backupify
A Kaseya COMPANY

TOP 5

Backup Blind Spots in Microsoft 365

Top 5 Backup Blind Spots in Microsoft 365

Rapid technological advancements in recent years have transformed the way organizations conduct business, enabling their employees to work remotely. Modern businesses increasingly rely on Software-as-a-Service (SaaS) applications to navigate these shifts. Today, SaaS apps are essential tools for businesses worldwide. These cloud-based solutions provide scalability, flexibility and cost-efficiency, enabling businesses to streamline operations, enhance collaboration and boost productivity. Among the numerous SaaS offerings available on the market, Microsoft 365 stands out as a leader in the business landscape.

Microsoft 365 includes a suite of powerful tools for professional email management, cloud storage, and file sharing, all designed to support various business functions. These tools integrate seamlessly, offering a cohesive platform that fosters collaboration and communication within organizations. Despite the numerous benefits Microsoft 365 offers to businesses of all sizes, the question remains: Is relying solely on the cloud service provider's native protection enough to safeguard your data?

This whitepaper examines potential security gaps in Microsoft's native protection. It identifies key risks and blind spots within Microsoft 365 to help you better protect your data and workloads. Read on to learn more about these risks and how to strengthen your Microsoft 365 data protection strategy.

Understanding Microsoft's native protection

Although Microsoft provides native data protection features, there are significant gaps that you need to address to ensure your organization's data is fully safeguarded..

Microsoft's data protection mechanisms

Exchange Online Protection (EOP) is Microsoft's cloud-based email filtering service designed to help protect organizations against spam, malware and other email threats. It's a part of the Microsoft 365 suite and provides a layer of security for incoming and outgoing emails. EOP utilizes advanced filtering techniques to intercept and prevent spam emails from reaching users' inboxes. It includes multiple anti-malware modules to detect and block viruses and other malicious software in email attachments and links.

Premium Microsoft licenses, such as an E5, include Microsoft Defender for Office 365, a comprehensive security solution designed to protect Microsoft 365 users from a wide range of cyberthreats. It provides advanced threat protection, detection and response capabilities for email and collaboration tools within the Office 365 suite, including SharePoint Online, OneDrive and Microsoft Teams.

Microsoft offers multifactor authentication (MFA) support for both Microsoft 365 and Office 365 users. This feature strengthens account security by requiring multiple verifications to access Office 365 services. This additional security layer helps prevent unauthorized account access, even if a user's password is compromised.

Native backup and recovery options

Microsoft 365 Backup is expected to be available for general use by mid-2024. This solution is designed to protect businesses against ransomware attacks by providing immutable backup protection and enabling data recovery within hours. Users can perform self-service backup and restore within the Microsoft Admin Center or through a trusted independent software vendor (ISV) partner.

Microsoft 365 automatically saves multiple versions of documents stored in SharePoint Online and OneDrive for Business, allowing users to restore previous versions if needed. It helps organizations safeguard against data loss due to accidental deletion, corruption, viruses or malware. Additionally, Version History enables tracking and management of changes to files, facilitating the recovery of earlier versions if any unwanted changes have been made to a file.

Deleted items in SharePoint and OneDrive are moved to the recycle bin, where users or administrators can restore them within a certain period (default is 93 days).

When users accidentally delete emails in Exchange Online, they are first moved to the Deleted Items folder and then to the Recoverable Items folder if they are deleted again. The default retention period for items in the Deleted Items folder is 14 days. After the recoverable period is over, administrators can still find and recover deleted items within 30 days through the Exchange Admin Center. Administrators can configure retention policies to retain emails for a specific duration.

According to IBM, organizations took 207 days on average to identify data compromise in 2023 — long after the 30-day retention period had phased out.

Data redundancy and availability

Data redundancy and availability in Microsoft 365 are foundational elements designed to ensure seamless access to information and uninterrupted services. Microsoft 365 achieves data redundancy by replicating user data across multiple geographically dispersed data centers. This multilayered approach means that if one data center experiences an outage or failure, another can immediately take over, minimizing downtime and ensuring continuous access to services.

While Microsoft replicates data to ensure continuous access to data, it is important to note that a replica isn't a backup. Replicas are intended to be an exact copy of data that is kept in sync with the original, providing near real-time duplication. This ensures high availability and minimal downtime in case of a primary system failure. However, replication does not protect against logical errors or corruption that might be transferred to the replica.

Limitations of native protection

Microsoft's native protection within its cloud services offers baseline security features designed to safeguard user data. However, while Microsoft's native protection forms a strong foundation, it primarily focuses on the security "of" the cloud infrastructure rather than the data managed "in" the cloud by users. This means that while Microsoft secures the underlying hardware and software, users (you) must take additional steps to protect their data from accidental deletions, insider threats and advanced cyberattacks.

The shared responsibility model

As businesses increasingly rely on cloud services like Microsoft 365, understanding the shared responsibility model becomes crucial for effective data management and security. This model delineates the security obligations between the cloud service provider (CSP) and the customer, ensuring both parties play a role in maintaining a secure cloud environment.

In a shared responsibility model, such as with a SaaS solution like Microsoft 365, the CSP (Microsoft) is responsible for application availability and the underlying infrastructure. In contrast, the customer (you) is responsible for application data, administration and user management. This model dictates that Microsoft ensures the integrity of the data center, covering security, infrastructure and operations to maintain the availability and performance of Microsoft 365 services. On the other hand, customers are operationally and contractually accountable for their tenant's integrity, the security of user credentials and the protection of their Microsoft 365 data.

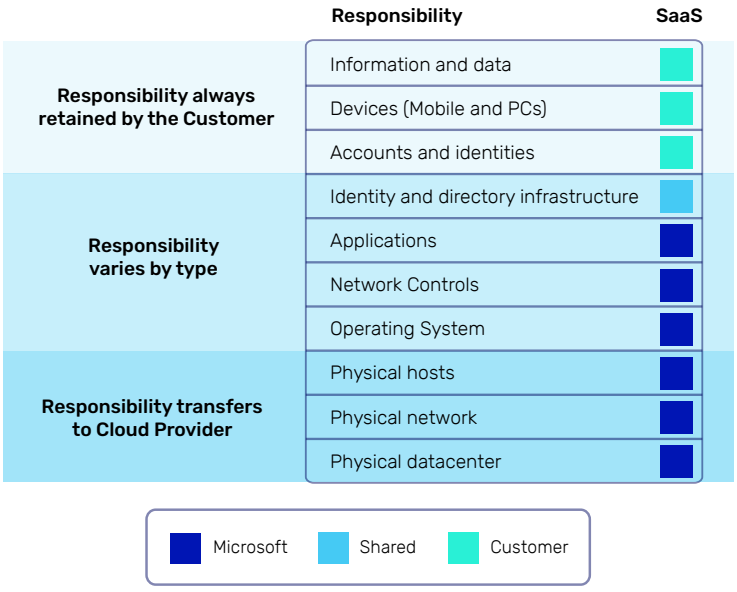

Figure 1: Shared responsibility in the cloud
Source: *Microsoft*

Retention rules and their constraints

Retention policies and retention labels in Microsoft 365 are essential tools for managing data lifecycles and ensuring compliance with regulatory requirements and internal policies. Businesses can apply retention labels and policies to sites, emails, documents and other content to ensure they are kept for a specified period. These features allow organizations to control how long content is retained, helping to secure sensitive information and facilitate efficient data management.

Administrators can apply retention rules to specific locations like Exchange mailboxes, SharePoint sites, OneDrive accounts and Microsoft Teams channels.

Retention rules can be configured to retain data for a specific period or indefinitely, depending on your organizational needs. For example, a retention rule might keep emails for seven years to comply with industry regulations. After the retention period expires, the data is automatically deleted or archived.

Although Microsoft's native retention settings help organizations retain their data for regulatory compliance, they do not function as a backup solution. Many businesses mistakenly believe that Microsoft retention policies and retention labels can be used to back up critical data. This misconception is dangerous and can jeopardize a company's data security. Besides, these features do not apply to all data within Microsoft 365 applications.

Retention policies and legal holds are only available in Microsoft Enterprise E3 and E5 plans. Depending on your organization's Microsoft 365 plan, each user is assigned a certain amount of storage capacity. When data is retained, it adds to the storage quota. If you delete data to save storage space or remain within the assigned storage limit, it cannot be recovered.

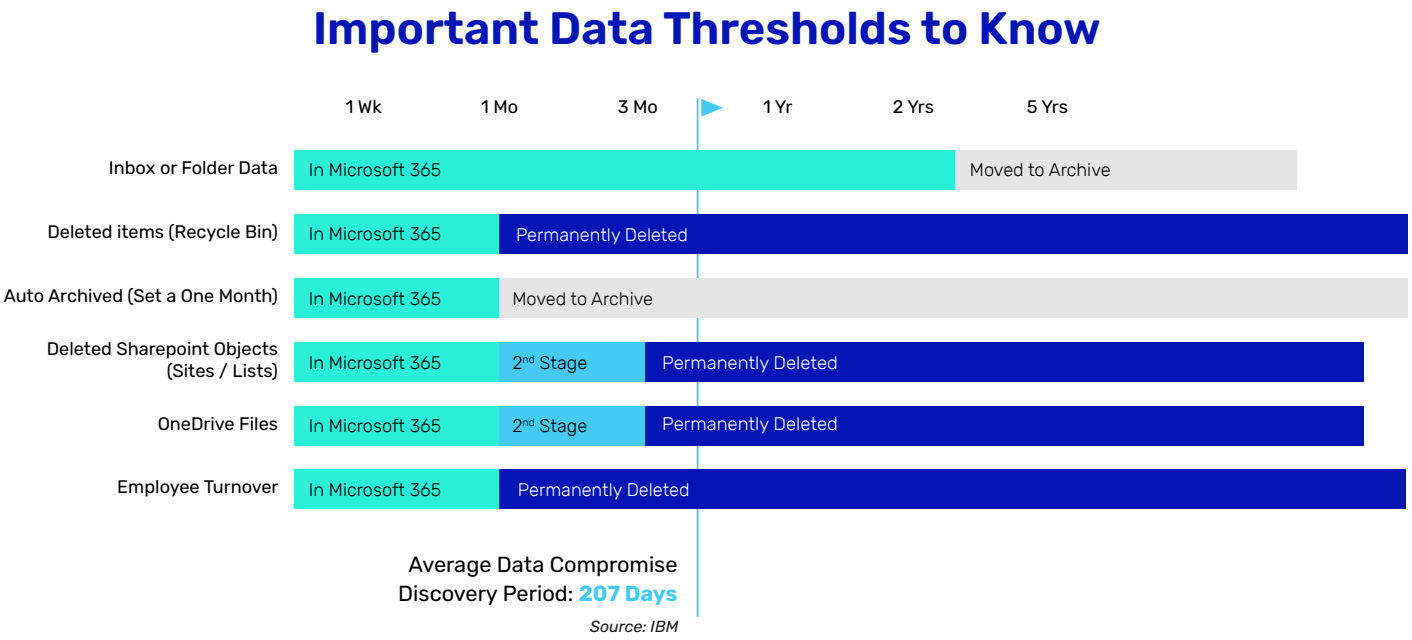

Figure 2: Building an effective data security strategy

Types of data loss not covered

Although Microsoft provides several native security and data loss prevention features, such as Exchange Online Protection, Microsoft Defender for Office 365, Office 365 Multifactor Authentication, retention policies and more, storing sensitive data in the cloud may still be a concern for some organizations due to potential vulnerabilities. Microsoft 365 does not comprehensively cover malicious insider threats, accidental deletions, data corruption due to configuration or sync issues or ransomware attacks, leaving your organization's sensitive data vulnerable to loss or corruption.

Key risks and top five blind spots in Microsoft 365

Many businesses today entrust their data to cloud service providers, believing that native protections are sufficient to safeguard their valuable information. However, relying solely on these built-in security measures can be risky. While cloud providers, such as Microsoft, offer essential security features, they don't cover all vulnerabilities. Here are the top five backup blind spots in Microsoft 365 that you must be vigilant of to protect your critical workloads effectively.

1 HUMAN ERROR

Human actions, whether accidental or intentional, play a significant role in data loss within SaaS environments. Some of the most common ones are:

Accidental deletions and overwrites

Accidental deletions and overwrites can occur when employees mistakenly remove critical files or replace existing data with incorrect versions.

Unintentional data corruption

Unintentional data corruption is another concern, where files may become unusable due to inadvertent changes or improper handling. These mistakes can disrupt workflows and result in significant data loss if not promptly addressed. According to Verizon's 2024 Data Breach Investigations Report, 68% of breaches were linked to unintentional human factors, such as individuals falling prey to social engineering attacks or making mistakes.

2 MALICIOUS ACTIVITIES

Microsoft 365 is not exempt from malicious activities.

Insider threats

Insider threats pose a substantial risk, where disgruntled employees or those with ulterior motives might deliberately delete or leak sensitive information. The Verizon report also found that internal actors were responsible for 35% of breaches.

Microsoft follows the "shared responsibility model," with customers as the "Controller" of their data and Microsoft as the "Processor." Microsoft is responsible for modifying data and handling changes to configurations, settings and policies upon request. This means they will process even malicious or accidental requests if authenticated by valid credentials.

External cyberattacks

External cyberattacks, including phishing and malware, can also compromise data security. Attackers often target Microsoft 365 accounts to gain unauthorized access to confidential business information, potentially leading to data breaches and financial losses. While ransomware attacks may not specifically target Microsoft 365 data, they can find their way into your organization by impacting other applications like Exchange Online and SharePoint Online.

Cybersecurity firm Obsidian reported a successful ransomware attack on SharePoint Online that exploited a Microsoft Global SaaS admin account, resulting in the theft of hundreds of files.

3 COMPLIANCE AND LEGAL RISKS

Compliance and legal risks are critical for organizations handling sensitive information.

Retention policy limitations and regulatory requirements

Microsoft 365's native retention policies might not meet all regulatory requirements, especially for industries with stringent data preservation rules. Businesses must ensure they can maintain data for required periods to comply with regulations and a void penalties.

While retention policies and retention labels help preserve data for a certain period, they are not a substitute for backups. Microsoft 365 retention policies are designed to meet compliance and regulatory requirements but may not offer the same level of data protection and recovery as dedicated backup solutions. Third-party backup solutions give users greater control over the duplication and distribution of data, enhancing its availability and integrity. Additionally, they often involve storing copies of data in multiple locations, bolstering security and redundancy.

Legal holds and eDiscovery challenges

Legal holds and eDiscovery challenges arise when organizations need to preserve data for litigation or investigations. These often necessitate advanced tools beyond Microsoft's native capabilities to manage and retrieve required information efficiently.

Microsoft 365 includes native litigation hold functionality for eDiscovery, but it isn't meant to restore lost data. Using litigation hold for all your data can be risky during an eDiscovery request, as everything becomes discoverable, increasing cybersecurity liability. Furthermore, it doesn't store data in a secondary physical location or allow direct email or account restoration. While manual recovery is possible, there's no direct restore option. A litigation hold is also not an effective method for recovering from ransomware.

In contrast, third-party SaaS backup solutions offer independent backups from Microsoft's servers, ensuring quick and efficient data restoration.

4 THIRD-PARTY APP INTEGRATIONS

Integrating third-party applications with Microsoft 365 enhances functionality but introduces additional risks.

Risks associated with connected third-party applications

Third-party applications may add convenience and boost efficiency. However, care should be taken when integrating third-party apps and extensions. Many third-party apps might be useful but not necessarily trustworthy. When you grant permission to such apps to access and manage your organization's data, they can encrypt files or steal or expose confidential information.

Data loss through API connections

Application programming interfaces (APIs) that connect applications can inadvertently expose data to vulnerabilities, leading to unauthorized access or data loss. Ensuring that third-party integrations adhere to security best practices is crucial for maintaining data integrity.

5

SERVICE OUTAGES AND DOWNTIME

Despite Microsoft's reliable infrastructure, service outages and downtime can still occur.

Microsoft service disruptions

In January 2024, Microsoft Teams, a popular team collaboration app, experienced a widespread outage that affected thousands of users. Such disruptions can halt business operations, affecting productivity and communication. Extended Microsoft 365 service outages could result in data inaccessibility or loss if not backed up externally. Your company must have contingency plans to manage and mitigate the impact of unexpected service outages, ensuring continuity during critical operations.

Business continuity concerns

Microsoft 365 provides a solid foundation for productivity and collaboration, but it isn't risk-free. Human errors, software glitches, insider threats, phishing scams and ransomware attacks pose a constant threat to your Microsoft 365 environment, which could lead to potential data loss or disrupt business operations. According to IBM's Cost of a Data Breach Report 2023, over 80% of breaches involved data stored in cloud environments.

Mitigating backup blind spots

To safeguard your data in Microsoft 365 effectively, you must adopt comprehensive strategies that go beyond relying on Microsoft's native security features.

Comprehensive backup strategies

Implementing reliable third-party backup solutions is crucial, as they provide extended data recovery options and protect against accidental deletions, programmatic errors and malicious activities. Backup solutions from reputed vendors like Backupify also offer advanced features such as granular recovery options and automated backups, ensuring data integrity and availability.

Data protection best practices

Regular audits and specialized employee training are vital to strengthening the overall security and resilience of your Microsoft 365 environment. Conducting frequent security audits helps identify and address vulnerabilities, ensuring compliance with best practices and regulatory requirements. Audits should cover access controls, third-party integrations and data management policies.

Equally important is building a culture of security awareness through continuous employee training programs. Educating staff on recognizing phishing attempts, safe data handling and understanding the importance of security measures empowers them to act as the first line of defense against potential threats.

Policy and governance

Creating strong data governance policies is essential for safeguarding data in Microsoft 365 and meeting regulatory standards. This includes setting clear guidelines on data classification, access controls and retention policies. Effective data governance helps you maintain data integrity, mitigate risks associated with data breaches and adhere to industry regulations.

It is also important that you align your backup strategies with these governance policies and compliance requirements. Microsoft 365's native backup options often fall short of meeting stringent regulatory standards, such as GDPR or HIPAA, which demand specific data retention periods and the ability to restore data from particular points in time. Implementing comprehensive third-party backup solutions ensures your organization can meet these requirements by allowing you to retain data for longer periods and providing a reliable means to retrieve data during audits or legal investigations.

Evaluating third-party backup solutions

Third-party backup solutions provide more extended retention policies, allowing recovery of older data and safeguarding against prolonged data loss. They also act as a safety net, filling the gaps left by native protections and providing peace of mind that critical business data is secure and recoverable in any scenario. Here are a few criteria to consider when evaluating third-party backup solutions for Microsoft 365..

Compatibility with Microsoft 365

A critical factor when selecting a backup solution is ensuring that it integrates smoothly with Microsoft 365. The solution should support all core applications, including OneDrive, SharePoint, Exchange and Teams. This compatibility ensures all data within the environment is appropriately backed up and can be restored when needed.

Security features

Security is paramount in data backup. Look for solutions that offer strong encryption methods both in transit and at rest, protecting data from unauthorized access. Your backup solution should include access controls, allowing administrators to define who can access and manage backups. Granular recovery options are also essential, enabling the restoration of specific files or emails without having to perform a full recovery. Another important feature is automated backups, which ensure consistent data protection without the need for manual intervention.

Ease of use and deployment

Consider a user-friendly and easy-to-deploy backup solution. This is essential for maintaining productivity and preventing downtime during the setup phase. An intuitive interface lowers the learning curve, enabling your teams to leverage the full capabilities of the backup solution without extensive onboarding or training periods.

Vendor reputation and support

It is important to consider the reputation of the backup solution provider before you seal the deal. Make sure to look for vendors with a solid history of safeguarding data and receiving positive reviews from satisfied customers. When it comes to data protection and recovery, every second matters. Therefore, reliable customer support is critical. Your backup vendor should offer assistance with setup, troubleshooting and recovery processes.

Another critical factor is flexibility and scalability. As your business expands, your data protection requirements will also change. Look for a backup vendor that offers flexibility and scalability, allowing the backup system to expand seamlessly as your organization's data requirements increase. This adaptability ensures your backup solution remains effective and relevant over time.

Experience effortless Microsoft 365 data protection with Backupify

Given the potential security gaps in Google Workspace, implementing a cutting-edge third-party backup solution is a no-brainer for businesses looking to strengthen the overall security and resilience of their mission-critical workloads.

Backupify is a "set and forget" backup solution for Microsoft 365 that saves you time, effort and money. In addition to granular recovery and point-in-time restore options, our solution also provides automated backups three times a day, ensuring your critical data across all your key apps is up to date and consistently backed up. You also have the option to run backups on demand at any time.

Backupify is incredibly easy to use. In just five minutes, you can set up and start protecting your Microsoft 365 data.

Backupify makes recovering lost data fast and easy — not weeks or days — just a few clicks.

Furthermore, our multilayered approach to security offers comprehensive protection against ransomware and other threats and enables efficient recovery when needed.

Ready to take full control of your data? **Watch the interactive demo** to discover how Backupify can transform the way you manage and protect your Microsoft 365 data.

TAKE PRODUCT TOUR

backupify
A Kaseya COMPANY

Corporate Headquarters
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

©2024 Kaseya Inc.
All rights reserved.
July 2024