

Greater Region 9 Seminar

Microsoft 365 and Azure Security Management

September 22, 2026 – Detroit, MI

Joey Cusimano, ICF – STACS Software Engineer – Baltimore, MD

Session Agenda

- Microsoft 365 (M365)
 - Microsoft Entra ID
 - Implementing and Enforcing Multi-Factor Authentication (MFA)
 - Microsoft Intune
- Microsoft Defender
- Microsoft Azure
 - Microsoft Defender for Cloud
- SecOps Weekly Review Checklist



Terminology



Suite of cloud-based Microsoft apps

- including Outlook, Office Apps, Teams, and OneDrive
- Entra ID - formerly Azure Active Directory
 - Identity and access management service for M365/Azure services (cloud active directory)
- Microsoft Defender
 - Suite of security tools and dashboards for Microsoft 365 services



Microsoft's virtual machine hosting platform for cloud environments

- Microsoft Defender for Cloud
 - Azure-focused suite of security tools and dashboards



Evolution of Defender

- Windows Defender for Desktop
 - Now Windows Security protection suite: firewall, virus& threat, etc.
- Microsoft Defender for M365 (cloud services)
 - Unified security portal at <https://security.microsoft.com>
- Microsoft Defender for Endpoint (user devices)
 - Onboarded/managed with Intune for mobile device management of Microsoft and non-MS devices
- Microsoft Defender for Cloud - Azure hosted environment
 - <https://portal.azure.com> under Microsoft Defender for Cloud menu
- Microsoft Defender for Identity
 - Advanced security features for M365 focused on identity and access management

Microsoft 365 Feature Crosswalk

	User Management	Email	Configuration & Device Management	Servers
Traditional Method	Active Directory	Exchange Server	GPOs/SCCM	On-Premise Hardware
Microsoft 365 Feature	 Entra ID	 Exchange Online	 Intune	 Microsoft Azure
Feature Portal	entra.microsoft.com	admin.exchange.microsoft.com	intune.microsoft.com	portal.azure.com
Security Portal	https://security.microsoft.com			
Security Auditing	 Identity Secure Score	 Defender Secure Score		 Defender for Cloud Secure Score

Licensing

- Licensing is per-user
- Subscription can be monthly or yearly, but cheaper if yearly
- Most features discussed today are included in Business Premium, but not Standard
- The admin portal can be used to see and manage licenses
<https://admin.microsoft.com>

Microsoft 365 for business

(and old names for reference)

Microsoft 365 Business Basic

(Office 365 Business Essentials)



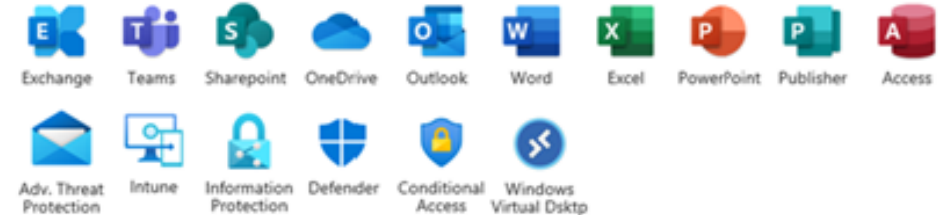
Microsoft 365 Business Standard

(Office 365 Business Premium)



Microsoft 365 Business Premium

(Microsoft 365 Business)



Microsoft 365 Apps

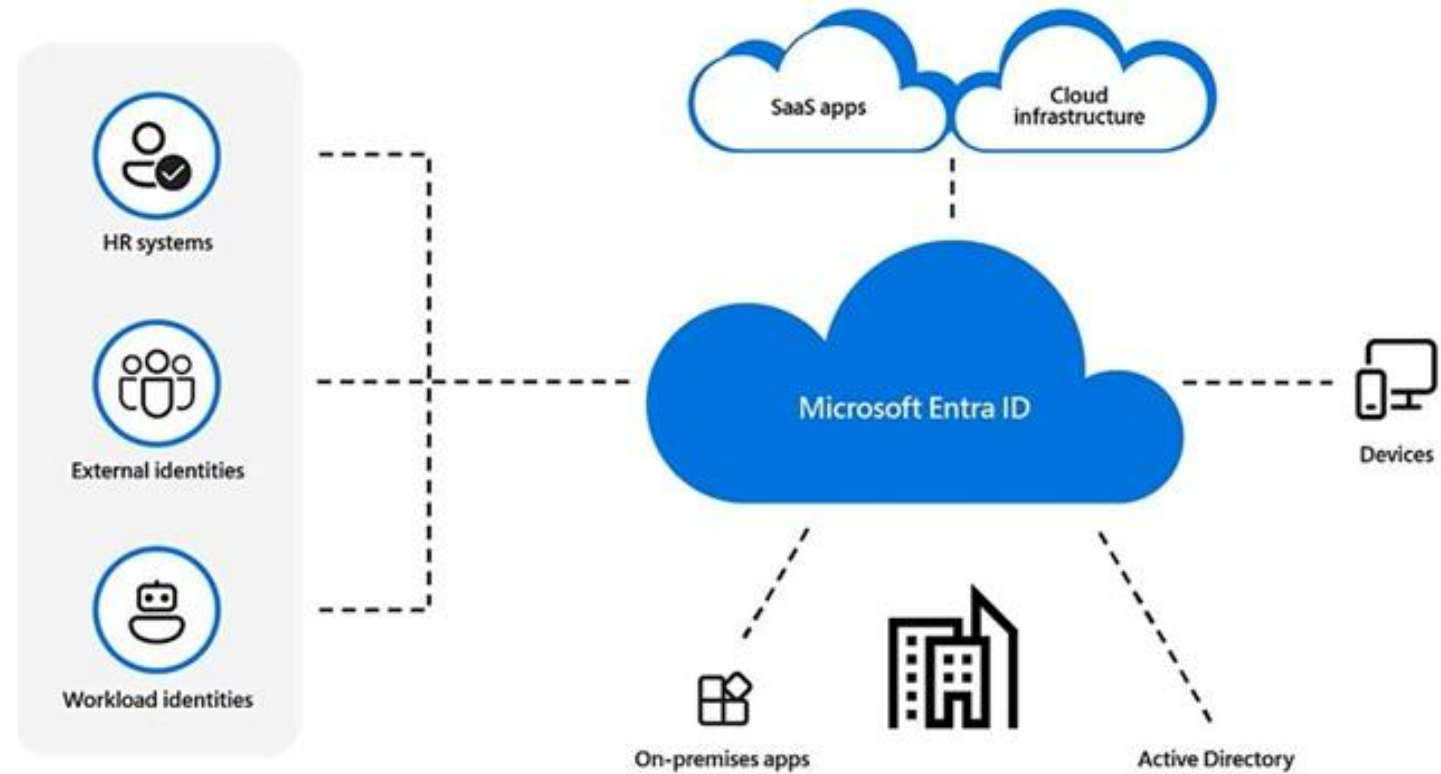
(Office 365 Business)



Note: Not all features/product logos shown.

Microsoft Entra ID

- License:
 - P1 (included with Business Premium) or
 - P2 (advanced features)
- User management
- Sign-in and audit logs
- Risky activities/sign-ins
 - Email alerts set-up
- Conditional access policies – authentication methods

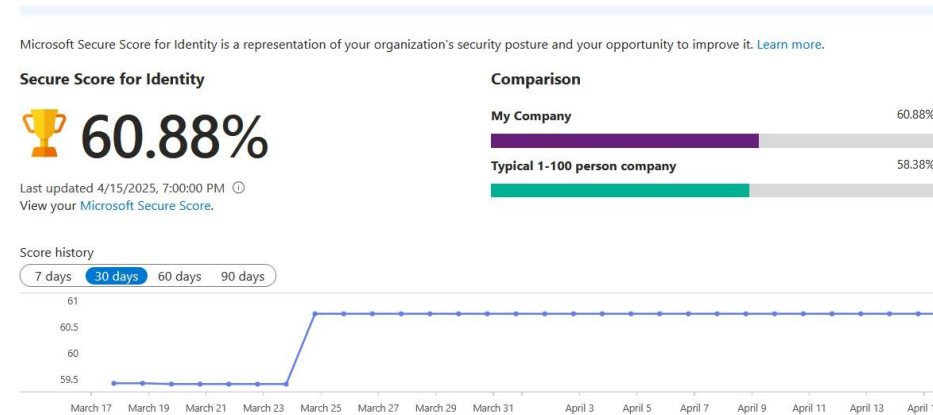


<https://entra.microsoft.com>

Identity Secure Score

- Uses recommendations and risk values to “score” your security posture against Microsoft’s auditing
- “Secure Score” concept is reused in Microsoft Defender and Microsoft Defender for Cloud as well
- Identity Secure Score focuses on user/role management and account security
- 100% requires P2 features to satisfy all recommendations

Identity Secure Score (cont.)



Improvement actions

 Download  Columns

Name ↑↓	Score Impact ↑↓	User Impact ↑↓	Implementation ... ↑↓	Status ↑↓
Ensure multifactor authentication is enabled for all users	13.64%	High	High	Planned
Enable Microsoft Entra ID Identity Protection sign-in risk policies	10.61%	Moderate	Moderate	Risk accepted
Enable Microsoft Entra ID Identity Protection user risk policies	10.61%	Moderate	Moderate	Risk accepted
Enable Conditional Access policies to block legacy authentication	12.12%	Moderate	Moderate	To address
Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other el...	7.58%	Low	High	To address
Ensure user consent to apps accessing company data on their behalf is not allowed	6.06%	Moderate	Low	Completed

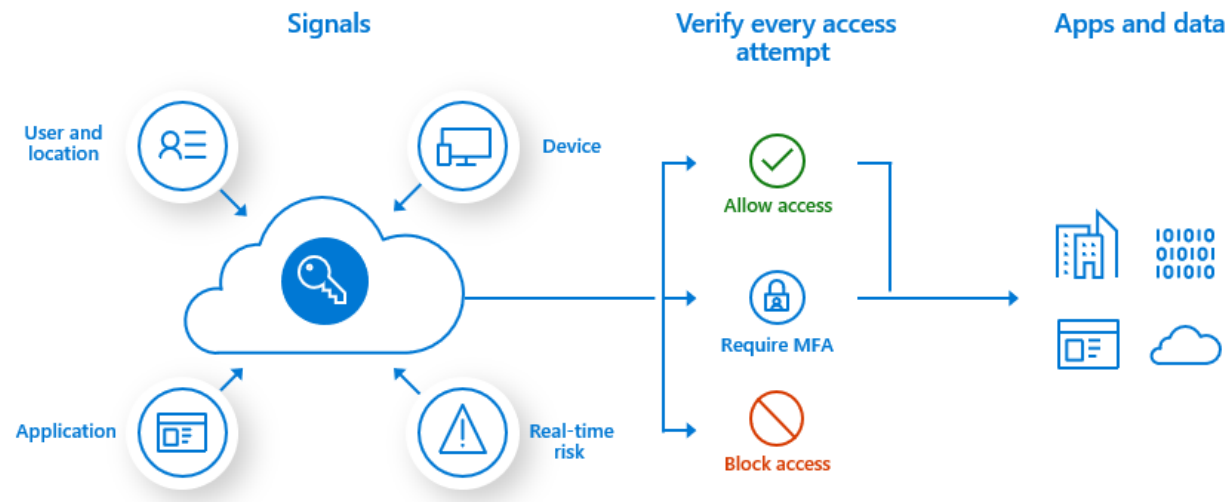
Multi-Factor Authentication (MFA)

- MFA is required for ALL M365 users
- Authenticator app is recommended
 - App generates code locally and offline
- SMS text and email is NOT recommended
 - No encryption and vulnerable to interception
 - Vulnerable to SIM-swapping attacks
- Beware of unsolicited MFA requests
 - They made it to the MFA step. Your password is compromised! Change it!
 - Avoid MFA fatigue attacks – don't just say "Yes" to make the notifications stop!
 - Train users to report unexpected MFA requests and never accept them!



Implementing MFA – Security Defaults

- Predefined set of rules created by Microsoft, available even with Business Standard
- Requires all users to register for MFA
- Admins must always perform MFA, users “when necessary”
 - Blocks legacy authentication – older/insecure protocols
i.e., IMAP, SMTP, POP3, Office 2010...



Implementing MFA – Conditional Access

- Conditional Access Policies

- Requires Business Premium
- Customizable rulesets
- Can require MFA for selected or all users
- Can require app MFA vs SMS/phone

☐ Require multifactor authentication ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication".
[Learn more](#) ⓘ

☒ Require authentication strength ⓘ

Require authentication ... ▾

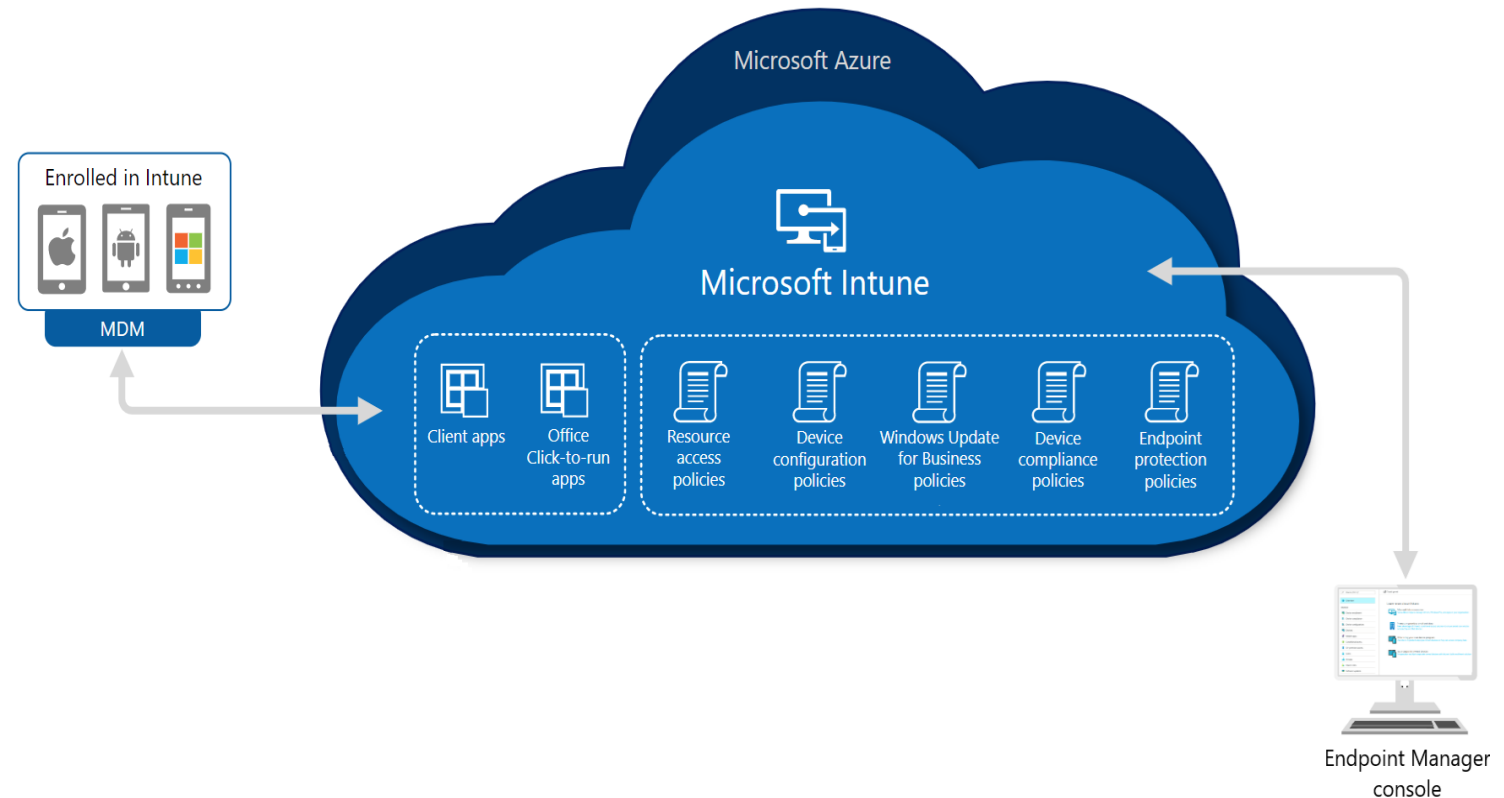
Multifactor authentication
Combinations of methods that satisfy strong authentication, such as Password + SMS

Passwordless MFA
Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

☐ Phishing-resistant MFA ⓘ
☐ Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key ⓘ

Microsoft Intune

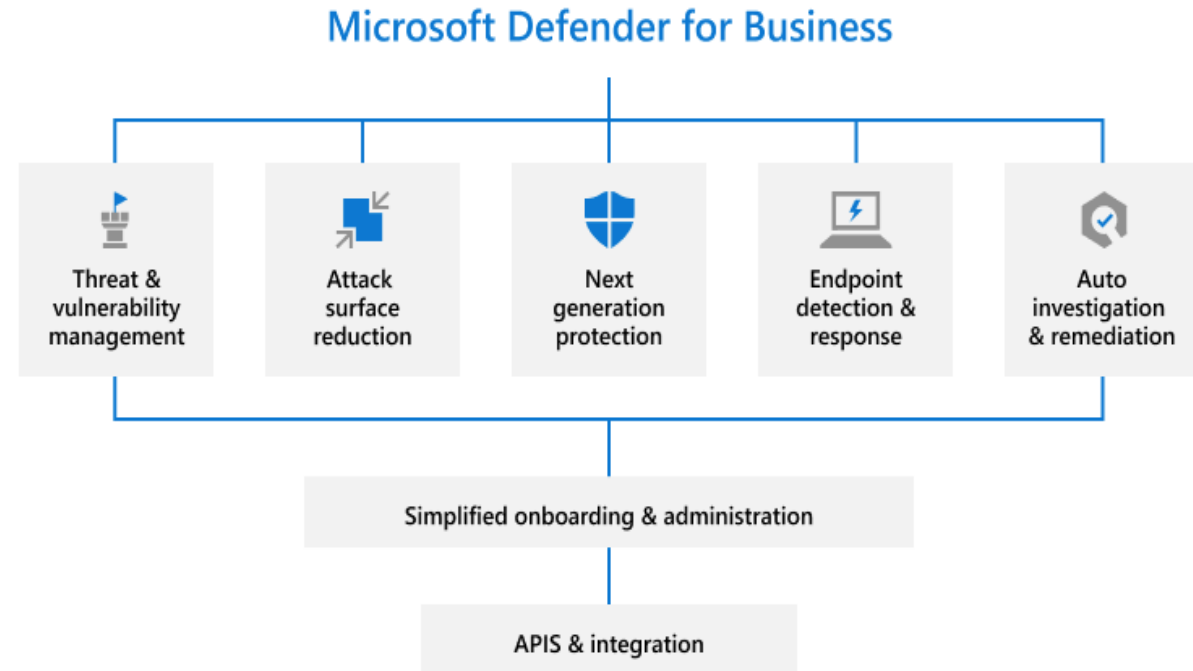
- License: Business Premium or E3+
- Configuration management using group policy settings as well as others
- Support for Apple and Android
- Can view antivirus scan reports and execute scans remotely
- Can view and manage Windows, Apple, Android updates
- Remote wipe capability
- Enrolled devices can be automatically integrated with Defender for Endpoint



<https://intune.microsoft.com>

Microsoft Defender

- Security suite for M365
- License: Business Premium
- Exposure Management:
 - High level view of security posture
 - Categorized findings and recommendations
- Vulnerability Management
 - Can provide vulnerability information on hosts using Defender for Endpoint
- Endpoint Detection and Response (EDR)
 - Real-time monitoring and detection of potential threats on hosts



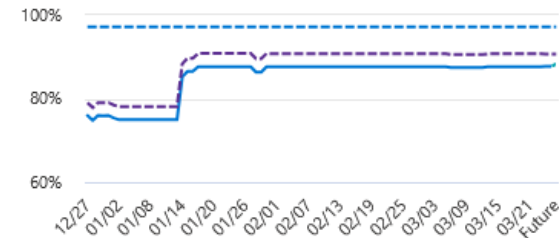
<https://security.microsoft.com>

Exposure Management – Secure Score

- View regularly to identify:
 - New recommendations released (will cause a decrease)
 - Unexpected decreases due to configuration changes
 - Items marked as “planned” that need to be addressed
 - Confirmation of fixes implemented
 - Be sure to show “achievable score”:
 - “Risk accepted” items will prevent reaching 100%
 - Outstanding items may not be achievable if they require a license that you do not have
- ☒ **Planned score**
Show projected score when planned actions are completed
- ☒ **Current license score**
Show score that can be achieved with your current Microsoft license
- ☒ **Achievable score**
Show score that can be achieved with your Microsoft licenses and current risk acceptance

Secure Score: 87.68%

958.34/1093 points achieved



Breakdown points by: Category

Identity	60.88%
Data	77.78%
Device	89.97%
Apps	87.74%

■ Points achieved ■ Opportunity
■ Planned score ■ Achievable score
■ Current license score

Vulnerability Management

- Recommendations
 - Exposure Management entries may link to items here
 - Reports needed software updates for Azure + Intune devices
- Device Inventory
 - Easily view installed software, versions, CVEs, registry paths
 - Security recommendations per device
 - Useful for finding software file locations/current versions

Name ↑ ↓	Vendor ↓	Installed ve... ↓
☐ .net	Microsoft	6.0.28.0
☐ .net	Microsoft	5.0.17.0
☒ .net	Microsoft	8.0.11.0
☐ .net Framework	Microsoft	4.8.1.0
☐ .net Framework	Microsoft	4.0.0.0
☐ Acrobat Dc	Adobe	2025.1.20435.0
☐ Active Directory Authentication Library For Sql ...	Microsoft	13.0.1300.275
☐ Azure Data Studio	Microsoft	1.37.0.0
☐ Chrome	Google	134.0.6998.167
☐ Creative Cloud	Adobe	6.5.0.348
☐ Db Browser For Sqlite	Db Browser For Sqlite Team	3.12.2.0
☐ Defender For Endpoint	Microsoft	10.8790.19045....
☐ Defender Security Intelligence Updates	Microsoft	1.425.264.0

6 ⓘ

1

Threat context

Exploits available
No

Recommendations

Impact
▼ 2.05

Software Evidence

File paths

C:\Program Files\dotnet\shared\Microsoft.NETCore.App\8.0.11\version


Evidence Last found

Mar 25, 2025 10:42:45 PM

Microsoft Graph

An API that can be used to pull data from Microsoft 365, notably audit logs...

For example, used in a Powershell script to pull all sign-ins from a set of administrator users from the past week:

	A	B	C	D	E	F
1	UserPrincipalName	CreatedDateTime	IPAddress	City	State	Countr
2	s @	3/25/2025 19:15	71.179.239.156	Glen Burnie	Maryland	US
3	s @	3/25/2025 17:24	71.179.239.156	Glen Burnie	Maryland	US
4	s @	3/25/2025 17:16	71.179.239.156	Glen Burnie	Maryland	US
5	s @	3/25/2025 16:40	71.179.239.156	Glen Burnie	Maryland	US
6	s @	3/25/2025 16:40	71.179.239.156	Glen Burnie	Maryland	US
7	s @	3/25/2025 16:29	71.179.239.156	Glen Burnie	Maryland	US
8	s @	3/25/2025 16:26	71.179.239.156	Glen Burnie	Maryland	US
9	s @	3/25/2025 16:26	71.179.239.156	Glen Burnie	Maryland	US
10	s @	3/25/2025 16:25	71.179.239.156	Glen Burnie	Maryland	US
11	s @	3/25/2025 16:24	71.179.239.156	Glen Burnie	Maryland	US
12	s @	3/25/2025 16:24	71.179.239.156	Glen Burnie	Maryland	US
13	s @	3/25/2025 16:22	71.179.239.156	Glen Burnie	Maryland	US
14	s @	3/25/2025 16:19	71.179.239.156	Glen Burnie	Maryland	US
15	s @	3/25/2025 16:19	71.179.239.156	Glen Burnie	Maryland	US
16	s @	3/25/2025 15:51	71.179.239.156	Glen Burnie	Maryland	US
17	s @	3/25/2025 15:50	71.179.239.156	Glen Burnie	Maryland	US
18	s @	3/21/2025 17:08	71.179.239.156	Glen Burnie	Maryland	US
19	s @	3/21/2025 14:17	71.179.239.156	Glen Burnie	Maryland	US
20	s @	3/20/2025 20:13	71.179.239.156	Glen Burnie	Maryland	US
21	s @	3/20/2025 18:51	71.179.239.156	Glen Burnie	Maryland	US
22						
23						

< > david@ndc.org | dsnapp@ndc.org | loren@ndc.org | secops@ndc.org

Microsoft Defender for Cloud

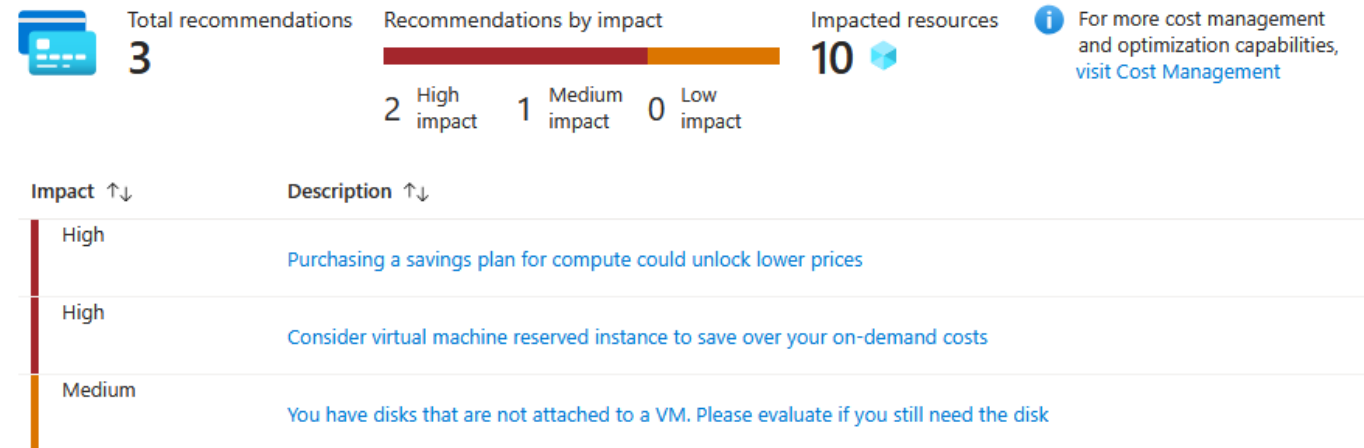
- Cloud-focused security portal
- Provides a Secure Score and security recommendations for:
 - Azure VMs
 - Azure resources (i.e. SQL databases)
 - Azure configurations
- Often highlights items that can be resolved via configuration management/group policy
- Provides monitoring and analytics for the Azure environment



<https://portal.azure.com>

Azure Cost Management

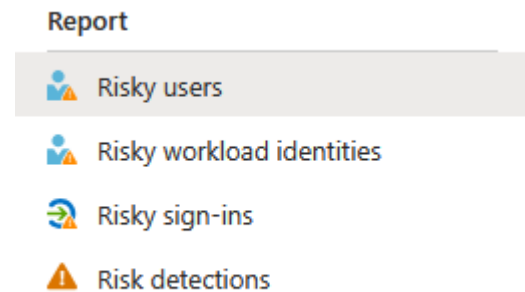
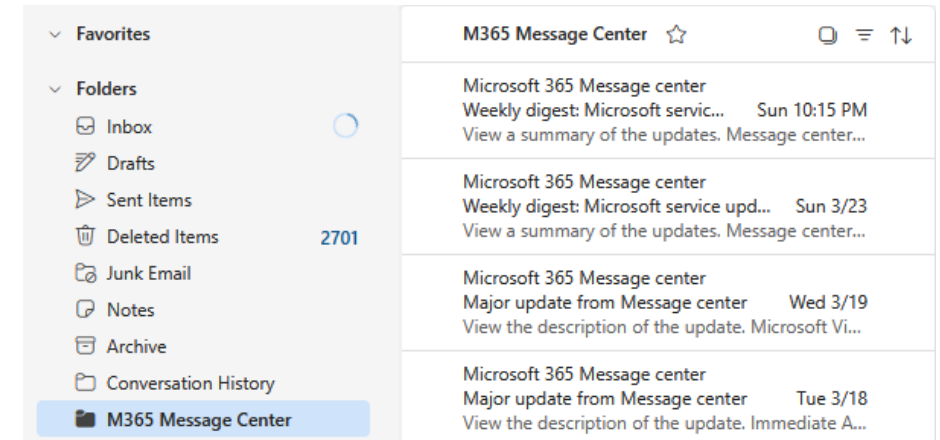
- Cost analysis
- Ability to set up price alerts
- Recommendations for savings on cloud infrastructure



<https://portal.azure.com>

Weekly SecOps Checklist

- Email
 - Skim M365 Message center emails (in their own folder) for relevant updates, action items – mostly administrative
- Entra
 - Risky users, workload identities, sign-ins, detections
 - Manual (scripted with Graph) review of successful sign-ins
- Intune
 - Defender Antivirus Report
 - Windows Update Report



Microsoft 365 Message Center Emails

- Weekly Digest with supplemental announcements
- Mostly informational feature updates/improvements applied in the background
- Can mention features being removed or changing – convey info about relevant products to Trustee/staff if appropriate

 **[Reminder] Power Apps – Update your firewall allowlist to include *.powerplatformusercontent.com**

MC1042732 | March 27 - Starting March 31, 2025, Power Apps will use a new endpoint, *.powerplatformusercontent.com, which needs to be added to your firewall allowlist. What action do I need to take? Please update your firewall to allowlist the *.powerplatformusercontent.com domain and its subdomains before March 31, 2025. Why is this action needed? If action is not taken, your Power Apps may experience performance issues after this change is made on March...
[View more](#)

 **(Updated) New Startup Boost task from Microsoft Office installer for Office applications**

MC1041470 | March 27 - Microsoft is introducing a new Startup Boost task to improve Office application performance, starting mid-May 2025. Admins can disable this feature via Group Policy. The task will be visible in Windows Task Scheduler and initially apply to Microsoft Word. Startup Boost requires sufficient system resources and can be disabled if needed.
[View more](#)

Weekly SecOps Checklist (cont.)

- Microsoft Defender

- Incidents, Alerts
- Secure Score
 - Ensure applied recommendations have taken effect
 - Identify cause(s) of any decrease
- Recommendations
 - Software updates often appear weekly
 - Review in-progress items and dedicate time to working on them or starting new ones
 - Make sure to check both Vulnerability Management and Exposure Management sections!

Date/Time	Activity	Resulting points
Mar 24, 2025 8:00 PM	0.23 points regressed for Enable Conditional Access policies to block legacy authentication because more users are affected	7.53/8
Mar 24, 2025 8:00 PM	1.11 points gained for Ensure multifactor authentication is enabled for all users because fewer users are affected	2.65/9
Mar 19, 2025 8:00 PM	0.01 points regressed for Enable Conditional Access policies to block legacy authentication because more users are affected	7.76/8

Weekly SecOps Checklist (cont.)

- Microsoft Defender for Cloud
 - Security Alerts
 - Secure Score
 - Ensure applied recommendations have taken effect
 - Identify cause(s) of any decrease (no history graph, unfortunately)
 - Query for needed software updates (previously in UI, moved to M365 Defender)
 - Use Powershell w/ Azure APIs to customize results and produce reports

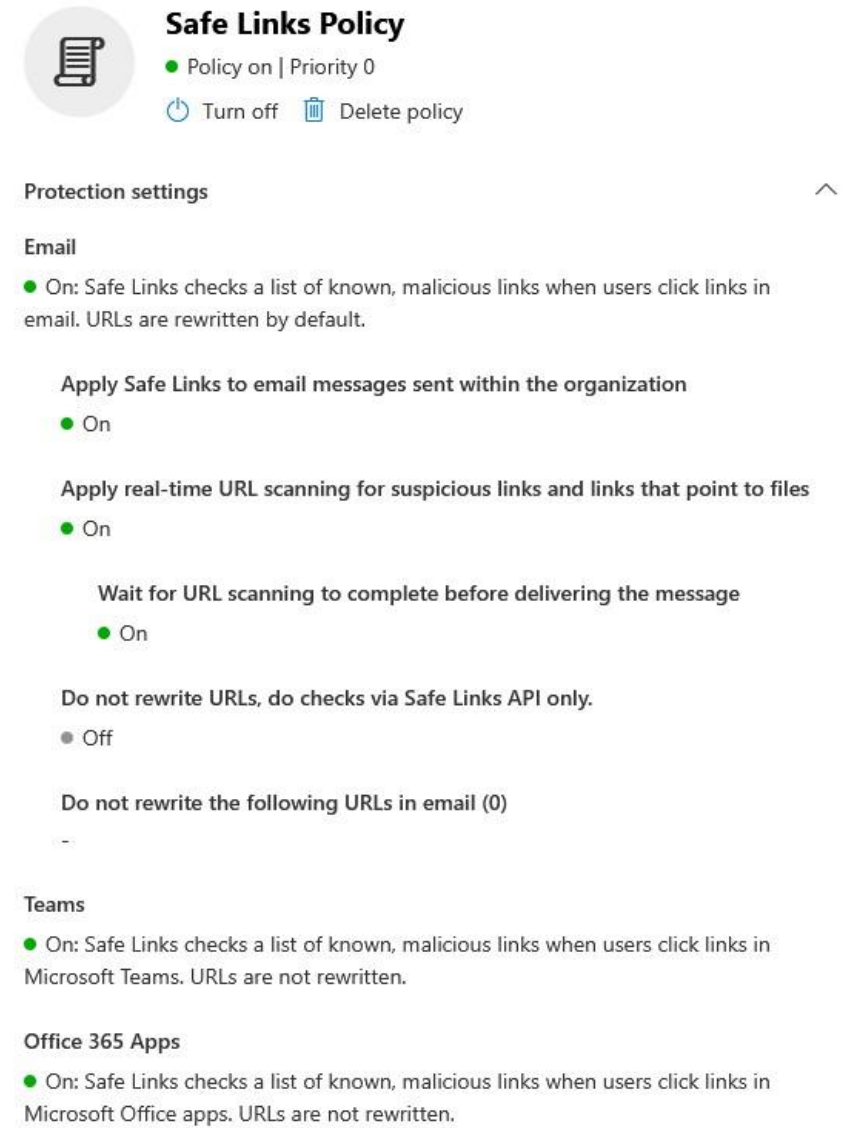
```
=====
Host: [REDACTED]
=====
(2026-09-10 02:31) chrome: ["152.0.7977.83"] → 153.0.8010.37
(2026-09-09 13:01) sql_server_2019: ["15.0.4480.2"] → 15.0.4490.9
=====
Host: [REDACTED]
=====
(2026-09-04 15:35) chrome: ["152.0.7977.83"] → 153.0.8010.37
```

Recommendation Examples

- Enable MFA for all users (Identity/Entra)
- Safe Links & Safe Attachments policies should exist and be applied (M365/Defender)
- Update Google Chrome (M365/Defender)
- Encrypt all BitLocker-supporter drives (M365/Defender)
- Disabled accounts with permissions on Azure resources should be removed (Azure/Defender for Cloud)
- Storage accounts should prevent shared key access (Azure/Defender for Cloud)

Safe Links/Attachments Policies

- Microsoft Defender > Policies and rules > Threat policies
- Designed to protect users from malicious links and attachments in emails
- Safe Links Policy: Scans URLs in emails a database of known malicious URLs
 - Scans are performed each time clicked
 - Rewrites URLs (optional) to ensure scans are done if link is shared
- Safe Attachments Policy: scan files in email before delivering to inbox
- Can be set up in monitor or block mode for testing



Safe Links Policy

● Policy on | Priority 0

⏻ Turn off 🗑 Delete policy

Protection settings ^

Email

● On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.

Apply Safe Links to email messages sent within the organization

● On

Apply real-time URL scanning for suspicious links and links that point to files

● On

Wait for URL scanning to complete before delivering the message

● On

Do not rewrite URLs, do checks via Safe Links API only.

● Off

Do not rewrite the following URLs in email (0)

Teams

● On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.

Office 365 Apps

● On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten.

Secure Score Challenges

- Some recommendations will require licenses you do not have
- Pending Windows/software updates can drop the score until applied
 - This can hit the score twice as hard if the update fixed a vulnerability!
- Some recommendations are not feasible to implement in your environment
 - Ex: password expiration when automation accounts are used
- Security and Microsoft features are always changing; recommendations change with them...
 - Sometimes Microsoft will inform you in Message Center or directly
 - Sometimes you'll just see a score drop

Secure Score Challenges

- Some recommendations will require licenses you do not have
- Pending Windows/software updates can drop the score until applied
 - This can hit the score twice as hard if the update fixed a vulnerability!
- Some recommendations are not feasible to implement in your environment
 - Ex: password expiration when automation accounts are used
- Security and Microsoft features are always changing; recommendations change with them...
 - Sometimes Microsoft will inform you in Message Center or directly
 - Sometimes you'll just see a score drop

Quick Links

NOTE: Use at your own discretion. Links may no longer be active in some cases.

- (<https://msportals.io/>) List of shortcut links for M365 pages.
- (<https://entra.microsoft.com>) Entra ID
- (<https://security.microsoft.com>) M365 Defender
- (<https://portal.azure.com>) Azure (M365 Defender for Cloud)
- (<https://admin.cloud.microsoft/exchange#/homepage>) Exchange Admin Center

Questions?



