NAKIVO®

Microsoft Office 365 Backup

Best Practices

www.nakivo.com

Introduction

Used by over 1 million companies worldwide[1], Microsoft Office 365 has become ubiquitous across industries. At many organizations, Microsoft's productivity suite is the foundation for daily communication and collaboration. As a result, Microsoft Office 365 is now a favorite target for malicious actors of all kinds, whether state actors, cybercriminals or disgruntled former employees. Just consider how easily an IT contractor recently deleted a company's 1,200 Microsoft 365 user accounts (out of a total of 1,500)[2]. The company had to shut down for 2 days as it tried to restore its employees' email accounts, contacts, calendars, documents, video, audio, and so on[3].

Any cybersecurity incident in Microsoft 365 triggers a chain of consequences, of which data loss, downtime and financial repercussions cause the most damage. Just like with other business workloads, data residing on SaaS platforms requires a holistic approach to data protection to ensure that it doesn't get permanently lost and that a business doesn't have to shut down for prolonged periods of time.

A good data protection strategy for Microsoft 365 should rest on three pillars that cover security, employee awareness and backups, that is, **security**, **education** and **data protection**.

Why Protect Microsoft Office 365 Data

Depending on the industry, organizations seek Microsoft Office 365 data protection for a variety of reasons. These reasons include avoiding downtime and workflow disruptions, ensuring regulatory compliance and meeting any potential legal requirements. But most importantly, these organizations want to avoid the cost of data loss. This cost consists of the financial impact, regulatory fines, litigation expenses, security expenses, PR expenses, stock value loss, brand value loss, reputational damage and customer turnover. Combined, the cost of data loss can run into millions of dollars, placing a burden on organizations and impacting their bottom line.

Organizations have realized that data residing in the cloud is not safe by default from data loss, whether resulting from ransomware, other malicious activities or just accidental data deletions. Any previous misconceptions about data security and protection responsibilities in Microsoft 365 data have been mostly dispelled.

1 Worldwide Office 365 User Numbers by Country, Statista, 2020
https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/

2 IT Contractor Sentenced to Two Years for Deleting Carlsbad Company's Microsoft User Accounts, Department of Justice, USA, 2018
https://www.justice.gov/usao-sdca/pr/it-contractor-sentenced-two-years-deleting-carlsbad-company-s-microsoft-user-accounts

3 Office 365 Cyberattack Lands Disgruntled IT Contractor in Jail, Threat Post, 2021
https://threatpost.com/office-365-cyberattack-disgruntled-contractor-jail/164986/

According to Microsoft's Shared Responsibility Model, Microsoft and the Microsoft 365 user share responsibility for securing the data on the platform. However, the user has sole responsibility for ensuring that this data is properly backed up with a third-party solution and can be recovered when needed[4].

The 3 Pillars of Microsoft Office 365 Data Protection

1. Secure

Cybersecurity is the first line of defense against Microsoft Office 365 data loss. Cybercriminals regularly take advantage of vulnerabilities in cybersecurity measures. To fortify Microsoft 365 security, you have several tools at your disposal. Some of these are native tools while others include third-party tools.

Microsoft 365 Native Security Tools

According to the Shared Responsibility Model, in addition to the physical security of the platform, Microsoft is partly responsible for client and endpoint protection. The company delivers built-in security tools that include Microsoft 365 Defender and multi-factor authentication (which covers 2-step verification or 2FA).

Microsoft 365 Defender

Microsoft 365 Defender is a comprehensive security suite designed to provide pre- and post-breach protection and insights. Drawing on the protection capabilities of Microsoft Defender for Office 365, Microsoft Defender for Identity, Azure AD Identity Protection, Microsoft Defender for Endpoint and Microsoft Cloud App Security, the security suite offers unified defense against a number of threats. In addition to mounting a defense against cyber threats, Microsoft 365 Defender also gathers valuable insights that can help you prevent future attacks.

The value of Microsoft 365 Defender for your data protection is highlighted by its ability to screen links in email messages and collaboration tools. Similarly, Microsoft 365 Defender can automatically detect and stop malicious insider actions. This means that Microsoft 365 Defender provides some degree of protection against four common causes of data loss: cyber attacks, malware, ransomware and malicious insiders.

Multi-Factor Authentication

Despite all the security precautions taken by Microsoft, Office 365 accounts are exposed to credential stuffing. It is a form of cyberattack where stolen credentials for one account are used to access another. Unfortunately, nothing prevents your employees from reusing their old passwords, which can be compromised in countless ways. Even if every employee

4 Driving Data Security Is a Shared Responsibility. Here's How You Can Protect Yourself, Microsoft, 2018 https://www.microsoft.com/security/blog/2018/06/19/driving-data-security-is-a-shared-responsibility-heres-how-you-can-protect-yourself/

has good cybersecurity habits, your organization's Microsoft Office 365 business data can benefit from an additional layer of protection. And better security starts with deploying multi-factor authentication (MFA).

Microsoft Office 365 supports three MFA methods:

- an SMS code
- a phone call
- Microsoft Authenticator

By tying employee identities to phones or phone numbers, which cannot be easily replicated, you drastically reduce the chance of unauthorized access to Microsoft Office 365 accounts.

You can enable MFA using:

- security defaults
- Conditional Access policies
- individual user permissions

While MFA shouldn't be your primary security measure, it is the first thing you should do to avoid data loss.

Third-Party Security Tools

Firewall

A firewall is another line of defense that you can use in your pursuit of Microsoft Office 365 data protection. A reliable and properly configured firewall can prevent untrusted traffic from accessing your organization's network and compromising connected devices. If you don't operate under tight budgetary constraints, implement multiple firewalls and create several access zones. Thus, you can quarantine malware and prevent it from infecting all network devices.

Look for the following functionality when choosing a firewall for your organization:

- **Application visibility and control on any port**
  Your firewall should be able to identify and control applications on all ports regardless of their protocols or decryption.
- **Inbound and outbound SSL decryption**
  The firewall should decrypt and inspect your network's inbound and outbound traffic to prevent URL filtering, file blocking, data filtering, and unauthorized data transmission.
- **Application malware scanning**
  Good corporate firewalls perform application-level scanning to protect your network from malware.

- **Unknown traffic policy control**
  You should be able to control unknown traffic based on a set of customizable policies.
- **Visibility and control of the remote workforce**
  The firewall you choose should facilitate remote work by controlling employee traffic regardless of their location.

To ensure a high level of security, opt for a dedicated firewall device rather than a router with basic firewall functionality.

Intrusion Prevention System

An intrusion prevention system (IPS) is another security layer that you should place behind the firewall to protect your network, in general, and Microsoft Office 365 data, in particular. IPS continuously monitors network traffic to detect vulnerabilities and anomalous activities. Upon detection, IPS either takes automated actions or reports its findings to system administrators.

IPS can apply to the following automated actions to network traffic:

- drop packets
- block traffic
- reset the connection

Configure your IPS to detect unauthorized access based on three approaches:

- **Signature-based detection**
  Matching network activities against a library of well-known exploit signatures
- **Anomaly-based detection**
  Matching network activities against the baseline network performance
- **Policy-based detection**
  Matching network activities against preconfigured security policies

With an IPS in place, you have a higher chance of identifying and blocking a network breach, thereby keeping your Microsoft Office 365 data out of harm's way.

Endpoint Detection and Response Systems

Whether it is an employee workstation, laptop or mobile device, all endpoints used to access Microsoft Office 365 should be protected. To promptly detect and stop anomalous endpoint-system-level activities, use an endpoint detection and response (EDR) system. The system continuously monitors endpoints. It applies automated responses to stop threats and prevents malware from spreading through your network.

Look for the following functionality when choosing an EDR system for your organization:

- **Real-time visibility**
  Real-time visibility allows to detect malicious activities at the early points of the attack chain.
- **Threat library**
  Anomalous activities should be matched against an extensive library of known threats and exploits.
- **Behavioral protection**
  Top-end EDR systems run behavioral analysis to identify signs of malicious activities
- **Data collection**
  Your EDR system should record the events preceding and following suspicious activities.

Nowhere endpoint protection is as important as in the area of remote work. Consider implementing a cloud-based endpoint EDR system to mitigate threats for every employee.

2. Educate

When it comes to Microsoft Office 365 data protection, your organization's employees can be a security asset. Employees can either be additional layers of cybersecurity or additional points of exposure. And making sure that they are a strong link in your cybersecurity efforts involves training them to recognize suspicious cybersecurity activities.

The following best practices can help you maximize the efficiency of your cybersecurity awareness training.

- **Identify the knowledge gaps**
  Start by figuring out what your organization's employees already know and what they need to learn. Finding the knowledge gaps can be as simple as distributing an online survey or as complicated as running a phishing simulation.
- **Encourage cross-departmental collaboration**
  Cross-departmental collaboration helps communicate the organization's cybersecurity policy and procedures to ensure that all employees are on the same page. Departments should also work together to account for shared needs and introduce necessary adjustments to cybersecurity awareness training.
- **Incentivize change**
  Motivate your employees to actively participate in the training program and observe suggested practices. This behaviour is critical for helping your organization take a strong cybersecurity stance. To achieve the best possible outcomes, link your training program to a clear incentive structure. For example, offer tangible rewards for reporting security threats and vulnerabilities.

- **Conduct regular cybersecurity awareness training**
  Take a consistent approach to security awareness by scheduling regular training sessions. The effectiveness of your Microsoft Office 365 data protection efforts can be greatly enhanced by approaching cybersecurity awareness as an ongoing practice. Scheduled training is critical not only because employees need to refresh their memories but also because the cybersecurity landscape is always changing.
- **Integrate post-training testing**
  The end goal of training is to bring observable change in employee behavior. You cannot know whether you've reached the goal without measuring the said change. To this end, you can run a cyber-attack simulation before and after the training.
- **Assign security roles**
  Assign cybersecurity roles to the top managerial positions in your organization, and provide them with additional cybersecurity training. Managers are well-positioned to oversee the security-related activities of their team members and offer necessary guidance. Thus, you considerably increase both the effectiveness of your training and the safety of your Microsoft Office 365 data.
- **Personalize cybersecurity risks and benefits**
  To get your message across, personalize cybersecurity risks and benefits for individual departments and, if possible, employees. This can make all stakeholders invested in raising the level of cybersecurity in your organization.
- **Collect employee feedback**
  Feedback collection offers a simple avenue of training improvement. Establish clear lines of communication for your employees to provide feedback. Make sure to collect, process and incorporate feedback into future cybersecurity awareness training sessions.
- **Gamify cybersecurity awareness training**
  Employees have a higher chance of engaging with your cybersecurity awareness content if its presentation is not dull. Add a competitive component to your training to create a rewarding learning experience. For example, encourage employees to accumulate points for identifying phishing emails.
- **Promote real-time response**
  The best cybersecurity awareness programs minimize the threat response time. Therefore, not only provide guidance on taking active steps to manage Microsoft Office 365 security threats but also actively promote it.

Your Microsoft Office 365 data is accessible to a large number of employees. Further broadening the cyber threat exposure is the fact that data is accessible via mobile devices. Being the weakest link in your organization's security infrastructure, all employees should receive sufficient cybersecurity awareness training.

3. Protect

The third, and arguably most important, pillar of Microsoft Office 365 data protection is backup. Operating without Microsoft Office 365 backup has major cybersecurity and regulatory compliance implications. No matter how effective your security and education measures are, it takes a single breach to put your entire organization at risk. Bear in mind that your Microsoft Office 365 data is subject to both malicious and unintentional deletion.

To boost your organization's resilience to ransomware and prevent other causes of data loss, running regular backups is essential. Consider the following characteristics of a reliable backup solution:

Storage space efficiency

Look for an incremental backup solution to minimize the amount of storage space needed to store your backups. A solution leveraging incremental backup technology runs the full backup the first time you use it. Then, the solution backs up only the data that has been modified since the initial full backup. Since your Microsoft Office 365 data always changes by small increments, you can backup only new and modified files rather than always running a full backup. Not only does incremental backup result in higher storage space efficiency, but it also minimizes the network load and resource consumption.

Backup job automation

Just like with business process automation, backup job automation allows you to reduce operational costs, increase productivity and optimize performance. As your organization grows, keeping track of backup jobs to run can become overly complicated. Therefore, adopt a backup solution with advanced automation functionality. Firstly, automation saves multiple hours of your routine data protection activities, thereby helping you redirect your attention elsewhere. Secondly, backup automation offers the surest way to avoid errors. Once Microsoft Office 365 accounts are added and backup schedules established, a reliable data protection solution should flawlessly run backup jobs without your involvement.

Flexible retention policies

The main issue with relying on Microsoft 365 for data protection is that the platform does not offer built-in long-term data retention functionality to facilitate point-in-time restores. That is why a third-party backup solution should allow you to customize your retention policies to be able to recover what you need, when you need it. Depending on your organization's needs and the regulations governing your industry, the solution should allow you to keep the number of recovery points that you need and rotate them daily, weekly, monthly and annually. This way, you save storage space as the oldest backups are replaced with newer ones while avoiding any retention gaps.

Granular recovery

Your backup solution is only as good as your ability to retrieve lost data when you need it. Make sure the solution you adopt comes with multiple recovery options. Specifically, you should be able to recover individual files to the original or a different location as needed. The granular recovery functionality allows avoiding the full recovery, which can save you precious minutes when lost customer contacts or missing emails need to be restored. The ability to find lost files, folders, document libraries, sites and emails using a simple search functionality is also important. Especially given that you might need the search functionality to fulfill e-discovery requests or for regulatory compliance.

Scalable architecture

Your backup solution should seamlessly accommodate your organization's expansion. As the demand for data protection grows, you should be able to handle it without changing your infrastructure or making considerable investments. By prioritizing scalability, you can reduce technical and financial constraints to data protection. This is important because you don't want to make data protection trade-offs when your organization hires more employees.

Multi-environment protection

Your pursuit of data protection does not have to be confined to Microsoft Office 365 data only. If your organization has virtual, physical or cloud environments, they also should be protected against data loss. However, on top of being financially inefficient, the adoption of separate data protection solutions for each environment also increases administration complexity. For this reason, look for a Microsoft Office 365 backup solution that can also protect all your environments. By opting for a multi-environment solution, you do not have to incur additional training expenses.

Backup for Microsoft Office 365 with NAKIVO Backup & Replication

Use NAKIVO Backup & Replication to back up Exchange Online, OneDrive for Business and SharePoint Online data. The multi-platform data protection solution offers incremental backup, advanced automation, near-instant recovery and other advanced features needed to ensure Microsoft Office 365 data recoverability. Once deployed, NAKIVO Backup & Replication seamlessly backs up Exchange Online, OneDrive for Business, and SharePoint Online data including emails, contacts, calendars, files, folders and site content for safe, on-premises storage.

Backup for Microsoft Office 365 with NAKIVO Backup & Replication

Use NAKIVO Backup & Replication to back up Exchange Online, OneDrive for Business and SharePoint Online data. The multi-platform data protection solution offers incremental backup, advanced automation, near-instant recovery and other advanced features needed to ensure Microsoft Office 365 data recoverability. Once deployed, NAKIVO Backup & Replication seamlessly backs up Exchange Online, OneDrive for Business, and SharePoint Online data including emails, contacts, calendars, files, folders and site content for safe, on-premises storage.

About NAKIVO

NAKIVO is a US-based corporation dedicated to delivering the ultimate backup and site recovery solution. With 21 consecutive quarters of double-digit growth, 5-star online community reviews, 98% customer satisfaction with support, and more than 18,000 paid customers worldwide, NAKIVO provides an unprecedented level of protection for virtual, physical, cloud and SaaS environments. As one of the fastest-growing data protection software vendors in the industry, NAKIVO provides a data protection solution for major companies such as Coca-Cola, Honda, SpaceX and Siemens, in addition to working with over 6,000 channel partners in 140 countries worldwide. Learn more at www.nakivo.com