Microsoft 365 Security Assessment

Product Overview

resolution
TECHNOLOGY

Microsoft 365 Security Assessment

Microsoft 365 provides a significant range of business communication and collaboration services, backed by foundational elements such as identity management and device management.

The range of available settings to secure and manage this environment can be overwhelming to those not involved in a Microsoft 365 security management role. While some aspects of the platform are configured to allow teams and partners to collaborate easily, are they best configured to protect your business data ?

Resolution Technology have developed a program to assist customers with a critical assessment of their Microsoft 365 security posture, taking queues from published industry best practices, Microsoft recommendations, and taking into account ‘real world’ observations of the alerts and trends from within the customers environment.

This review is an great starting point for learning about Microsoft 365 security topics and concerns and developing a roadmap to ensuring Microsoft 365 continues to serve the businesses communication requirements, without creating security risks.

Microsoft 365 Security Assessment

Experienced Consultants

The team at Resolution Technology have a broad perspective on cyber security gained from 10+ years of building, designing, and managing environments which include stringent security requirements. We are able to put security and potential risks into the context of the customers business, and make relevant, actionable recommendations that add value.

Established processes

We have a clearly defined and efficient process to perform the assessment, which will provide the customer a result in a fast timeframe (2-3 weeks from initiation).

Actionable guidance

The recommendations made though the assessment will provide the customer with a practical and actionable plan for improvement and risk reduction, and Resolution Technology will be well placed to help implement whatever is recommended.

Microsoft 365 Security Assessment

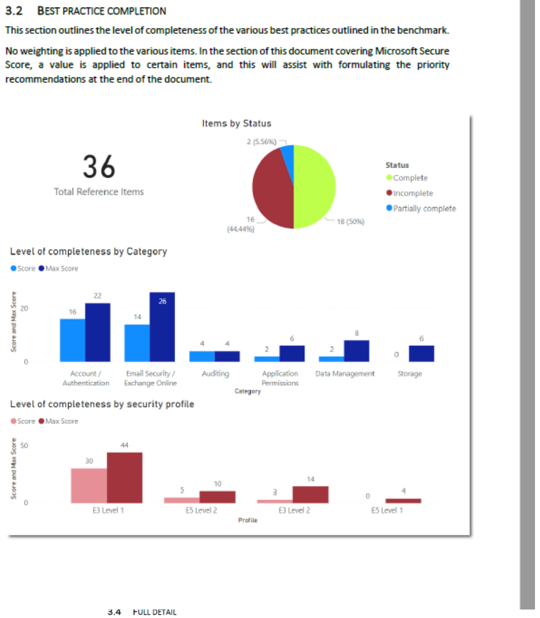
Microsoft 365 Security Review

[redacted]

resolution TECHNOLOGY

Resolution Technology
Ground Floor, 27 Mayneview
Street, Milton QLD 4006

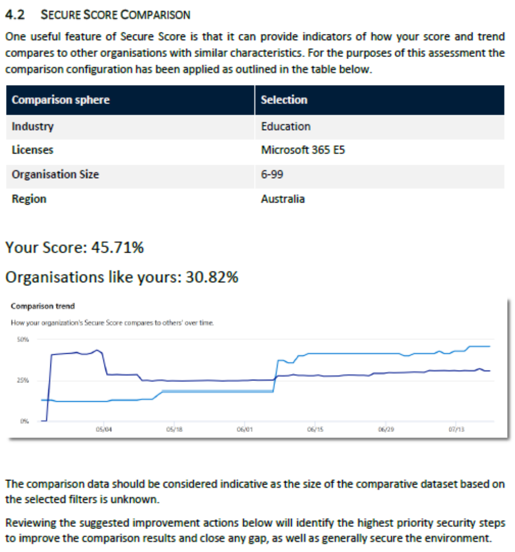
Phone: +61 7 3513 8900
sales@resolutionit.com.au
www.resolutionit.com.au



3.2 Best Practice Completion

This section outlines the level of completeness of the various best practices outlined in the benchmark.

No weighting is applied to the various items. In the section of this document covering Microsoft Secure Score, a value is applied to certain items, and this will assist with formulating the priority recommendations at the end of the document.



4.2 Secure Score Comparison

One useful feature of Secure Score is that it can provide indicators of how your score and trend compares to other organisations with similar characteristics. For the purposes of this assessment the comparison configuration has been applied as outlined in the table below.

Comparison sphere	Selection
Industry	Education
Licenses	Microsoft 365 E5
Organisation Size	6-99
Region	Australia

Your Score: 45.71%

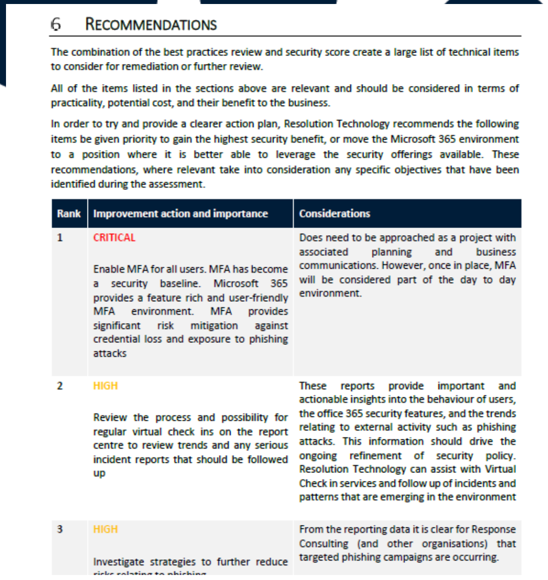
Organisations like yours: 30.82%

Comparison trend

How your organization's Secure Score compares to others' over time.

The comparison data should be considered indicative as the size of the comparative dataset based on the selected filters is unknown.

Reviewing the suggested improvement actions below will identify the highest priority security steps to improve the comparison results and close any gap, as well as generally secure the environment.



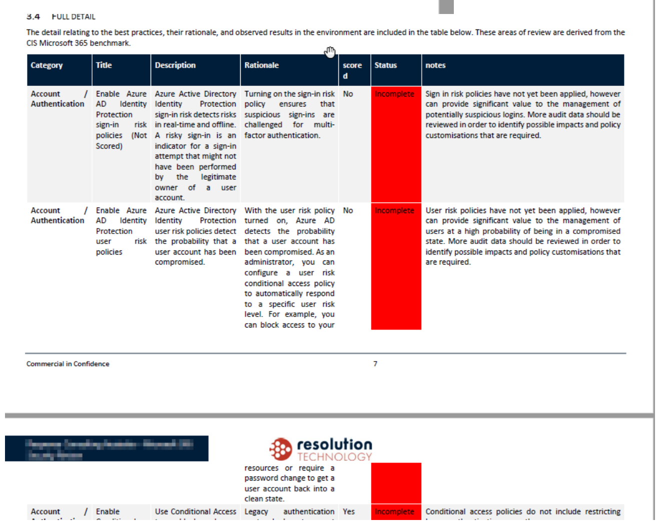
6 Recommendations

The combination of the best practices review and security score create a large list of technical items to consider for remediation or further review.

All of the items listed in the sections above are relevant and should be considered in terms of practicality, potential cost, and their benefit to the business.

In order to try and provide a clearer action plan, Resolution Technology recommends the following items be given priority to gain the highest security benefit, or move the Microsoft 365 environment to a position where it is better able to leverage the security offerings available. These recommendations, where relevant take into consideration any specific objectives that have been identified during the assessment.

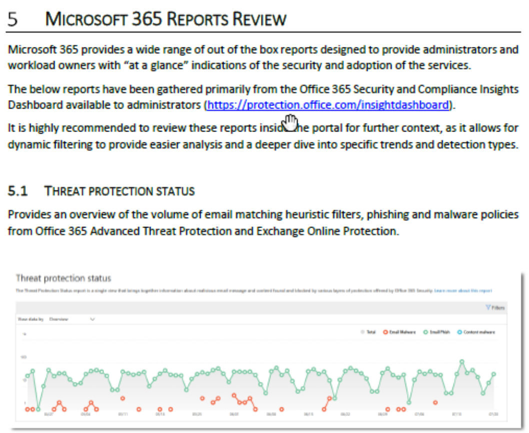
Rank	Improvement action and importance	Considerations
1	CRITICAL Enable MFA for all users. MFA has become a security baseline. Microsoft 365 provides a feature rich and user-friendly MFA environment. MFA provides significant risk mitigation against credential loss and exposure to phishing attacks	Does need to be approached as a project with associated planning and business communications. However, once in place, MFA will be considered part of the day to day environment.
2	HIGH Review the process and possibility for regular virtual check ins on the report centre to review trends and any serious incident reports that should be followed up	These reports provide important and actionable insights into the behaviour of users, the office 365 security features, and the trends relating to external activity such as phishing attacks. This information should drive the ongoing refinement of security policy. Resolution Technology can assist with Virtual Check in services and follow up of incidents and patterns that are emerging in the environment
3	HIGH Investigate strategies to further reduce risks relating to phishing	From the reporting data it is clear for Response Consulting (and other organisations) that targeted phishing campaigns are occurring.



3.4 Full Detail

The detail relating to the best practices, their rationale, and observed results in the environment are included in the table below. These areas of review are derived from the CIS Microsoft 365 benchmark.

Category	Title	Description	Rationale	scored	Status	notes
Account / Authentication	Enable Azure AD Identity Protection sign-in risk policies (Not Scored)	Azure Active Directory Identity Protection sign-in risk detects risks in real-time and offline. A risky sign-in is an indicator for a sign-in attempt that might not have been performed by the legitimate owner of a user account.	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication.	No	Incomplete	Sign in risk policies have not yet been applied, however can provide significant value to the management of potentially suspicious logins. More audit data should be reviewed in order to identify possible impacts and policy customisations that are required.
Account / Authentication	Enable Azure AD Identity Protection user risk policies	Azure Active Directory Identity Protection user risk policies detect the probability that a user account has been compromised.	With the user risk policy turned on, Azure AD detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.	No	Incomplete	User risk policies have not yet been applied, however can provide significant value to the management of users at a high probability of being in a compromised state. More audit data should be reviewed in order to identify possible impacts and policy customisations that are required.
Account /	Enable	Use Conditional Access	Legacy authentication	Yes	Incomplete	Conditional access policies do not include restricting



5 Microsoft 365 Reports Review

Microsoft 365 provides a wide range of out of the box reports designed to provide administrators and workload owners with “at a glance” indications of the security and adoption of the services.

The below reports have been gathered primarily from the Office 365 Security and Compliance Insights Dashboard available to administrators (https://protection.office.com/insightdashboard).

It is highly recommended to review these reports inside the portal for further context, as it allows for dynamic filtering to provide easier analysis and a deeper dive into specific trends and detection types.

5.1 Threat Protection Status

Provides an overview of the volume of email matching heuristic filters, phishing and malware policies from Office 365 Advanced Threat Protection and Exchange Online Protection.

Threat protection status

resolution TECHNOLOGY

Microsoft 365 Security Assessment (Price Guide)

Item	Unit Price ex.GST
Microsoft 365 Security Assessment	$5,500

resolution
TECHNOLOGY

Frequently Asked Questions

What type of assessment is this ?

This is a remote review of the state of the Microsoft 365 environment. The process will involve discussions with the customer about their concerns and also a close out session, but it is limited to the Microsoft 365 environment.

Will you fix the security problems you find ?

We will be able to assist further, however the assessment process is not designed to make any changes to an environment. The goal is to make observations and recommendations. Further proposals for remediation, broader projects and license uplift will be delivered as required.

What are the deliverables of the service?

As part of this offering the customer will receive the following discrete items:

- A kick-off discussion
- A key findings and recommendations report
- A close out presentation to review the report and next steps

resolution
TECHNOLOGY