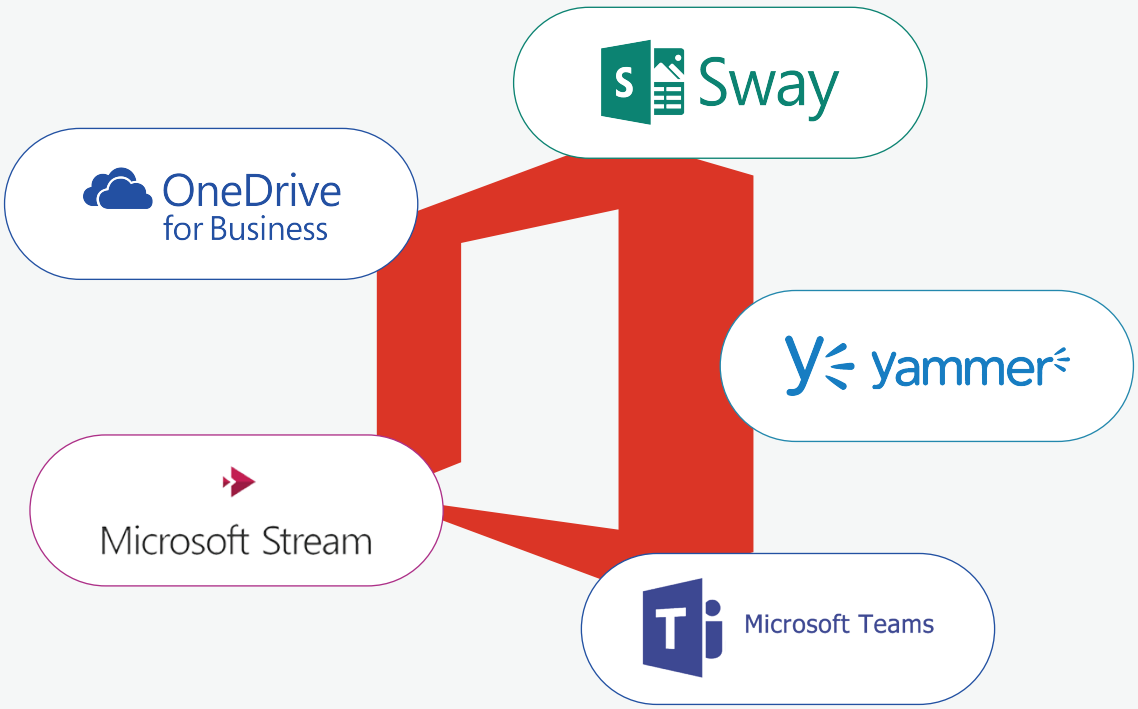
An admin's guide to

securing **Microsoft 365 productivity apps**



ManageEngine

M365 Manager Plus

ManageEngine
M365 Manager Plus

Table of Contents

Why are Microsoft 365 apps prone to leaks?

According to Skyhigh's Microsoft 365 Adoption and Risk Report,[1] 17.1 percent of files in OneDrive for Business contain sensitive data such as financial records, payment information, personally identifiable information (PII), protected health information (PHI), business plans, and source code. With so much sensitive data available on just one Office 365 collaboration tool, a disastrous data leak is an all-too-real possibility.

Data leaks are often caused by external malicious activities such as phishing, brute-force attacks, and privileged account attacks, but they can also be the result of mistakes committed by regular employees, privileged IT users, temporary staff, and others. For example, an employee may unknowingly give all users permission to access a document, or share an important file with an external user.

In this e-book, we'll discuss how in-depth monitoring of Microsoft 365 collaboration apps can help admins minimize the chance of data leaks.

Searching for a needle in a haystack

The Microsoft 365 Adoption and Risk Report also finds that, on average, an organization generates 5.4 million user events per month in Office 365. Every user activity—uploading, downloading, viewing, or sharing files; modifying document settings; and more—is logged in Microsoft 365's collaboration tools. Out of these millions of events, only a few hundred may actually be considered anomalous activities, and of those hundreds, only a handful may actually be indicators of a data breach. To track down those handful of threatening events, admins need a tool that can:

1. Audit activities granularly across Microsoft 365 collaboration tools and provide details such as what resources users can access, which users have elevated privileges, and whether sensitive data files are being shared internally or externally.
2. Report extensively on the details of an event, including the what, who, when, and where, to spot issues and evaluate if they pose any risk.
3. Send instant alerts upon detecting suspicious activities so admins can investigate and react to potential data breaches quickly.

[1] http://info.skyhighnetworks.com/rs/274-AUP-214/images/Skyhigh%20O365%20Report%20Q2%202016.pdf

Limitations of Microsoft 365 native tool

Though Microsoft 365 provides a native tool to audit the events in Microsoft 365 collaboration apps, it falls short in helping admins ensure complete security because:

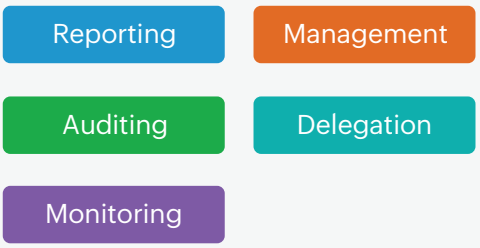
- Limited filtering capabilities make it difficult to search across audit logs and analyze the possible risks in an Microsoft 365 setup.
- The tool provides only a few predefined reports on Microsoft 365 events, forcing admins to spend valuable time building custom reports.
- The Security and Compliance Center only allows admins to search for events that happened within the last 90 days. This limited visibility into audit logs is insufficient for performing security audits and investigations.
- The 90-day log storage limitation forces admins to export and save audit logs. Besides increasing admins' workload, this takes up a large amount of storage space in the organization's database.
- Admins can only download a maximum of 50,000 log entries to a CSV file from a single audit log search, which isn't a lot, especially for mid-sized and large organizations. Additionally, CSV files can easily be manipulated.

Why M365 Manager Plus is better than native tools

M365 Manager Plus gives a comprehensive view of events happening in OneDrive for Business, Yammer, Microsoft Teams, Microsoft Stream, and other Microsoft 365 apps. M365 Manager Plus provides:

- Preconfigured reports to offer a granular view of any changes to important data. Admins can easily see changes made to files, folders, security groups, file access settings, and more.
- Easy access to logs during compliance audits and security investigations; audit logs are also stored indefinitely.
- The option to archive audit logs at the admin's convenience and restore deleted audit logs with a single click.
- No restriction on the number of logs that can be exported. Admins can export or archive logs in PDF, XLS, and HTML formats as well.

M365 Manager Plus Features



Securing Microsoft 365 productivity apps

OneDrive for Business

OneDrive for Business is one of the most popular Microsoft 365 collaboration tools. It allows users to store and secure files, share them with co-workers or external users, and more. Since OneDrive for Business stores and allows the sharing of large amounts of sensitive data, it's important to monitor every event closely. Using M365 Manager Plus, admins can track:

- **File and folder activities:** Monitor file and folder changes such as creation, modification, deletion, renaming, copying, and restoration.
- **Sharing activities:** Track details about company-wide shared links; sharing invitations; anonymous links; access requests; shared files, folders, and sites; and more.
- **Sync activities:** Monitor which files are uploaded or downloaded from OneDrive for Business, which devices are allowed to sync or are blocked from syncing, and more.
- **Security group changes**: Track security group changes, such as the addition of new members, so users aren't given unwanted privileges.

Use case

A healthcare organization's employees access a high-profile patient's medical records even though they have no legitimate reason to access this data. This type of violation of HIPAA provisions can attract huge fines for an organization if the data contained in the records is leaked. Using M365 Manager Plus' OneDrive File Accessed alerting profile, admins will receive notification about file accesses. Admins can create a custom view for particular sensitive files to know who has accessed them. This pinpointed auditing maximizes the chances of identifying every unauthorized access to help with remediation.

Microsoft Teams

Microsoft Teams allows organizations to collaborate not only within the organization, but also with outside users. Guests can participate in meetings as well as get access to chats, files, and more. This is convenient, but also increases the risk of data leaks.

- **Team events:** Audit the creation of teams and channels; addition or removal of members from teams; and other user activities.
- **Setting changes:** Track organization, team, and channel setting changes to identify whether the workplace has been compromised. Generate reports to see what changes were made by whom and when.

Use case

A construction company initiates a new project. The project manager uses Microsoft Teams to collaborate with various stakeholders, including suppliers and consultants. The manager adds these guests as and when necessary. In this case, the IT admin needs to know the details of the added guest to ensure there's no security risk. Using M365 Manager Plus' auditing and alerting profile for Added members to team, IT admins will know when a new member is added to a team.

Sway

Sway helps users easily create and share reports, stories, presentations, and more with coworkers. Users can change the privacy settings for Sway whenever they need to. Admins need to constantly monitor activities in Sway to ensure sensitive data doesn't end up in the wrong hands due to a user's mistake. M365 Manager Plus helps admins overcome this security challenge by keeping track of:

- **Sway activities:** Monitor which Sway were viewed, created, modified, deleted, and more.
- **Sway sharing:** Track which Sway have enabled the external sharing option and duplication option.
- **Enabled or disabled Sway:** Audit details on which user enabled or disabled the Sway service and when.

Use case

A marketing manager wants to share a Sway presentation with their company's clients. The manager modifies the share permission to Anyone with a link. Using M365 Manager Plus' Modified sway share level audit and alert profiles, admins can be notified about this modification to share permissions. The admins can then investigate the incident and ensure that it's a valid case of external document sharing.

Microsoft Stream

Microsoft Stream allows users to upload, view, and share recordings of meetings, presentations, or any other videos securely across the organization. By using M365 Manager Plus, admins can monitor the following activities to ensure no data leak occurs while sharing videos:

- **User activities:** Track modification of user settings, admin tenant settings, admin global role members, and more.
- **Group channel activities:** Monitor creation and modification of groups and channels, group membership modifications, and more.
- **Video activities:** Track activities such as the creation, modification, and deletion of videos; changing of video permissions; and more.

Use case

A company's R&D team creates a new product prototype video meant only for team members. The permissions are edited to share the video with a group comprising the top-level management; however, the video is shared with the wrong group and downloaded by a user that shouldn't have access. By using M365 Manager Plus' Invoke video download alert profile to track video downloads, admins can track who has downloaded videos and take action to limit any damage.

Yammer

Yammer is widely used to enhance engagement with people inside or outside an organization. Using M365 Manager Plus' auditing feature, admins can track actions of users and admins to lower the risk of data breaches. With M365 Manager Plus, admins can monitor:

- **User activities:** Monitor the modification and creation of groups and files, file sharing, file downloads, file updates, and more.
- **Admin settings changes:** Track the modification of profile settings, private content mode, hard/soft delete settings, and more.

Use case

The admin of a Yammer network was temporarily granted access to private content while investigating a technical issue. However, the admin did not turn off access after troubleshooting, so they still have access to private content. This could result in unwanted snooping into private content. Using M365 Manager Plus' capability to audit Settings Changes by Admin, this mistake can be identified and rectified before sensitive data is accessed.

Top Three

M365 Manager Plus security features

1. Comprehensive Exchange Online auditing and reporting to secure your organization from hackers.

   Exchange Online reporting | Exchange Online auditing

2. Hassle-free Azure AD auditing and reporting to track users, groups, contacts, and licenses.

   Azure AD reporting | Azure AD auditing

3. Exhaustive reporting on all administrator activities to strengthen your organization's security.

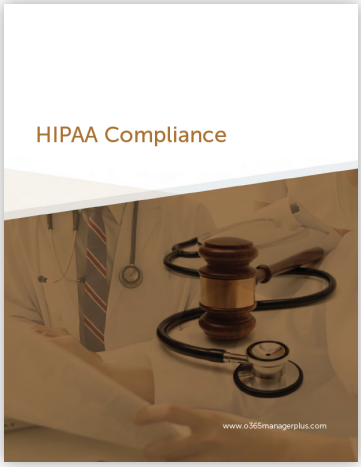
   Microsoft 365 activity reports

IT compliance checklists for **SOX, FISMA, GLBA, HIPAA, and PCI DSS**

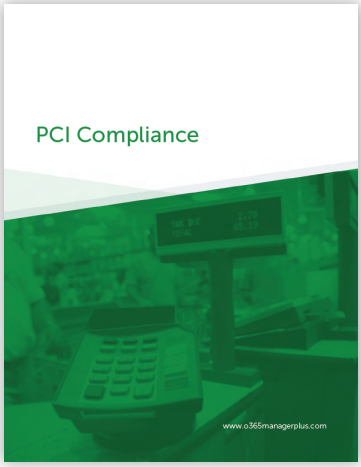
[Download SOX compliance checklist]

[Download FISMA compliance checklist]

[Download GLBA compliance checklist]



[Download HIPAA compliance checklist]



[Download PCI DSS compliance checklist]

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
M365 Manager Plus

M365 Manager Plus is an extensive Microsoft 365 tool used for reporting, managing, monitoring, auditing, and creating alerts for critical incidents. With its user-friendly interface, you can easily manage Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote Download