ManageEngine
M365 Manager Plus

Seven Best Practices to Secure your Microsoft 365

Introduction

With over 135 million monthly active users worldwide, Microsoft 365 is the most widely used cloud application suite. For many organizations, Microsoft 365 is the entry point into cloud computing. As your organization begins to migrate sensitive and business-criti-cal data to cloud platforms like Microsoft 365, several security concerns may be on your mind: Is the data secure? Who has access to it? What if unauthorized users compro-mise privileged accounts? What about meeting compliance requirements?

When it comes to Microsoft 365, you can leverage the monitoring capabilities provided by Microsoft and other Microsoft 365 administration tools like M365 Manager Plus to simplify Microsoft 365 security monitoring.

In this white paper we'll look at security monitoring best practices for Microsoft 365, including what types of activities you should monitor, what types of threats to look for, and what tools you can use to do all this.

Microsoft 365 activities you should monitor

Knowing where to start with Microsoft 365 security monitoring can be a challenge. For starters, you need to know what activities to monitor and what those activities can tell you about your IT security. In general, the types of Microsoft 365 activities you should be monitoring (if you're not already doing so) include:

User access: Learn who is accessing your Microsoft 365 subscription, when, and from where. Set up a baseline for normal user access behavior and detect any deviations to spot attack attempts. For instance, a user trying to sign in from an abnormal location is surely suspicious and warrants analysis.

Administrator actions: Once attackers gain access to your environment, they often try to escalate their privileges to gain access to your sensitive data—as do malicious insiders. Monitoring changes to admin roles, how admin activities are logged, and admin access rights can help you detect potential external and internal threats at their earliest stages.

Permissions changes: Monitoring for changes to file sharing permissions and policies in OneDrive for Business can help you spot the early signs of a potential data breach. In addition, monitoring file activities by user, including when files are uploaded, deleted, edited, and restored, can help you to detect and investigate anomalous activities.

Changes to Microsoft 365 policies: Your Microsoft 365 policies define users' access rights to resources as well as what activities those users can perform in your Microsoft 365 environ-ment. Any unwanted changes to these policies will result in a security loophole. This is why you need to continuously monitor for changes to policies, including changes to poli-cies for Exchange malware and content filtering. Changes to these policies could enable spammers to send phishing emails and malicious attachments. You should also keep an eye on any changes that weaken your organization's password policies.

Activities with known malicious actors: Monitoring your Microsoft 365 activities in context with known attack vectors helps mitigate attacks at their earlies stages. Identifying activi-ties such as file sharing with known malicious hosts and multiple file uploads with known ransomware file extensions can alert you about possible security threats.

Best practices for Microsoft 365 security monitoring

There are several steps you can take to secure your Microsoft 365 environment. Below, we'll discuss seven best practices your organization should follow for comprehensive Microsoft 365 security monitoring.

Best practice 1:

Set up password policies and multi-factor authentication (MFA)

In the Microsoft 365 Admin Center, you can fortify your Azure AD security by setting up policies for strong passwords, password expiration, and MFA for access to Microsoft 365. These good security practices, but alone, they're not enough. You should also continu-ously monitor user login activities to look for signs of compromised user credentials.

Best practice 2:

Monitor all Azure AD user sign-in activities

When an anomalous user signs in to your Microsoft 365 environment, you need to know all the details associated with this incident to stop the breach in its tracks. For example, if your CFO is currently in New York but signs in from China, you should know right away. Monitor all user sign-in activity to Azure AD to establish a baseline of normal user activity. Using this baseline, you can identify anomalies such as unusual sign ins based on time, frequency, or location. Monitor for sudden spikes in sign-in attempts or repeated sign-in failures, as these can be indications of a brute force attack. You can monitor user sign-in activities with Azure AD reports or a third-party Microsoft 365 security monitoring solution like M365 Manager Plus.

Best practice 3:

Establish a policy of least privilege

You may already be familiar with this universal security best practice, but given its importance in the context of Microsoft 365 security, it's worth reevaluating your organiza-tion's current policies. In general, you should grant your admins as few privileges as possible—enough for them to accomplish their work and nothing more. Changes in admin privileges can indicate a bad actor inside your environment trying to gain access to your business' confidential data, so it's important to continuously monitor those activities through the administrative audit logs.

Best practice 4:
Monitor Microsoft 365 administrator audit logs

By default, administrators have rights and permissions to access audit logs, monitor user activities, and detect anomalies. But there's always the chance a malicious insider with admin privileges may try to tamper with the audit logs to hide their tracks. This is why, in addition to changes in roles and permissions, you should monitor all administrator activities.

You can audit these activities with Microsoft 365's administrative audit log feature:

- File and page activities
- Folder activities
- Sharing and access request activities
- Synchronization activities
- Site administration activities
- Exchange mailbox activities
- Sway activities
- User administration activities
- Azure AD group administration activities
- Application administration activities
- Role administration activities
- Directory administration activities
- eDiscovery activities
- Power BI activities
- Microsoft Teams activities
- Yammer activities
- Exchange admin activities

Best practice 5:
Monitor all user activities in OneDrive for Business

It's important to monitor all user access and activities (delete, upload, edit, restore, etc.) to the business-critical data stored in OneDrive for Business. By establishing a baseline of regular user activity, you can detect anomalies that warrant investigation. For example, a user that's restoring a bunch of deleted files in OneDrive for Business could be a malicious actor attempting to retrieve historical data. Of course, there's always the chance an employee simply deleted some important files by accident, but either way, it's worth investigating.

In addition, maintaining a log of all user file activities can not only help you meet compliance requirements like PCI DSS, but also with any forensic investigations you may need to conduct following a data breach.

Best practice 6:

Monitor changes to OneDrive for Business sharing permissions, and file sharing with external entities

When your users share files with entities outside of your organization, you need to know about it. This is why you need to monitor for changes in OneDrive for Business that enable external sharing permissions. With advanced tools like M365 Manager Plus, you can create your own audit profiles and configure real-time email alerts to be sent to you whenever file sharing permissions have been modified.

Best practice 7:

Monitor changes to Exchange Online filtering policies

In the Microsoft Exchange Admin Center (EAC), you can define your content filtering (spam) and malware policies among other configurations. However, defining these policies is not a "set-it-and-forget-it" activity. Rather, you should continuously monitor for changes to these policies that indicate an attack or policy violation. If changes are made that weaken your content or malware filtering policies, spammers will be able to send spam, including phishing emails or emails containing attachments laden with malware.

What tools should you use to monitor Microsoft 365?

There are many tools and resources available to help you secure and monitor your Microsoft 365 environment. In fact, it can be overwhelming just trying to figure out where to start.

Microsoft 365 Security & Compliance Center

Microsoft calls its Microsoft 365 Security & Compliance Center a one-stop portal for pro-tecting your data in Microsoft 365. It offers helpful functions such as archiving mailboxes, data loss prevention, searching for content and user activities, managing devices,as-signing permissions, and retaining documents.

Microsoft 365 Cloud App Security

Microsoft offers Microsoft 365 Cloud App Security, previously known as Microsoft 365 Advanced Security Management, which gives you insight into suspicious activity in Microsoft 365 so you can investigate potentially problematic situations and take action to address security issues when they arise. With Microsoft 365 Cloud App Security, you can receive notifications of triggered alerts for atypical or suspicious activities, see how your organization's data in Microsoft 365 is accessed and used, suspend user accounts exhibiting suspicious activity, and require users to log back in to Microsoft 365 apps after an alert has been triggered.

At the time of writing, Microsoft 365 Advanced Security Management is available in Microsoft 365 Enterprises E5 and as an add-on to other Microsoft 365 Enterprise plans.

Microsoft 365 Management API and unified security management

The Microsoft 365 Management API extends the security and compliance capabilities of Microsoft 365 to dedicated security management solutions, including M365 Manager Plus. Through the RESTful API, external applications can obtain information about user, admin, system, and policy actions and events from Microsoft 365 and Azure Active Direc-tory activity logs. This means that you can manage Microsoft 365 security monitoring in your existing security management platform, if it supports the API.

Why you should consider using a third-party security monitoring tool

While Microsoft provides many tools, capabilities, and resources for security and compliance, finding where to provision, configure, and use each service can be tremendously challenging. While the user experience is just one factor to consider, there are plenty of other reasons why you may want to consider using a third-party security monitoring solution for Microsoft 365.

An additional layer of security monitoring

A dedicated security monitoring solution can provide an additional layer of security assurance and critical threat detection capabilities for your Microsoft 365 environment, including pre-built rules, alarms, and analytics.

Centralized visibility of your entire security posture

When you analyze user activities in the Microsoft Security and Compliance Center, you have to search for related security information across multiple tools and logs to get the full context of the threat during investigation and response. A unified security management solution dismantles data silos by aggregating all security-related data in one place. This data includes information about your assets, their known vulnerabilities, user activities, and more, which makes for much more efficient incident investigation.

Retain audit logs beyond 90 days

As of today, Microsoft purges any Microsoft 365 logs that are older than 90 days. If you're looking for better log retention periods to comply with regulations, you can leverage a solution like M365 Manager Plus to collect Microsoft 365 logs and store them infinitely.