Microsoft

Enterprise Security Assessment (ESA)

Assessment Data Gathering Instructions

Enterprise Security Assessment (ESA)

Our recommendation to enhance your security score enterprise-wide

Scope:
The ESA is an enterprise-wide evaluation to identify detailed recommendations to enhance your enterprise Security score

Audience:
C-Level, Security teams & Architects

Value:

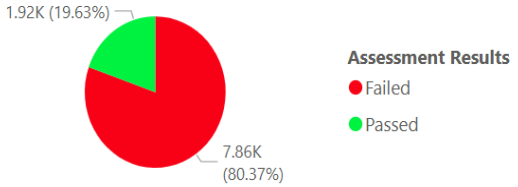
- **One Power BI Dashboard to combine**: Microsoft Cloud Security Benchmark Azure Secure Score and Microsoft Secure Score
- **Comprehensive Visualization**: Enterprise-wide data summary with option to drill down on Products or Components
- **Actionable Recommendations**: Actionable recommendations for each Product or Component with the option to update regularly to track progress
- **Time-Efficient**: Requires only 10 minutes for data gathering and 1-2 hours for the readout session with the option of remediation deep dives

Power BI Dashboard

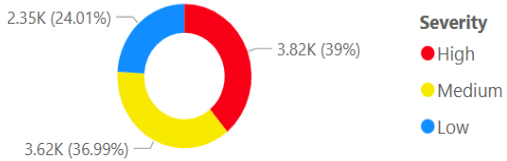
Executive Summary for Contoso Hotels

Microsoft Cloud Security Benchmark

Assessment Results



Azure Benchmark Severity

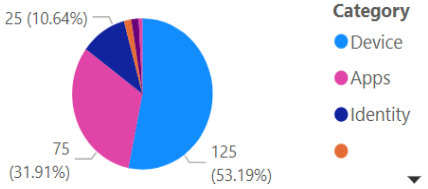


Top Security Benchmark High Recommendations

Compliance Control	High
Establish network segmentation boundaries	648
Use only approved applications in virtual machine	348
Rapidly and automatically remediate vulnerabilities	338
Encrypt sensitive data in transit	323
Use modern anti-malware software	200

Microsoft Secure Score 50.28%

Breakdown by Category

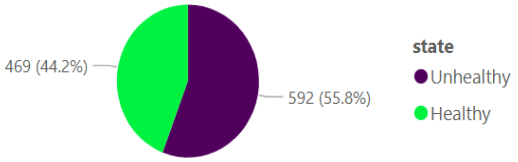


Microsoft Secure Score Recommendation

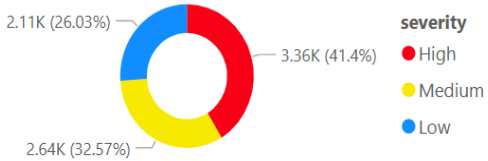
Product	Score impact
SharePoint Online	0.07%
Salesforce	3.48%
Microsoft Teams	0.37%
Microsoft Information Protection	0.07%
Exchange Online	0.44%
Defender for Office	6.78%
Defender for Identity	1.92%
Defender for Endpoint	48.96%
Azure Active Directory	3.43%
Total	**65.52%**

Azure Secure Score 35%

Resource Health



Azure Secure Score Severity



Top Azure Secure Score High Recommendations

Compliance Control	High
Restrict unauthorized network access	459
Apply system updates	423
Implement security best practices	422
Apply adaptive application control	348
Enable enhanced security features	251

What is a Enterprise Security Assessment?

An enterprise security assessment is a comprehensive evaluation designed to identify and summarize security recommendations in an enterprise’s environment.

Provides detailed visuals via a Power BI dashboard, highlighting areas needing attention and enabling repeated use.

Delivers actionable recommendations, ensuring continuous improvement of the customer's security posture.

Engagement Approach

Data Gathering

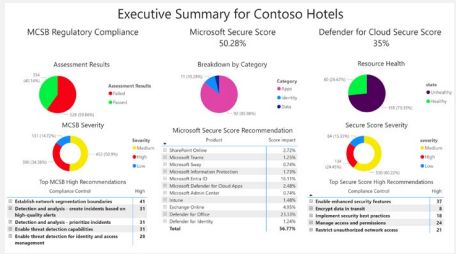
Customer will need to gather data by exporting three .csv files and providing them to Microsoft.

1. Defender for Cloud Secure Score recommendations for all subscriptions in scope.
2. Microsoft Cloud Security Benchmark recommendations for all subscriptions in scope.
3. Microsoft Secure Score export.

Customer work

Data Integration in Power BI Dashboard

- **Microsoft will review and analyze the data and integrate it into a Power BI dashboard for visualization and filtering.**
- **Microsoft will create a proposed roadmap to serve as a jumpstart implementation plan and develop an executive summary presentation highlighting the top findings.**



Microsoft work

Presentation of Results

- **Microsoft will present the assessment results and the proposed roadmap in a two-hour meeting and share the Power BI dashboard with the customer.**

Teams Meeting

Assessment Data

Assessment information is based on data from the following sources:

Microsoft Cloud Security Benchmark (MCSB)

The Microsoft Cloud Security Benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and multi-cloud environments. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Defender for Cloud – Secure Score Recommendations

The recommendations in Microsoft Defender for Cloud helps improve cloud security posture by aggregating security findings into a single score, allowing for a quick assessment of the current security situation. Recommendations are grouped into security controls, which are logical groups of related security recommendations reflecting vulnerable attack surfaces.

Microsoft Secure Score

Microsoft Secure Score provides a holistic measure of an organization's security posture across various Microsoft services, including Microsoft 365 and Azure, focusing on identity, data, devices, apps, and infrastructure (for example, Entra ID, Teams, Exchange Online, SharePoint Online, and more).

Data Sources

You need to export three .csv files from the following sources

Defender for Cloud – Secure Score

The recommendations in Microsoft Defender for Cloud helps improve cloud security posture by aggregating security findings into a single score. Recommendations are grouped into security controls, which are logical groups of related security recommendations reflecting vulnerable attack surfaces

Defender for Cloud - MCSB

The Microsoft Cloud Security Benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and multi-cloud environments. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Minimum **Azure** Permissions required:
Reader

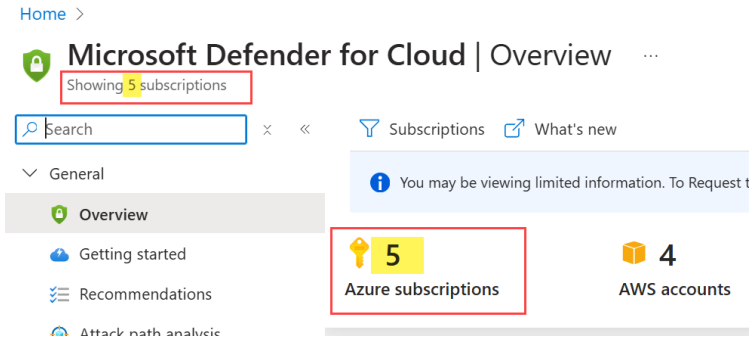
Microsoft Defender XDR

Microsoft Secure Score provides a holistic measure of an organization's security posture across various Microsoft services, including Microsoft 365 and Azure, focusing on identity, data, devices, apps, and infrastructure (for example, Entra ID, Teams, Exchange Online, SharePoint Online, and more).

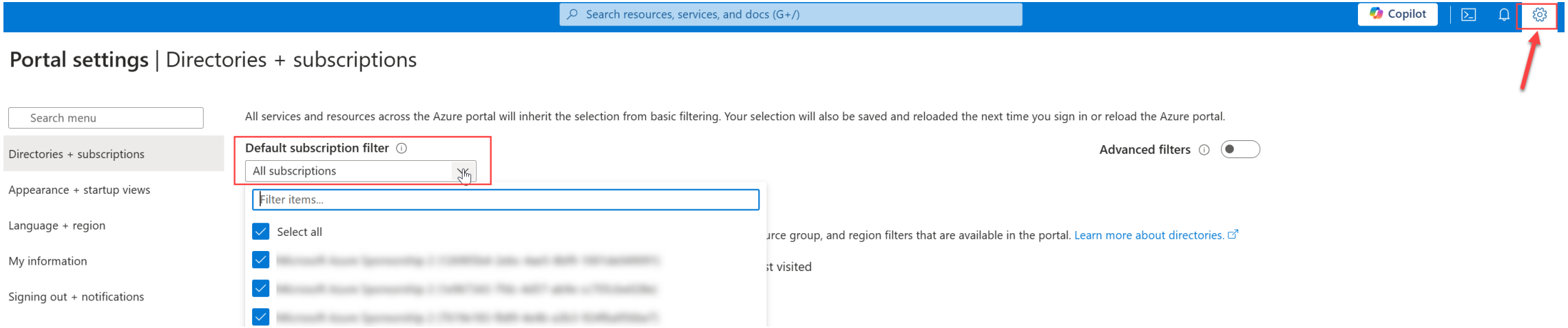
Minimum **Entra ID** permission required:
Global Reader

Review and filter selected subscriptions

In the Azure Portal, navigate to Defender for Cloud and review the selected subscriptions:

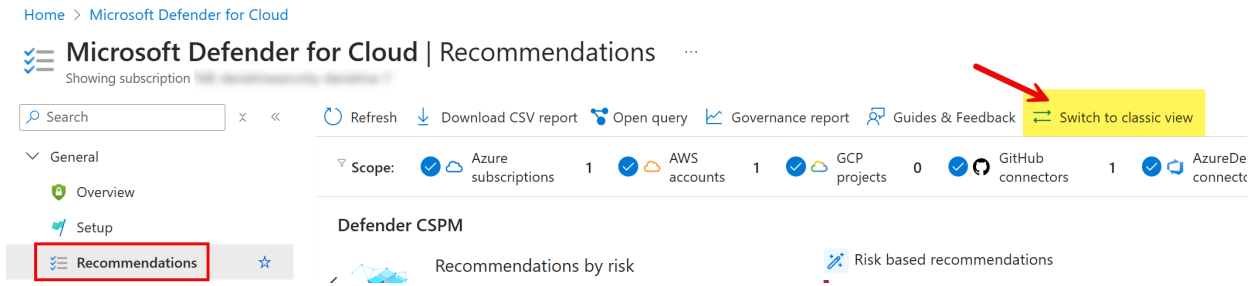


You may want to use the Azure Portal subscription filter to include or exclude subscriptions from the export, based on the scope of your assessment or to split the download into multiple parts/subscriptions:



Export Defender for Cloud: Secure Score

In Defender for Cloud, select “Recommendations”:

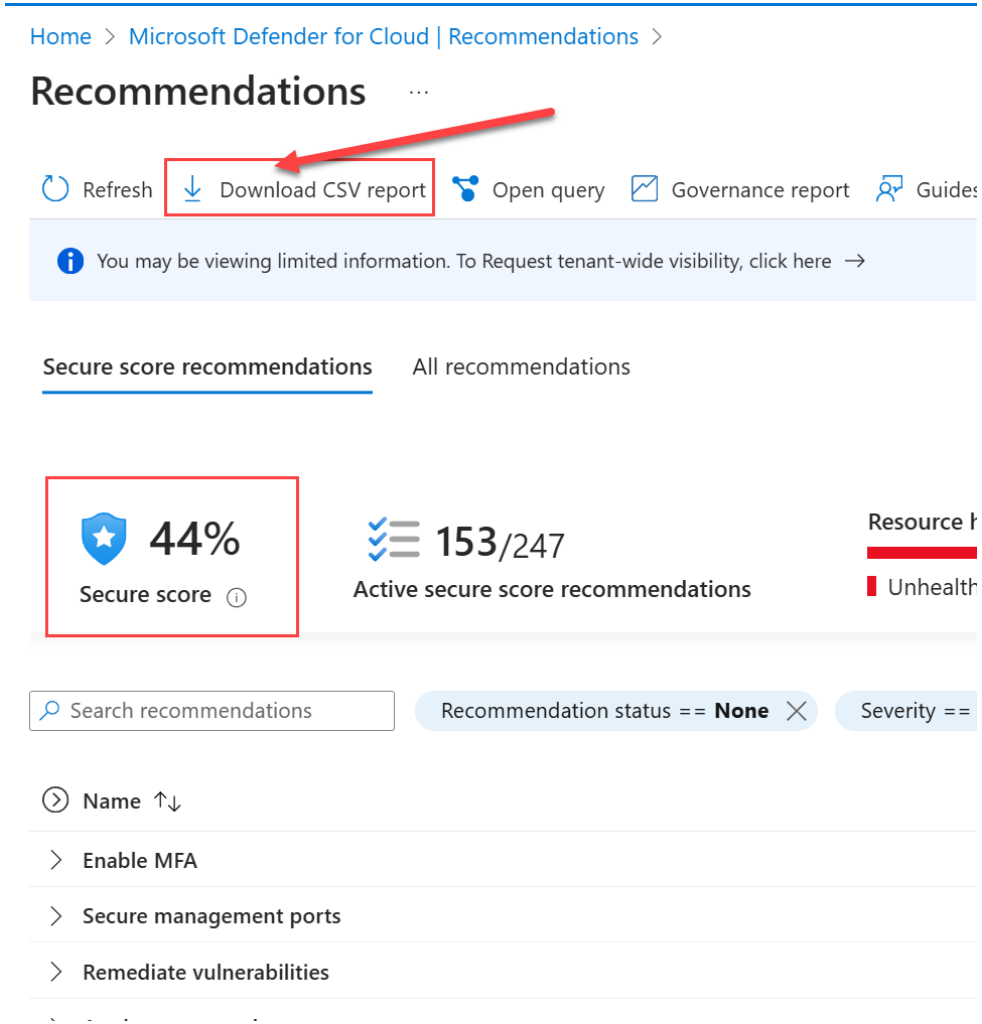


<u>Important</u>:

Make sure that the **<u>classic view</u>** of the recommendations is selected.

Export Defender for Cloud: Secure Score

In the **classic view** of Recommendations, select "Download CSV report"

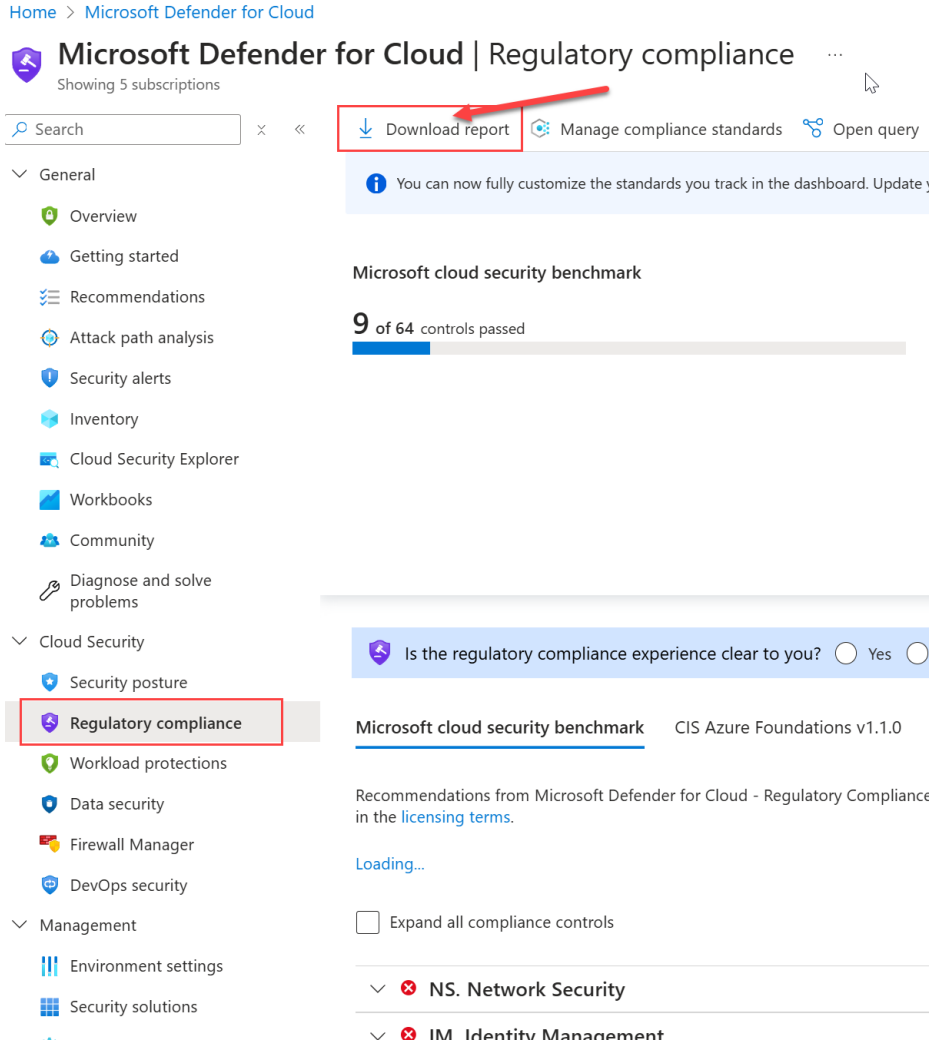


<u>Important</u>:

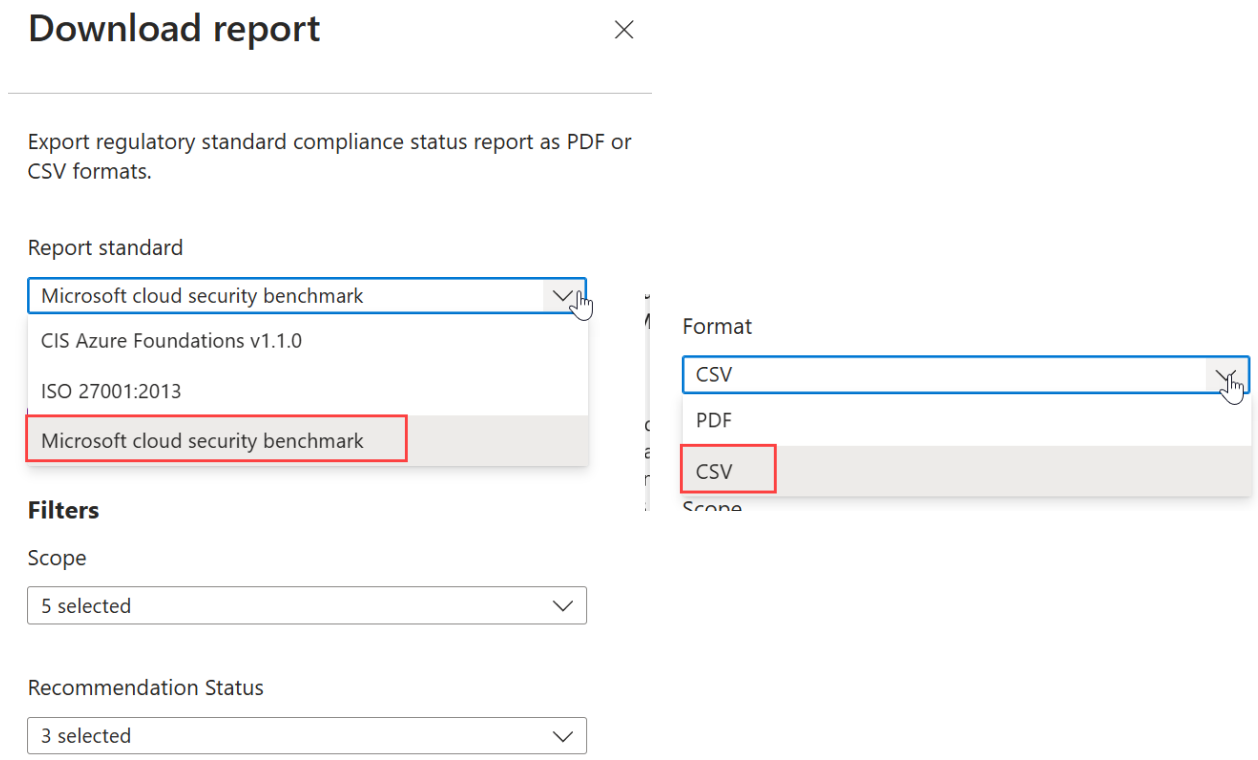
Make a note of the Secure Score value, as this number will also be shared with Microsoft.

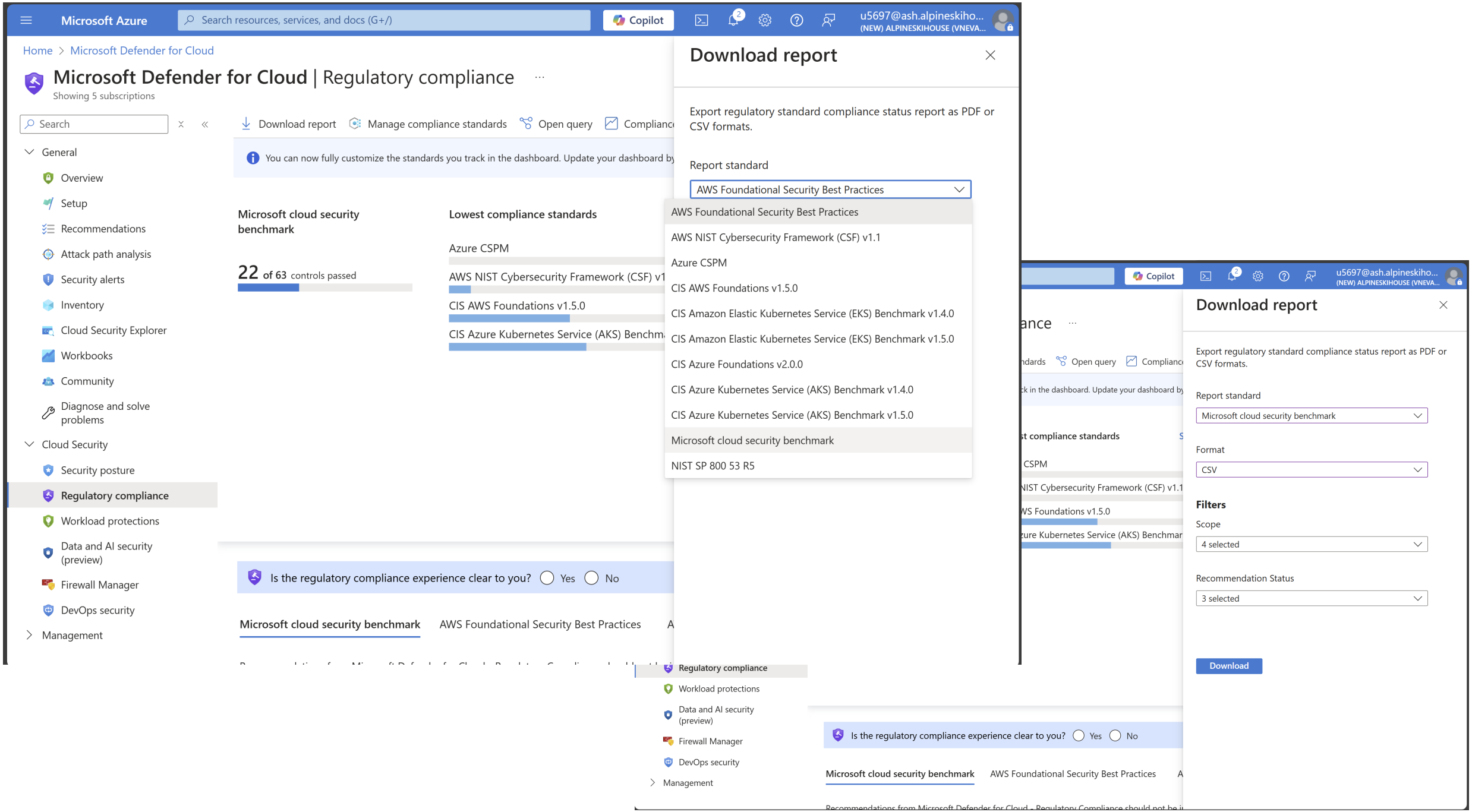
Export Defender for Cloud: MCSB

In Defender for Cloud, select “Regulatory compliance” and then choose “Download report”:



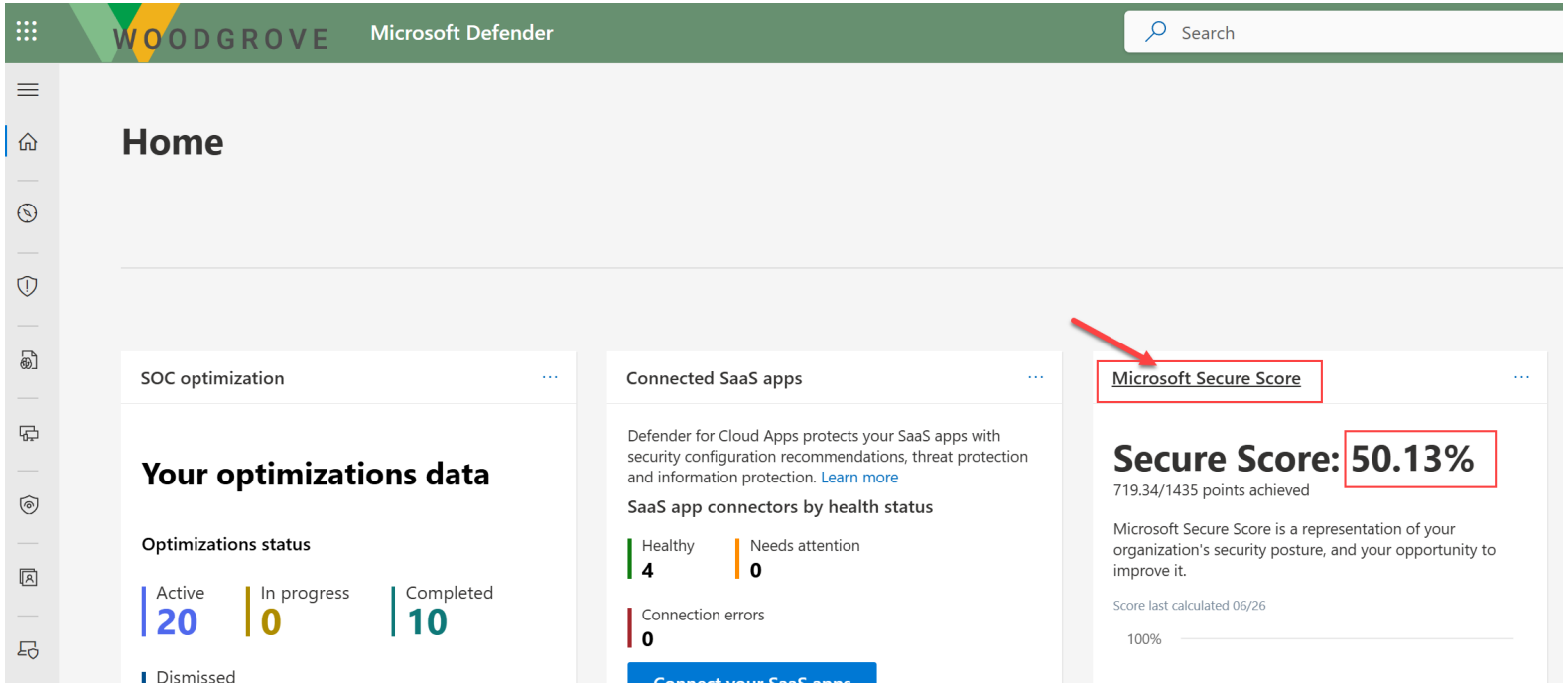
Within “Download report,” ensure that the “**Microsoft Cloud Security Benchmark**” is selected and that the report format is set to **CSV**:




Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
u5697@ash.alpineskiho...
(NEW) ALPINESKIHOUSE (VNEVA...
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Regulatory compliance
Showing 5 subscriptions
Search
General
Overview
Setup
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Security posture
Regulatory compliance
Workload protections
Data and AI security (preview)
Firewall Manager
DevOps security
Management
Download report
Manage compliance standards
Open query
You can now fully customize the standards you track in the dashboard. Update your dashboard by
Microsoft cloud security benchmark
22 of 63 controls passed
Lowest compliance standards
Azure CSPM
AWS NIST Cybersecurity Framework (CSF) v1
CIS AWS Foundations v1.5.0
CIS Azure Kubernetes Service (AKS) Benchm
Is the regulatory compliance experience clear to you?
Yes
No
Microsoft cloud security benchmark
AWS Foundational Security Best Practices
Download report
Export regulatory standard compliance status report as PDF or CSV formats.
Report standard
AWS Foundational Security Best Practices
AWS Foundational Security Best Practices
AWS NIST Cybersecurity Framework (CSF) v1.1
Azure CSPM
CIS AWS Foundations v1.5.0
CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.4.0
CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.5.0
CIS Azure Foundations v2.0.0
CIS Azure Kubernetes Service (AKS) Benchmark v1.4.0
CIS Azure Kubernetes Service (AKS) Benchmark v1.5.0
Microsoft cloud security benchmark
NIST SP 800 53 R5
Download report
Export regulatory standard compliance status report as PDF or CSV formats.
Report standard
Microsoft cloud security benchmark
Format
CSV
Filters
Scope
4 selected
Recommendation Status
3 selected
Download

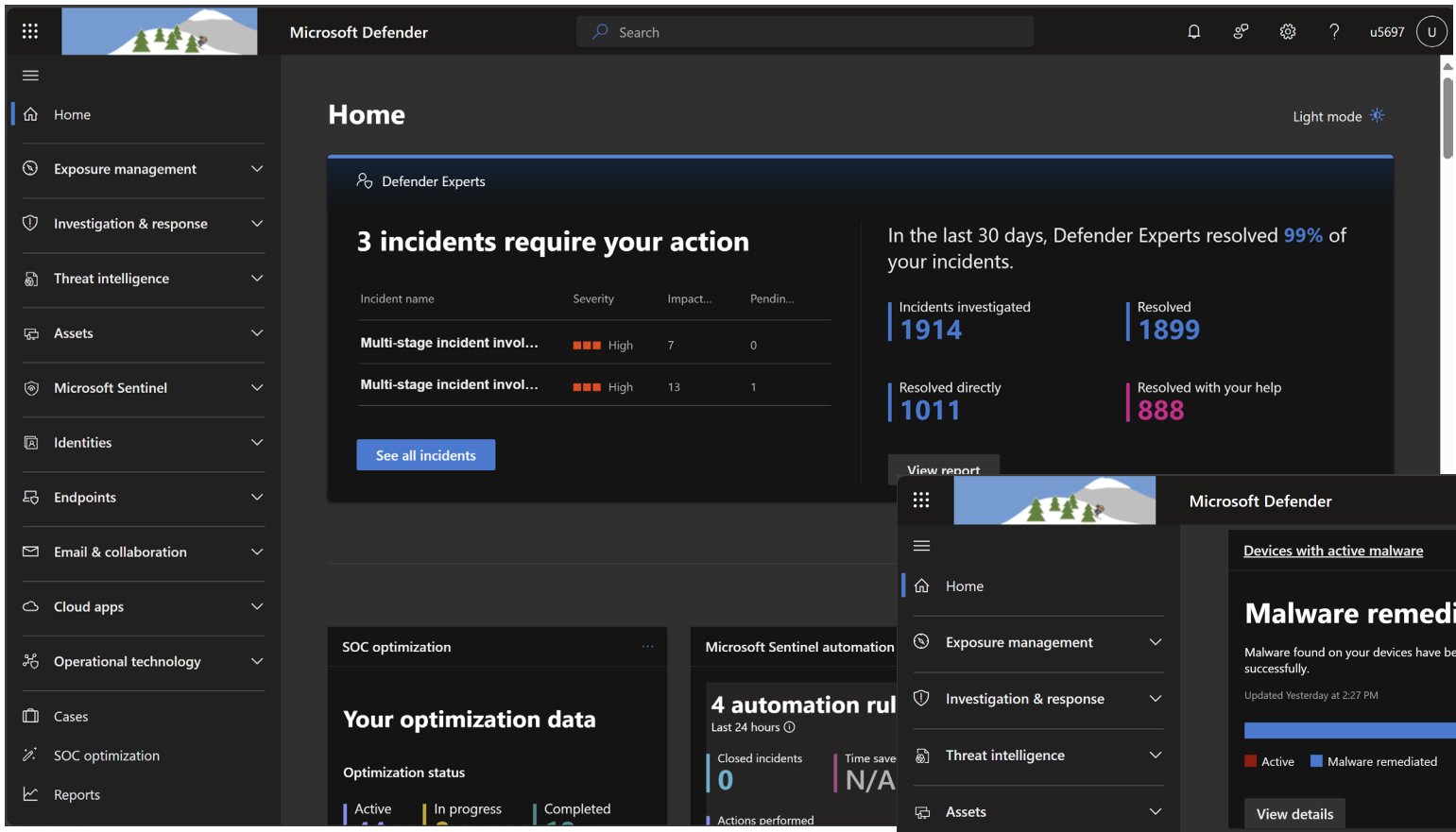
Export Microsoft Defender XDR

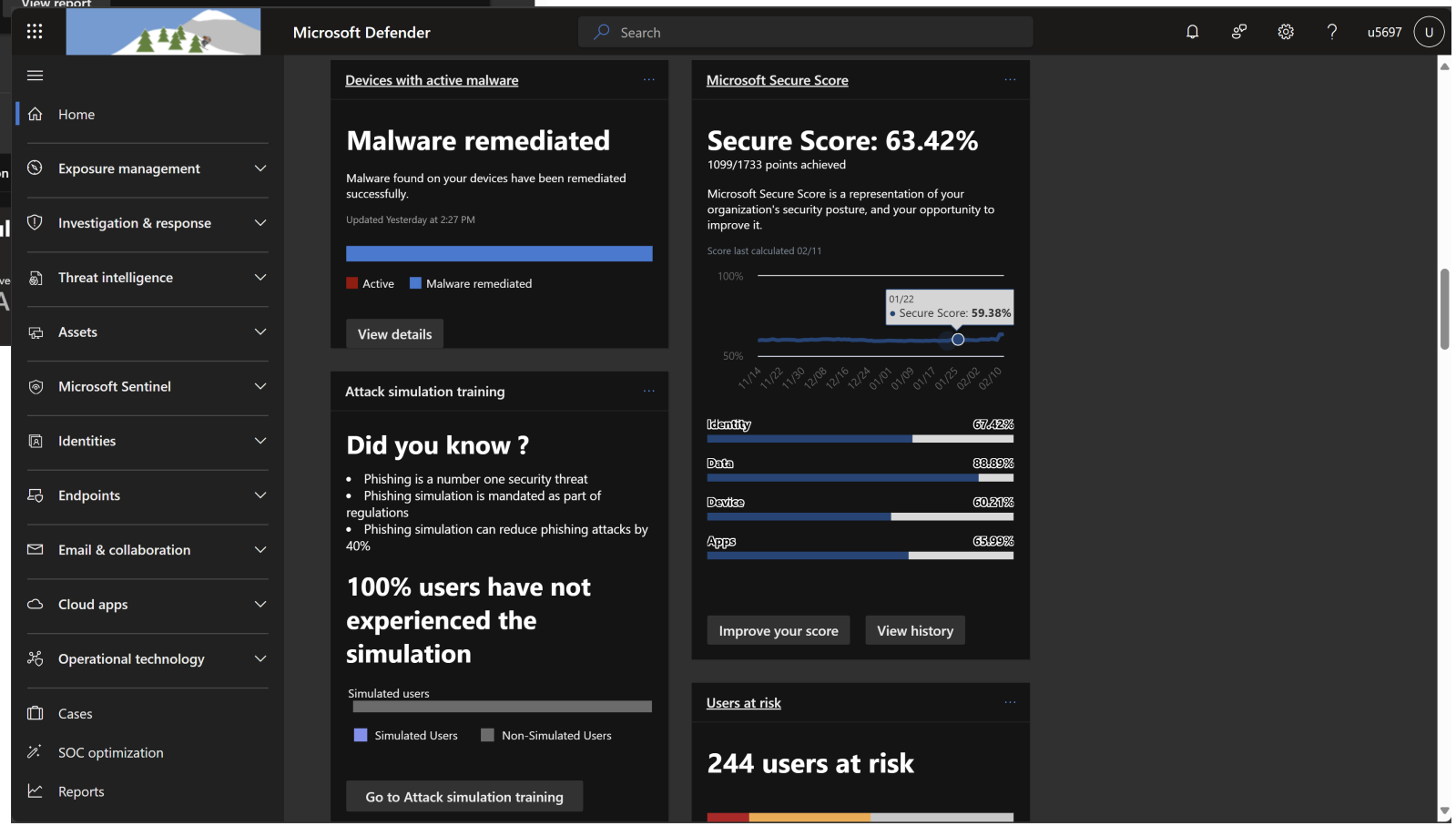
Navigate to: https://security.microsoft.com and click on “Microsoft Secure Score”:



Important:

Make a note of the Secure Score value, as this number will also be shared with Microsoft.


Microsoft Defender
Search
u5697
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Operational technology
Cases
SOC optimization
Reports
Home
Light mode
Defender Experts
3 incidents require your action
Incident name
Severity
Impact...
Pendin...
Multi-stage incident invol...
High
7
0
Multi-stage incident invol...
High
13
1
See all incidents
In the last 30 days, Defender Experts resolved 99% of your incidents.
Incidents investigated
1914
Resolved
1899
Resolved directly
1011
Resolved with your help
888
View report
SOC optimization
Your optimization data
Optimization status
Active
In progress
Completed
Microsoft Sentinel automation
4 automation rul
Last 24 hours
Closed incidents
0
Time save
N/A
Actions performed


Microsoft Defender
Search
u5697
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Operational technology
Cases
SOC optimization
Reports
Devices with active malware
Malware remediated
Malware found on your devices have been remediated successfully.
Updated Yesterday at 2:27 PM
Active
Malware remediated
View details
Attack simulation training
Did you know ?
Phishing is a number one security threat
Phishing simulation is mandated as part of regulations
Phishing simulation can reduce phishing attacks by 40%
100% users have not experienced the simulation
Simulated users
Simulated Users
Non-Simulated Users
Go to Attack simulation training
Microsoft Secure Score
Secure Score: 63.42%
1099/1733 points achieved
Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.
Score last calculated 02/11
100%
50%
01/22
Secure Score: 59.38%
11/14
11/22
11/30
12/08
12/16
12/24
01/01
01/09
01/17
01/25
02/02
02/10
Identity
67.42%
Data
88.89%
Device
60.21%
Apps
65.99%
Improve your score
View history
Users at risk
244 users at risk

Export Microsoft Defender XDR

Within Microsoft Secure Score, click on “Recommended actions”:

Microsoft Defender

Search

u5697

U

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

Operational technology

Cases

SOC optimization

Reports

Microsoft Secure Score

There are new permissions options available for Secure Score. You can now configure users' Secure Score data visibility based on data source.

Learn more about this change.

Configure in URBAC

Overview | Recommended actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

325 items

Search

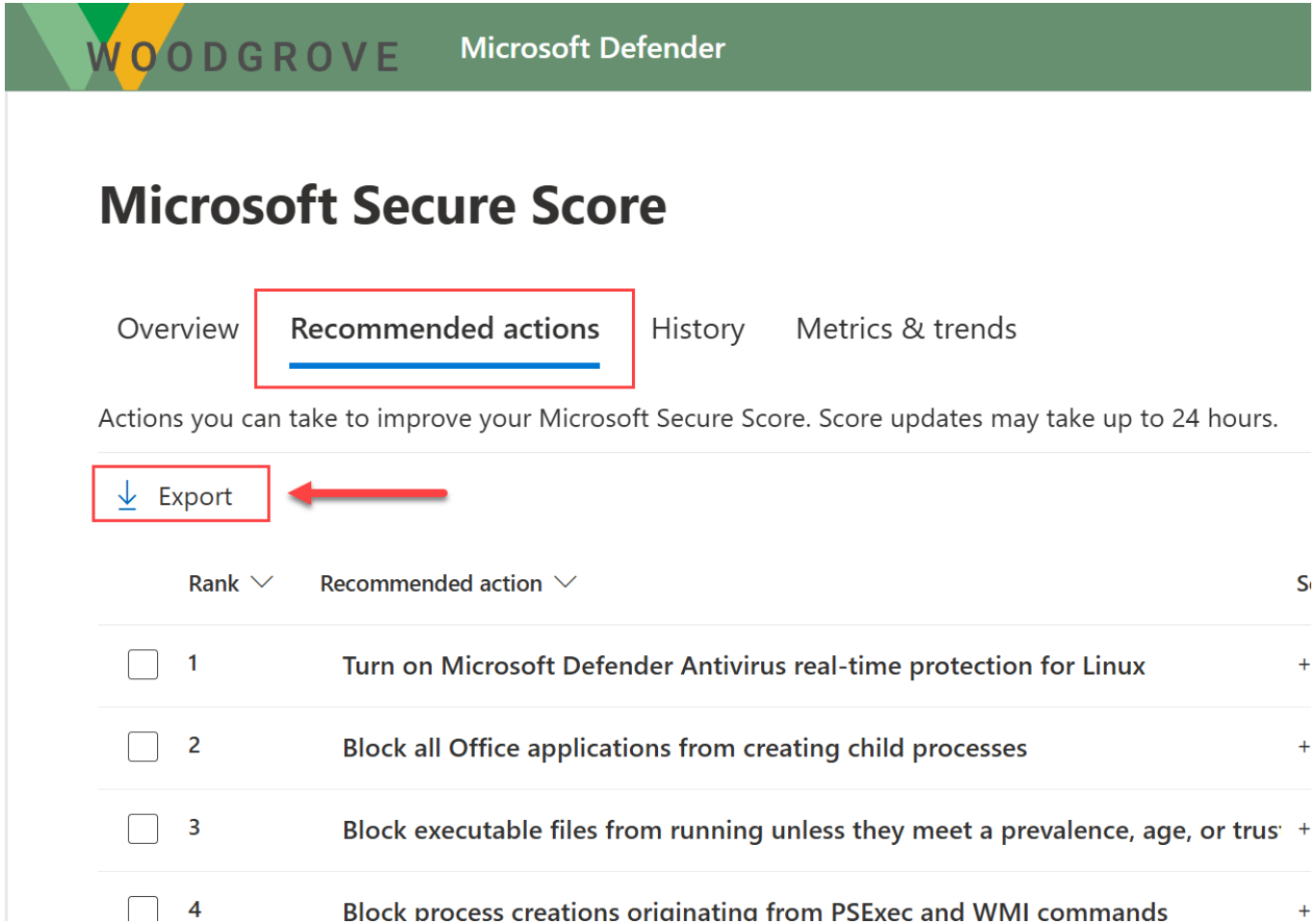
Filter

Group by

Rank	Recommended action	Score i...	Points achi...	Status	Regress...	Have license?	Cat...	Prod
1	Turn on PUA protection in block mode	+0.52%	0.31/9	To address	Yes	Yes	Device	Defe
2	Enable 'Local Security Authority (LSA) protection'	+0.46%	0/8	To address	No	Yes	Device	Defe
3	Set User Account Control (UAC) to automatically deny elevatior	+0.46%	0/8	To address	No	Yes	Device	Defe
4	Disable 'Enumerate administrator accounts on elevation'	+0.46%	0/8	To address	No	Yes	Device	Defe
5	Enable 'Require additional authentication at startup'	+0.46%	0/8	To address	No	Yes	Device	Defe
6	Disable 'Autoplay' for all drives	+0.46%	0/8	To address	No	Yes	Device	Defe
7	Set default behavior for 'AutoRun' to 'Enabled: Do not execute	+0.46%	0/8	To address	No	Yes	Device	Defe
8	Set LAN Manager authentication level to 'Send NTLMv2 respon	+0.46%	0/8	To address	No	Yes	Device	Defe
9	Disable 'Allow Basic authentication' for WinRM Client	+0.46%	0/8	To address	No	Yes	Device	Defe
10	Disable 'Allow Basic authentication' for WinRM Service	+0.46%	0/8	To address	No	Yes	Device	Defe

Export Microsoft Defender XDR

Click on “Export” to download the CSV report:



Final Steps

- Please share the **three** downloaded CSV files with Microsoft.
- Additionally, include the Defender for Cloud Secure Score and the Microsoft Secure Score values captured earlier.

Microsoft will complete the security assessment and present the results during the scheduled Teams meeting.


Microsoft

Microsoft

Enterprise Security Assessment (ESA)

Refreshing Power BI Report Instructions

Refreshing Power BI Report

You need to have the export of these three .csv files from the following sources

Defender for Cloud – Secure Score

The recommendations in Microsoft Defender for Cloud helps improve cloud security posture by aggregating security findings into a single score. Recommendations are grouped into security controls, which are logical groups of related security recommendations reflecting vulnerable attack surfaces

Defender for Cloud - MCSB

The Microsoft Cloud Security Benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and multi-cloud environments. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

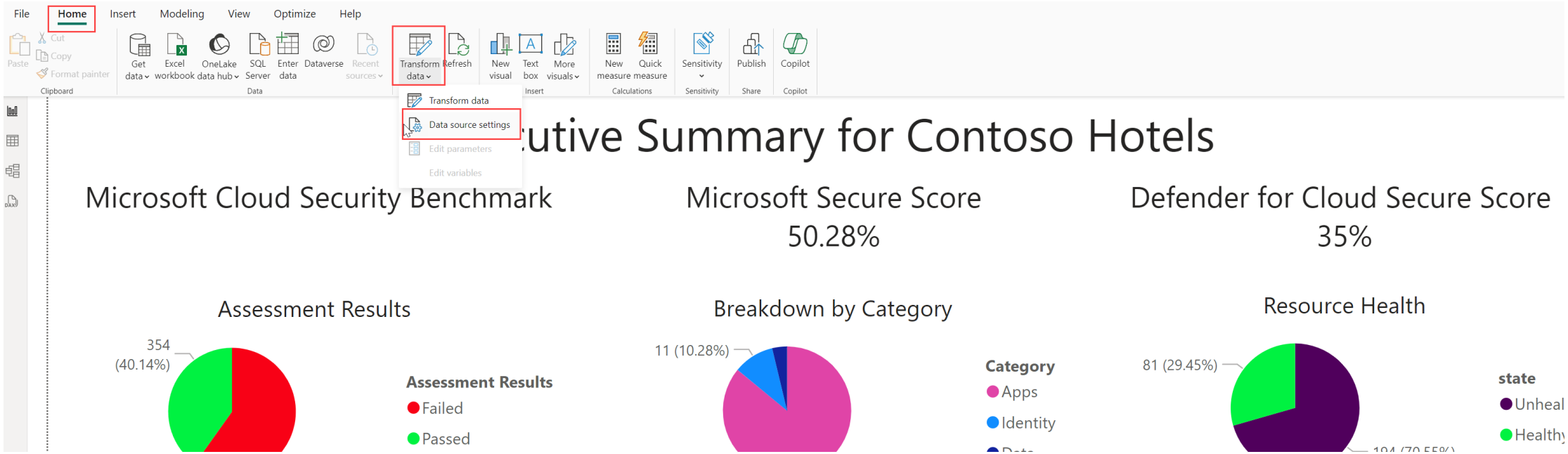
Microsoft Defender XDR

Microsoft Secure Score provides a holistic measure of an organization's security posture across various Microsoft services, including Microsoft 365 and Azure, focusing on identity, data, devices, apps, and infrastructure (for example, Entra ID, Teams, Exchange Online, SharePoint Online, and more).

Follow the instructions for data gathering in the document:
Enterprise Security Assessment - Data Gathering.pdf

Refreshing Power BI Report

Open the Power BI Report, go to Home > Transform Data > Data Source Settings:

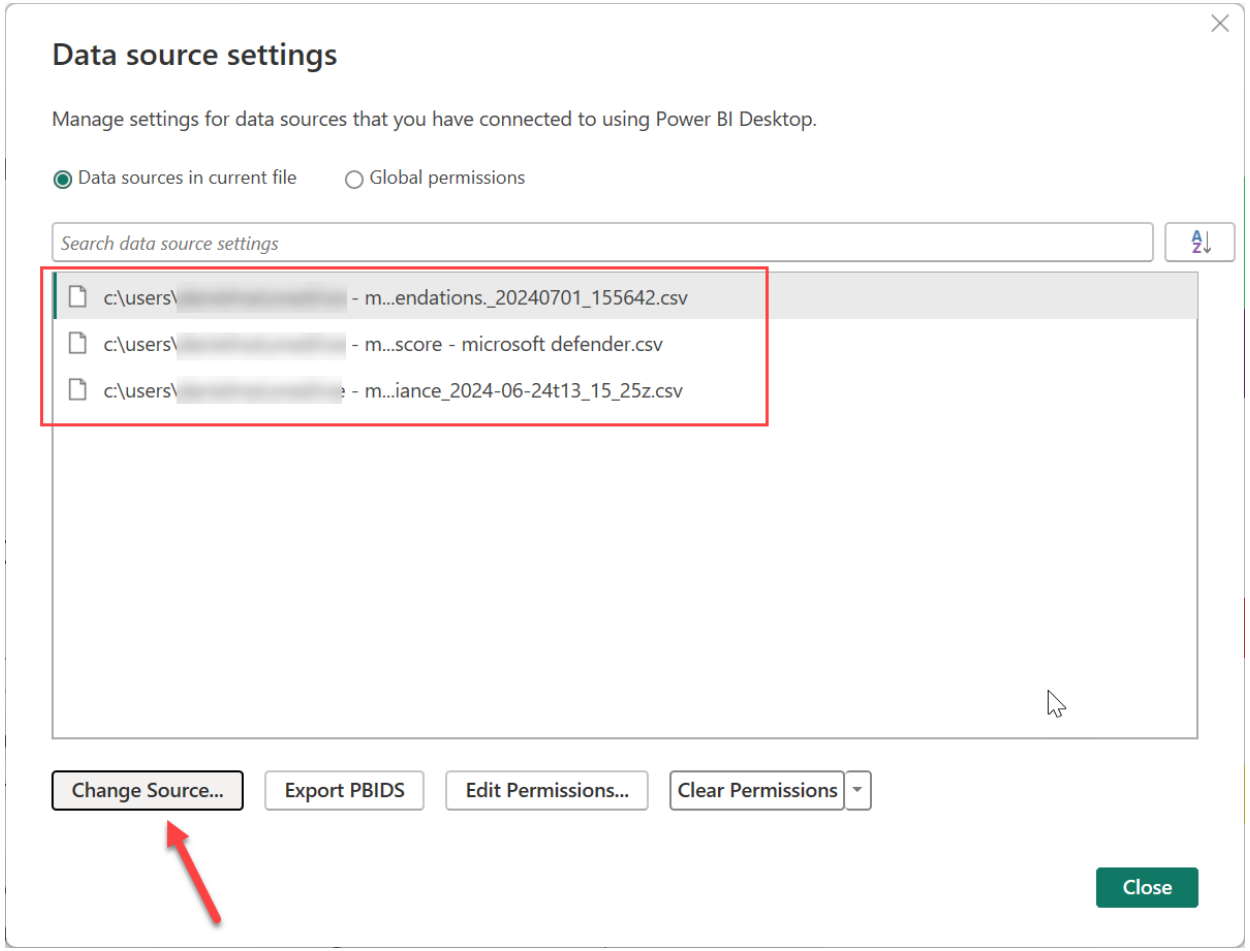


Refreshing Power BI Report

When the *Data source settings* window opens, you will see the three data sources for the assessment.

Hover over each one to identify which file is which. It's important to ensure you replace the correct file with the new one.

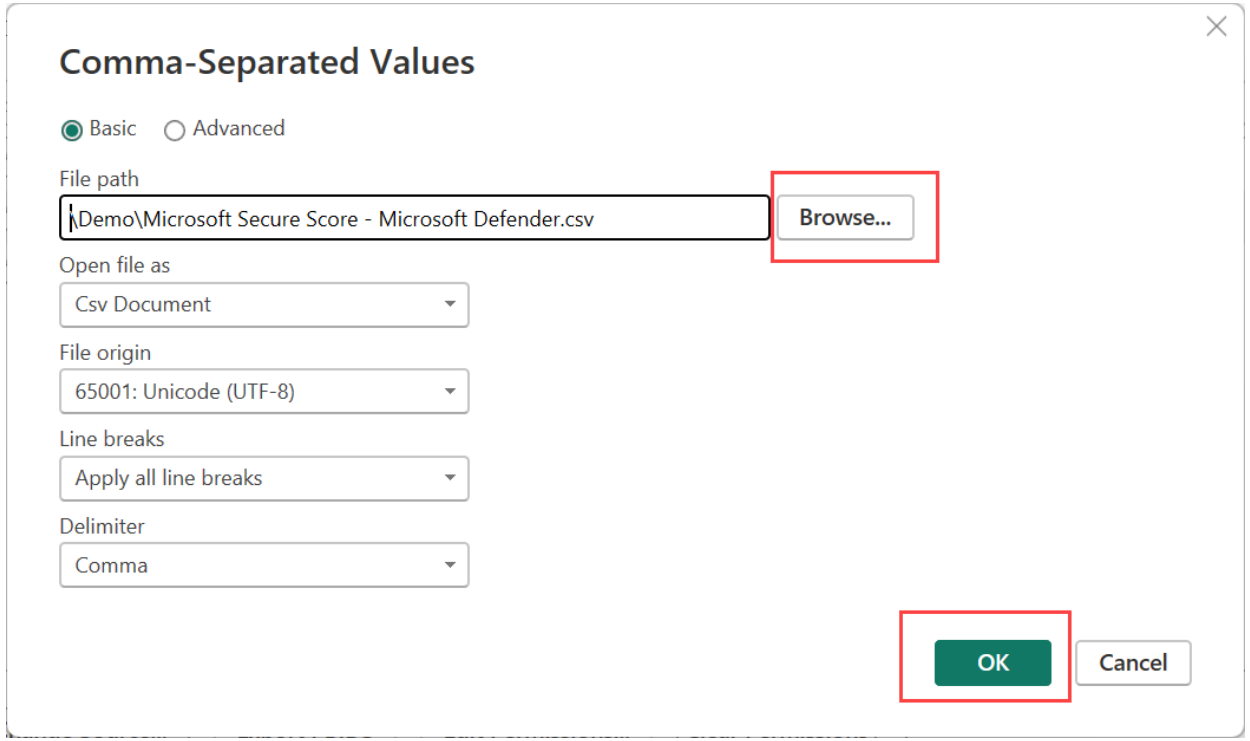
Select the correct entry and click "*Change Source*"



Refreshing Power BI Report

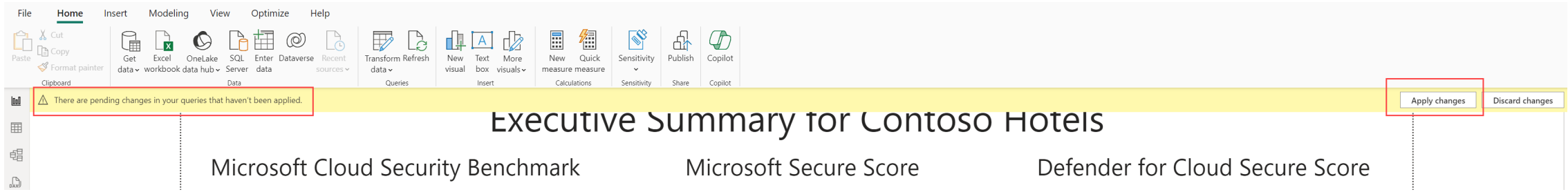
Click "*Browse…*" and navigate to the updated data files you exported earlier.

Repeat this for all 3 data files.



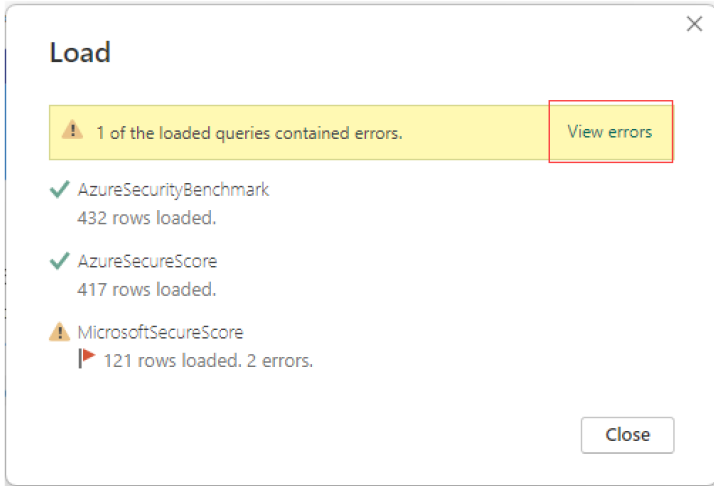
Refreshing Power BI Report

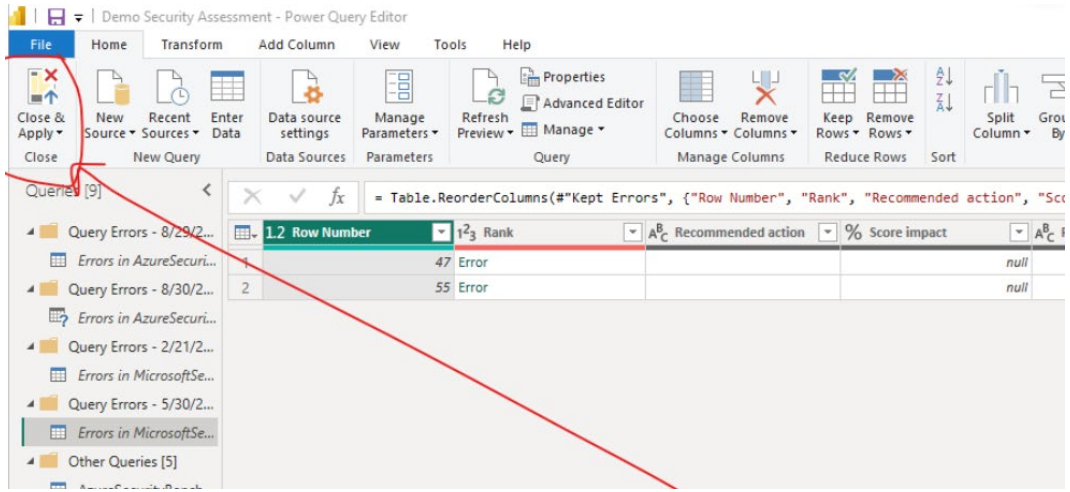
The final step is to apply the changes in the Power BI Report. You will see a banner that there are pending changes. Select "*Apply changes*":



Refreshing Power BI Report

If you get any data errors, and this is not uncommon, click on "*View Errors*". This will open the Power BI Query Editor:

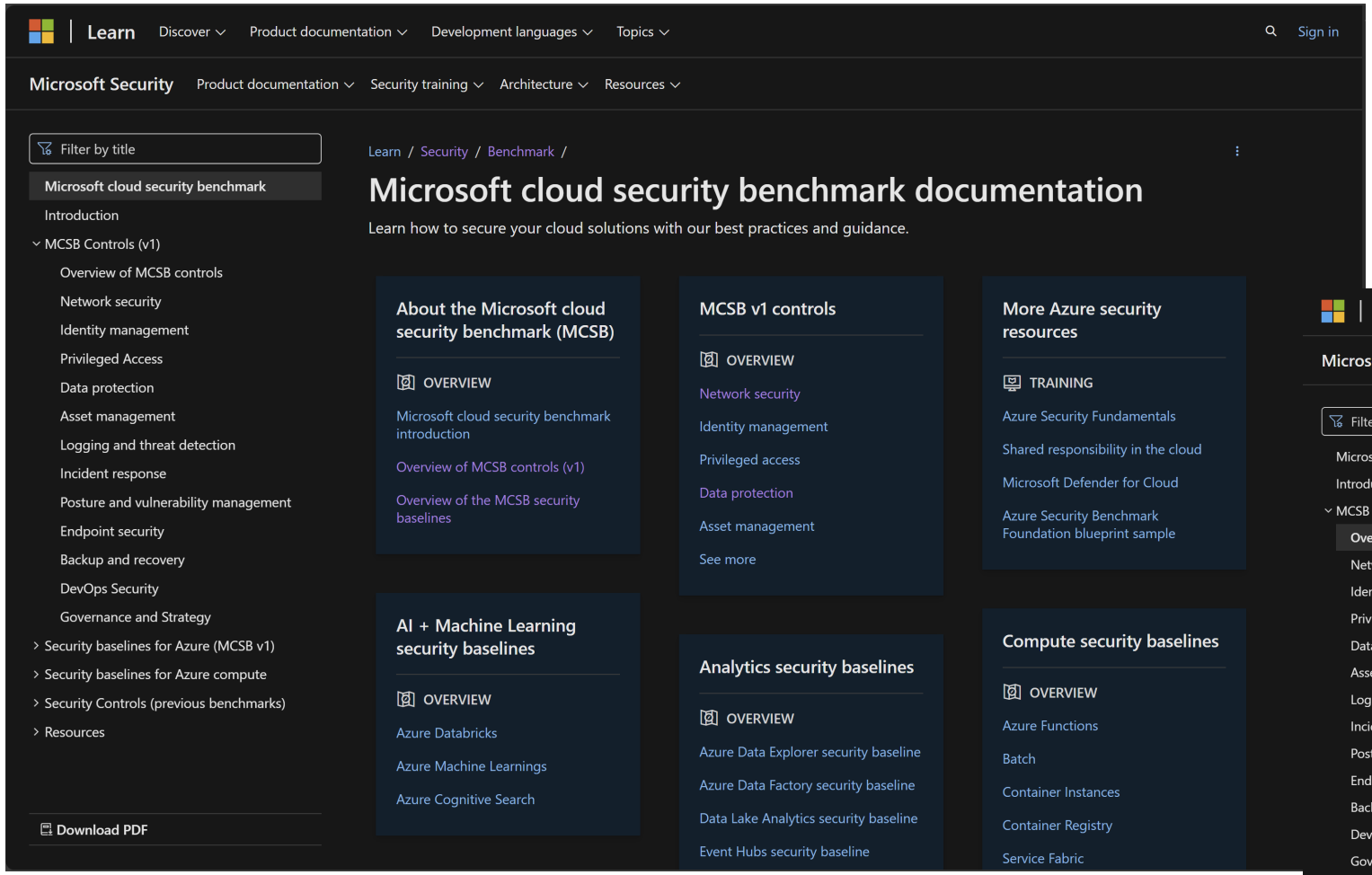




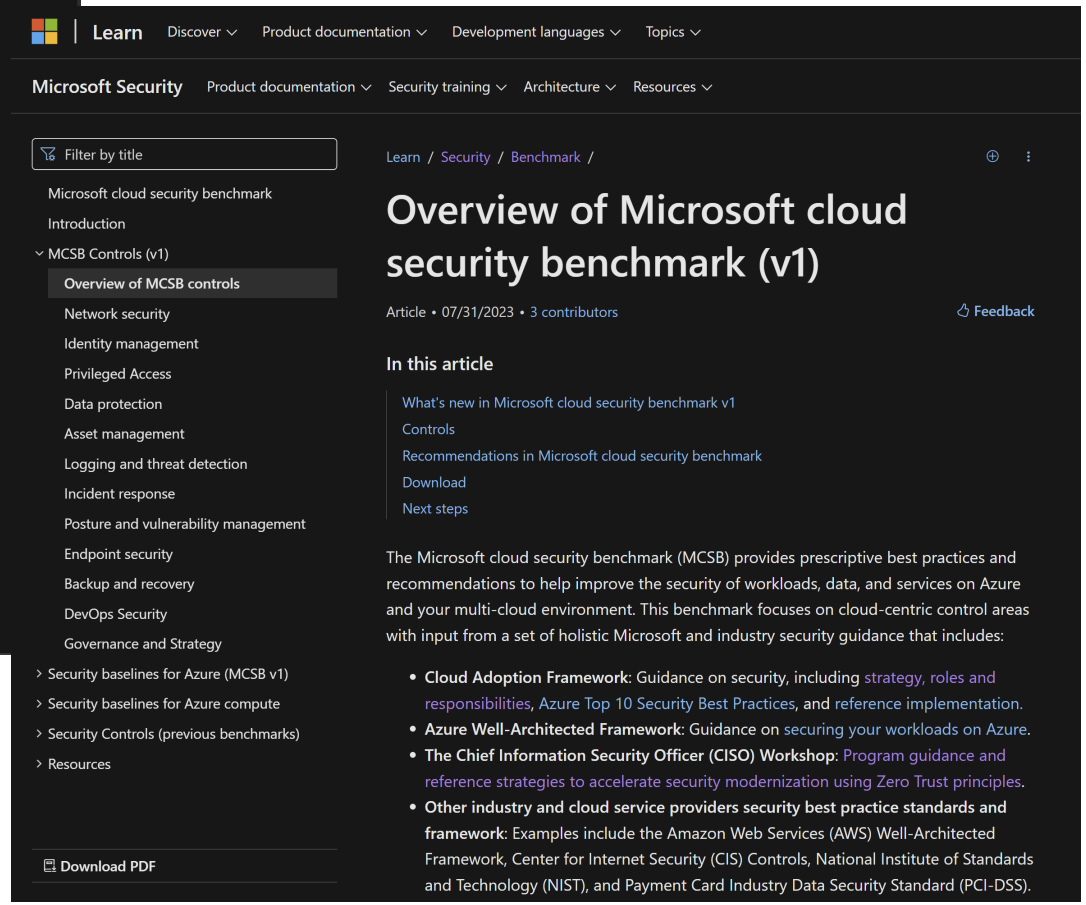
You only need to click on "*Close & Apply*" – no other actions should be required.
This will take you back to your report and your data will be refreshed.

You can repeat this exercise as many times as needed. It may be helpful to use "*Save As*" for each report prior to refreshing the data, allowing you to keep a snapshot of what the data looked like in the past.

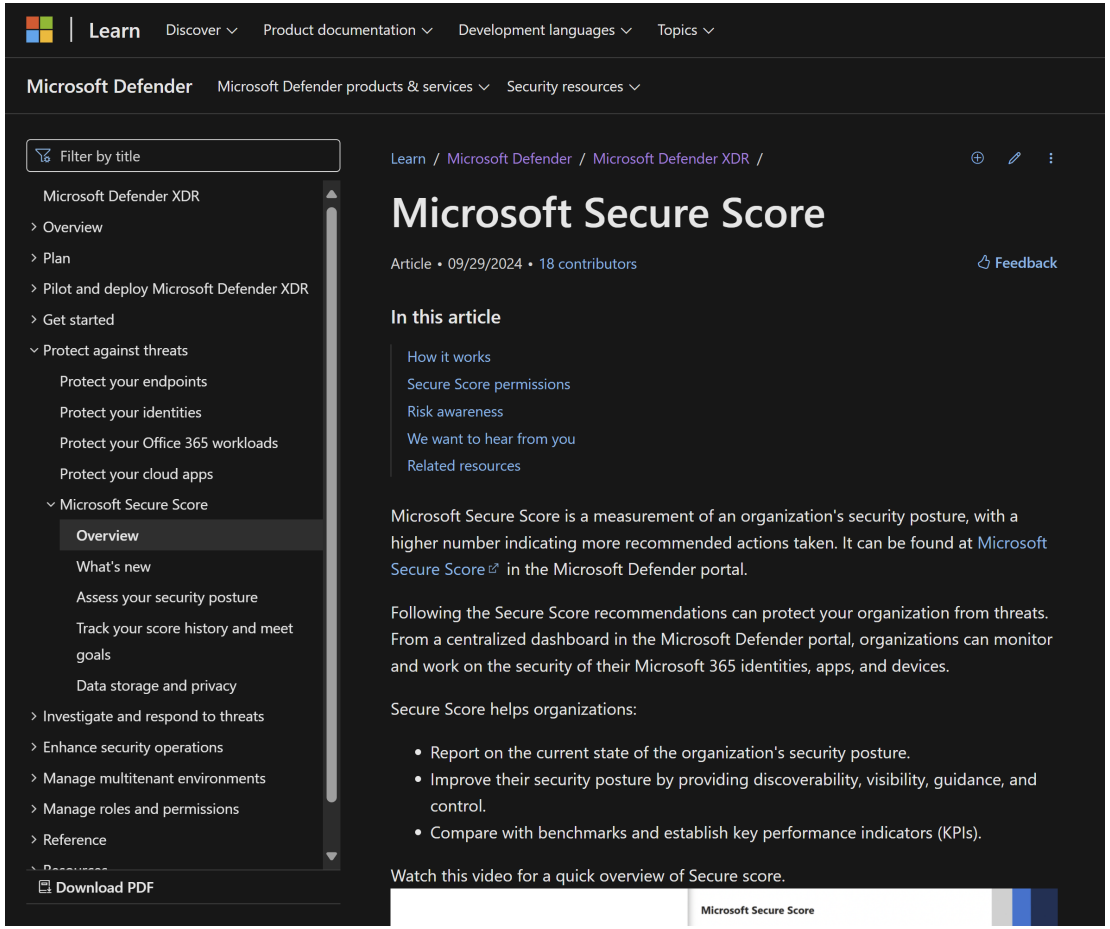

Microsoft



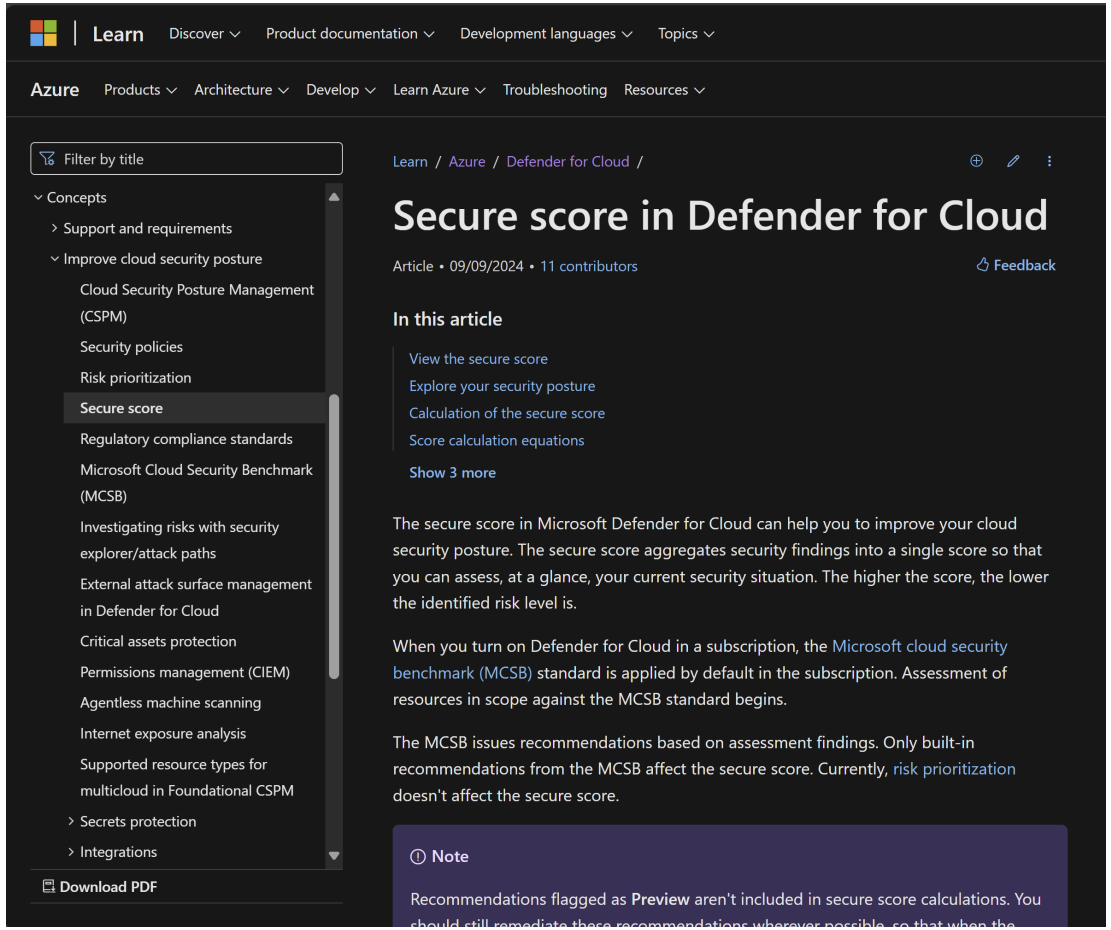
https://learn.microsoft.com/en-us/security/benchmark/azure/



https://learn.microsoft.com/en-us/security/benchmark/azure/overview



https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score



https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

Learn | Discover | Product documentation | Development languages | Topics

Microsoft Entra | Microsoft Entra ID | External ID | Global Secure Access | ID Governance | Permissions Management | Microsoft Security documentation | Tro

Filter by title

- Monitoring and health documentation
- Overview
  - Identity Monitoring and health
  - Identity Recommendations
  - Identity Workbooks
- Concepts
  - Audit logs
  - Sign-in logs
  - Provisioning logs
  - Microsoft Graph activity logs
  - Activity log schemas
  - Microsoft Entra Health
  - Log options for streaming to endpoints
  - Monitoring options and considerations
  - Identity Secure Score
  - Usage and insights report
- Quickstarts
- How-to guides
  - Access activity logs
  - Analyze provisioning logs
  - Analyze activity logs with Microsoft Graph

Download PDF

Learn / Microsoft Entra / Microsoft Entra ID / Monitoring and health /

What is Identity Secure Score?

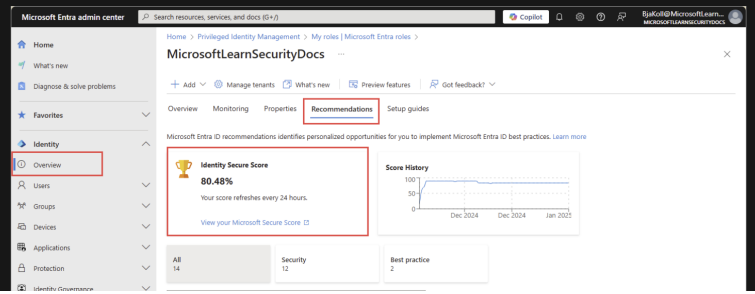
Article • 01/26/2025 • 3 contributors

Feedback

In this article

- How does the Identity Secure Score benefit me?
- How does it work?
- Prerequisites
- How do I use the Identity Secure Score?
- Frequently asked questions

The Identity Secure Score is shown as a percentage that functions as an indicator for how aligned you are with Microsoft's recommendations for security. Each improvement action in Identity Secure Score is tailored to your configuration. You can access the score and view individual recommendations related to your score in Microsoft Entra recommendations. You can also see how your score has changed over time.



How does the Identity Secure Score relate to the Microsoft 365 secure score?

The Microsoft secure score contains five distinct control and score categories:

- Identity
- Data
- Devices
- Infrastructure
- Apps

The Identity Secure Score represents the identity part of the Microsoft secure score. This overlap means that your recommendations for the Identity Secure Score and the identity score in Microsoft are the same.

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-identity-secure-score