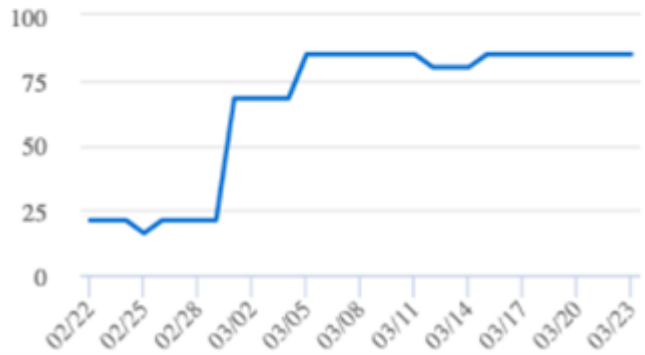
NX

Office365 Security Optimization Analysis

Security Score	Compliance Score
Total score: 85/238 This score reflects the collective security state of your identities, data, devices, apps, and infrastructure. Updated 03/23/2020 	Overall compliance score Your compliance score: 75%  12120/16101 points achieved

Background

We often think of technologies or services not as a cohesive system, but as the sum to total parts. In optimizing the connectivity of your systems, what we see as an important focus for your company is the Office 365 Secure Score. This score rates your security configurations and settings.

Your score gives you a sense how great your company is doing with its adherence to Microsoft's security best practices. MicrosoftSecure Score will help analyze each organization's Office 365 security based on administrative activities as well as audit security settingsand allows us to make recommendations.

After implementation of needed and recommended actions, the score is re-evaluated to re-assess if you have leveraged the various features across 365 to provide your customers and client with the most secure experience.

What We Assessed

There exists a multitude of features highlighted below within Microsoft 365 that should be reviewed and configured with appropriate settings. These features should each be used in accordance with Betah's IT Security requirements. The following were considered when identifying and deciding how to protect sensitive data.

Data Governance – Assists with classifying content, defining retention rules and data destruction
Classifications – Labels can be applied to emails/docs to enforce policies and retention settings
Data Privacy – GDPR requirements and access to their personal data
Threat Management – Threat tracking and attack simulators can be performed to assess risk

Assessment Standards

This assessment was conducted against the following industry standards.

1. National Institute Standards and Technology Cybersecurity Framework (NIST CSF)
2. Federal Information Processing Standards

Results

The areas listed below define the competencies we are looking for when analyzing your Office365 environment for optimization regarding security best practices.

- **Identity**
  - Access and Authorization
  - Password Policy
  - Rights Management
- **Data**
  - Data Loss Prevention
  - Archiving
  - Auditing
  - Storage
- **Device**
  - Mobile Device Management
- **Apps**
  - Multi-Factor Authentication
- **Infrastructure**
  - Email / Exchange

We have reviewed your existing onboarding process for new users against the list below. This list serves as best practices regarding security and information technology when onboarding a new user. An 'X'

indicated the absence of a policy or process in place. A '' indicates Betah Associates does currently have and employ a policy or process for this security-related task.

Identity

Access and Authorization

Deleting or blocking accounts that haven't been used in the last 30 days, after checking with owners, helps prevent unauthorized use of inactive accounts. These accounts can be targets for attackers who are looking to find ways to access your data without being noticed. You have 16 accounts that have not been used in the last 30 days. Listed below is a policy that will help improve the security of your Office365 instance.

Delete/block accounts not used in last 30 days

With self-service password reset in Azure Active Directory, users no longer need to engage helpdesk to reset passwords. You have **71 of 71** users who don't have self-service password reset enabled. Listed below is a policy that will help improve the security of your Office365 instance.

Enable self-service password reset

Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication. You have **71 of 71** users that don't have the sign-in risky policy turned on. Listed below is a policy that will help improve the security of your Office365 instance.

Turn on sign-in risk policy

Password Policy

We found a password expiration policy in place of 90 days with a user notification time of 14 days. This is in alignment with Microsoft's security best practices. Listed below is a policy that will help improve the security of your Office365 instance.

Office 365 Passwords Are Not Set to Expire

Rights Management

Using Information Rights Management protections (IRM) on email and document data prevents accidental or malicious exposure of data outside of your organization. Attackers targeting specific, high value data assets are blocked from opening them without user credentials. Listed below is a policy that will help improve the security of your Office365 instance.

X Apply IRM protections to documents

You can tighten the security of your services by regulating the access of third-party integrated applications and only allow access to necessary applications that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts. There are currently no policies in place for this security control. Listed below is a policy that will help improve the security of your Office365 instance.

X Do not allow users to grant consent to unmanaged applications

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The most severe rating from any category becomes the information system's overall security categorization. Upon review of the , we did not find any retention labels or tags being applied to data based on a category or classification system that could be used to assess the exposure of sensitive information to unauthorized users. Listed below is a policy that will help improve the security of your Office365 instance.

X Ensure data classification, retention labeling and archiving policies are set up and used

Data

Data Loss Prevention

Data Loss Prevention (DLP) policies can be used to comply with business standards and industry regulations that mandate the protection of sensitive information to prevent accidental or malicious disclosure. DLP sends alerts after it scans for potentially sensitive data, suchas social security and credit card numbers. Setting up DLP policies will let you identify, monitor, and automatically protect sensitive information. Upon initial analysis, we did find you have zero Data Loss Prevention (DLP) policies applied. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Apply Data Loss Prevention Policies
- X Ensure that between two and four global admins are designated
- X Ensure O365 ATP SafeLinks for Office Applications is Enabled
- X Ensure Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled

Archiving

When a label is applied to email or docs (automatically or by the user), the content is retained based on the settings you chose. For example, you can create labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. Upon review of the , we did not find any retention labels or tags being applied to data based on a category or classification system. Listedbelow is a policy that will help improve the security of your Office365 instance.

- X Ensure labels used for data classification policies are set up and enabled

Auditing

Your important data should be piped to a security information and event management (SIEM) solution for additional monitoring and correlation. Once you have set up audit logging for your mailboxes, you can identify who is logging into mailboxes and sending emails or conducting tasks performed by the administrator, the mailbox owner, or a designated user. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Enable Audit Logging
- X Ensure Microsoft 365 audit log search is Enabled
- X Ensure mailbox auditing for all users is Enabled

Storage

Making sure all unauthorized users do not access sensitive information that is stored as data-at-rest is an important part of security. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Ensure the customer lockbox feature is enabled
- X Ensure external domains are not allowed in Skype or Teams
- X Ensure that external users cannot share files, folders, and sites they do not own

Device

Mobile Device Management

A mobile device manager ensures the proper policies are defined and agreements are in place for employees of the business that access BETAH resources using mobile devices. Policies can be configured to determine which devices/users can communicate with the email servers, shared drives and other internal resources. Policies can also be used to enforce compliance to Government policies such as device encryption and remote wiping. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Ensure mobile devices require the use of a password
- X Ensure that mobile device password reuse is prohibited
- X Ensure that mobile devices are set to never expire passwords
- X Ensure that users cannot connect from devices that are jailbroken or rooted
- X Ensure that settings are enabled to lock multiple devices after a period of inactivity to prevent unauthorized access
- X Ensure that mobile device encryption is enabled to prevent unauthorized access to data
- X Ensure that mobile devices require complex passwords to prevent brute force attacks
- X Ensure that devices connecting have anti-virus software and intrusion monitoring.
- X Ensure mobile device management policies are required for email profiles

Apps

Multi-Factor Authentication

Multi-factor authentication (MFA) helps protect devices, resources and data that is accessed by BETAH users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised. You have 32 out of 71 users registered and protected with MFA. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Multifactor authentication is enabled for all users in administrative roles
- X Ensure all users can complete multi-factor authentication for secure access

Infrastructure

Email / Exchange

Message encryption in Office 365 requires the recipient to log in to read and reply to the encrypted message. Email communication is important and vital to BETAH. This is also why it is often the biggest security threat to an organization. Listed below are policies / settings that will help improve the security of your Office365 instance.

- X Ensure the Common Attachment Types Filter is enabled
- X Ensure malware and spam policies are enabled
- X Ensure that an anti-phishing policy has been created
- X Ensure mail transport rules do not whitelist specific domains
- X Ensure the Advanced Threat Protection Safe Links policy is enabled
- X Ensure the Advanced Threat Protection Safe Attachments policy is enabled
- X Enable mailbox auditing and unified audit log search

We found several users who have auto-forwards setup to forward emails sent to the @betah.com email address to an external email. Listed below is a policy that will help improve the security of your Office365 instance

mail transport rules do not forward email to external domains

Recommendations

Below is a list of recommendations by Zoom Technologies, in accordance with Microsoft, that can be implemented in the BETAH Office365 account to improve the security footprint. In reviewing your account, we have determined the below mentioned items to be useful to implement regarding the security of your business.

Improvement Action	Impact	Portal	Zoom / Ease	Next Steps
Ensure all users can complete multi-factor authentication for secure access	High	Azure Active Directory		
Enable self-service password reset	Mid	Azure Active Directory		
Do not allow users to grant consent to unmanaged applications	Mid	Azure Active Directory		
Apply IRM protections to documents	Mid	Azure Active Directory		
Configure expiration time for external sharing links	Mid	SharePoint Online		
Use limited administrative roles	Low	Azure Active Directory		
Delete/block accounts not used in last 30 days	Mid	Azure Active Directory		
Setup data labeling and tagging used for retention and arching (FIPS 199)	High	Exchange Online		
Allow anonymous guest sharing links for sites and docs	Mid	SharePoint Online		
Ensure mail transport rules do not forward email to external domains	Mid	Exchange Online		
Apply Data Loss Prevention policies	Mid	Microsoft Information Protection		
Turn on sign-in and user risk policy	Mid	Azure Active Directory		
Enable policy to block legacy authentication	Mid	Azure Active Directory		
Implement Mobile Device Management solution	High	Azure Active Directory		