VAST
IT without Limits™

THE DEFINITIVE GUIDE TO MICROSOFT 365 BACKUP AND DATA PROTECTION

White Paper

THE BIG GAP IN MICROSOFT 365 SERVICES

There's a big gap in Microsoft's M365 services that many businesses aren't aware of.

When businesses started adopting cloud technology, there was a lot of concern over which applications should be located in the cloud. A common recommendation was to keep mission critical software on premises; cloud was seen as too risky for the mission critical, specialized software that delivered a competitive advantage or supported significant business operations.

Today, there's no hesitation about using the cloud, and cloud's robustness and reliability have proved a solid fit for critical applications. It's also become evident that *general business software, such as e-mail, is mission critical.*

As a result, both large and small organizations have turned to Microsoft 365 (M365) to access the business applications that are used every day throughout their entire organization. More than 250 million commercial users rely on M365 every month, creating more unstructured business data than ever before.

M365 offers businesses email, the traditional Office Suite of general business applications, and numerous productivity and collaboration tools including Exchange, SharePoint, and Teams. The suite provides intuitive and straightforward access to messaging, productivity, and collaboration software, enabling colleagues to share work seamlessly, whether they're working in the office or remotely. Numerous CRM, finance applications, and other third-party platforms can be integrated with M365.

In addition, although M365 is a cloud-based service, users can work with M365 applications even when offline. When internet connectivity is restored, M365 will send changes to the cloud and sync data in a matter of seconds.

What M365 *doesn't* offer is a built-in data protection and disaster recovery solution, which represents a big gap in its services. It is irresponsible to just put data in the cloud and assume it's safe. There is always the threat of cybersecurity issues. You also can't assume the cloud vendor will handle those threats. In fact, data protection in the cloud is a joint responsibility between Microsoft and the M365 customer.

Microsoft states, *"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."* Research firm Gartner also recommends businesses supplement Microsoft's limited native backup capabilities with a third-party solution in order to meet business needs.

TYPES OF DATA RISKS

The primal fear with cloud-based software is loss of access to data due to a system outage, but significant M365 outages are relatively infrequent and the impact of system downtime can be minimized by using multiple regions. The greater threat is that of permanent loss of the data itself. This potential loss can be realized through several mechanisms:

1

RANSOMWARE

Ransomware has grown to be one of the largest security threats facing businesses. The Ponemon Institute reports that ransomware attacks typically cost more than other attacks, averaging $4.62 million; Cybercrime Magazine reports the global costs of ransomware are estimated to be $265 billion by 2031, with a new attack occurring every 2 seconds. More than half of businesses already report having been targeted by ransomware. There's even "Ransomware-as-a-Service," making it easy for any bad actor to execute a ransomware attack.

It's true that Microsoft offers some tools to defend against ransomware as part of M365, including Exchange Online Protection and Microsoft Defender. But while these tools can help defend against an attack, no defense is guaranteed 100% successful. Businesses must ensure they have a mechanism to recover files damaged or lost due to a ransomware or other malware attack that penetrates the defenses.

Versioning and the recycle bin provide a basic recovery capability, but this isn't a comprehensive solution and can be awkward to use. Data is stored for a limited time period, and if the ransomware attack isn't identified and addressed quickly, the necessary files may no longer be available. Some ransomware may be able to reach in and corrupt files in the recycle bin, so even if the file is there, it may not be useful for recovery purposes.

The only way a business can be sure it will have a complete and consistent set of files to restore after a ransomware attack in M365 is to use a third-party solution that creates and maintains immutable backups outside the M365 environment.

2 HUMAN AND SYSTEM ERROR

Human error is another frequent cause of data loss; although employee mistakes don't garner the headlines that ransomware attacks generate, human error causes more data loss than malicious attacks. It's very easy and very common for an employee to accidentally delete files. On top of accidental data deletion, errors in data synchronization on OneDrive can lead to corruption and permanent loss of files and folders.

This type of data loss doesn't announce itself via a flashing message on a screen the way ransomware does, and it can take time before the business even realizes there's a problem. Unfortunately, that elapsed time can mean it's no longer possible to retrieve the data within M365. Even if an end user immediately recognizes they made a mistake, they may not have the knowledge to find the appropriate version in the recycle bin. Using a third-party backup and data recovery solution means the ticking clock slows and recovery can be managed by a trained technical team.

3 INTERNAL THREATS

Human error is dangerous but innocent; disgruntled employees or former employees on a vendetta can cause extensive data loss through deliberate actions.

Microsoft cannot tell whether a user's actions are legitimate or malicious as long as the user has the rights to access the data. In fact, proper user identity and privilege management is a key aspect of data security in M365 just as it is in any other IT system. To achieve this, businesses should use role-based access controls and ensure that privileges are updated when a user changes job functions or leaves the business.

Despite the importance of those controls, reviewing privileges is often a low-priority task, and removing access when an employee resigns can also be overlooked, providing a window of opportunity for employees to cause deliberate damage.

Even when privileges are properly revoked, it's important to note that a Microsoft 365 account gets suspended once a worker departs the organization. If lost data is detected later, IT will have limited ability to review that worker's data or reverse the loss. Archiving an employee's data as part of the separation process does not solve the problem, as the archival process does not preserve deleted content.

Only a third-party backup solution can ensure that data lost or damaged by a malicious employee can be recovered. With a third-party solution, you can also ensure that data of departed employees from your organization is retained and available for use when needed.

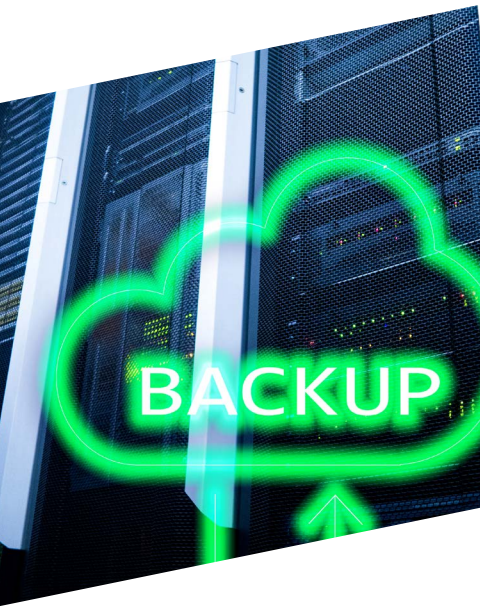
4

DATA RETENTION ISSUES

Relying on M365's built-in capabilities to meet compliance and regulatory requirements around data retention is also challenging. By default, data is retained anywhere from 1 to 180 days, depending on the content; related content handled by different services (such as messages in Teams and meeting invitations delivered by Outlook) is preserved according to different rules. Depending on your Microsoft tier, it may be possible to apply a retention policy that ensures data is permanently retained, but there may still be gaps due to departed employees' data becoming unavailable.

In addition, content retained this way can be difficult to work with. The retained data is stored in different locations depending on whether it's from SharePoint, OneDrive, Exchange, Teams, or Yammer. The ability to search and work with retained data is also limited, as is integration with third-party e-discovery tools. Another major concern is that the retained data is stored in the primary production environment, which does not satisfy disaster recovery principles.

Leveraging a third-party M365 backup solution allows businesses to create a comprehensive data retention process that makes it easy to work with the retained data.



ADVANTAGES OF USING A THIRD-PARTY MICROSOFT 365 BACKUP AND DATA PROTECTION SOLUTION

As discussed above, the native recovery capabilities in the M365 products are incomplete. Backup and retention policies are inconsistent across the product suite. Default retention settings are inadequate and the default retention locations, such as the Deleted Items folder and the Recoverable Items folder, are vulnerable to insider threats and to the passage of time leading to permanent removal of data. When data is lost, the recovery procedures may need to be applied individually to each affected user, making it difficult to restore data to multiple users impacted by an incident.

Using a third-party solution to back up a Microsoft 365 environment addresses those limitations. Third-party solutions for M365 backup also enable businesses to:

- **Reduce vendor lock-in.** There isn't much risk that Microsoft will go out of business, leading to loss of data, and most businesses are committed to the use of Microsoft products. Nevertheless, keeping a copy of your data outside of Microsoft provides assurance that you will retain access to your data no matter what happens with Microsoft or more easily transition should you later select another vendor.

- **Gain flexibility.** With a third-party M365 backup solution, the precise details of backups can be customized to your business needs. In addition, you gain flexibility in restoring data, both in choosing the specific items to be restored and in selecting the environment to restore them to. You aren't limited to restoring data to the M365 cloud; M365 data can be restored to a local instance when that better suits your needs. In addition, backing up outside of M365 gives you easy access to data for use by other applications that don't integrate with M365.

- **Recover more quickly with better vendor support.** Although Microsoft states data protection is a shared responsibility, they don't offer much assistance when you need to recover your data. Using M365 to protect data means largely going it yourself; Microsoft provides little support through the process. Recovery isn't a procedure IT teams are very familiar with, since they don't do it very often, and it takes time to locate the data, determine the details of the recovery process, and execute and verify the procedure. With third-party backup solutions, particularly with support from a partner like VAST, those issues are eliminated. As a result, recovery times are reduced and businesses are able to meet their recovery time objectives and service level agreements.

- **Implement a uniform backup management strategy.** When you use M365 as your backup tool, your backups are limited to M365 data sources and are stored in M365, as well. This means managing those backups is a completely different process from managing backups of all your other enterprise data. Many third-party backup vendors provide options to backup other enterprise cloud products and data stored on premises as well as M365; they also offer the flexibility to store backups in the cloud or on premises. Taken together, this allows a business to implement consistent backup management across multiple data sources. It also simplifies migration and data sharing in a hybrid M365 environment. Using a third-party vendor product may also provide a single user interface for managing backups no matter where the data originates and is stored, simplifying training and operations.

- **Meet current and future compliance requirements.** If compliance rules for your industry change, there's no guarantee the built-in data protection tools in M365 will allow you to satisfy the new requirements. If you use a third-party backup tool and define your own backup management process, you can customize your process, adapt to the changes, and minimize the risks of improperly protecting your data.

- **Detect and prevent damage to data.** Some third-party backup products include features that help detect threats, leaks, and potential damage to data. These tools include anomaly detection that can identify suspicious behavior, including unauthorized data restores, along with forensics to assess the scope of damage and solutions to aid rapid recovery. Third-party backups also offer immutable storage, meaning the backed-up data is tamper-proof and assured valid for use in recovery.

- **Achieve a best-practices data protection process.** The best practice standard for data backups and disaster recovery requires adhering to the 3-2-1 rule: at least three copies of data, on at least two different types of media, with at least one copy stored offsite. It's not possible to implement that best practice when using only the native backup tools available in M365. A third-party product isolates your data from the Microsoft cloud and provides the highest level of protection available.

IMPLEMENTING THIRD-PARTY M365 BACKUP AND DATA PROTECTION

The details of the third-party data protection process will vary depending on the solution selected. The most critical decision is likely to be whether you will deploy the cloud edition or the on-premises version. This decision depends on factors including the size of your M365 data, the speed of your internet connection, and the availability of local storage. The backup solution then needs to be configured to connect to M365 so it can access and copy the data to the destination environment.

Most third-party M365 backup products include enhanced search capabilities. This enables you to search the backed-up data, whether for eDiscovery or to identify data files to be restored. Recovering lost data simply requires selecting the data to restore and specifying the destination.

FINAL THOUGHTS

Using M365 effectively depends upon more than simply adding user licenses and ensuring that employees have access to their tools. Backup, recovery, and data protection considerations need to be addressed in order to ensure the business is protected against loss of data and is able to meet compliance regulations. For most businesses, the most effective means of doing this is to layer a third-party, dedicated M365 backup and recovery solution onto their M365 deployment.

CONCLUSION

Choose VAST as Your Back-Up and Recovery Partner for Microsoft 365 Data

Gold Microsoft Partner

Turn to VAST for scalable, cost-effective, and comprehensive data backup and recovery solutions to protect your Microsoft 365 data. As a gold Microsoft partner, VAST supports multiple third-party M365 backup and recovery tools. Our expert assessments enable businesses to identify their M365 data risks and select the optimal backup solution. Our cost-effective support for routine backups and disaster recoveries that meet business SLAs makes using mission critical cloud-based M365 software plus a third-party backup tool the smart business decision.

Contact VAST to implement the Microsoft 365 backup solution that best fits your business needs.

1319 Butterfield Road, Suite 504
Downers Grove, IL 60515

Phone: 630-964-6060
Toll Free: 800-432-VAST

info@vastITservices.com

www.vastITservices.com