Silicon Overdrive

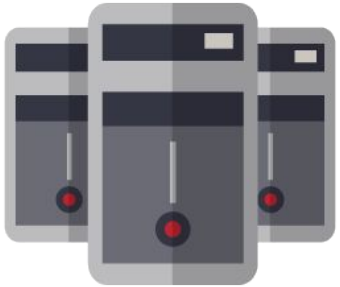
IT SERVICES AND SOFTWARE DEVELOPMENT

Secure Score helps organizations

1. Report on the current state of the organization's security posture.
2. Improve their security posture by providing discoverability, visibility, guidance, and control.
3. Compare with benchmarks and establish key performance indicators (KPIs).

How it works

A User is given points for



- Configuring recommended security features,
- Performing security-related tasks
- Addressing the improvement action with a third-party application or software.

Some improvement actions only give points when fully completed, and some give partial points if they are completed for some devices or users. Security should be balanced with usability, and not every recommendation can work for your environment.

How improvement actions are scored

- Most are scored in a binary fashion
- Some points are given as a percentage of the total configuration
    - For example, if the improvement action states you get 30 points by protecting all your users with multi-factor authentication and you only have 5 of 100 total users protected, you would be given a partial score of around 2 points (5 protected / 100 total * 30 max pts = 2 pts partial score).

Products included in Secure Score

- Office 365
  - SharePoint Online
  - Exchange Online
  - OneDrive for Business
  - Microsoft Information Protection
- Azure AD
- Intune
- Cloud App Security

Required permissions

- Read and write roles
  - CompanyAdministrator
  - SecurityAdministrator
  - ExchangeAdmin
  - SharePointAdmin

Required permissions

- Read-only roles
  - HelpdeskAdmin
  - UserAccountAdmin
  - ServiceSupportAdmin
  - SecurityReader
  - SecurityOperator
  - GlobalReader

Required permissions

- Graph API
  - SecurityEvents.Read.All (for read-only role)
  - SecurityEvents.ReadWrite.All (for read and write role)

Gain visibility into your security posture

- Identity (Azure AD accounts & roles, with Azure ATP coming soon)
- Data (Microsoft Information Protection)
- Device (Microsoft Defender ATP devices, coming soon)
- App (email and cloud apps, including Office 365 and Microsoft Cloud App Security)
- Infrastructure (Azure resources)


Microsoft 365 security
Home
Alerts
Monitoring & reports
Secure score
Hunting
Classification
Policies
More resources
Microsoft Secure Score
Overview
Improvement actions
History
Your secure score
Total score : 248 / 697
Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.
Identity 77 / 224
Protection state of your Azure AD accounts and roles
Data 70 / 128
Protection state of your Office 365 documents
Device 31 / 225
Protection state of your devices
App 70 / 120
Protection state of your email and cloud apps
Infrastructure No data available
Protection state of your Azure resources
Learn more about Microsoft Secure Score
Get your score using Microsoft Graph API
History
13 points in 30 days
Total score
Your secure score over time and how you compare to other organizations.
300
250
200
150
100
50
0
01/08
01/11
01/14
01/17
01/20
01/23
01/26
01/29
02/01
02/04
Your score
Industry average
Global average
Similar seat count
View history
Improvement actions
Not completed 48
Completed 21
Resolved through third-party 1
Ignored 1
Improvement action
Score
Category
Require MFA for all users 0/30 Identity
Turn on mailbox auditing for all users 0/10 Data
Enable Password Hash Sync if hybrid 0/10 Identity
Register all users for multi-factor authentication 0/20 Identity
Review permissions & block risky OAuth applications conne... 0/15 Apps
Consume audit data weekly 0/5 Data
Enable self-service password reset 0/5 Identity
Designate less than 5 global admins 0/1 Identity
Show more
Need help?
Feedback

Take action to improve your score

Ranking

Ranking is based on the number of remaining points left to achieve, implementation difficulty, user impact, and complexity. The highest ranked improvement actions have a large number of points remaining with low difficulty, user impact, and complexity.

Take action to improve your score

Actions

1. View settings
2. Resolve through third party
3. Ignore
4. Review

Designate less than 5 global admins

0/1 points

Status

Not completed

Description

Reducing the number of global admins limits the number of accounts with high privileges that need to be closely monitored. If any of those accounts are compromised, critical devices and data are open to attacks. Designating less than 5 global admins reduces the attack surface area. You have 27 global admins.

Category
Identity

User impact
Low

Protects against
Account Breach
Elevation of Privilege
Malicious Insider

Complexity
Low

Next steps

Designate alternate roles for global admins so they can complete necessary tasks with the least amount of privilege required. For example, if a user is primarily responsible for Exchange Online administration, they should be assigned that role instead. Be sure to have at least two global admins designated to allow for full access to the network if one of the accounts is compromised.

How will this affect my users?

Admins who have been designated alternate roles will lose some of the privileges that they had before (although they might keep some privileges depending on the role). Make sure that these users have enough privileges to complete their day-to-day work.

Notes

View settings | Resolved through third-party | Ignore

Review mailbox forwarding rules weekly

5/5 points

Status

Completed

Description

Regularly reviewing mailbox forwarding rules to external domains maintains visibility into a popular data exfiltration tactic used by attackers.

Category
Data

User impact
Low

Protects against
Account Breach
Data Exfiltration
Malicious Insider

Complexity
Low

Next steps

The button below will take you to GitHub where you can download a PowerShell script that will generate two csv files, "MailboxDelegatePermissions" and "MailForwardingRulesToExternalDomains" in your System32 folder. Run this script and review the reports created on a weekly basis to look for signs of exfiltration. Alternatively, you can review mail forwarding rule creation activity in the last week from the Audit log search.

How will this affect my users?

This change will have no effect on your users.

Notes

Write a note

Review

Monitor improvements over time

Risk awareness

Microsoft Secure Score is a numerical summary of your security posture based on system configurations, user behavior and other security-related measurements; it is not an absolute measurement of how likely your system or data will be breached. Rather, it represents the extent to which you have adopted security controls in your Microsoft environment which can help offset the risk of being breached. No online service is completely immune from security breaches, and secure score should not be interpreted as a guarantee against security breach in any manner.

What's coming?

- **Removing “not scored” and “review” improvement actions**
- **Simplification of the point system**
- **Preview features**