AvePoint

# Your Ultimate Office 365 Backup Handbook

Enhance Your Microsoft Office 365 Data Management Strategy

# Table of Contents

## Contents

Chapter 1: Data Loss in North America ........ 1

The rising cost of lost data ........ 2

Chapter 2: How Data is Lost ........ 3

Technical faults or glitches ........ 4

Rogue IT administrators ........ 4

User error/accidental deletion of data ........ 5

Cybercrime ........ 6

Chapter 3: Data Management and Office 365 ........ 7

Secure data storage ........ 8

Next generation cybersecurity ........ 8

Backup and restore ........ 9

End user education and training ........ 9

Chapter 4: How Office 365 and AvePoint help protect your data ........ 10

Native capabilities of Office 365 ........ 11

Data sovereignty: country borders can be hurdles ........ 11

New frontiers call for new data management strategies ........ 12

Ensuring business critical backup capabilities ........ 12

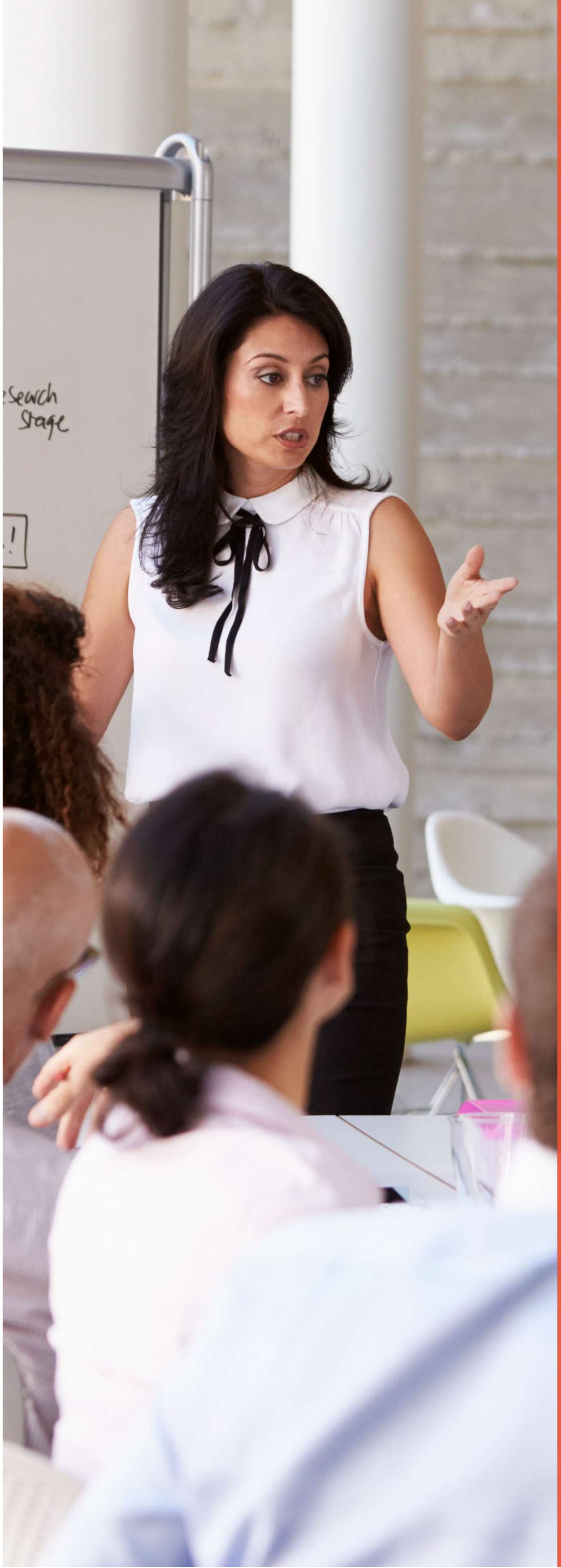
Chapter 5: Cloud Backup Case Studies & Licensing Options ........ 13

Davanti Consulting Restores Office 365 Content in Less than 30 Minutes ........ 13

Atea Backs up 1 TB of SharePoint Data, Ensures GDPR Compliance ........ 14

Unlimited Backup Options From AvePoint ........ 15

References and Resources ........ 16



# Chapter 1: Data Loss in North America

It’s no secret we are living in a rapidly expanding datasphere, where information is usually accessed on laptops instead of in libraries. Globally, more than 16 zettabytes of data was generated in 2016 alone, which equates to more than 17 trillion gigabytes (Reinsel, Gantz, & Rydning, April 2017). That number continues to grow exponentially with the rise of connected devices and expanding internet of things (IoT) technologies.

As we grapple with how to productively use such vast amounts of data, we also struggle to understand how to best store and protect all that information. With more than 60 million companies actively using Office 365, some customers are left wondering how best to approach backup as part of their content and data management strategy.

Nowadays, most businesses have some method to backup information. Globally, data protection vendors are popular: 57% of businesses use two or more data protection vendors (Dell EMC, 2016). These vendors help customers store, protect, manage and retrieve misplaced data.

# The rising cost of lost data

When a data loss event does occur, companies report losing an average of 2.36 TB of information, and recovery can cost millions (Dell EMC, 2016). The financial drain can be compounded with legal or regulatory fees, which are about to become more stringent for organizations handling European citizen data.

Once the General Data Protection Regulation (GDPR) took effect in May 2018, companies scrambled to ensure they were compliant, or risked facing a massive fine.

The EU has already started sharing some tough love with technology companies in the ramp up to GDPR. During a recent probe, the EU fined Google a record-breaking €2.4 billion in antitrust fees for manipulating search engine results. GDPR uses a tiered approach to fines, with the maximum fine for noncompliant companies reaching, "up to 4% of annual global turnover or €20 million (whichever is greater) (European Union, n.d.)."

What's more, the EU is quick to point out that "both controllers and processors" will be held accountable to GDPR regulation, meaning cloud services are just as responsible as the customers using their services.

With GDPR, data management and protection are becoming more essential for businesses across Europe, or global companies that do business with European customers. Today, more than 40% of companies are automatically backing up data to the cloud, but that means there are many companies that aren't benefiting from all that cloud backup has to offer (Dell EMC, 2016).

# Chapter 2: How Data is Lost

Because data is not tangible, it can be easy to lose. There are many reasons data loss can occur, from simple misclicks to more sinister network breaches. Usually, businesses need to dip into their data repository to recover information when there is a data loss event, such as:

- A cybersecurity breach
- An IT malfunction
- Accidental deletion of data

## Technical faults or glitches

While glitches are becoming less common as technology evolves, they do happen. The customized features of Office 365 offer a lot of benefits, however custom designs, solutions, workflows, branding and other modifications to user facing sites introduce the potential for technical faults and glitches. This means customization may need to be rolled back once errors have been found.

Data loss by technical fault can also be caused by hardware and software failures, firmware bugs, data corruption and loss of power (Dell EMC, 2016). These issues can be unexpected and unanticipated, seemingly occurring out of nowhere, which means businesses are not well prepared to recover from them.

To make matters worse, technical difficulties can impact more than just data. Depending on the system affected, data loss can result in hours, or even days, of downtime. Disaster recovery plans are necessary to plan for redundant systems as well as redundant data if the worst should occur.

## Rogue IT administrators

IT staff are the gatekeepers to the data repository where data is stored. However, a disgruntled IT manager could purposely delete or steal information. This can account for up to 10% of data loss globally (Dell EMC, 2016).

This type of data loss can be due to intentional corporate espionage or opportunistic individuals who sell corporate data for material gain. According to Information Age, this type of data loss is likely under-reported as companies don’t want to appear suspicious of their own employees (Rossi, 2016).

Administrators have a great amount of power over company data, and, while not common practice, can download personal copies of data and delete the corporate files. When it comes to data management, unfortunately businesses need to consider all potential threats, both externally and internally.

# User error/accidental deletion of data

User error was the most common cause of data loss until 2016. Employees may accidently delete an important folder, or forget to save changes to a presentation they've been working on for the past several hours. It happens to nearly everyone at some point.

Users are also the culprits when it comes to unintentional data leakage while participating in shadow IT. While many apps and services are useful and do indeed help employees do their jobs better, these tools are not within the safe haven of the company network. That means outside services are unchecked and unmonitored. Users could unwittingly put sensitive company data at risk while simply trying to increase their own efficiency, creativity or productivity. A Frost & Sullivan study found more than 80% of survey respondents admitted to using non-approved SaaS applications in their jobs.

Users have a habit of working around the solutions provided by IT, which means data that would ordinarily be part of the corporate knowledge repositories (SharePoint sites, Groups, newsfeeds, etc.) are now being stored in personal mailboxes and OneDrives. Let's not forget how easy it can be to lose this data as well: when an employee retires or leaves the organization, OneDrive and Exchange data can be wiped out by simple retention policies, losing valuable information.

Accidental deletion due to user error is common. Users can easily delete data and conversations in SharePoint, Groups or teams—and even overwrite versions of existing data—that's why it's important to keep track of data and monitor future discovery requests.

Employee data can easily be recovered –as long as a third party solution is in place.

## Cybercrime

If user error is the most common culprit of data loss, cybercrime is the most frightening. Cybercrime refers to malicious, criminal activity carried out via a computer or the internet. The frequency and associated damages of cyber-attacks are increasing as more of our data lives online.

**Cybercriminals are generally:**

- Profit-seeking cybercriminals
- Adrenaline-seeking hackers
- Strategy-seeking nation-states

Their attacks come in many forms as well. Targeted, personalized email scams (called phishing) can fool end users into clicking on a nefarious link or opening an infected attachment. Many of these emails are now gateways to ransomware, such as the wide-spread Petya, NotPetya and WannaCry attacks in 2017.

Ransomware is the number one cybersecurity threat and attacks are occurring at an all-time high. An attack typically involves an outside threat compromising a system to block access to its data until they are provided with a ransom.

For example, Danish shipping company Maersk fell victim to NotPetya ransomware, which reportedly cost the company upwards of €250 million (Muncaster, Maersk Admits NotPetya Might Cost it $300m, 2017).

As digital information and technology become further integrated into day-to-day work, the threat of cybercrime and ransomware is sure to increase. Unfortunately, there is no surefire way to defend against these attacks. Security is about mitigating risk and finding the right third-party tool that can offer detection, protection, and recovery, if necessary.

Concerned about ransomware? Learn how to prepare and protect yourself with our Ransomware Protection Kit.

# Chapter 3:
# Data Management and Office 365

Backup is just one piece of the data management puzzle. Customers using Office 365 as their productivity solution should develop a robust strategy that incorporates several key functions.

Certified Microsoft Partners can help develop, implement and manage these strategies, which should include the four pillars included in this chapter.

## Secure data storage

According to recent research, less than 10% of the world's data is currently stored in the cloud (Wall, 2016). Many companies assume that using on-premise server storage solutions are the safest option, but with the real-time security features and assurances of cloud storage, on-premise is becoming less popular.

Companies that manage cloud storage have cybersecurity top of mind at all times, and therefore tend to have robust systems that are fortified against data leakage.

Companies that manage cloud storage have cybersecurity top of mind at all times, and therefore tend to have robust systems that are fortified against data leakage.

In addition, as the amount of data produced increases, the physical space needed for storage servers in-house is becoming unrealistic, which is another key perk of storing information in the cloud. Companies that use a managed cloud service find they actually save money since less space and resources are needed to manage data in the cloud

## Next generation cybersecurity

Even if Office 365 data is stored in the cloud, it is necessary to build up the defenses of in-house networks to protect important information. Securely storing data is important, but whenever it is accessed, there can be a vulnerability at the endpoint (computer, phone, app, website, etc.).

Today, the strongest firewall alone can't defend against the barrage of cybercrime. Not all companies have invested in a strong, multi-layered security solution for their network. On top of a firewall, any business needs additional security measures, like real-time network monitoring, spam monitoring and updated threat definitions.

The more layers in a company's security infrastructure, the more barriers there are between sensitive data and cyber thieves.

The more layers in a company's security infrastructure, the more barriers there are between sensitive data and cyber thieves.

## Backup and restore

Errors, corruption and theft happen…that’s why it’s imperative you keep a protected copy of data stored elsewhere.

Even cloud storage companies must prioritize backups. Data storage in the cloud generally comes with redundancy assurances so if data is lost in one location, it can be recovered and restored from another.

**Ensuring you have a safeguarded copy of data in the event the original is lost, corrupted or stolen is essential.**

## End user education and training

As we learned in Chapter 2, user error is by far the most common way data is lost. Whether it be via shadow IT or accidental deletion, end users are another important part of any company’s data management strategy. Rather than viewing users as a risk, empower them to be a part of the security solution.

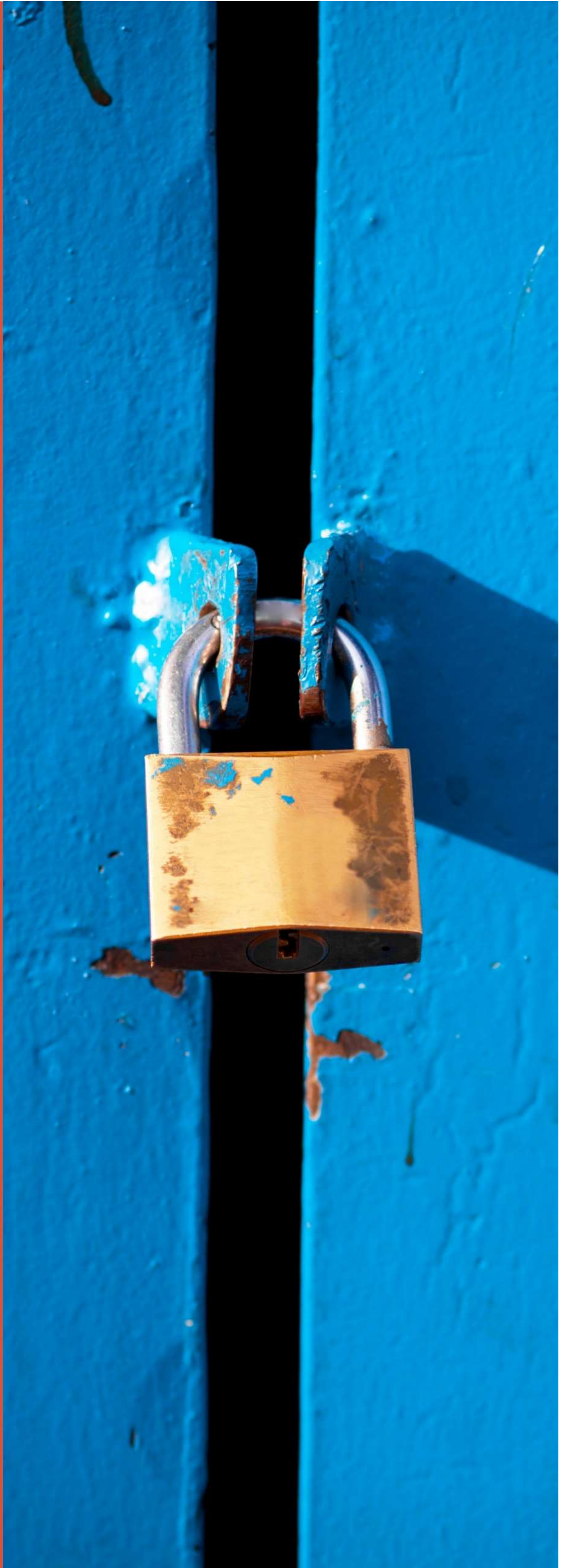
The best way to benefit from the power of your end users is to bring them into the data management process. Educate them about the company’s content strategy and how they can help protect their hard work and that of their colleagues. Include a primer on cybersecurity measures and step-by-step guidance on how to handle potential breaches or data loss scenarios, and let end users feel empowered to take the right action if things go sideways.

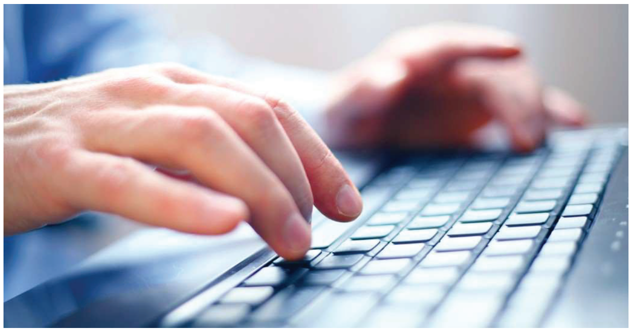
**Educate them about the company’s content strategy and how they can help protect their hard work and that of their colleagues.**

# Chapter 4: How Office 365 and AvePoint help protect your data

The most popular cloud productivity solution is Microsoft Office 365—far outpacing Google apps (Bitglass, Dec. 13, 2016). It is used globally, and includes a set of helpful safeguards to prevent data loss. This includes confirming if users would like to delete a file or storing files in the Recycle Bin for a short amount of time. However, sometimes these safeguards aren't enough.

When it comes to fully protecting, backing up and restoring data, customers need additional support.





## Native capabilities of Office 365

Microsoft assures customers that business data can be restored within certain timeframes and to certain extents largely based on where the data is stored. But what happens when you need data beyond those two weeks?

For example: a user might store data on OneDrive for Business, but once it's been sent to the recycling bin, only the most recent version of that data will be recoverable for 90 days.

Although SharePoint's online site content gets similar treatment, different versions can still be restored from the recycling bin. No matter what, as soon as you move any data or content to the recycling bin, the clock starts ticking and your deadline for recovery and restore looms.

If you need to recover content once the has deadline passed, you're out of luck…kiss it goodbye for good. Microsoft uses site collection as the level for data restoration, so any changes or updates to the site since the last backup won't be recovered.

What's more, Microsoft's recovery time objective (RTO) is 48 hours, which poses an issue for customers with tighter service level agreements (SLAs) (Oster, 2016).

## Data sovereignty: country borders can be hurdles

One key concern some organizations have with data protection in the cloud is data sovereignty. In other words, "where is my Office 365 data physically stored?" Some countries require data centers be located within the country's boundaries.

However, since security is not diminished, many businesses opt to let their data be stored regionally or globally to gain additional flexibility. For example, Germany has Microsoft data centers within its borders, and many public sector and government agencies tend to prefer data reside there.

On the other hand, the majority of private enterprises use the European tenant data centers, which can house data from several countries.

## New frontiers call for new data management strategies

Many customers that have used Microsoft Office for years are still working on fully transitioning to the new culture of cloud computing.

While companies that have used on-premises solutions have rigorous data protection plans and SLAs in place, those strategies don't directly translate to the cloud.

Really, the cloud is a new frontier and requires new ways of thinking about data management.

Existing programs around email archiving, long-term cold storage, e-discovery and content backup cycles should be re-evaluated against current cloud features. Many will change dramatically as the price and availability of storage is changed by the cloud.

## Ensuring business critical backup capabilities

Office 365 usage is on the rise across the world, and fortunately there are many avenues to get support and advice for customers who want to improve their data management strategy. While Office 365 has some safety net features, it doesn't have a full-fledged backup service. However, the native capabilities of Office 365 can be amplified by working with a certified Microsoft partner, such as AvePoint.

In the event of a disaster, lost or corrupted data can be rapidly recovered with AvePoint Cloud Backup, which protects data for Exchange Online, OneDrive for Business, SharePoint Online, Office 365 Groups, Google Workspaces, Salesforce and CRM. In addition, AvePoint now offers unlimited backup for customers worldwide.

Cloud Backup can also help prevent data loss by proactively detecting suspicious behavior that could be a result of ransomware. After the solution detects unusual activity, you receive detailed reports to shorten the investigation and flag the areas of questions. If necessary, you can restore all or specific OneDrive data.

AvePoint's backup service automatically performs scheduled backups while encrypting the data with customer-owned encryption keys, adding another layer of security. While specific scenarios can vary, backups are generally run approximately every six hours and can also be run manually if needed.

Customers can choose to store the data anywhere, from the default storage location provided by AvePoint or another specified storage location. AvePoint can help migrate data if storage location needs change, supporting the license update for customers and changing the default storage selection.

# Chapter 5: Cloud Backup Case Studies

**Restoring Office 365 Content in Less Than 30 Minutes**
Davanti Consulting is a New Zealand-based business and technology consultancy with deep expertise in customer engagement, cloud architecture, salesforce.com and mobility.

Davanti chose to migrate from Telecom New Zealand's technology stack to Office 365 due to its users' and clients' familiarity with Office applications as well as the ability to access Exchange and SharePoint Online.

> *"From the outset, I knew that cloud services do not necessarily guarantee disaster recovery and business continuity. While Microsoft does a fantastic job at making sure systems are up and available, if we lost content or if data was corrupted, it could be difficult to get it back through Microsoft's service level agreements for data recovery."* – Senior Business Manager, Davanti

Davanti set up weekly incremental backups using AvePoint Online Services' for SharePoint Online content as well as daily backups for Exchange Online shared mailboxes. Automated backups were set up and running within half an hour.

Davanti was also able to utilize AvePoint Online Services granular content recovery capabilities without having to roll back the entire environment and interrupt business operations.

This became critical when an office coordinator accidentally deleted an entire Exchange Online shared mailbox. Davanti's senior business manager was able to save the day and leverage AvePoint Online Services to restore the entire mailbox within a half hour.

# Atea Backs up 1 TB of SharePoint Data, Ensures GDPR Compliance

Atea is a Nordic-based market leader in IT infrastructure for businesses and public sector organizations in Europe's Nordic and Baltic regions.

With SharePoint 2010, 2013, and Office 365—SharePoint Online, Atea's 7,000 end users can easily manage projects and exchange information both internally and externally, on-premise and in the cloud. To backup and restore content for its hybrid SharePoint deployment, Atea had relied on the native functionalities provided by Microsoft, yet determined it needed more nuanced backup and restore tasks for its 1 TB of SharePoint data.

> **The most significant business advantage of implementing DocAve has been providing more comprehensive support, faster response times, and more flexible solutions to our end users.**
> **– Group CIO**

Atea leveraged DocAve and AvePoint Online Services to back up its intranet and workspaces to the company server more efficiently than with native functionalities. Full backups on SharePoint on-premise and SharePoint online are performed weekly, and if an item is lost or accidentally deleted, Atea can restore it within 20 minutes. This is a time savings of 60 percent compared to the original restoration time.

Ensuring data management practices that were compliant with the General Data Protection Regulation (GDPR) was also a critical goal. To align with these requirements, Atea needed to track user permissions. Thanks to DocAve Content Manager and DocAve Report Center, Atea can now move, copy, and restructure business data across SharePoint environments, as well as ensure new content is properly managed by tracking permissions.

Atea is not only preparing for GDPR and simplify content management, but also delivering a high-quality service level to its users—something not possible before.

AvePoint

# Unlimited Backup

Pick Your Plan. Maintain Flexibility. Stress-free Growth.

## Unlimited Storage or Unlimited Users — You Make the Call

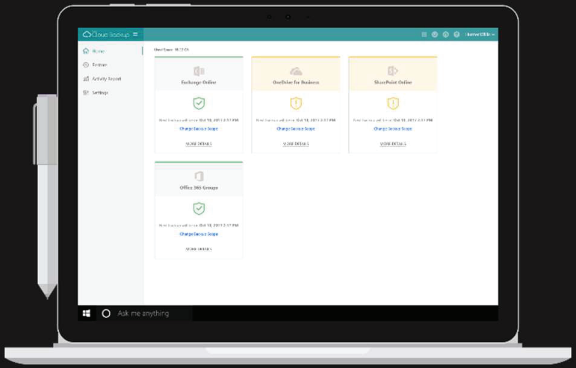
Without a robust backup solution, companies expose themselves to a myriad of risks. These include having their data held hostage by cybercriminals (ransomware), being non-compliant with industry data retention regulations and receiving hefty fines as a result of new GDPR laws protecting European citizen data.

AvePoint Cloud Backup is the industry's most comprehensive backup, and flexible restore solution for Office 365.

It is part of AvePoint Online Services, hosted on Microsoft Azure and delivered as a SaaS application.

With automated backups up to four times daily for Projects, OneDrives, Mailboxes, Teams, and Groups and ransomware detection that flags unusual activity within OneDrive – we keep organizations' critical data protected. With fast and flexible restore for entire sites or mailboxes, or granular documents and security settings, companies can minimize data loss.

AvePoint offers two unlimited Cloud Backup licensing options, based on user count for unlimited storage capacity, or content volume, for unlimited user capacity.



**User-based Licensing for Unlimited Storage**

Designed for organizations with less than 5,000 people, the user-based licensing option grants companies unlimited storage for their licensed users.

There's no way we can access the data, and it's protected with AES 256 Encryption.

Storage-based Licensing for Unlimited Users

AvePoint's unlimited user licensing option enables organizations to maintain flexibility to add and protect users dynamically.

Companies can add unlimited users for their licensed backup storage allocation, or the "organizational maximum," and only pay for the storage they choose.

To learn more about Office 365 unlimited backup solutions visit: www.avepoint.com/products/office365-services/office-365-backup.

AvePoint

# References and Resources

- Dell EMC. (2016). *DELL EMC Global Data Protection Index II.*

- European Union. (n.d.). *GDPR Portal: Site Overview*. Retrieved from EUGDPR.org: http://www.eugdpr.org/

- Frost and Sullivan (2013). McAfee Finds Eighty Percent of Employees Use Unapproved Apps at Work, https://www.mcafee.com/us/about/news/2013/q4/20131204-01.aspx

- USA Today (2017). 2016 Was a Record Year for Data Breaches, https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked/

- Oster, B. (2016, April 6). The Top 4 Concerns You Need to Address for Foolproof Office 365 Backup. *AvePoint Blog*, pp. https://www.avepoint.com/blog/avepoint-blog/top-office-365-data-backup-concerns/.

- Ralph, O. (2016, March 8). Malicious attacks account for bulk of data loss. *Financial Times*, pp. https://www.ft.com/content/7dec0636-e541-11e5-bc31-138df2ae9ee6?mhq5j=e1.

- Reinsel, D., Gantz, J., & Rydning, J. (April 2017). *Data Age 2025: The Evolution of Data to Life-Critical.* IDC.

- Riccio, K. (2017, May 31). Disgruntled Employees and Data: a Bad Combination. *DataCenter Knowledge*, pp. http://www.datacenterknowledge.com/archives/2017/05/31/disgruntled-employees-data-bad-combination.

- Rossi, B. (2016, April 12). Rogue employees may be riskier than outside hackers – so how do you stop them? *Information Age*, pp. http://www.information-age.com/rogue-employees-may-be-riskier-outside-hackers-so-how-do-you-stop-them-123461253/.

- Wall, M. (2016, April 29). Can we trust cloud providers to keep our data safe*? BBC.*