- **5.5** Billion Mailboxes
- **1.1** EB of Data (logical)
- **35** Trillion Items

Daily Processing

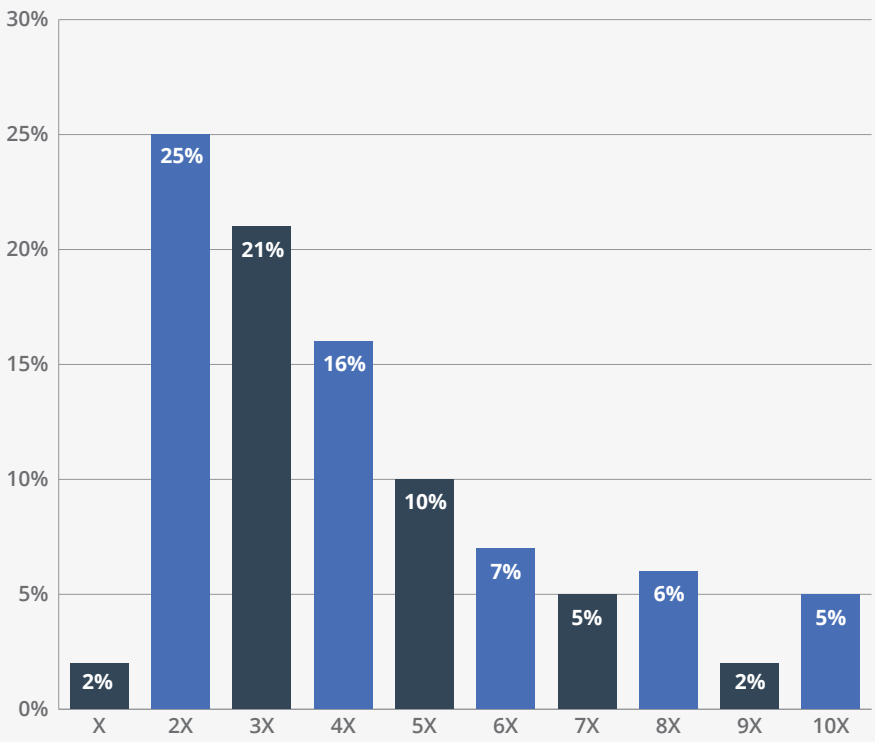
- **7.2** Billion Messages Delivered
- **490** Billion Requests Routed
- **1.4** Trillion Items Read/Opened
- **9.6** PB Jet Logs Processed

Average Growth Rate

Our calculator's default assumption is a 15 percent growth rate, which may be our most conservative assumption in our model.

For example, in an AIIM Industry Watch survey we sponsored entitled, "Building an Effective Strategy for Content Integration and Migration," 98 percent of respondents estimated their data growth to be 2X or higher in two years. 37 percent estimated 5X or higher.

Think about the huge amounts of data and information currently coming into your organization (call the current volume "X"). What do you predict this volume will be in two years?



Employee Growth and Turnover Rate

Our employee growth rate assumption assumes organizational growth just a hair over the overall growth of the national economy, which grew at just over 2 percent in 2019. For the employee turnover rate, we also assumed a very conservative 3 percent, whereas HR associations place the national rate closer to 19 percent.

Versions

We assume 20 percent of an organization's data has been touched or modified 5 times. Some documents will be modified extensively, but typically 80 percent of data stored by an organization is "dark data" -- legacy data that is unknown to most if not all workers.

Additional assumptions for cost, hours spent maintaining servers:

1
virtual machine for every 5 TBs

$1.50
per license/user for self-hosted model software

.04264
cost per gig per month (Azure storage and one redundant backup)

$60.00
per hour x 2 hours per month per virtual machine maintenance

These assumptions are all based around current market conditions and prices. We assume one local redudant copy of the data, however, many self-hosted backup vendors actually recommend two redundancies as a best practice.

AvePoint Cloud Backup

Teams that are already using Microsoft Office 365 but need a higher level of data protection and recoverability should look to a SaaS data backup solution that's designed for frictionless Office 365 integration.

The best indicator of this compatibility is to find a service provider with a long-standing Microsoft partnership.

AvePoint Cloud Backup provides organizations with automatic backups and granular, item-level restoration capabilities—not to mention the company is also a four-time Microsoft Partner of the year, a Microsoft Global ISV Partner, and they've also been named to the Inc. 500|5000 six times and the Deloitte Technology Fast 500™ five times.

AvePoint's solutions build on native SaaS security capabilities with ISO 27001:2013 certification with respect to secure software development and maintenance process including support of business functions like Infosec, IT, HR, Sales and Marketing, Project Management, Operations and Call Center.

AvePoint's Cloud Backup platform also empowers organizations to:

- **Accident-proof their SLAs.** Meet stringent SLAs with automatic backups up to four times a day and get the flexibility to customize your SLAs for RPO and RTO, instead of relying on Microsoft's default restoration and retention policy.

- **Own their data.** Maintain full access and control over your backup data, not just what's in your Recycle Bins. If you need to store backup files for a longer term than the 15-30 days provided by Microsoft, you can compress and encrypt on the storage platform of your choice.
- **Recover on their own terms.** You choose what to restore and where to restore it. Access a backup from weeks ago, or access files during any service disruption: perform in-place or out-of-place restores for granular objects or content, without overwriting valuable data since the last backup, or having to go through Microsoft Support.
- **Integrate existing security processes.** BYOK, BYOS and BYOA solutions keep your existing security practices operating:
- **Customer-Owned Encryption Keys.** Azure KeyVault ensures unique keys for each tenant, owned and managed by each customer to prevent unauthorized access.
- **Customer-Owned Data Storage.** Data Residency provides hosted options through Azure or through any customer-owned cloud and server storage service.
- **Customer-Owned Authentication.** Single Sign-on with Office 365 Credentials and Azure AD applications ensures customers retain control of the authentication and authorization of AOS.

AvePoint's Cloud Backup also gives organizations the ability to delegate restore capabilities to divisional admins, all sitting within the same Microsoft Office 365 tenant.

AvePoint's Cloud Backup solution keeps business-critical emails, calendars, sites, groups, teams, projects, files, and conversations secure—with unlimited, automatic backup and anywhere storage.

Case Studies

MSP Ictivity Takes Full Advantage of Cloud Backup's SaaS Capabilities for Their Clients

Success Highlights

- Fast implementation
- Reduced IT overhead

Customer Profile

IT must make processes more efficient, support employees in their tasks and add value to customers. Moreover, IT must support the strategic ambitions of an organization. This sounds logical, but very few organizations realize this. Ictivity knows what it takes to achieve this.

They take over operational activities, from managed services in a specific area to outsourcing of the entire IT environment. In all cases they have only one goal in mind: helping you to get the maximum value from IT.

The Challenge

In their frequent work for healthcare clients, Ictivity finds that their customers' most critical need is centered around data retention compliance. For example, "patients' data needs to be kept for 15 years and personal data for 7 years," said Visser. "When [the healthcare client] moves to Office 365, they needed another solution to back up."

As one of the fastest growing MSPs in Europe, Ictivity made sure to conduct their due diligence. They tested three backup solutions before ultimately purchasing AvePoint's Cloud Backup through Ingram Micro.

The AvePoint Solution

Visser explains that previously all client restore requests had been going through System Admins, which is one of the more common concerns with native backup and restore functionality due to the unnecessary time cost.

> *"We were really looking for something that gives [clients] a self-service option to restore," said Visser. "The time that it took to bring an item back was very slow and a large process. Over the last few years, Office 365 has grown very fast including apps other than Exchange. So, the need for a good backup and restore with self-service was very important for our customers."*

Ictivity finds Cloud Backup's chatbot within Teams – AvePoint Virtual Assistant (AVA) – to be a very useful feature that allows their customers to directly execute small restorations of data such as a single file or map.

Visser explains, "that was our biggest concern. We needed a tool that gives the end users an easy way to find their data and bring it back."

Ultimately, Ictivity wants the experience of a backup solution to be as seamless as possible requiring little customer attention.

"Our customers don't even know that the product is AvePoint. We just provide them with the functionality and services from Ictivity," said Visser.

The Bottom Line

During Ictivity's testing of Cloud Backup, they found AvePoint's support to be second to none.

"Every question was very quickly answered. However, we didn't have any problems when we implemented the solution and we now have four customers using it," said Visser.

Overall, Ictivity is very pleased with AvePoint's Cloud Backup solution and how advanced the product is.

> *"As an MSP, it's very important that the solution is SaaS. All of the other solutions we looked at, I had to build the whole infrastructure for, requiring a lot of technical guys," explained Visser. "I don't need to do that with AvePoint. That along with AVA and the multi-tenancy management platform have been the most important things."*

Dublin Airport Authority handles with care 38 TB of Office 365 Data, using AvePoint Cloud Backup

DublinAirport

Success Highlights

- Successfully backing up 38 TB across Exchange Online, SharePoint Online, OneDrive for Business, Office 365 Groups and Microsoft Teams.
- Reduced workload of IT staff, allowing them to work on more higher priority projects
- Data Regulated SLAs fulfilled

Customer Profile

daa is a global airports and travel retail group with businesses in 13 countries. The organization is owned by the Irish State and headquartered at Dublin Airport.

The organization manages Dublin and Cork airports and have overseas airport operations and investments in Cyprus, Germany, and Saudi Arabia.

Their travel retail subsidiary ARI also has outlets in Europe, North America, the Middle East, India and Asia-Pacific. daa also provides international aviation advisory services.

daa has about 4,000 users of which about 60 percent are knowledge workers with the remaining 40 percent consisting of kiosk/firstline workers who work in roles such as maintenance.

The Challenge

Given that daa is a regulated organization, they have taken a more conservative and careful approach to Office 365 driven in large part by their partners who help deliver their mission critical systems.

The organization realised they need a third-party backup solution as the standard Microsoft 90-day retention period for deleted content was not sufficient to meet their internal retention policies.

Following advice from external analysts like Gartner, daa also decided to create an exit strategy from Office 365 in the highly unlikely event that they decide to move away from the platform.

"To support this strategy, we needed an independent location for our data," stated Kevin Ryan, IT operations team lead at daa.

The AvePoint Solution

After conducting extensive market research, AvePoint Cloud Backup was the only product which met all their operational and IT security requirements.

Their security requirements included encryption of data, multi-factor authentication, ISO 27001:2013 compliance, and data deletion via GDPR Article 17.

> ***"The only way to have full protection from ransomware is to invest in a 3rd party backup solution like AvePoint Cloud Backup," said Ryan.***

Operationally, they wanted a solution that could backup multiple Office 365 workloads at a granular (item/permissions) level while also protecting them against potential malicious insiders.

The onboarding and support experience exceeded their expectations. "One of the other impressive things about AvePoint, is their support. Having worked with multiple vendors and providers and various sizes and structures of support over the years, I would have to say that AvePoint support is up there with the best, in my experience."

The Bottom Line

daa has been using AvePoint Cloud Backup for three years and has been very impressed with the usability of the SaaS product.

"Ease of use really stands out for this product – it just works. From an operational perspective, I am obsessed with minimising complexity," stated Ryan. It frees up the team to do what they want to do so they stay interested and engaged. It keeps our stakeholders happy – everybody wins!" stated Ryan.

This is in stark contrast to their backup solution for their on-premises data that spans 20 servers, four separate SANS and requires a team to support.

Introducing four different restore points each day was also a major change for daa, but one that save their users and admins "quite some time."

Overall, daa has had a very positive experience.

> ***"AvePoint provides a modern service and is a company that seem to have really thought about how to make our lives easier, while ensure that our data is protected," stated Ryan.***

Walls Construction Protects Critical Data from Ransomware Attack with AvePoint Cloud Backup

Success Highlights

- Reduced time spent managing cloud backup by 90%
- Reduced time spent on permission management by 70%
- Increased insight into permission rights for Mobile users

Customer Profile

Walls Construction Limited is an Irish owned building contractor operating nationally with offices in Dublin and Cork. The business was established by PJ Walls in 1950 and is today recognised as one of Ireland's leading construction companies.

The Challenge

Following their roll out of Office 365 and SharePoint Online, Walls experienced an incident with one of their members of staff being hit with a malicious ransomware attack.

The staff member's OneDrive was replicated and then deleted, resulting in the complete loss of that user's data. Walls Construction IT Manager, Robbie Armstrong, realized that despite the robust security features provided by Office 365 and strong security awareness of his user base, company data had to be protected through a third-party backup solution.

"With the amount of control that Office 365 brings to end users, it is not realistic for a company to

completely monitor every deletion. So we had to have a way to very quickly and easily recover from something like this, and began evaluating Office 365 backup products," said Armstrong.

Additionally, his team wanted to become more efficient in managing Office 365 so they could focus on higher value tasks.

"We were looking for a third-party solution to make our administrative work less tedious. Some of the steps in Office 365 are too laborious, especially as Microsoft gives SharePoint a cleaner user interface which by doing so sometimes hides functionality that we need," said Armstrong.

Part of this administrative worked involved constant permission and access management modifications. Due to the nature of its industry, a number of Walls Constructions' employees are hired on a project basis resulting in a highly mobile workforce.

The AvePoint Solution

After Walls Construction's experience of being hit by ransomware, they evaluated multiple leading backup solutions.

The ability to scale across many applications, customize the settings, and automate backups were the primary features that ultimately lead to the decision of AvePoint's Cloud Backup.

"The amount of work that had to be done has completely changed. AvePoint Cloud Backup being automatic makes it so simple. We don't have to worry about anything and a recovery takes only about four clicks. From a backup management perspective, Cloud Backup has removed 90% of our time costs," said Armstrong.

While they have only had to make about four to five recoveries over the last six months, Armstrong says those recoveries, "would have been a nightmare without the solution, it couldn't be any easier the way it is now."

Walls Construction also decided to leverage AvePoint's Cloud Management solution to address the mobile user base and the need for batch permission changes, cloning permission levels, and pulling access reports.

The Administrator module in particular has cut down their permission management effort by 70%.

"We have been using the Administrator module in Cloud Management primarily for removing dead and dormant accounts," said Armstrong. "But we also leveraged the tool to discover a junior member had full admin rights to every single project and every library within our document management system. This was discovered by the Administrator solution before we issued that user's credentials. Therefore allowing us to make the required changes preventing access to sensitive areas."

Walls also uses Cloud Management's reporting functionality through Report Center and Administrator. The presets most frequently accessed are the permission and compliance reports. These reports show who has access to what and last accessed time.

"I will run reports based on who has access to what, dead accounts, and when something was last accessed. We understand that far more reports can be pulled with Report Center and will soon be leveraging the solution more when we have the time," says Armstrong.

The Bottom Line

Walls Construction is very satisfied with both the solutions and the service from AvePoint.

> ***In Armstrong's words; "The best service you will ever receive, is one that you don't have to interact with. I think I have only had to reach out to AvePoint once or twice over the years. We have never had a problem."***

Walls Construction is now not only more confident in their permission and backup, but they have also been able to free up a majority of their time to focus on adding value to the business and taking full advantage of their Microsoft investment.

Additional Resources

Request a demo or try now for free for up to 30 days ! Specify the tenenat you'd like to use for your free trial:
https://www.avepoint.com/products/cloud/backup/office-365-backup

Analyst Report

- Back Up Your SaaS Data — Because Most SaaS Providers Don't

Webinar

- Practical Guide: Office 365 Backup Strategies That Scale
- Make It Easy! Office 365 and SharePoint Employee On/Off-boarding
- Debunking Myths: Native Office 365 Backup Coverage and Gaps
- Cloud Backup: Delegate Access to Restore Capabilities & Meet Your New Virtual Assistant
- Everything You Need To Know About Cloud Backup
- TKO DocAve Online Backup vs AvePoint Cloud Backup Customer Success Webinar

Blog

- 8 Things You Should DEMAND From Your Office 365 SaaS Vendor
- How To Protect Your Data with SharePoint Online Backup
- Backup Office 365 Groups with AvePoint Online Services
- Protecting Your Email in the Microsoft Cloud: Exchange Online Backup
- Office 365 Backup Retention Policy, 3 Things You Need to Know!
- AvePoint's Unlimited Office 365 Backup, Why Its Right For You

AvePoint®

525 Washington Blvd, Ste 1400 | Jersey City, NJ 07310

P: +1.201.793.1111 | E: sales@avepoint.com | www.avepoint.com