WHITE PAPER

# Best Practices for Office 365 Security Monitoring

## Introduction

Microsoft Office 365 has largely defined how teams collaborate in the cloud. Today, it's the most widely used cloud application suite by organizations, with over 100 million monthly active users worldwide[1].

For many organizations, Office 365 marks an entry point into cloud computing—and with it, cloud security. As organizations migrate sensitive and business-critical data to the Microsoft cloud, many security concerns arise: Is our data secure? Who has access to it, both internally and externally? What if unauthorized users compromise account credentials? How can we detect ransomware and other malware in Office 365? What do we need to do to maintain compliance?

According to the 2017 Cloud Security Spotlight Report conducted by the Information Security Community on LinkedIn[2], the top three cloud security concerns are protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%).

With these cloud security concerns in mind, organizations must take steps to secure and monitor their Office 365 environments. Fortunately, organizations can leverage security monitoring capabilities provided by Microsoft and other security management vendors like AlienVault® to ease Office 365 security monitoring.

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

## What Activities Should You Monitor in Office 365?

It can be a challenge to know where to start with your Office 365 security monitoring, what activities to monitor, and what those activities can tell you about your security posture. In general, the types of activities that you should be monitoring in Office 365 (if you are not already doing so) include:

- **User Access:** Know who is accessing your Office 365 subscription, when, and from where. By establishing a baseline of normal user access behavior, you can then identify anomalous or suspicious user activities, for example, a user trying to sign in from a country where your organization doesn't have any presence. In addition, spikes in repeated login attempts can alert you to a potential bruteforce login attack.

[1] Microsoft Earnings Call, 27 April 2017, https://c.s-microsoft.com/en-us/CMSFiles/TranscriptFY17Q3.docx?version=8584c192-0242-d952-f743-256ec919ac42

[2] The 2017 survey gathered information from 1,900 security professionals, over half of whom reported to be using Office 365. View the full survey report here.

- **Administrator Actions:** Once attackers gain access inside your environment, they often try to escalate their privileges to gain more control and access to your sensitive data—as do malicious insiders. Monitoring changes to admin roles and access rights as well as to changes to how admin activities are logged can alert you to potential external and internal threats.
- **File Access & Sharing:** Monitoring for changes to file sharing permissions and policies in OneDrive and SharePoint can alert you to the early signs of a potential data breach. In addition, monitoring file activities by user, including file upload, delete, edit and restore, can help you to detect and investigate anomalous activities.
- **Changes to Office 365 Policies:** Your Office 365 policies define the expected behaviors and parameters of operations of your users and of the solutions within Office 365, and so you should continuously monitor for changes to policies that may expose you to potential risks. This includes changes to Exchange malware and content filtering policies that may enable spammers to send phishing emails and malicious attachments; and changes that weaken your organization's password policies.
- **Activities with Known Malicious Actors:** By monitoring your Office 365 activities in context to the latest threat intelligence, you can more quickly detect malicious ransomware and other malware in your Office 365 environment. Identifying activities such as file sharing with known malicious hosts and multiple file uploads with known ransomware file extensions can alert you to such an attack.

## OFFICE 365 ACTIVITIES TO MONITOR FOR SECURITY & COMPLIANCE

| ACTIVITY TYPE | WHAT TO MONITOR | WHAT TO INVESTIGATE |
|---|---|---|
| **User and Administrator Access** | › Login successes and failures<br>› Logins by time and location<br>› Repeated login failures followed by login success | › Compromised user credentials<br>› Bruteforce login attempts<br>› Sign-in attempts from unfamiliar locations |
| **Administrator Actions** | › New user creations<br>› Repeated user deletions<br>› Changes to network admin permissions<br>› New site collection admin creation<br>› Changes to admin audit logging configuration | › Malicious escalation of privilege<br>› Compromised admin credentials<br>› Policy changes and violations |
| **File Access & Sharing** | › User access to SharePoint & OneDrive files<br>› Restoring of deleted OneDrive files<br>› Changes to SharePoint & OneDrive sharing policies<br>› File sharing enabled with external entities | › Unauthorized sharing of files, folders or SharePoint sites outside the organization<br>› Attempts to access historical data by restoring deleted files<br>› Policy changes and violations |
| **Policy Changes** | › Changes to O365 policies including Exchange Online (e.g. Malware Policies, SPAM Filtering Policies), Data Leakage Protection Policy, and more | › Policy changes and violations |
| **Activities with Known Bad Actors** | › Communication or file sharing with known malicious hosts<br>› Multiple file uploads with file extensions known to be used in ransomware attacks | › Possible ransomware or other malware attack |

# Best Practices for Office 365 Security Monitoring

Organizations that use Office 365 can take the following steps to establish good security monitoring practices for their Office 365 environments.

## Monitor All User Access to Office 365. Know Who Logs In, When and from Where

To maintain a healthy cloud security posture, start by securing and monitoring your users' account credentials and access to Office 365.

With Azure Active Directory (Azure AD), you have a centralized way to manage your users' account credentials and access to Office 365 applications from the cloud. You can even synchronize Azure AD with your on-premises Active Directory, and use it as a single sign-on service (SSO) to thousands of cloud apps, including DropBox and Salesforce.com. This makes Azure AD the center of all your identity and access management activities.

### Best Practice: Set Up Password Policies and Multi-Factor Authentication (MFA) in Office 365

In the Office 365 Admin Center, you can fortify your Azure AD security by setting up policies for strong passwords, password expiry dates, and multi-factor authentication (MFA) for access to Office 365[3]. These activities are good security practices, but alone, they're not enough. You should also continuously monitor user login activities to look for signs of compromised user credentials.

### Best Practice: Monitor All Azure AD User Sign-In Activities

When anomalous user sign-in activities occur, you need to know immediately so you can investigate the events and stop a potential data breach in its tracks. For example, if your CFO is currently in New York but signs in from China at 4:00AM, you should be alerted immediately to that activity.

You should monitor all user sign-in activities to Azure AD to establish a baseline of normal user activity, against which you can identify anomalies in time, frequency, or location of sign-in. Monitor for sudden spikes in sign-in attempts or repeated sign-in failures, which can indicate a bruteforce attack.

You can monitor user sign-in activities with Azure AD reports[4] (advanced reporting may require Azure AD Premium edition) or a third-party Office 365 security monitoring solution like **AlienVault USM Anywhere™**.

## Audit Administrative Actions in Your Office 365 Account

While monitoring user activities can give insight to who is doing what inside your Office 365 environment, monitoring your admin activities provides critical insight into who is changing your Office 365 environment and how. Because administrative activities carry the potential for bigger risks to your organization's data, it's important to establish security best practices around your administrators' activities.

### Best Practice: Establish a Policy of Least Privilege

You may already be familiar with this universal security best practice, but it bears repeating in the context of your Office 365 security. Microsoft uses role-based access controls (RBAC) for admins, which you can manage from the Office 365 Admin Center[5]. In general, you should grant your admins the least amount of privilege as possible for them to accomplish their work.

---

[3] MFA currently requires an Azure AD Premium subscription

[4] Advanced reporting may require Azure AD Premium edition. **Learn More >**

[5] Learn more about Office 365 Admin Roles **here**.

Changes in admin privilege levels may indicate a bad actor inside your environment trying to gain more control over your account and data, so it's important to continuously monitor those activities through the administrative audit logs.

### Best Practice: Monitor Office 365 Administrator Audit Logs

In addition to changes in roles and permissions, you should monitor all administrator activities with the administrative audit log feature in Office 365. Office 365 audit logs can also be connected to your existing SIEM or unified security management tool if it supports the Office 365 Management Activity API (discussed below).

Audited admin activities include user account creations and deletions, new SharePoint site collection admin, new Yammer network admin, and much more. Changes to the configuration of the Office 365 audit logs may also indicate that a bad actor is trying to tamper with the log data to cover his tracks. (Another best practice here is to send your Office 365 audit log data to a separate log management solution that offers tamper-proof storage to meet your security and compliance requirements.)

Audited Activities in Office 365[6] include:

- 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

## Monitor the Integrity of Your SharePoint and OneDrive Data

Data security and integrity in the cloud is the biggest cloud security concern for IT security professionals today. And, it's easy to understand why.

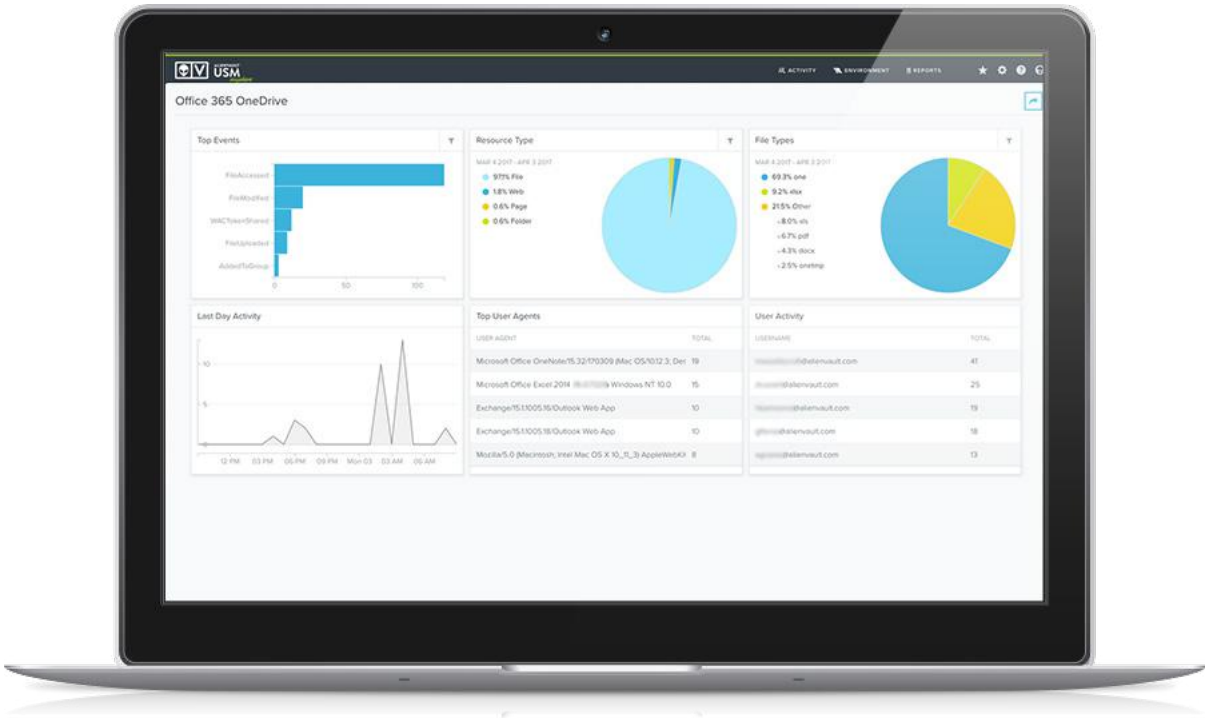
As your users migrate and share business-critical data in SharePoint Online and OneDrive for Business, you need to know who has access to it, who is making changes to it, and who is sharing it with entities outside the organization. However, this activity generates a lot of events, in fact, too many for you to track manually. You can leverage the Microsoft Security & Compliance Center or a solution that leverages the Office 365 Management Activity API to view activity trends, detect anomalies, and identify activities involving known malicious actors or ransomware.

### Best Practice: Monitor All User Activities in SharePoint and OneDrive

It's important to monitor all user access and activities (delete, upload, edit, restore, etc.) to the business-critical data stored in your SharePoint and OneDrive. By establishing a baseline of user activities, you can detect anomalies that warrant investigation. For example, a user that restores many deleted files in OneDrive may indicate a possible attempt by a malicious actor to retrieve historical data (Or perhaps, Mark accidently deleted some important files. Either way, you'll want to investigate.)

[6] "Search the audit log in the Office 365 Security & Compliance Center," Microsoft. https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c?ui=en-US&rs=en-US&ad=US#ID0EABAAA=Audited_activities

In addition, maintaining a log of all user file activities can also support any forensics investigations you may need to conduct following a data breach as well as file integrity monitoring security controls needed to meet compliance requirements like PCI DSS.




Office 365 OneDrive Activities Dashboard in USM Anywhere

### Best Practice: Monitor Changes to SharePoint and OneDrive Sharing Permissions & File Sharing with External Entities

When your users share files with entities outside of your organization, you need to know. Thus, you should monitor for changes in SharePoint and OneDrive that enable external sharing permissions. Using a threat intelligence subscription like AlienVault Open Threat Exchange™ (OTX™), you should monitor for file sharing with known malicious hosts, which could indicate a data breach.

### Best Practice: Monitor File Activities involving Known Bad Actors

A third-party security monitoring solution with integrated threat intelligence goes beyond the built-in features in Office 365 to detect file activities involving known bad actors. For example, multiple file uploads with known ransomware extensions such as '.encrypt' can alert you to a ransomware attack, so that you can take immediate action to isolate the environment.

## Protect Your Users' Mailboxes from Spam and Phishing Attacks in Exchange Online

91% of all cyberattacks today start with a phishing email[7]. In the age of socially engineered attacks, with organizations sending all types of data through email, protecting your data and the integrity of Office 365 users' mailboxes is more challenging than ever. It takes diligence and continuous effort to create, refine, and monitor policies that determine which inbound messages your users receive and which are blocked or sent to junk mail.

[7] "91% Of Cyberattacks Start With A Phishing Email." Dark Reading, 2016. http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

### Best Practice: Monitor Changes to Exchange Online Filtering Policies

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

## What Tools Should You Use to Monitor Office 365?

There are many tools and resources available to help you secure and monitor your Office 365 environment. In fact, it can be overwhelming to know where to start.

You can find a broad list of Microsoft-provided Office 365 security tools and topics **here**.

### Microsoft Security & Compliance Center

Microsoft calls its Office 365 Security & Compliance Center a one-stop portal for protecting your data in Office 365. It is helpful for functions such as archiving mailboxes, data loss prevention to protect sensitive information, searching for content and user activities, device management, permissions and document retention.

You can learn more about the Microsoft Security & Compliance Center **here**.

### Office 365 Advanced Security Management

Microsoft offers Office 365 Advanced Security Management for anomaly detection and activity tracking across your Office 365 account. The tool offers basic anomaly detection capabilities to watch for anomalous login, access, and account activity. If you already know what types of activities you want to monitor, you can manually define anomaly detection policies and activity policies that will alert you when those policies are matched. You can also populate a list of applications that are connected to your Office 365 account by uploading log files from your network devices.

At the time of writing, Office 365 Advanced Security Management is available in Office 365 E5 and as add-on to other Office 365 enterprise plans[8].

### Office 365 Management API & Unified Security Management

The Office 365 Management API[9] extends the security and compliance capabilities of Office 365 to dedicated security management solutions, including **AlienVault USM Anywhere**. Through the RESTful API, external applications can obtain information about user, admin, system, and policy actions and events from Office 365 and Azure Active Directory activity logs. This means that you can manage your Office 365 security monitoring in your existing security management platform, if it supports the API.

## Why You Should Consider a Third-Party Security Monitoring Tool for Office 365

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

[8] https://blogs.office.com/2016/06/01/gain-enhanced-visibility-and-control-with-office-365-advanced-security-management/

[9] https://msdn.microsoft.com/en-us/office-365/office-365-managment-apis-overview

### An Additional Layer of Security Monitoring

Even after you have set up your Office 365 policies and alerts, do you have confidence that you have configured everything correctly, that the configurations will point you to the right threats, and that they will continue to do so as threats evolve? A dedicated security monitoring solution can provide an additional layer of security assurance and critical threat detection capabilities for your Office 365 environment, including pre-built rules, alarms, and analytics

### Centralized Visibility of your Entire Security Posture

When you analyze user activities in Microsoft Security and Compliance Center, you must often also search for related security information across other tools and logs to get the full threat context you need for investigation and response. A unified security management solution dismantles data siloes by aggregating all security-related data in a single pane of glass: information about your assets, their known vulnerabilities, user activities, and more. This makes incident investigation more efficient.

### Integrated Threat Intelligence

While Microsoft does provide threat intelligence services like **Advanced Threat Protection and Threat Intelligence**, they only provide those services within the silo of Office 365. In contrast, a unified security management solution, like USM Anywhere, with its **integrated threat intelligence**, applies the latest threat context to all events and activities across your IT environment, in the cloud and on-premises.

### Retain Audit Logs Beyond 90-Days

As of today, Microsoft purges any Office 365 logs that are older than 90 days. Organizations seeking longer log retention periods, such as for compliance with regulations, can leverage a solution like USM Anywhere to collect their Office 365 logs and store them for significantly longer periods of time.

## AlienVault USM Anywhere for Office 365 Security Monitoring

AlienVault USM Anywhere delivers the **Office 365 security and compliance monitoring** you need to protect your users and your data hosted in the Office 365 environment.

USM monitors your Office 365 and alerts you to anomalies in:

- Administrator actions that may indicate an internal or external attempt to escalate privileges or breach data
- Anomalous user sign-in activities by time and location that may indicate compromised account credentials or a bruteforce login attempt
- Changes to files and file sharing permissions in SharePoint Online and OneDrive that may indicate a potential data breach or ransomware attacks
- Changes to Exchange Online policies that could enable spam and malware
- Communication with known malicious actors, and much more

### How It Works

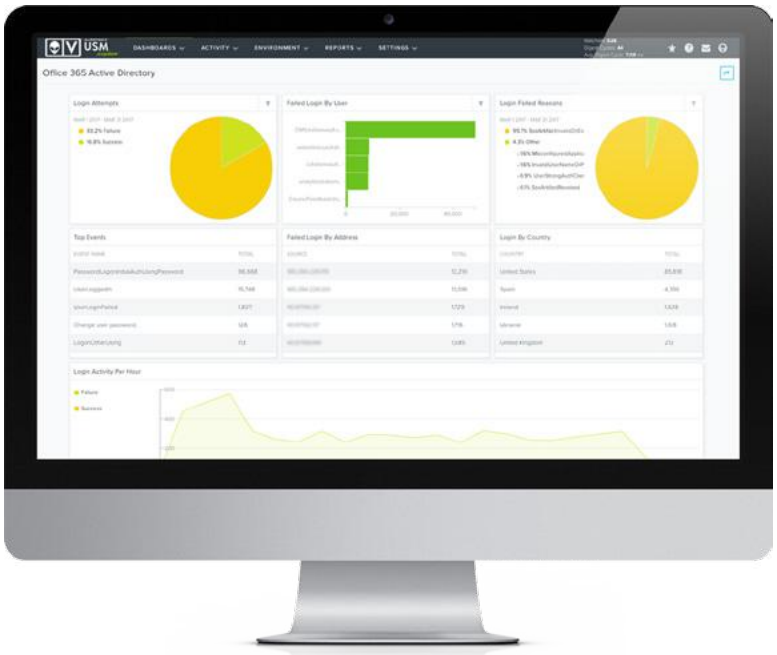
USM Anywhere collects Office 365 events through the Office 365 Management API. It analyzes those events in context to the latest threat intelligence from the **AlienVault Labs Security Research Team** and alerts you to potential threats and policy violations in your Office 365 environment. The AlienVault Labs Team writes and continuously updates Office 365-specific correlation rules and remediation guidance as threats evolve in the wild, so you don't have to. And because your Office 365 events and alarms are side by side with the rest of your asset, vulnerability, and threat data in USM Anywhere, you can investigate faster without having to manually connect data points from across multiple systems.


## Interactive Dashboards & Analytics

USM Anywhere visualizes your Office 365 events in rich, interactive dashboards, making monitoring fast and simple. For example, the pre-built dashboard for Azure AD shows real-time Azure AD activity trends, from where users are logging in, and login failure reasons. This contextualized data helps you to quickly detect threats such as brute force login attempts, compromised accounts, and more. You can also drill down and pivot on any data point, making incident investigation fast and simple.

## The Advantages of Unified Security Management

With USM Anywhere, you get complete, continuous visibility of your Office 365 security and compliance posture. USM Anywhere is the only solution that delivers unified essential security capabilities to give you actionable security visibility into your Office 365 environment. It delivers onto a single solution:




- Asset Discovery and Inventory
- Vulnerability Assessment
- Intrusion Detection
- Behavioral Monitoring
- SIEM Event Correlation
- Log Management & long-term storage

Plus, its ecosystem of AlienApps extend your security orchestration capabilities to connected third-party security and cloud technologies, like Cisco Umbrella and Office 365. In doing so, USM Anywhere can serve as the central hub for all your security and compliance efforts.

USM Anywhere centralizes security monitoring for all your IT environments: public cloud, private cloud, and on-premises physical or virtual infrastructure. So, you can have continuous security monitoring as you migrate services and workloads across environments through one affordable solution.

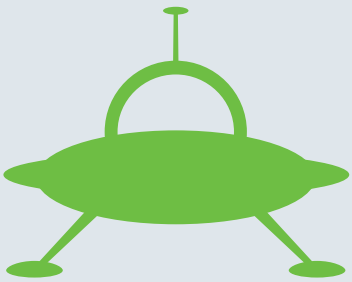
Because USM Anywhere is delivered as a SaaS solution, you can deploy rapidly and get security insight within minutes, save significant costs on hardware, and readily scale as your infrastructure expands. It delivers high reliability and performance without the overhead of maintenance.

## Learn More:

Office 365 Security Monitoring with USM Anywhere

Explore USM Anywhere in our Online Demo

Start Detecting Threats Today with a Free Trial of USM Anywhere



## About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and **award-winning approach**, trusted by **thousands of customers**, combines the essential security controls of our all-in-one platform, AlienVault **Unified Security Management**, with the power of AlienVault's **Open Threat Exchange**, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.