MICROSOFT CLOUD ASSESSMENT

Microsoft Cloud Security Assessment

Scan Date: 2025/01/03

Your Customer / Prospect

Your Company Name

2025/03/03

Your IT Company
www.youritcompany.com
888-888-8888
sales@youritcompany,com

YourIT!
Your Logo Goes Here

Prepared for:
Your Customer / Prospect
Scan Date:
2025/01/03

Table of Contents

01 Overview

02 Current Secure Score

03 Secure Score Trend

04 Control Scores

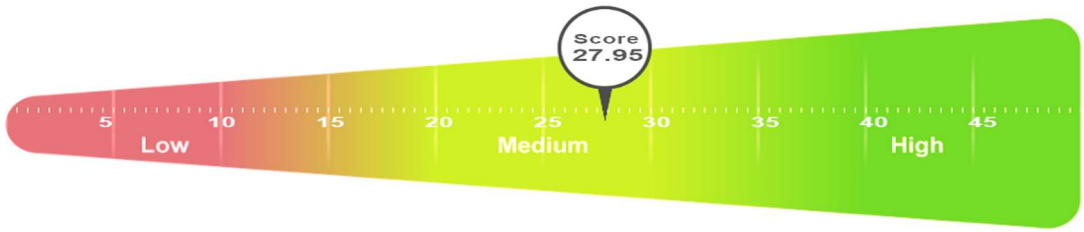
05 Alert Analysis

1 - Overview

This report presents a consolidated view of the security of the Microsoft Cloud environment. The assessment consists of a view of your current Microsoft Secure Score and shows trends over time. The Microsoft Secure Score is a proprietary security score provided by Microsoft. It is an aggregate of scores provided by implementing various security controls and best practices. The score is a relative measure and while there is a theoretical maximum, it may not always be possible or desirable to the business to obtain the maximum score possible. This report further breaks down the various Microsoft Controls and their associated Control Scores. A trained IT professional should review the controls and assist in identifying and prioritizing which controls should be implemented. The final aspect of this security assessment is a review of alerts which have recently occurred.

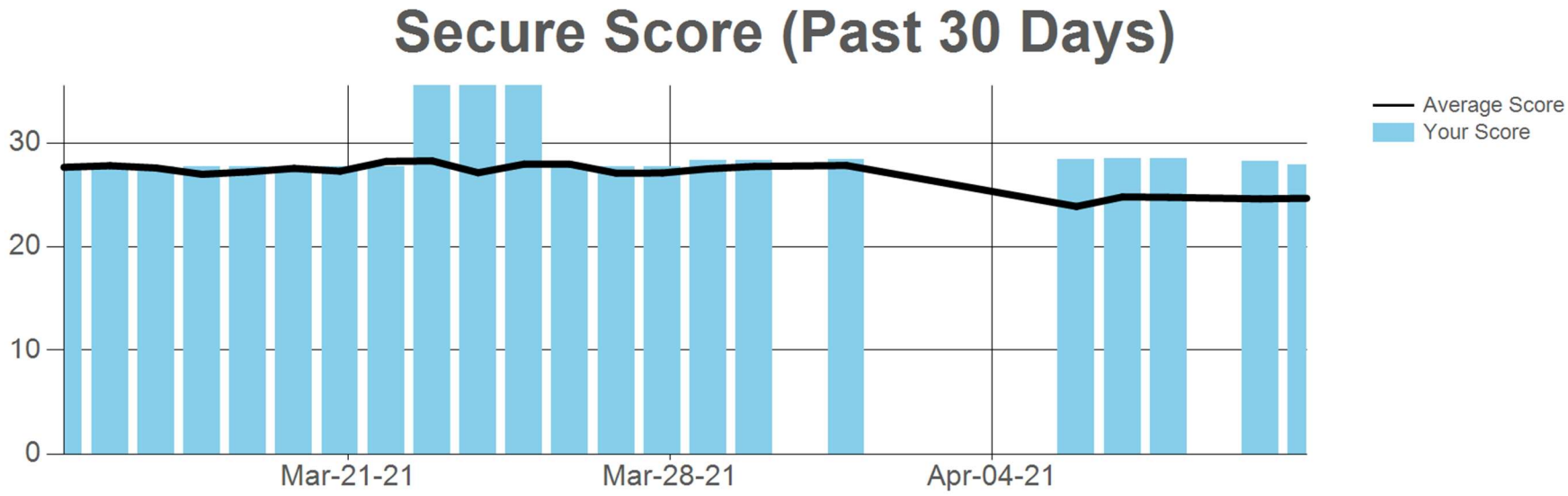
2 - Current Secure Score

This is your current Microsoft Security Score. The spectrum is centered around the average score of your peer group. Even though your score may appear at the maximum end of the spectrum, it may not be at the theoretical max. The theoretical max changes based on the number of users, devices, groups, and subscriptions. Your current theoretical maximum is **59**.



3 - Secure Score Trend

The following chart shows changes to your Secure Score over time. It also shows the average score of your peer group as a reference. The secure score should be used as a relative measure of security. A qualified IT professional can assess and prioritize which security controls are appropriate for your organization.



4 - Control Scores

Implementing best practice controls can result in a more secure environment. Microsoft assigns a control score based on the organization's progress in implementing these measures. Below is a table showing the individual controls and your specific scores. Scores of 0 indicate controls that should be evaluated and implemented if possible.

CONTROL NAME	DESCRIPTION	SCORE
apps		
TLSDeprecation	Review all your clients to check which ones use TLS 1.0/1.1 and 3DES to communicate with Office 365. The goal is to upgrade your clients to move away from using weaker protocols and cipher. You can access a report showing all the TLS 1.0/1.1 and 3DES connections in your tenants grouped by user and agent information. After all your clients are migrated and the usage below is zero, you will be awarded full points.	1
CustomerLockBoxEnabled	Turning on the customer lockbox feature requires that approval is obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There's an expiration time on the request and content access is removed after the support engineer has fixed the issue.	0
Apps		
meeting_restrictanonymousjoin_v1	By restricting anonymous users from joining Microsoft Teams meetings, you have full control over meeting access. Anonymous users may not be from your organization and could have joined for malicious purposes, such as gaining information about your organization through conversations.	0
identity		
AdminMFAV2	Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.	10
PWAgePolicyNew	Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason, and recommends that cloud-only tenants set the password policy to never expire.	8

CONTROL NAME	DESCRIPTION	SCORE
MFARegistrationV2	Multi-factor authentication (MFA) helps protect devices and data that are accessible to these 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.	6.75
OneAdmin	Having more than one global administrator helps if you are unable to fulfill the needs or obligations of your organization. It's important to have a delegate or an emergency account someone from your team can access if necessary. It also allows admins the ability to monitor each other for signs of a breach.	1
BlockLegacyAuthentication	Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.	0.2
IntegratedApps	Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps 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.	0
SelfServicePasswordReset	With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used.	0
UserRiskPolicy	With the user risk policy turned on, Azure Active Directory 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.	0
Identity		
RoleOverlap	Limited administrators are users who have more privileges than standard users, but not as many privileges as global admins. Leveraging limited administrator roles to perform required administrative work reduces the number of high value, high impact global admin role holders you have. Assigning users roles like Password Administrator or Exchange Online Administrator, instead of Global Administrator, reduces the likelihood of a global administrative privileged account being breached.	1
SigninRiskPolicy	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).	0

5 - Alert Analysis

Alerts are generated automatically and can be configured in your Microsoft Cloud environment. If no alerts are found, it may be that alerting and auditing are turned off in your particular environment. A review of alerts should be performed on a periodic basis to identify underlying issues and potential security events.

No alerts within 30 days.

EVENT DATE	TITLE
2020/05/20 11:45:00 AM -04:00	Email reported by user as malware or phish
2020/05/20 9:15:00 AM -04:00	Email reported by user as malware or phish
2020/05/19 7:15:00 PM -04:00	User restricted from sending email
2020/05/19 4:30:00 PM -04:00	Suspicious email sending patterns detected
2020/05/19 3:30:00 PM -04:00	Suspicious email sending patterns detected
2020/05/19 3:00:00 PM -04:00	Email reported by user as malware or phish
2020/05/19 2:00:00 PM -04:00	Suspicious email sending patterns detected
2020/05/19 11:45:00 AM -04:00	Creation of forwarding/redirect rule
2020/05/19 9:15:00 AM -04:00	Suspicious email sending patterns detected
2020/05/19 9:00:00 AM -04:00	Creation of forwarding/redirect rule
2020/05/18 5:00:00 PM -04:00	Suspicious email sending patterns detected
2020/05/18 12:45:00 PM -04:00	Creation of forwarding/redirect rule
2020/05/18 9:30:00 AM -04:00	Creation of forwarding/redirect rule
2020/05/17 11:45:00 AM -04:00	Users targeted by phish campaigns

EVENT DATE	TITLE
2020/05/15 11:45:00 PM -04:00	Users targeted by phish campaigns
2020/05/15 11:45:00 PM -04:00	Users targeted by malware campaigns
2020/05/15 6:15:00 PM -04:00	Suspicious email sending patterns detected
2020/05/15 2:59:00 PM -04:00	Creation of forwarding/redirect rule
2020/05/15 11:15:00 AM -04:00	Suspicious email sending patterns detected
2020/05/15 12:00:00 AM -04:00	Users targeted by phish campaigns