PENTHARA
TECHNOLOGIES

Free Microsoft 365 Security Assessment

Know where your business stands against security threats with the complete visibility of your Microsoft 365 Security world at zero cost.

Get this assessment at no cost to you today.

Table Of Contents

About Us

The Penthara Security Assessment for Microsoft 365 comes from the deep experience in dealing with situations where bad actors have hacked into organizations' infrastructure and services.

By taking a proactive approach and looking closely at common misconfigurations, weak spots in processes, and exploitation methods, organizations can lower the overall risk and ensure optimized protection and visibility for events within a Microsoft 365 tenant.

Our Zero Cost Assessment

Offers an overall cyber security health check of your M365 environment. We can tailor it to your specific organisational requirements or concerns (for example, compliance regulations).

The overall aim is to assist businesses to understand their security stance and take positive actions to improve their security posture.

Overview:

In the new era of cloud transformation and rising security incidents, Microsoft 365 is the most accepted and trusted cloud data-host service for enterprises. For the same reason, it is the highly targeted cloud platform for the threat actors as well.

If not configured appropriately for your specific use case, the Microsoft 365 platform can allow some bad actors to take advantage and steal your data.

Since security is not just limited to technology, it also includes your business processes, controls, policies, standards, and education programs. Some bad actors nowadays go very far and steal your data or impersonate you by social engineering as well.

It is not uncommon to see an email from the manager asking the accounts team to clear an invoice ASAP, which can be spoofed or impersonated.

Compromising Microsoft 365 tenants opens the gateway for attackers to remotely access sensitive cloud data, without breaching the corporate perimeter.

Assessing your Microsoft 365 environment provides recommendations to ensure you remain secure.

These threat actors can breach Microsoft 365 tenants by exploiting:

- Weak or legacy authentication mechanisms
- Security controls that have not been optimally configured
- Accounts with privileged access levels
- Accounts with weak passwords or those that do not require multifactor authentication

Penthara’s Approach

Our security assessment evaluates common Microsoft 365 platform areas and access controls across six core focus areas:

Security architecture and hardening

Threat detection and response

Identity and access management

Visibility

Disaster recovery

Data protection

1. Security Architecture and Hardening

Evaluation:

Examine the management of user identities and permissions within Microsoft 365, including user authentication and authorization processes.

Purpose:

To guarantee that only authorized users can access your Microsoft 365 services, reducing the risk of unauthorized access or da
ta breaches.

2. Identity and Access Management

Evaluation:

Assess the overall structure and configuration of your Microsoft 365 environment to identify vulnerabilities and weaknesses.

Purpose:

To ensure that your Microsoft 365 setup is designed and configured with security in mind, minimizing potential entry points for attackers.

3. Visibility

Evaluation:

Analyze the monitoring and logging capabilities within Microsoft 365 to gain insights into user activities and potential security incidents.

Purpose:

To establish effective visibility into your Microsoft 365 environment to detect and respond to security threats promptly.

4. Data Protection

Evaluation:

Review data encryption, access controls, and data loss prevention measures to safeguard sensitive information stored in Microsoft 365.

Purpose:

To ensure the confidentiality and integrity of your data, preventing data leaks and unauthorized access.

5. Disaster Recovery

Evaluation:

Assess the backup and recovery procedures in place for Microsoft 365 data, including email, files, and configurations.

Purpose:

To establish a reliable plan to recover critical data in the event of unexpected incidents or data loss scenarios.

6. Threat Detection and Response

Evaluation:

Examine the capabilities for detecting and responding to security threats and incidents within Microsoft 365.

Purpose:

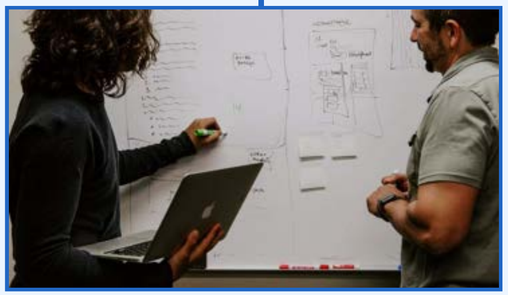
To strengthen your ability to identify and mitigate security threats promptly, minimizing the impact of potential breaches.

Assessment Duration:

This absolutely free Microsoft 365 security assessment will typically take 2 - 4 weeks and consists of four phases. Penthara team will perform the following activities:

Assessment Kickoff & Technical setup

Data Collection



Report Preparation

Report Presentation

In your own Microsoft environment

We only use Microsoft tools to analyze your security logs and warnings. Moreover, we process all information in your own Microsoft 365 tenant. This means that your data remains secure in your own environment.

Assessment Stages:

Assessment Kickoff & Technical Setup:

- Examine the capabilities for detecting and responding to security threats and incidents within Microsoft 365.
- To strengthen your ability to identify and mitigate security threats promptly, minimizing the impact of potential breaches.

Data Collection:

- Gather essential data related to your Microsoft 365 environment, including configurations, access logs, and security settings.
- Obtain a comprehensive dataset for analysis, allowing a thorough examination of your Microsoft 365 security posture.

Report Preparation:

- Analysis of the collected data, identification of security gaps and vulnerabilities.
- Create a comprehensive and actionable report that provides insights into the security strengths and weaknesses of your Microsoft 365 setup.

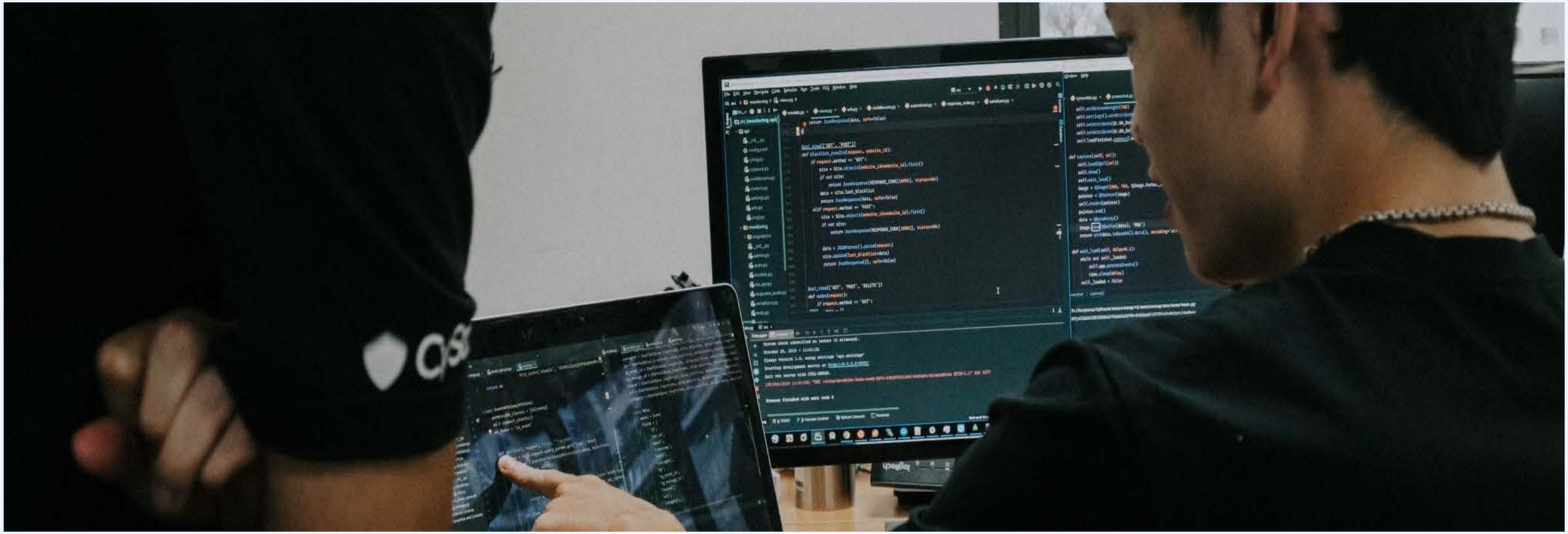
Report Presentation:

- Present the assessment findings and recommendations to the stakeholders within your organization.
- Communicate the results of the assessment clearly, provide insights into potential risks, and offer actionable recommendations for enhancing Microsoft 365 security.

During the entire evaluation, we minimize the workload on your IT teams as far as possible, and the evaluation will have absolutely no impact on your end users.

Post Assessment

We are available to help you post-assessment, if required, to configure and manage your security posture.



Our Deliverables:

At the completion of the engagement, Penthara's team will provide a detailed report that includes:

Prioritized and basic recommendations for further hardening the security posture of your Microsoft 365 tenant.

Specific Microsoft 365 security best practices to align with current configurations and operational processes.

A snapshot of the existing Microsoft 365 tenant security configuration.

Practical recommendations for enhancing visibility and detection.

Suitable for:

An existing Microsoft 365 customer

- With Microsoft 365 E3 or E5 licenses.
- Concerned about the security of your Microsoft 365 environment.
- Exploring the latest best practices, security guidance, and advice.
- Looking for reassurances surrounding security.
- Planning to attain a security and compliance accreditation.

Microsoft 365 Security Assessment involves:

This comprehensive assessment will cover the following Microsoft 365 components:

- **Security and Access**
  - *MFA Settings*
  - *Identity protection*
  - *Conditional Access*
  - *Defender for 365*
  - *Email Security*
- **Endpoint Management**
- **Exchange Online**
- **Microsoft Teams**
- **External Collaboration Settings**
- **Microsoft 365 Secure Score**
- **Collaboration and external sharing**
- **SharePoint / OneDrive Admin center**

1. Security and Access

Assessment of the overall security measures in place within your Microsoft 365 environment, including:

MFA Settings (Multi-Factor Authentication): Assessment of multi-factor authentication configurations by verifying identities to add an extra layer of security to user logins.

Identity Protection: Evaluation of identity protection measures to protect user identities and prevent unauthorized access and identity-related threats.

Conditional Access: Assessment of policies and rules governing access to Microsoft 365 resources based on specific conditions and criteria to ensure secure and appropriate access for users.

Defender for 365: Deployment and configuration evaluation or threat protection to enhance threat detection and response capabilities to safeguard Microsoft 365 assets.

Email Security: Evaluation of Mail Flow assessment, mailbox, and group permissions, connectors, etc. to protect email communication within Microsoft 365 and ensure the confidentiality and integrity of email communications and attachments.

2. Collaboration and External Sharing:

Examination of how collaboration tools for Business within Microsoft 365 (Microsoft Teams, SharePoint Online, and OneDrive), are configured and used like general sharing settings, and permissions on sites and libraries to secure collaboration while mitigating potential data leakage risks.

3. External Collaboration Settings:

Reviewing the settings related to external collaboration, including sharing permissions and policies to safeguard data while enabling external collaboration when necessary.

4. SharePoint / OneDrive Admin Center:

Assessment of the security and access controls in SharePoint and OneDrive environments. This will help protect and manage document storage and sharing within these services effectively.

5. Endpoint Management:

Examination of endpoint security settings to prevent unauthorized access and protect sensitive data enhancing the Endpoint Security.

6. Exchange Online:

Reviewing the security configurations and policies for Exchange Online, which manages email services to ensure email security and prevent email-based threats.

7. Microsoft Teams:

Assessment of security settings and controls within the Microsoft Teams collaboration platform like Teams ownership, channel settings, sharing settings, etc. to Promote secure and productive communication and collaboration.

8. Microsoft 365 Secure Score:

Calculating and analyzing the Microsoft 365 Secure Score provides insights into your security posture. This aids in measuring and improving your overall security effectiveness based on the Secure Score recommendations.

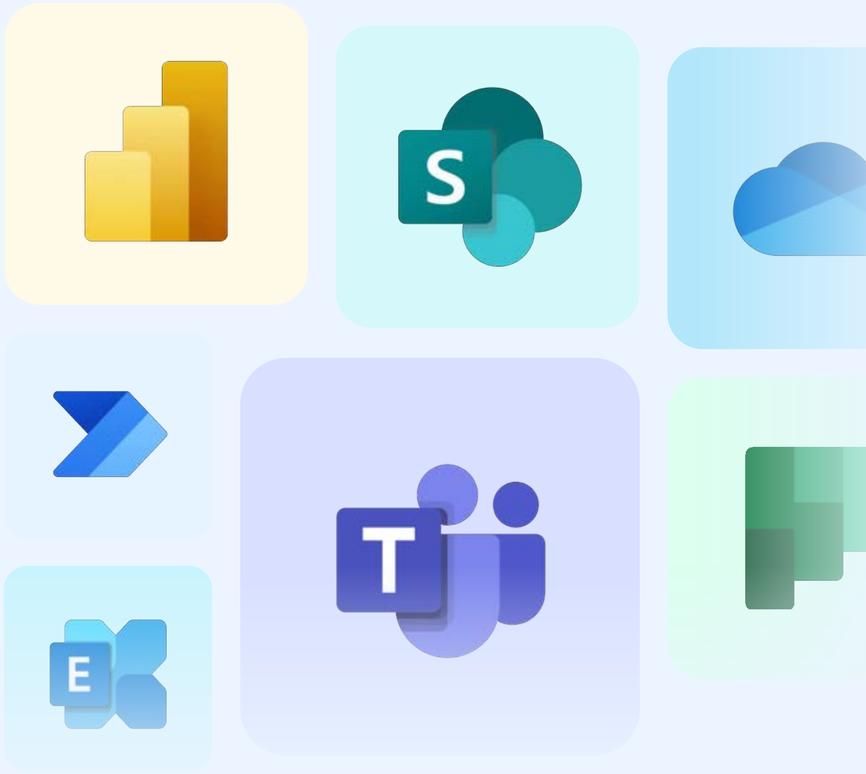
Take your Next Step

Penthara Technologies is offering this Microsoft 365 Security Assessment at zero cost with the aim to help businesses quantify the potential benefits of Microsoft 365, improving return on investment, and enhancing the security of their digital environment.

Let’s talk about how Microsoft 365 expertise at Penthara Technologies can help you achieve your security goals.

Book A Slot →

Learn more: www.penthara.com



PENTHARA
TECHNOLOGIES

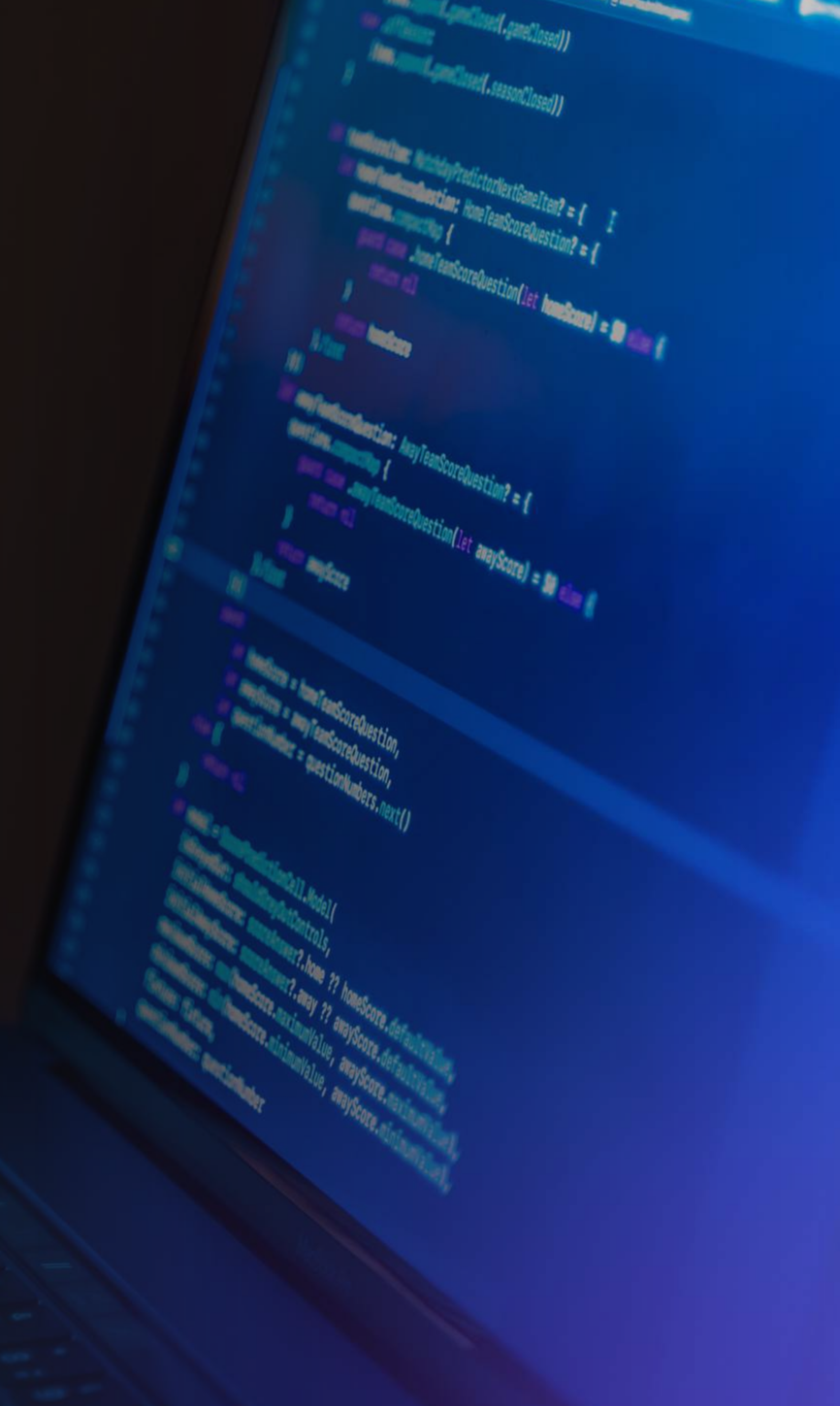
Get in touch

+91-62843-00850

info@penthara.com

Stalk us online

www.penthara.com



Disclaimer: