

Microsoft 365 Security Handbook

Microsoft 365 is the most widely deployed SaaS solution globally and is indispensable for modern-day business operations. Its suite of offerings, extensive configuration settings, and limitless customization capabilities make securing this complex platform effectively a formidable challenge.

This comprehensive handbook aims to arm security professionals with a deep understanding of Microsoft 365 and the necessary measures to keep the platform and its data secure. It presents a detailed overview of the platform, highlights potential security risks, and provides actionable guidance on effective risk mitigation strategies.

Reading Time: 15 mins

Overview

Microsoft 365 (formerly known as Office 365) is an integrated suite of productivity and collaboration applications. Its offering includes popular tools such as Microsoft Word, Excel, PowerPoint, Outlook, Teams, OneDrive, and SharePoint, among others. The applications are delivered via a cloud-based model, enabling users to access their data and work collaboratively from any location.

Contents

Overview	1
Use Cases	2
Microsoft 365 Security Incidents	2
Shared Responsibility Model	3
Microsoft Model	3
What Data is Stored in Microsoft 365	4
Configuration Data	4
Operational Data	4
Roles & Responsibilities	5
Microsoft 365 Operators	5
Microsoft 365 Users	5
RBAC Structure	6
Microsoft RBAC Structure	6
Common risks associated with RBAC	6
Customization in Microsoft 365	7
Customization Capabilities	7
Common risks associated with Customization:	7
3rd Party Apps	8
SaaS-to-SaaS Ecosystem	8
Common risks associated with 3rd Party Apps	8
Risks Associated with Third-Party Apps	8
Logging Capabilities	9
Logs and Event Types	9
Top Security Risks	10
Summary	11

Use Cases

Microsoft 365 offers a comprehensive suite of cloud-based productivity tools. The typical use cases span across various organizational needs and include:

- 1. Content Creation & Management:** Microsoft 365 serves as a digital workspace for creating and managing content. Applications like Word, Excel, and PowerPoint allow users to create, edit, and share documents, spreadsheets, and presentations, respectively.
- 2. Communication & Collaboration:** Through Outlook and Teams, Microsoft 365 enables internal and external communications via email, chat, voice, and video calls. It also offers a collaborative workspace that facilitates team discussions, content sharing, and project management.
- 3. File Storage & Sharing:** OneDrive, SharePoint, and Teams in Microsoft 365 provide secure and efficient platforms for file storage and sharing. These tools enable individuals and teams to store, access, and share documents and other files from anywhere, anytime.
- 4. Task & Project Management:** Tools like Planner, To Do, and the project management capabilities within Teams provide users with an array of options to manage tasks, projects, and workflows.
- 5. Business Process Automation & Custom Applications:** With Power Automate and Power Apps, organizations can automate business processes and build custom applications, further enhancing productivity and efficiency.
- 6. Analytics & Insights:** Through Power BI, organizations can leverage data analytics, visualization, and business intelligence features. These help users in making data-driven decisions, tracking KPIs, and uncovering trends and insights.

This wide-ranging functionality of Microsoft 365, along with its ability to handle sensitive data, numerous integrations, customizations, and user roles, introduces a layer of complexity that necessitates a strong understanding of the platform to maintain a secure environment. Thus, it is important to understand the breadth of Microsoft 365's features, operations, and potential vulnerabilities to ensure the effective protection of your systems and data.

Microsoft 365 Security Incidents

As SaaS adoption grows, the risk for breaches that threaten business operations and the security of highly sensitive data escalates. Below are a few notable Microsoft security incidents seen in the press:

- **Microsoft: Lapsus\$ Used Employee Account to Steal Source Code:** Microsoft confirmed that the Lapsus\$ extortion group hacked one of its employee's accounts to get "limited access" to project source code repositories. [Read more.](#)
- **Microsoft employees accidentally exposed login credentials for Microsoft Azure:** Even Microsoft isn't immune to accidental credential sharing due to simply not following best security practices. Recently, Microsoft confirmed that their own employees accidentally uploaded sensitive login credentials to Microsoft's Azure servers systems to GitHub. These credentials were then exposed to the open internet for anyone to access and begin moving vertically or horizontally through the network. [Read more.](#)
- **Capita cyberattack disrupted access to its Microsoft Office 365 apps:** Capita offers a wide range of services for customers in the finance, IT, healthcare, education, and government sectors, many of which reported outages in access to Microsoft 365. Capita gave very little information to the press other than they experienced an IT issue that impacted its internal systems. [Read more.](#)



Shared Responsibility Model

Microsoft Model

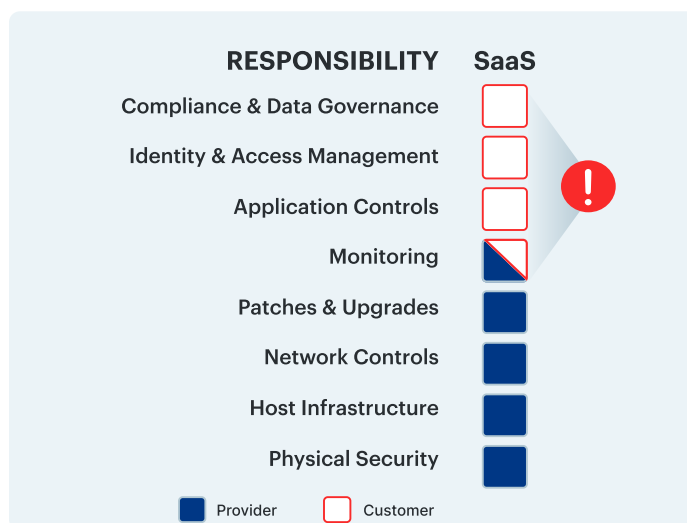
Microsoft 365 operates on a shared responsibility model, which means that both Microsoft and the customer have distinct responsibilities for ensuring the security and integrity of the platform. Understanding these responsibilities is crucial for maintaining a secure Microsoft 365 environment. Here's an overview of the shared responsibilities:

Microsoft Responsibilities

- **Infrastructure and Data Centers:** Microsoft is responsible for managing the underlying infrastructure, including data centers, network infrastructure, and hardware.
- **Application Security:** Microsoft is responsible for securing the Microsoft 365 applications, such as Exchange Online, SharePoint Online, and Teams, ensuring their availability, reliability, and protection against common security threats.
- **Patching and Updates:** Microsoft is responsible for applying security patches and updates to the Microsoft 365 platform to address vulnerabilities and protect against emerging threats.
- **Identity and Access Management:** Microsoft provides robust identity and access management controls, including multi-factor authentication and role-based access control (RBAC), to protect user accounts and prevent unauthorized access to the platform.

Customer Responsibilities

- **User Management:** Customers are responsible for managing user accounts, including provisioning and deprovisioning users, assigning appropriate access permissions, and enforcing strong password policies.
- **Data Protection:** Customers have the responsibility to protect their data within Microsoft 365, including implementing appropriate data loss prevention (DLP) policies, encryption, and backup strategies.
- **Configuration and customization:** Customers are responsible for configuring and customizing the Microsoft 365 environment to align with their specific security requirements, such as defining sharing settings, setting up data retention policies, and managing app permissions.
- **User Awareness and Training:** Customers should educate their users about security best practices, including recognizing and reporting potential threats, practicing good password hygiene, and understanding the importance of data privacy.
- **Compliance and Legal Obligations:** Customers must ensure compliance with industry regulations and legal obligations, such as data privacy laws and industry-specific requirements, when using Microsoft 365.



Summary

The shared responsibility model with Microsoft 365 emphasizes the joint effort required to maintain a secure environment. While Microsoft takes responsibility for the infrastructure, application security, and platform updates, customers must manage user accounts, protect their data, configure the environment, educate users, and comply with legal obligations. By understanding and fulfilling their respective responsibilities, organizations can establish a strong security posture for Microsoft 365.

What Data is Stored in Microsoft 365



Configuration Data

Configuration data is integral to Microsoft 365, dictating how its services and applications operate. It facilitates tailored management of system components, enabling admins to control access, security, and customization. This data not only enhances functionality and user experience but also bolsters security and compliance, guiding permissions, data loss prevention rules, and policy enforcement.

- **Personal Identifiable Information (PII):** This includes information such as usernames, email addresses, contact details, and profile information, as well as security credentials like passwords or security questions. Administrators can manage and configure user settings, including permissions and access to various services and applications.
- **Group Configuration:** Microsoft 365 allows the creation and management of groups for different teams, departments, or projects. The configuration data for groups includes group names, members, permissions, and access to shared resources.
- **Email Settings:** This includes data related to Exchange Online configuration, such as mailbox settings, spam filter settings, rules, and policies. It also includes settings for email clients and protocols such as POP, IMAP, and SMTP.
- **SharePoint and OneDrive Settings:** This involves the configuration settings of SharePoint sites and OneDrive storage. It includes permissions, versioning settings, site libraries, site collections, and other related configurations.
- **Teams Settings:** Microsoft Teams is a key part of Microsoft 365, facilitating communication and collaboration. Its configuration data includes settings related to channels, teams, meetings, voice, video, and chat options.
- **Security and Compliance Settings:** These include configurations around data loss prevention (DLP) policies, retention policies, audit log settings, eDiscovery settings, threat protection settings, and information protection settings.
- **Application Settings:** This refers to settings for the various Microsoft 365 apps like Word, Excel, PowerPoint, etc. It can include preferences, templates, add-ins, and other customizable aspects of these applications.
- **Power Platform Settings:** For organizations using Power BI, Power Apps, Power Automate, and Power Virtual Agents, settings related to these services are also stored. This can include data connections, app settings, report configurations, automation flows, and more.

- **Device Management Settings:** For organizations using Microsoft's device management solutions (like Intune), this includes configurations related to device compliance policies, app protection policies, device enrollment settings, etc.

Operational Data

Microsoft 365 encompasses a wide range of data storage capabilities to meet the various needs of organizations. The platform stores various types of data, including configuration data and operational data, some of which may contain sensitive information.

- **Emails and Attachments:** Microsoft 365 stores email communications, including message content, attachments, and metadata, in Exchange Online mailboxes. This data often contains sensitive information, such as confidential business communications, intellectual property, or personally identifiable information (PII).
- **Documents and Files:** SharePoint Online serves as a document management and collaboration platform, storing files, folders, and associated metadata. These documents may contain sensitive business data, financial information, customer records, or proprietary content.
- **Chats and Conversations:** Microsoft Teams facilitates chat based communication and stores chat conversations, shared files, and meeting recordings. Chats may contain sensitive discussions, confidential project details, or confidential attachments.
- **User Activity Logs:** Microsoft 365 captures user activity logs, including login events, file access, and administrative actions. These logs provide insights into user behavior and are essential for auditing, compliance, and security monitoring purposes.
- **Calendars and Events:** Exchange Online stores user calendars, appointments, and meeting schedules, enabling efficient scheduling and resource management. Calendar data may include sensitive business meetings, client appointments, or confidential event details.

Summary

Security considerations for configuration and operational data include ensuring only authorized users have access to specific data based on their roles, implementing data encryption, regular auditing of access logs, secure data disposal procedures, and adherence to regulatory compliance (such as GDPR, CCPA, HIPAA, etc.) and industry standards (ISO 27001, SOC 2, etc.).

Roles & Responsibilities

Microsoft 365 Operators

Managing Microsoft 365 in an organization involves various roles, each having their unique responsibilities and areas of focus. Here are some common roles that help manage a typical Microsoft 365 deployment:

- 1. Microsoft 365 Administrator:** The Microsoft 365 Administrator oversees the overall deployment of Microsoft 365. They are responsible for setting up services, managing users and groups, and controlling access to resources. They also handle routine maintenance, updates, and resolve technical issues.
- 2. IT Support/Help Desk:** This role provides direct support to end-users. They troubleshoot problems, provide guidance on application usage, and escalate issues to administrators as needed. They often manage user access and passwords and assist with minor technical difficulties.
- 3. Security Administrator:** The Security Administrator focuses on the safe use of Microsoft 365 tools. They establish security protocols, monitor threats, handle breaches, and ensure compliance with relevant regulations. They also oversee access controls and user permissions to minimise risk.
- 4. Compliance Officer:** This role ensures that the organization meets legal and corporate data policies when using Microsoft 365. They handle data governance, manage retention policies, and handle eDiscovery requests. They work closely with the Security Administrator to ensure data privacy and security.
- 5. Teams Administrator:** Given the widespread use of Microsoft Teams in many organizations, a specific role is often designated to manage this app. Teams Administrators handle the setup of teams, channels, and manage permissions. They also troubleshoot issues and train users on Teams usage.
- 6. SharePoint Administrator:** This role handles the SharePoint Online environment, managing site collections, permissions, and design elements. They may also be involved in content management and workflow design.
- 7. OneDrive Administrator:** The OneDrive Administrator manages the organization's OneDrive for Business implementation. They oversee storage limits, sharing capabilities, and synchronization.

The titles and responsibilities of these roles can vary from organization to organization based on size, needs, and complexity. Additionally, it's not uncommon for roles to overlap, or for a single person to handle multiple roles, especially in smaller organizations.

Microsoft 365 Users

Microsoft 365 is used by a wide range of internal users in an organization, each interacting with the platform in different ways based on their role and needs. The actual usage can differ significantly based on the organization's specific needs, and many users often interact with multiple Microsoft 365 components in order to perform daily tasks:

- 1. Employees:** These are the largest group of users, utilising Word for documents, Excel for data management, PowerPoint for presentations, and Outlook and Teams for communication.
- 2. Project Teams:** These users may leverage suites such as Teams for project collaboration and communication, and Planner and Microsoft To Do for task management.
- 3. IT Staff:** These users interact with Microsoft 365 more technically, handling user accounts, security configurations, and platform troubleshooting.
- 4. Human Resources (HR):** HR uses Microsoft 365 for recruitment, onboarding, training, and performance reviews, using Forms for feedback and SharePoint as an HR resource portal.

Microsoft 365's flexibility allows not only internal users but also external users to interact with the platform. They typically include:

- 1. Clients:** Clients can be given access to specific files and folders in OneDrive or SharePoint for document sharing and collaboration. They can also be invited to Teams meetings and shared calendars.
- 2. Partners:** Business partners may require access to shared documents or to collaborate on projects using Teams. Microsoft 365 allows the user to control the level of access and permissions for each external user.
- 3. Contractors and Consultants:** Contractors and consultants might require access to email, documents, and other resources within Microsoft 365. The level of access can be defined based on their specific roles and requirements.

Summary

To maintain a secure Microsoft 365 environment, understanding the user interactions and establishing proper security measures are vital. It is important to have robust security policies, regular audits of external user activities, and ongoing security training for all users. Moreover, maintaining good communication with external users about security expectations and best practices is crucial.

RBAC Structure

Microsoft RBAC Structure

Microsoft 365 employs a Role-Based Access Control (RBAC) framework to manage user permissions and access to its various features and data. RBAC plays a crucial role in enforcing the principle of least privilege and enhancing data security by granting users the appropriate level of access based on their roles and responsibilities within the Microsoft 365 environment. The RBAC constructs in Microsoft 365 consist of the following key components:

- 1. Roles:** Roles in Microsoft 365 define a set of privileges and permissions assigned to users based on their job functions and responsibilities. These roles govern the actions and data that users can access within the platform.
- 2. Permissions:** Permissions in Microsoft 365 determine the specific actions and operations that users can perform within their assigned roles. Permissions are granular, allowing organizations to tailor access rights to different functionalities and data sets.
- 3. Role Assignments:** Role assignments link users to specific roles in Microsoft 365, ensuring that individuals have the appropriate access privileges necessary to fulfil their job duties effectively and securely.

Common risks associated with RBAC

- **Role Misconfiguration:** Improper assignment of roles or misconfiguration of role permissions can result in users having excessive privileges or unauthorized access to sensitive data within Microsoft 365, potentially leading to data breaches, unauthorized modifications, or accidental exposure of critical information.
- **Privilege Escalation:** Inadequate enforcement of RBAC policies may enable users to escalate their privileges, granting them access to functions or data beyond their intended scope. This can result in unauthorized access, data leaks, or the compromise of confidential business information.
- **Inconsistent Role Definitions:** Inconsistencies in role definitions across different applications or workloads within Microsoft 365 can lead to confusion, improper access, and potential security vulnerabilities. This can impact operational efficiency and data integrity, as well as introduce compliance risks.
- **Lack of Role Reviews:** Failing to continuously review and update role assignments can lead to the accumulation of unnecessary privileges or outdated access permissions, increasing the risk of unauthorized access. This can result in compliance violations, data breaches, or the compromise of sensitive business data.
- **Insider Threats:** Malicious insiders with authorized access can abuse their privileges within Microsoft 365, potentially compromising data integrity or confidentiality. Monitoring user activities and implementing appropriate access controls can help mitigate this risk. This can result in financial losses, reputational damage, regulatory penalties, or legal repercussions.

Summary

To mitigate these risks and ensure effective RBAC in Microsoft 365, organizations should conduct regular reviews and audits of role assignments, validate and align roles with job functions, enforce the principle of least privilege, and monitor user activities to detect and respond to any unauthorized or suspicious actions. By adhering to RBAC best practices, organizations can maintain a secure Microsoft 365 environment while providing users with the necessary access to perform their duties effectively.

Customization in Microsoft 365

Customization Capabilities

Microsoft 365 offers extensive customization to align the platform with the unique needs of an organization. While these adjustments can improve efficiency and cater to specific business requirements, they also present security risks. Let's explore some key areas of customization and their associated security implications:

- **PowerShell:** PowerShell is a robust scripting language used for automating tasks and enhancing functionality within Microsoft 365. While it is a powerful tool, it can potentially introduce vulnerabilities if not appropriately managed. Scripts that aren't properly written or tested can lead to security breaches or data loss. Moreover, cybercriminals are aware of this weakness and often exploit PowerShell, emphasizing the need for tight control over its use.
- **Application Customization:** Microsoft 365 includes various applications like SharePoint, Teams, and Power Apps, each providing their customization options. However, modifying these apps can sometimes alter the default security configurations, creating potential security weaknesses. These could inadvertently allow unauthorized access, data leaks, or increased vulnerability to cyber-attacks.
- **Workflow Automation:** Through Microsoft Power Automate, organizations can create customized automated workflows across different applications. However, improper configuration of these workflows might lead to unintentional data exposure. Therefore, automated workflows involving sensitive data need careful handling and review to avoid potential security risks.
- **Data Storage and Sharing:** Customizing how data is stored, processed, or shared within Microsoft 365 can lead to unauthorized data access or data leakage. Therefore, any customization altering data handling must be thoroughly evaluated for potential impacts on data security.
- **Lack of Expertise:** Customizing Microsoft 365 often requires advanced knowledge of the platform. If performed by individuals without adequate expertise, customization may unintentionally alter important security settings or bypass built-in security features, increasing the risk profile.
- **Interoperability Issues:** Customizations, particularly when integrating with other systems or apps, can create unforeseen security issues. Not all systems or applications may adhere to the same security standards as Microsoft 365, potentially leading to vulnerabilities.
- **Oversharing and Permission Creep:** Customization can often involve adjusting permissions and sharing settings. Inappropriately broad permissions, or "permission creep," can expose sensitive data and resources to users who shouldn't have access.
- **Inadequate Testing:** Customizations that are not thoroughly tested can introduce security risks. It is crucial that any changes made to the system are properly vetted for potential security implications.
- **Non-compliance:** Depending on the industry, customizations might lead to compliance issues. Certain regulations mandate specific data handling and security measures, which could be compromised with unsuitable customizations.

Summary

In conclusion, while customization of Microsoft 365 can enhance the productivity and user experience, it needs to be approached with caution. A thorough understanding of potential security implications, coupled with careful management and monitoring, is crucial to maintaining a secure digital environment.

Common risks associated with Customization:

- **Misconfigurations:** Any customization, if not properly configured, can introduce vulnerabilities. Improper settings or adjustments can leave data exposed, allow unauthorized access, or weaken security policies, thereby increasing the risk of data breaches or loss.
- **Complexity:** As customization increases, the complexity of the system also rises, making it harder to monitor and manage effectively. This complexity can obscure potential threats or vulnerabilities, making it easier for them to go undetected.

3rd Party Apps

SaaS-to-SaaS Ecosystem

Third-party apps play a crucial role in expanding the functional of Microsoft 365, offering enhanced features and integrations.

While many well-known apps have established security measures, it is important to be aware of the associated risks, particularly when considering lesser-known or niche applications. Organizations should be mindful of the fact that employees often have the ability to install third-party apps, which introduces an additional level of risk.

Here is a list of commonly deployed 3rd party integrations with Microsoft 365:

- 1. Zoom:** Schedule and conduct video meetings seamlessly with Zoom's integration into Microsoft 365.
- 2. Trello:** Track projects and manage tasks efficiently by integrating Trello with Microsoft 365.
- 3. DocuSign:** Sign documents electronically within Microsoft 365, improving workflow efficiency and reducing paper based processes.
- 4. Adobe Creative Cloud:** Seamlessly connect Adobe Creative Cloud tools with Microsoft 365, streamlining design and productivity workflows.
- 5. Tableau:** Enhance data visualization and analysis by integrating Tableau with Microsoft 365.
- 6. Asana:** Improve project management capabilities by integrating Asana with Microsoft 365.
- 7. Zoho CRM:** Integrate Zoho CRM with Microsoft 365 to streamline customer data flow and enhance sales and marketing activities.
- 8. Smartsheet:** Enhance project management and work execution by integrating Smartsheet with Microsoft 365.

Common risks associated with 3rd Party Apps

When integrating third-party apps into Microsoft 365, it is crucial to consider the following security aspects:

- **Data Security:** Assess how the app handles and stores sensitive data to ensure proper security measures are in place, such as encryption and secure data transmission.
- **Vendor Trustworthiness:** Evaluate the reputation and credibility of the app's vendor, ensuring they adhere to industry security standards and provide regular updates and support.



- **Permissions and Access Control:** Review the app's permissions and access requirements, granting only the necessary privileges to minimise the risk of unauthorized data access.
- **Compliance Requirements:** Ensure that the app aligns with applicable data protection regulations and industry compliance standards to avoid potential legal and regulatory issues.

Risks Associated with Third-Party Apps

- **Malware and Security Exploits:** Unsolicited or unauthorized apps may contain malware or security vulnerabilities that can compromise the integrity of the Microsoft 365 environment.
- **Data Breaches and Leakage:** Inadequate security measures or excessive data access permissions can lead to unauthorized data breaches or leakage.
- **Lack of Updates and Support:** Lesser-known apps may lack regular updates or comprehensive support, leaving them more susceptible to security vulnerabilities.
- **Non-Compliance:** Integrating apps that do not adhere to data protection or industry compliance standards can result in compliance violations and legal consequences.

Summary

To mitigate risks from third-party apps in Microsoft 365, organizations should thoroughly vet apps, considering their security measures and data handling policies. Adherence to the least privilege principle can prevent unauthorized data access. Regular updates and continuous monitoring of these apps can address emerging security threats promptly. Finally, compliance checks and a robust risk management framework can help maintain legal standards and identify potential issues, ensuring a secure integration of third-party apps.

Logging Capabilities

Logs and Event Types

Microsoft 365 provides robust logging capabilities that help organizations monitor and analyze system activities, enhance security, and ensure compliance. Here are the key types of logs available in Microsoft 365 and how they assist organizations:

- **Audit Logs:** Microsoft 365 generates comprehensive audit logs that capture a wide range of system activities, including user logins, data access and modifications, administrative actions, and configuration changes. These logs provide an audit trail of actions taken within the system, enabling organizations to track user activity, investigate security incidents, and demonstrate compliance with regulatory requirements.
- **Security Logs:** Microsoft 365 maintains security logs that record security-related events, such as failed login attempts, suspicious activities, malware detection, and security policy violations. These logs help organizations detect and investigate potential security breaches, identify patterns of unauthorized access, and take appropriate measures to strengthen their security posture.
- **Access Logs:** Microsoft 365 logs access events that track user authentication, session durations, and activities related to user access. These logs provide visibility into user interactions with the system, helping organizations monitor user behavior, identify abnormal access patterns, and detect potential insider threats or unauthorized access attempts.
- **Exchange Online Message Trace Logs:** Capture information about email messages sent and received within Exchange Online. Organizations can use these logs to track message delivery, investigate email-related incidents, and ensure compliance with email security policies.

- **SharePoint and OneDrive Audit Logs:** Microsoft 365 offers audit logs specifically for SharePoint and OneDrive, capturing activities such as file uploads, downloads, modifications, and sharing events. These logs help organizations track data usage, monitor file access and modifications, and detect suspicious activities that may indicate data exfiltration or unauthorized access.
- **Azure Active Directory Logs:** Microsoft 365 integrates with Azure Active Directory (AAD), generating logs that record user sign-ins, password resets, role assignments, and other AAD related activities. These logs enable organizations to monitor user authentication events, detect anomalous sign-in behavior, and strengthen identity and access management controls.

Summary

By leveraging these logging capabilities, organizations can gain visibility into their Microsoft 365 environment, detect security incidents, investigate suspicious activities, and demonstrate compliance with industry regulations. Regular monitoring, analysis, and retention of logs help organizations identify threats, assess system performance, and take proactive measures to protect sensitive data and ensure a secure and compliant Microsoft 365 environment.


Top Security Risks

Security professionals need to be aware of various security risks associated with Microsoft 365 to ensure the protection of sensitive data and maintain a secure environment. Here are some common Microsoft 365 security risks that require attention:

- **Misconfigurations:** Misconfigurations in Microsoft 365 settings and permissions can leave data and applications exposed. It is essential to continuously review and validate configurations to prevent unauthorized access or unintended data leakage.
- **Phishing Attacks:** Phishing emails and social engineering remain prevalent risks. Users can unknowingly disclose credentials or sensitive information, leading to unauthorized access or data breaches. Ongoing security awareness training is crucial to mitigate this risk.
- **Unauthorized Access:** Weak authentication mechanisms, compromised user credentials, or inadequate access controls can result in unauthorized access to Microsoft 365 resources, leading to data breaches, data loss, or unauthorized modification.
- **Data Leakage:** Improper data sharing settings or accidental exposure of sensitive information can result in data leakage. Organizations should enforce appropriate data loss prevention (DLP) policies and educate users about handling sensitive data.
- **Insider Threats:** Malicious actions or inadvertent mistakes by employees can pose a significant risk to Microsoft 365 security. Monitoring user activities, implementing role-based access controls, and fostering a strong security culture can help mitigate insider threats.
- **Malware and Ransomware:** Malicious software, including malware and ransomware, can infect Microsoft 365 environments, compromising data integrity, availability, and confidentiality. Robust anti-malware and ransomware protection measures are necessary to counter this risk.
- **Third Party Apps:** Employees utilizing unsanctioned or unauthorized third-party apps can introduce security vulnerabilities, as these apps may lack adequate security measures or compliance with organizational policies. Strict app approval processes and user education can minimize the risks associated with third party apps.
- **Insider Data Theft:** Employees with authorized access to sensitive data may intentionally or unintentionally steal or leak valuable information. Organizations should implement data access controls, data loss prevention (DLP) solutions, and employee monitoring to detect and prevent insider data theft.
- **Lack of Regular Updates:** Delaying or neglecting security updates and patches for Microsoft 365 can leave vulnerabilities unaddressed, making the environment susceptible to

exploitation. Implementing a proactive patch management process is essential to reduce the risk of known vulnerabilities.

How can AppOmni help



AppOmni SaaS security makes it easy for security and IT teams to protect and monitor their entire SaaS environment. AppOmni was founded by a team of security veterans from top SaaS providers and cybersecurity vendors. Using their expertise, they put together the following list of best SaaS security practices and recommendations:

- **Baseline Security Policies:** Configurable out of the box baselines security policies to help map to recommended best practice security configurations.
- **Compliance Policies:** Map a Microsoft 365 instance to the CIS Benchmark, ISO27001, SOC2, NIST CSF, NIST 80053 and Sarbanes Oxley.
- **Sensitive Permission Monitoring:** Identify users, groups and applications who have been assigned high risk permissions.
- **Monitor users assigned to sensitive Groups, Teams and Roles:** Ensure that any change in RBAC assignments within Microsoft 365 does not result in users gaining access to assets beyond their job requirements.
- **Monitor creation of new groups, teams and roles:** Be alerted to new groups, team and role creations and easily review an inventory of existing groups and orgs.
- **Provide visibility of and monitoring around Policies:** Microsoft 365's broad range of policies allow users to control how their Microsoft 365 environment functions, AppOmni's ability to monitor these policies for configuration drift helps users ensure their configuration is not drifting away from their business intent.
- **Monitor SaaS-to-SaaS connections:** AppOmni's App Ecosystem capabilities can provide visibility of fourth party SaaS applications which have been connected to a Microsoft 365 instance, potentially exposing data.
- **Threat Detection:** Monitor for known threat actor tactics and techniques or build custom threat detection rules to map more tightly to businesses concerns.

Summary

In order to protect sensitive data and maintain a secure environment, it is crucial for security professionals to gain a deep understanding of how Microsoft 365 is utilised within their organization, continuously review the security posture, and implement appropriate security controls.

This comprehensive handbook has covered various aspects including application overview, user roles, customization, third party app integration, shared responsibility model, data storage, security risks, RBAC constructs, logging capabilities, and more. By proactively addressing these considerations and staying vigilant about evolving security threats, security professionals can ensure the effective protection of their organization's Microsoft 365 environment and mitigate potential risks

To learn more, email us at info@appomni.com or visit appomni.com.