



# 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

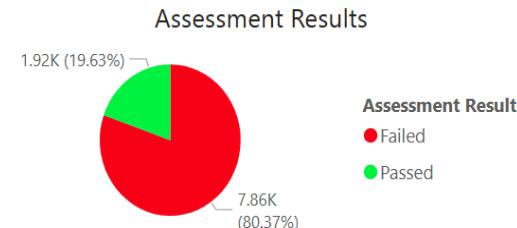
## Value:

- 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

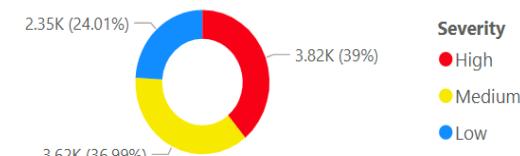
## Power BI Dashboard

### Executive Summary for Contoso Hotels

#### Microsoft Cloud Security Benchmark



#### Azure Benchmark Severity

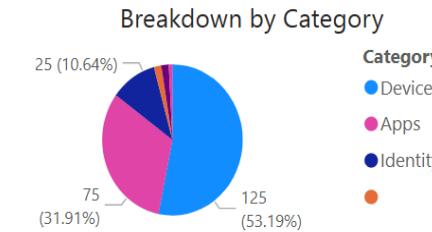


#### Top Security Benchmark High Recommendations

	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%

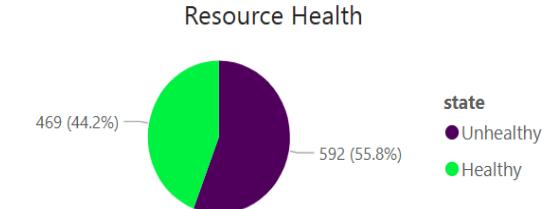


#### Microsoft Secure Score Recommendation

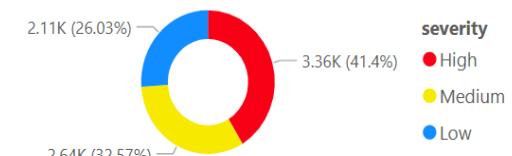
Product	Score impact
SharePoint Online	0.07%
Salesforce	3.48%
Microsoft Teams	0.37%
Microsoft Information Protection	0.07%
Exchange Online	0.44%
Defender for Office	6.78%
Defender for Identity	1.92%
Defender for Endpoint	48.96%
Azure Active Directory	3.43%
Total	65.52%

#### Azure Secure Score

35%



#### 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.

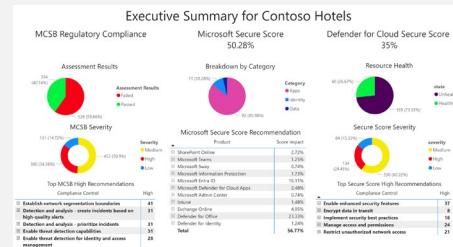
1. Defender for Cloud Secure Score recommendations for all subscriptions in scope.
  2. Microsoft Cloud Security Benchmark recommendations for all subscriptions in scope.
  3. Microsoft Secure Score export.

## 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.



## 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 **Azure** Permissions required:  
**Reader**

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:

The screenshot shows the Microsoft Defender for Cloud | Overview page. At the top left is a lock icon and the text "Showing 5 subscriptions". Below this is a search bar and navigation links for "Subscriptions" and "What's new". A message box says "You may be viewing limited information. To Request t...". On the left, a sidebar has "General" expanded, showing "Overview" (selected), "Getting started", "Recommendations", and "Attack surface analysis". In the center, there are two cards: one for "Azure subscriptions" (5) and one for "AWS accounts" (4).

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:

The screenshot shows the "Portal settings | Directories + subscriptions" page. At the top is a search bar and a Copilot button. On the left is a sidebar with "Search menu", "Directories + subscriptions" (selected), "Appearance + startup views", "Language + region", "My information", and "Signing out + notifications". In the center, there is a "Default subscription filter" section with a dropdown set to "All subscriptions". Below it is a "Filter items..." input field and a list of checked filters: "Select all", "Last visited", and "Most recently used". A red arrow points to the gear icon in the top right corner of the page header.

# Export Defender for Cloud: Secure Score

In Defender for Cloud, select “Recommendations”:

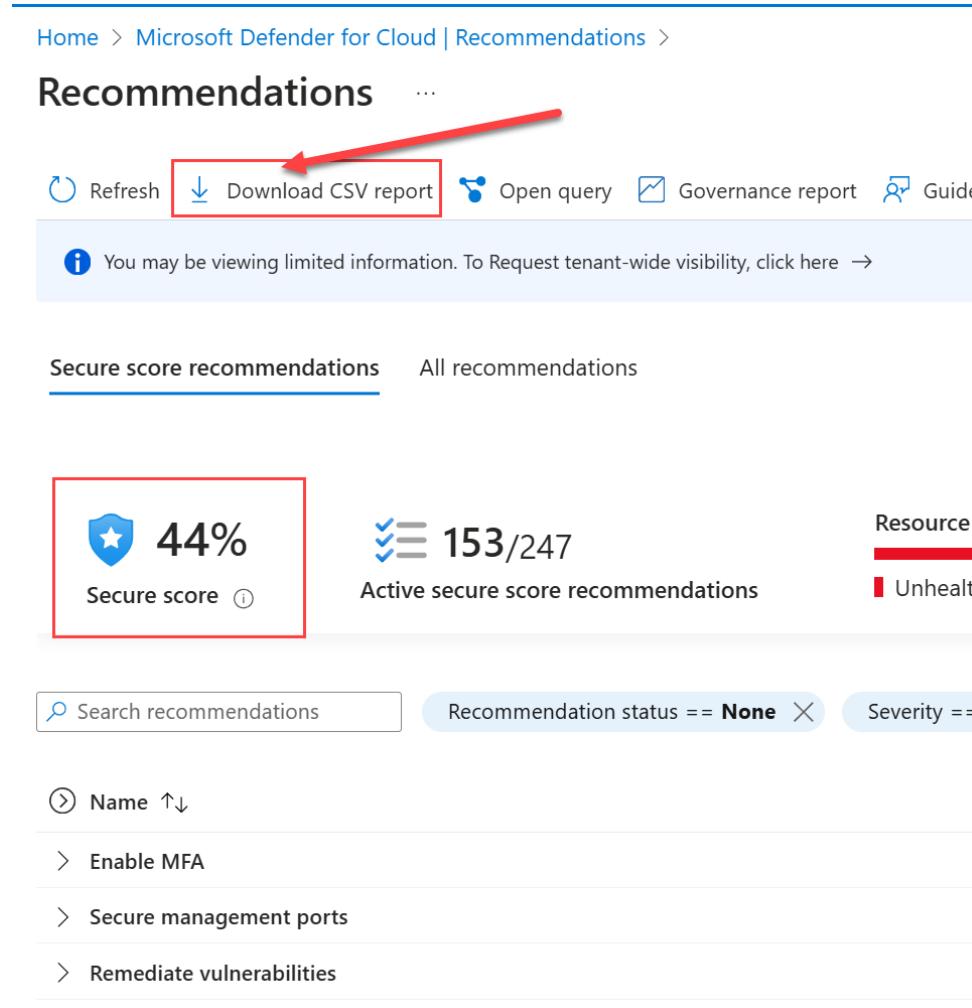
The screenshot shows the Microsoft Defender for Cloud interface. At the top left, it says "Home > Microsoft Defender for Cloud". The main title is "Microsoft Defender for Cloud | Recommendations". Below the title, there's a search bar and several navigation links: Refresh, Download CSV report, Open query, Governance report, Guides & Feedback, and a yellow-highlighted "Switch to classic view" button. A red arrow points to this button. On the left, there's a sidebar with "General", "Overview", "Setup", and a red-bordered "Recommendations" tab. At the bottom, there are sections for "Defender CSPM" and "Recommendations by risk" with a "Risk based recommendations" link.

## **Important:**

Make sure that the **classic view** of the recommendations is selected.

# Export Defender for Cloud: Secure Score

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



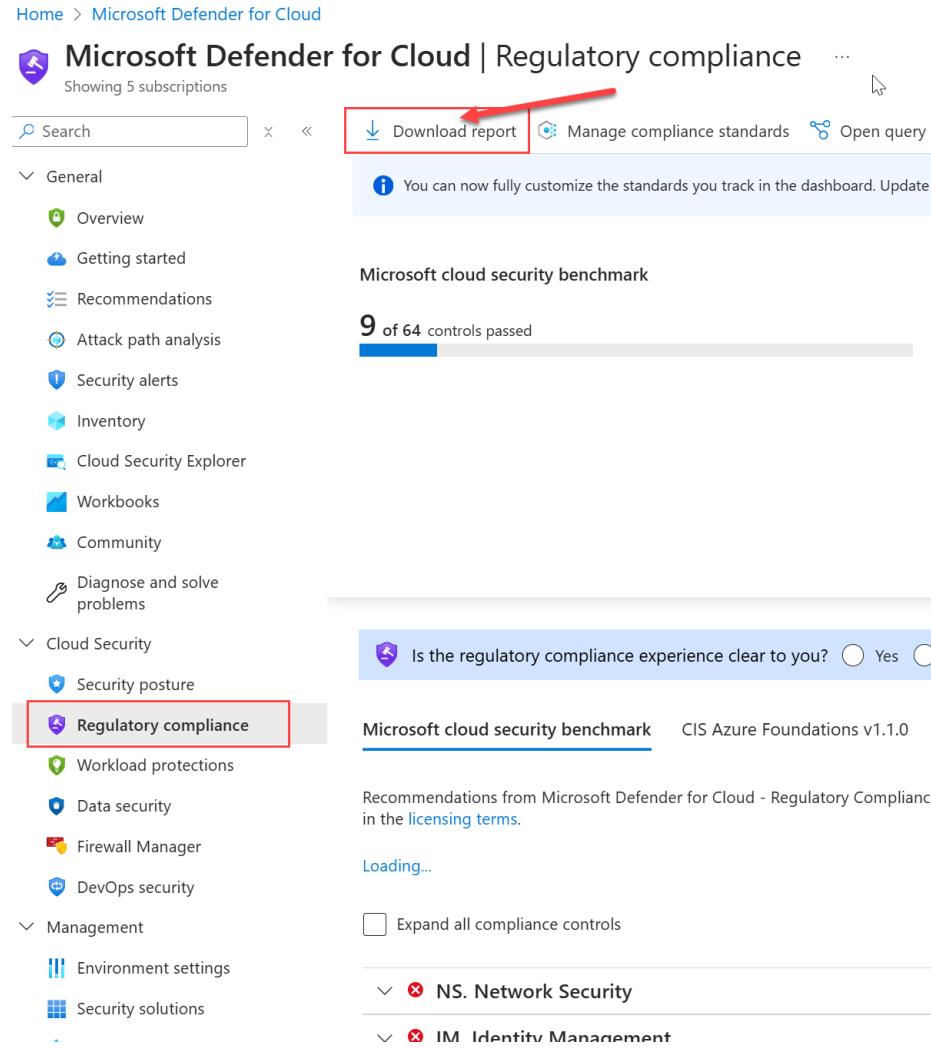
The screenshot shows the Microsoft Defender for Cloud Recommendations page in classic view. At the top, there's a navigation bar with 'Home > Microsoft Defender for Cloud | Recommendations >'. Below it, a 'Recommendations' section has a 'Refresh' button, a 'Download CSV report' button (which is highlighted with a red box and a red arrow pointing to it), 'Open query', 'Governance report', and 'Guides' buttons. A note below says 'You may be viewing limited information. To Request tenant-wide visibility, click here →'. Under the 'Secure score recommendations' tab, there's a summary box with a shield icon, '44%' secure score, and '153/247' active secure score recommendations. A resource health bar shows a red segment labeled 'Unhealthy'. Below this are search/filter fields for 'Search recommendations', 'Recommendation status == None', and 'Severity =='. A sorting dropdown shows 'Name ↑↓'. A list of recommendations follows, including 'Enable MFA', 'Secure management ports', and 'Remediate vulnerabilities'.

## Important:

**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”:



Home > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Regulatory compliance

Showing 5 subscriptions

Search  X ...

[Download report](#) [Manage compliance standards](#) [Open query](#)

You can now fully customize the standards you track in the dashboard. Update ↗

General

- Overview
- Getting started
- 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 security
- Firewall Manager
- DevOps security

Management

- Environment settings
- Security solutions

Microsoft cloud security benchmark

9 of 64 controls passed

Is the regulatory compliance experience clear to you?  Yes  No

Microsoft cloud security benchmark CIS Azure Foundations v1.1.0

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance in the [licensing terms](#).

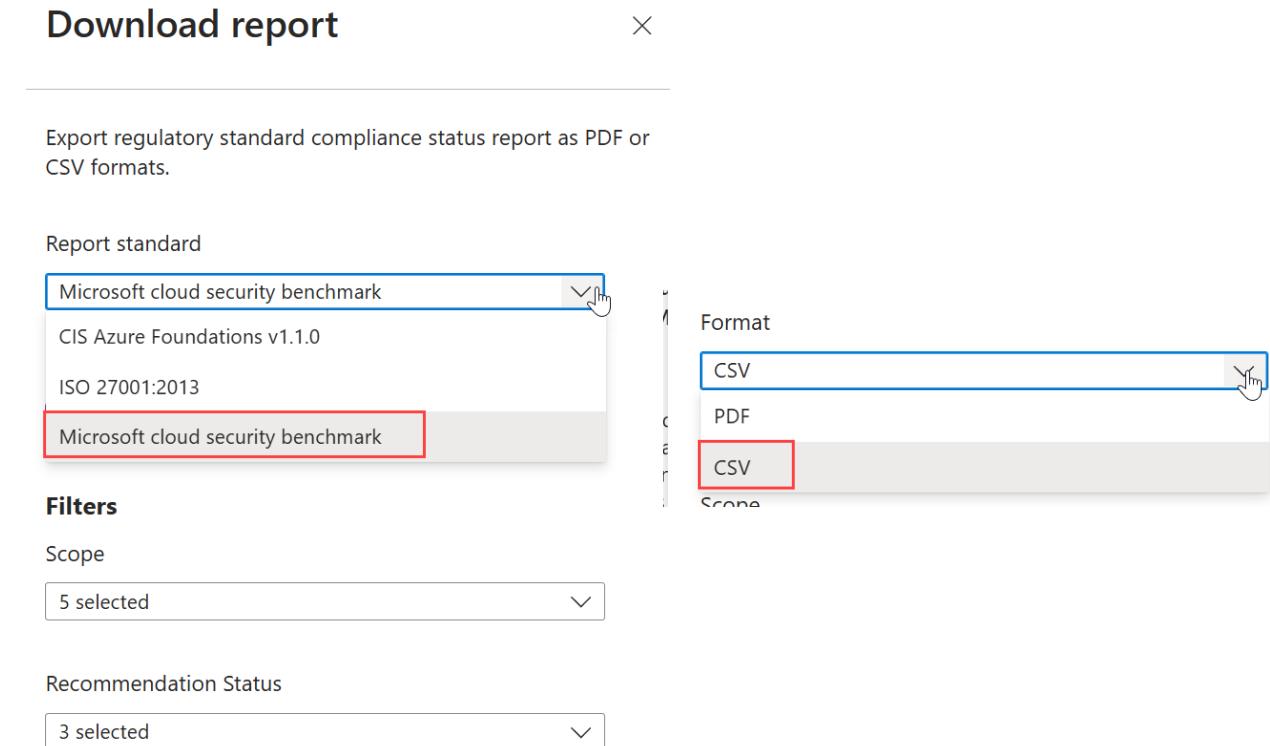
Loading...

Expand all compliance controls

NS. Network Security ✖

IM. Identity Management ✖

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



### Download report

Export regulatory standard compliance status report as PDF or CSV formats.

Report standard

- Microsoft cloud security benchmark
- CIS Azure Foundations v1.1.0
- ISO 27001:2013
- Microsoft cloud security benchmark**

Format

- CSV**
- PDF
- CSV**

Filters

Scope

5 selected

Recommendation Status

3 selected

Home &gt; Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Regulatory compliance

Showing 5 subscriptions

Search



Download report



Manage compliance standards



Open query



Compliance

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

&gt; Management

### 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) Benchmark

### 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

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":

The screenshot shows the Microsoft Defender XDR Home page for the organization 'WOODGROVE'. On the left, there's a sidebar with various icons. The main area has three cards: 'SOC optimization' (with 20 Active, 0 In progress, and 10 Completed optimizations), 'Connected SaaS apps' (with 4 Healthy and 0 Needs attention SaaS app connectors), and 'Microsoft Secure Score'. The 'Microsoft Secure Score' card displays a score of 50.13% (719.34/1435 points achieved) with a red arrow pointing to it. Below the score, it says 'Secure Score is a representation of your organization's security posture, and your opportunity to improve it.' A note at the bottom states 'Score last calculated 06/26'.

## **Important:**

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

Microsoft Defender

Search

Light mode

u5697

Home

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	Resolved
1914	1899

Resolved directly	Resolved with your help
1011	888

View report

SOC optimization

### Your optimization data

Optimization status

Active In progress Completed

Microsoft Sentinel automation

### 4 automation rule

Last 24 hours

Closed incidents 0 Time save N/A Actions performed

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

Operational technology

Cases

SOC optimization

Reports

Microsoft Defender

Search

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

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 Secure Score

Overview   Recommended actions   History   Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture,

Applied filters:

Your secure score

Include ▼

**Secure Score: 50.13%**

719.34/1435 points achieved

100%

75%

50%



Actions to review



Top recommended actions

[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

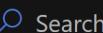
There are new permissions options available for Secure Score. You can now configure users' Secure Score data visibility based on data source. [Learn more about this change.](#)

[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

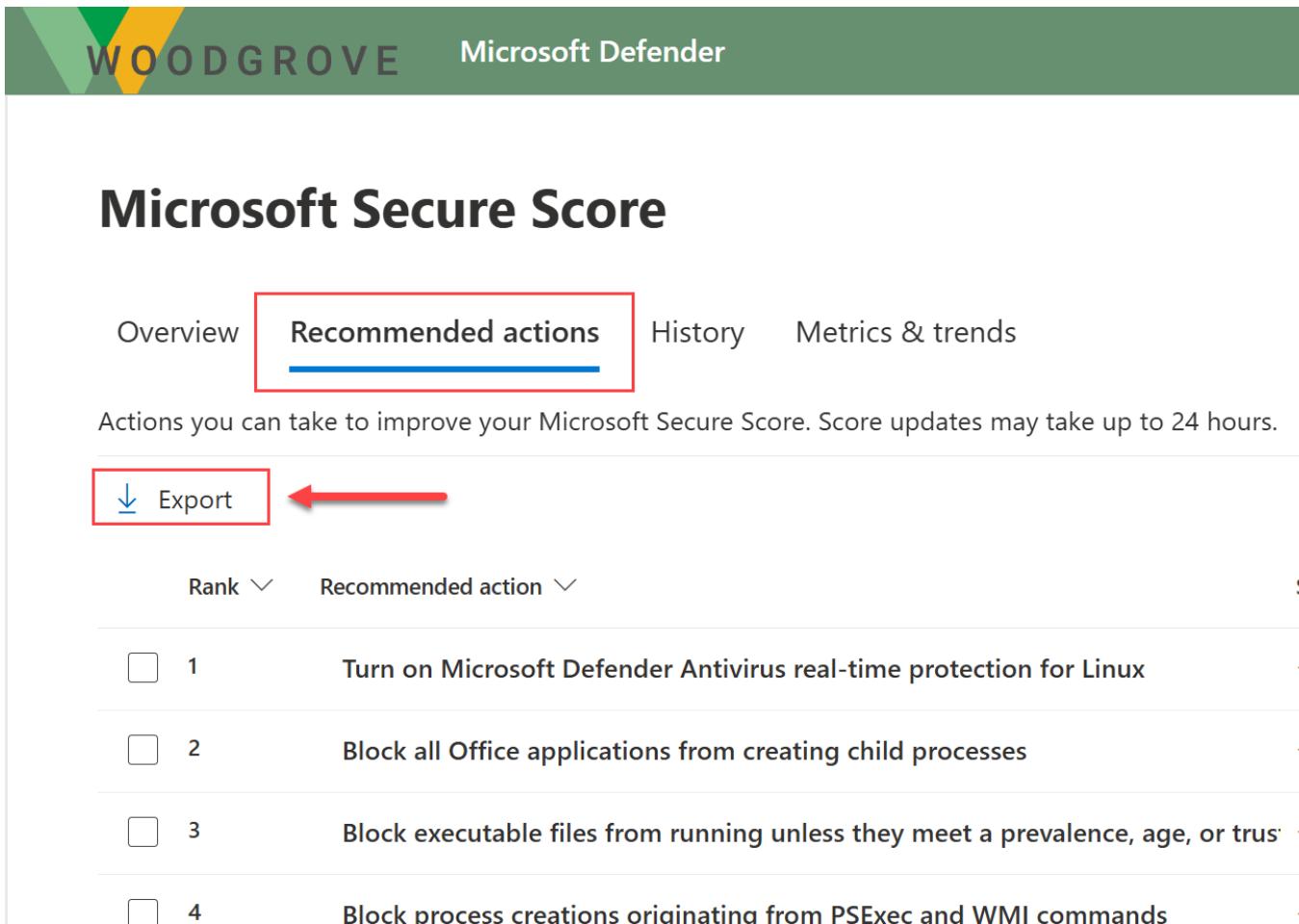


Group by

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	Defense
2	Enable 'Local Security Authority (LSA) protection'	+0.46%	0/8	To address	No	Yes	Device	Defense
3	Set User Account Control (UAC) to automatically deny elevation	+0.46%	0/8	To address	No	Yes	Device	Defense
4	Disable 'Enumerate administrator accounts on elevation'	+0.46%	0/8	To address	No	Yes	Device	Defense
5	Enable 'Require additional authentication at startup'	+0.46%	0/8	To address	No	Yes	Device	Defense
6	Disable 'Autoplay' for all drives	+0.46%	0/8	To address	No	Yes	Device	Defense
7	Set default behavior for 'AutoRun' to 'Enabled: Do not execute'	+0.46%	0/8	To address	No	Yes	Device	Defense
8	Set LAN Manager authentication level to 'Send NTLMv2 responses'	+0.46%	0/8	To address	No	Yes	Device	Defense
9	Disable 'Allow Basic authentication' for WinRM Client	+0.46%	0/8	To address	No	Yes	Device	Defense
10	Disable 'Allow Basic authentication' for WinRM Service	+0.46%	0/8	To address	No	Yes	Device	Defense

# Export Microsoft Defender XDR

Click on "Export" to download the CSV report:



The screenshot shows the Microsoft Secure Score dashboard for the organization "WOODGROVE". The top navigation bar includes the organization logo and the text "Microsoft Defender". Below the header, the title "Microsoft Secure Score" is displayed. The dashboard features four tabs: "Overview", "Recommended actions" (which is currently selected and highlighted with a red border), "History", and "Metrics & trends". A message below the tabs states: "Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours." At the bottom left, there is a prominent "Export" button with a downward arrow icon, also enclosed in a red box and pointing to by a red arrow. The main content area displays a list of recommended actions, each with a checkbox, a rank (1 through 4), a description, and a "+" sign indicating more details.

Rank	Recommended action	Score
1	Turn on Microsoft Defender Antivirus real-time protection for Linux	+
2	Block all Office applications from creating child processes	+
3	Block executable files from running unless they meet a prevalence, age, or trust level	+
4	Block process creations originating from PSEXEC and WMI commands	+

# 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



# 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.



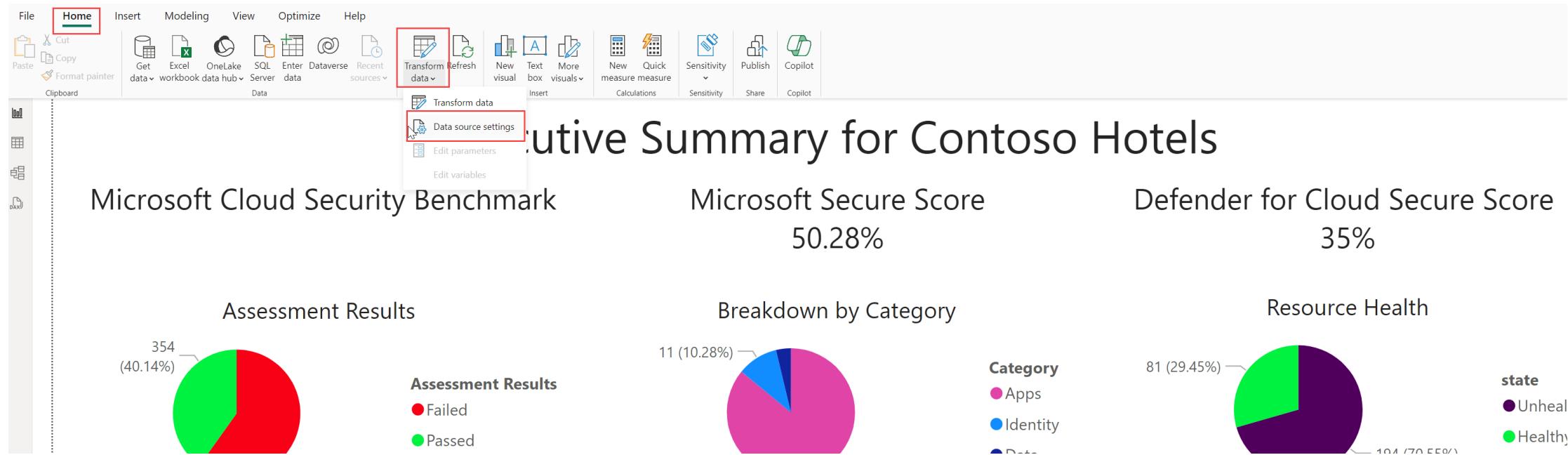
## Microsoft Defender XDR

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:

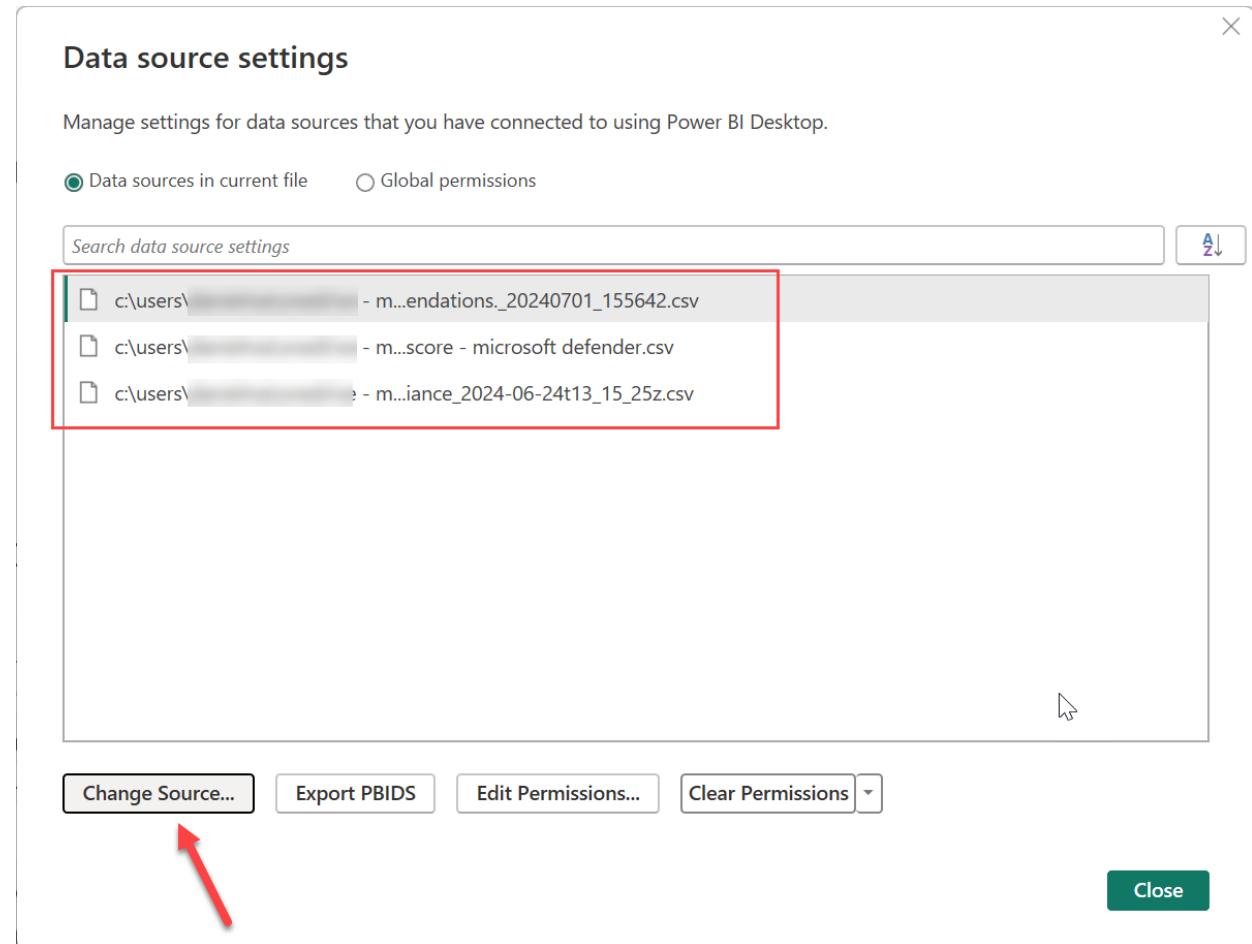


# Refreshing Power BI Report

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.

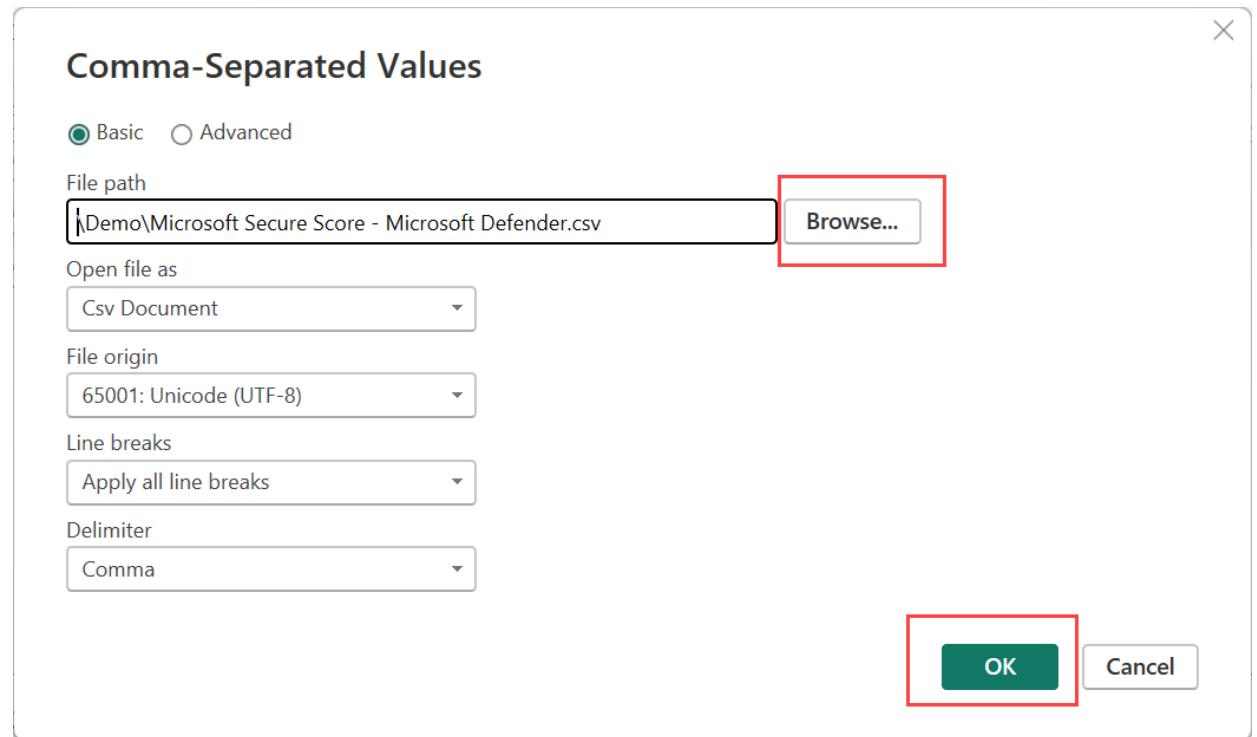
Select the correct entry and click "*Change Source*"



# Refreshing Power BI Report

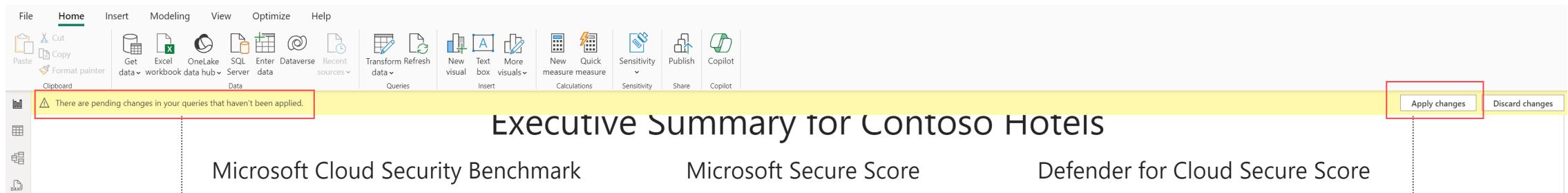
Click “Browse...” and navigate to the updated data files you exported earlier.

Repeat this for all 3 data files.



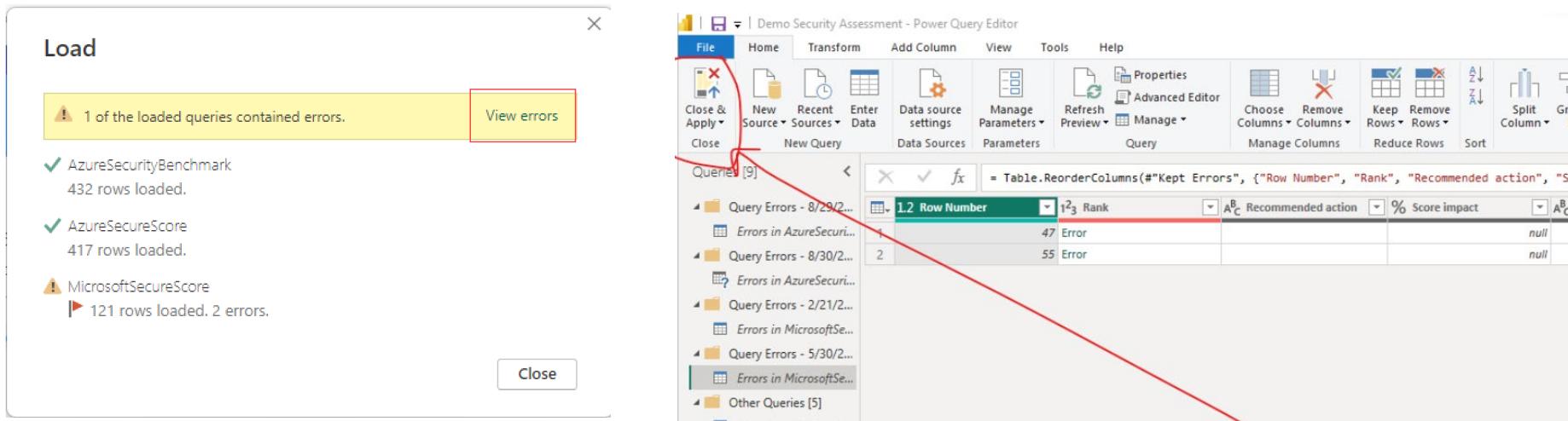
# Refreshing Power BI Report

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

[Filter by title](#)

## Microsoft cloud security benchmark

[Introduction](#)[MCSB Controls \(v1\)](#)[Overview of MCSB controls](#)[Network security](#)[Identity management](#)[Privileged Access](#)[Data protection](#)[Asset management](#)[Logging and threat detection](#)[Incident response](#)[Posture and vulnerability management](#)[Endpoint security](#)[Backup and recovery](#)[DevOps Security](#)[Governance and Strategy](#)[➤ Security baselines for Azure \(MCSB v1\)](#)[➤ Security baselines for Azure compute](#)[➤ Security Controls \(previous benchmarks\)](#)[➤ Resources](#)[Download PDF](#)

# Microsoft cloud security benchmark documentation

Learn how to secure your cloud solutions with our best practices and guidance.

## About the Microsoft cloud security benchmark (MCSB)

### OVERVIEW

[Microsoft cloud security benchmark introduction](#)[Overview of MCSB controls \(v1\)](#)[Overview of the MCSB security baselines](#)

## AI + Machine Learning security baselines

### OVERVIEW

[Azure Databricks](#)[Azure Machine Learning](#)[Azure Cognitive Search](#)

## Analytics security baselines

### OVERVIEW

[Azure Data Explorer security baseline](#)[Azure Data Factory security baseline](#)[Data Lake Analytics security baseline](#)[Event Hubs security baseline](#)

## MCSB v1 controls

### OVERVIEW

[Network security](#)[Identity management](#)[Privileged access](#)[Data protection](#)[Asset management](#)[See more](#)

## More Azure security resources

### TRAINING

[Azure Security Fundamentals](#)[Shared responsibility in the cloud](#)[Microsoft Defender for Cloud](#)[Azure Security Benchmark Foundation blueprint sample](#)

## Compute security baselines

### OVERVIEW

[Azure Functions](#)[Batch](#)[Container Instances](#)[Container Registry](#)[Service Fabric](#)

## More Azure security resources

### TRAINING

[Azure Security Fundamentals](#)[Shared responsibility in the cloud](#)[Microsoft Defender for Cloud](#)[Azure Security Benchmark Foundation blueprint sample](#)

## Compute security baselines

### OVERVIEW

[Azure Functions](#)[Batch](#)[Container Instances](#)[Container Registry](#)[Service Fabric](#)

# Overview of Microsoft cloud security benchmark (v1)

Article • 07/31/2023 • 3 contributors

[Feedback](#)

## In this article

[What's new in Microsoft cloud security benchmark v1](#)[Controls](#)[Recommendations in Microsoft cloud security benchmark](#)[Download](#)[Next steps](#)

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 your multi-cloud environment. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance that includes:

- [Cloud Adoption Framework](#): Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.
- [Azure Well-Architected Framework](#): Guidance on securing your workloads on Azure.
- [The Chief Information Security Officer \(CISO\) Workshop](#): Program guidance and reference strategies to accelerate security modernization using Zero Trust principles.
- [Other industry and cloud service providers security best practice standards and framework](#): Examples include the Amazon Web Services (AWS) Well-Architected Framework, Center for Internet Security (CIS) Controls, National Institute of Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS).

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

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

Learn Discover Product documentation Development languages Topics

Microsoft Defender Microsoft Defender products & services Security resources

Filter by title

Microsoft Defender XDR

- > Overview
- > Plan
- > Pilot and deploy Microsoft Defender XDR
- > Get started
- > Protect against threats
  - Protect your endpoints
  - Protect your identities
  - Protect your Office 365 workloads
  - Protect your cloud apps
- > Microsoft Secure Score
  - Overview
  - What's new
  - Assess your security posture
  - Track your score history and meet goals
  - Data storage and privacy
- > Investigate and respond to threats
- > Enhance security operations
- > Manage multitenant environments
- > Manage roles and permissions
- > Reference
- > Resources

Download PDF

Learn / Microsoft Defender / Microsoft Defender XDR /

# Microsoft Secure Score

Article • 09/29/2024 • 18 contributors

Feedback

In this article

- How it works
- Secure Score permissions
- Risk awareness
- We want to hear from you
- Related resources

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more recommended actions taken. It can be found at [Microsoft Secure Score](#) in the Microsoft Defender portal.

Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Secure Score helps organizations:

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

Watch this video for a quick overview of Secure score.

Microsoft Secure Score

Filter by title

Azure Products Architecture Develop Learn Azure Troubleshooting Resources

Learn / Azure / Defender for Cloud /

# Secure score in Defender for Cloud

Article • 09/09/2024 • 11 contributors

Feedback

In this article

- View the secure score
- Explore your security posture
- Calculation of the secure score
- Score calculation equations

Show 3 more

The secure score in Microsoft Defender for Cloud can help you to improve your cloud security posture. The secure score aggregates security findings into a single score so that you can assess, at a glance, your current security situation. The higher the score, the lower the identified risk level is.

When you turn on Defender for Cloud in a subscription, the Microsoft cloud security benchmark (MCSB) standard is applied by default in the subscription. Assessment of resources in scope against the MCSB standard begins.

The MCSB issues recommendations based on assessment findings. Only built-in recommendations from the MCSB affect the secure score. Currently, risk prioritization doesn't affect the secure score.

**Note**

Recommendations flagged as Preview aren't included in secure score calculations. You should still remediate these recommendations wherever possible, so that when the

<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>

Filter by title

Monitoring and health documentation

Overview

- Identity Monitoring and health
- Identity Recommendations
- Identity Workbooks

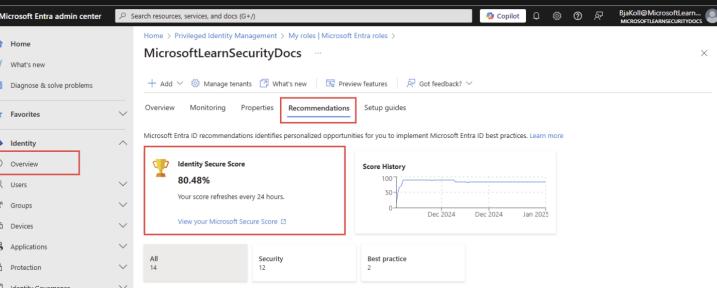
Concepts

- 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>