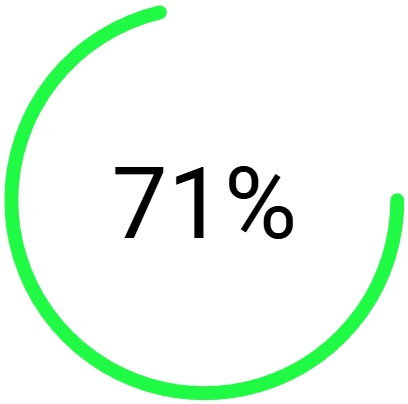
September 19, 2025

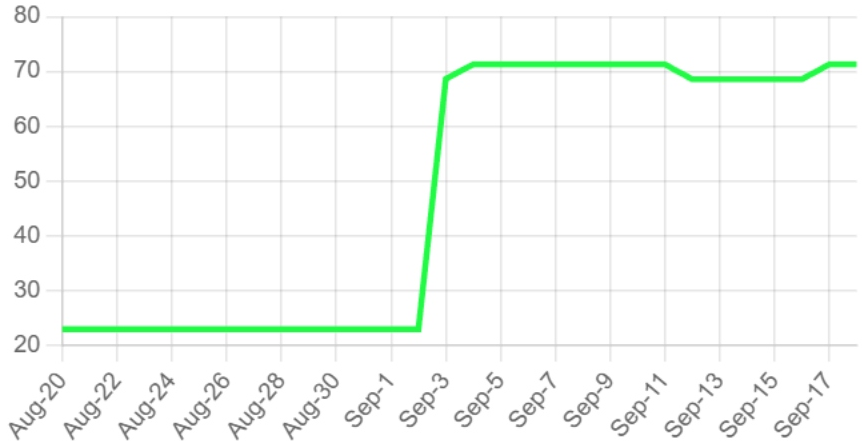
T-Minus 365
Cloud Assessment Report

Executive Summary

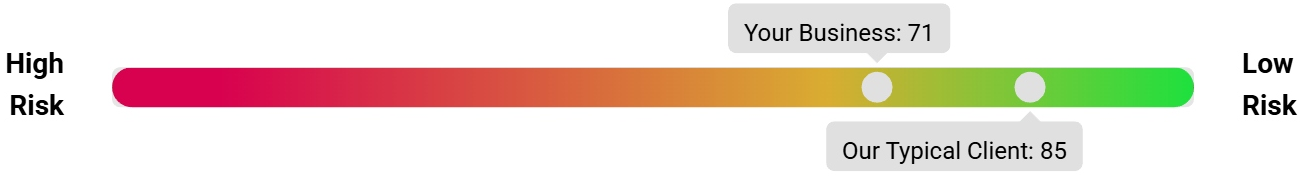
Secure Score



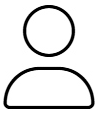
790/1108



The Secure Score is a reflection of your organization's security posture. It is a measure of how well your organization is leveraging the security features in Microsoft 365. The Secure Score is calculated based on the security features that you have enabled and the actions that you have taken to protect your organization. The higher the score, the more secure your organization is.



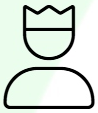
User Health



55

Total Users

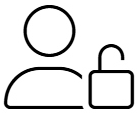
The total number of users in the tenant. This includes all users, registered in Entra including unlicensed users, guest users, and service accounts.



5

Tenants should have 2-4 users with the Global Administrator role

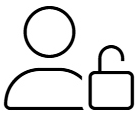
Global Administrators have full access to all administrative features in the tenant. It is recommended to have at least two global administrators to ensure that there is always a backup in case one administrator is unavailable. Excessive global administrators can increase the risk of unauthorized access to the tenant.



22

Users without Multi-Factor Authentication

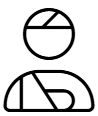
Multi-Factor Authentication (MFA) is a security feature that requires users to provide two or more verification factors to sign in to their account. Users without MFA are at a higher risk of unauthorized access to their account.



1

Users with weak Multi-Factor Authentication

Users with weak Multi-Factor Authentication (MFA) have MFA enabled, but are using weak authentication methods. Weak authentication methods include SMS, Voice, and Email. These methods are less secure than other MFA methods and can be more easily compromised.

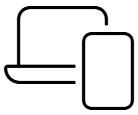


0

Users with risky sign-ins

Risky users are users who have had risky sign-ins. Risky sign-ins can indicate that a user's account has been compromised or is at risk of being compromised. It is important to review risky users and take action to secure their accounts.

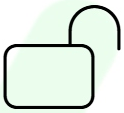
Device Health



30

Devices enrolled in Microsoft Entra

Entra is a device management solution that provides a single pane of glass for managing devices across multiple platforms.



2

Devices without encryption enabled

Devices without encryption enabled are at risk of data exposure due theft or loss.

3

Devices that are not compliant with the organization's security policies

Devices that are not compliant with the organization's security policies are at risk of being compromised and should be investigated immediately.

19

Devices that have not been used in the last 30 days

Stale Devices are at greater risk of being compromised due to lack of security updates and patches and potential loss or theft.

Applications & Data

Default Sharing Policy

Anyone

By default, links are generated which can be accessed by anyone internal or external to the organization

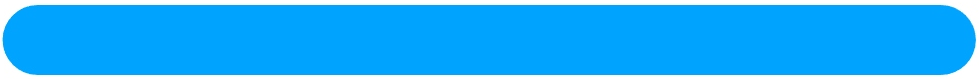
Top Risky Applications

Nodejs	1 Device Count	22 Weaknesses	Public Exploit
Python	1 Device Count	8 Weaknesses	Public Exploit
Git	1 Device Count	8 Weaknesses	Public Exploit
Edge Chromium-Based	1 Device Count	5 Weaknesses	Public Exploit
Visual Studio Code	1 Device Count	6 Weaknesses	Public Exploit

Email Health

tminus365.com Domain	Yes Default	SPF Check	Verified	DMARC - Quarantine
tminus365com.mail.onmicrosoft.com Domain	No Default	SPF Check	Verified	DMARC
tminus365com.onmicrosoft.com Domain	No Default	SPF Check	Verified	DMARC

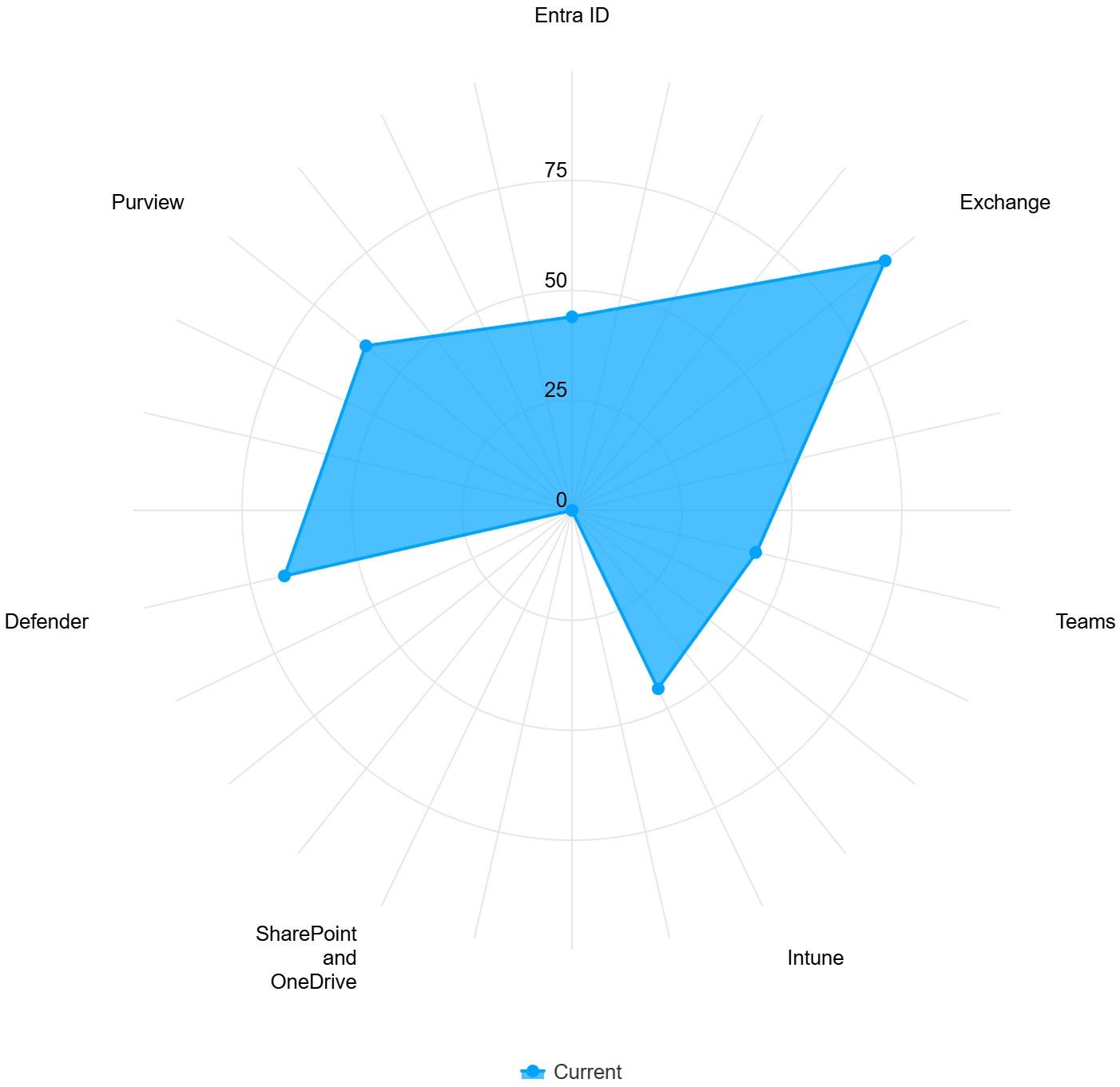
752
Emails Scanned



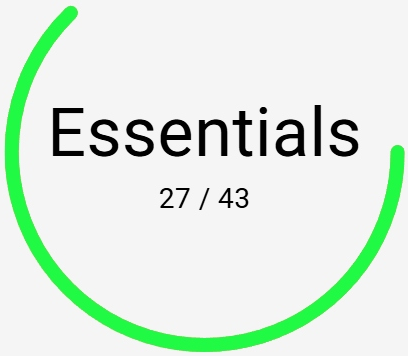
664
Emails Delivered

88
Emails Blocked

Microsoft Security Baseline



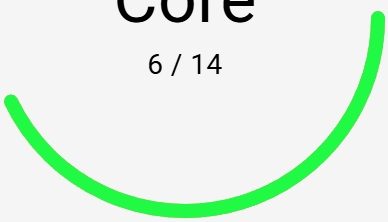
Microsoft Security Baseline Overview



Essentials

27 / 43

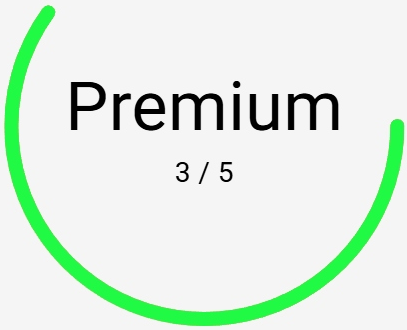
- 27 - Passed
- 11 - Failed
- 0 - Assumed Risk
- 5 - Not Set



Core

6 / 14

- 6 - Passed
- 5 - Failed
- 0 - Assumed Risk
- 3 - Not Set



Premium

3 / 5

- 3 - Passed
- 2 - Failed
- 0 - Assumed Risk
- 0 - Not Set

Advanced

2 / 9

- 2 - Passed
- 3 - Failed
- 0 - Assumed Risk
- 4 - Not Set

Exclude unset results

1 - Entra ID

1.1 - Multi-factor authentication is enforced for all users
A conditional access policy that enforces MFA for all users, excluding a break glass account.

- MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.
- MFA is enforced for Azure Management
  Conditional Access Policy found that enables MFA for Azure Management.
- Users are enrolled in MFA and covered by a policy
  22 users do not have MFA enabled

1.2 - MFA is required for all Admins

- MFA is enforced on accounts with highly privileged roles
  Conditional Access Policy found that is enforcing MFA for admins.

1.3 - Legacy Authentication is blocked

- Legacy Authentication shall be blocked
  Conditional Access Policy found

1.4 - Break Glass users are created for emergency access

- Break Glass users are created for emergency access
  Manual.

1.5 - Ensure that between two and four global admins are designated

- Ensure that between two and four global admins are designated
  5 Global admin were detected.
  high

1.6 - Highly privileged accounts shall be cloud-only

- Ensure Administrative accounts are cloud-only
  All Global Admins are cloud-only.

1.7 - Non-admin users shall be prevented from providing consent to 3rd party applications

- Only Admins shall be allowed to register 3rd party applications
  Authorization Policy
- Non-admin users shall be prevented from providing consent to 3rd party applications
  Authorization Policy.

1.8 - Guest users have limited access to properties and memberships of directory objects

Guest users have limited access to properties and memberships of directory objects
Guest users have limited access to properties and memberships of directory objects.

1.9 - Passwords shall not expire

Passwords shall not expire
Passwords do not expire.

1.10 - MFA shall be required to enroll devices to Azure AD

MFA shall be required to enroll devices to Azure AD
A conditional access policy is either missing or misconfigured.

1.11 - Local Administrator settings are configured for device joins

Local Administrator settings are configured for device joins
Local Administrator settings are configured for device joins.

1.12 - Dormant Accounts are disabled with 45 days of Inactivity

Dormant accounts are disabled after 45 days
30 accounts were found active that have not signed in for over 45 days.
medium

1.13 - Browser Sessions are limited for Privileged Users

Browser Sessions shall not be persistent for privileged users
No conditional access policy found.

1.14 - Devices shall be deleted that haven't checked in for over 30 days

Devices shall be deleted that haven't checked in for over 45 days.
19 Devices have not checked in for 45+ days
medium

1.15 - All corporate approved applications are cataloged and periodically reviewed

All corporate approved applications are cataloged and periodically reviewed
74 Enterprise applications were detected.

1.16 - Dynamic Groups are leveraged for automated group management

Dynamic Groups are leveraged for automated group management
Dynamic Group(s) detected.

1.17 - MFA Shall be required for Intune Enrollment

MFA Shall be required for Intune Enrollment
A conditional access policy is either missing or misconfigured.

- **1.18 -** Require Managed Devices for Sign in
  - Managed Devices shall be required for authentication
    No conditional access policy found.
- **1.19 -** Device Compliance is required for access to resources
  - Noncompliant devices shall be blocked from accessing corporate resources.
    No conditional access policy found or misconfigured
- **1.20 -** Require Phishing Resistant MFA for Admins
  - Ensure 'Phishing-resistant MFA strength' is required for Administrators
    MFA used for authenticating administrators is not phishing resistant
- **1.21 -** High risk users and sign-ins are blocked
  - Ensure 'sign-in risk' is blocked for medium and high risk
    No conditional access policy found
- **1.22 -** Privileged Identity Management (PIM) is configured for JIT access
  - Ensure 'Privileged Identity Management' is used to manage roles
    Not Set
  - Ensure approval is required for Global Administrator role activation
    Manual.
- **1.23 -** Microsoft Sentinel in configured in ingest logs from Entra and Defender
  - Microsoft Sentinel shall be configured to ingest log information
    Manual.

2 - Exchange

2.1 - SPF, DKIM, and DMARC records are set up for every domain

- Ensure that SPF records are published for all Exchange Domains
  SPF configured for primary domain
- Ensure DMARC Records for all Exchange Online domains are published
  DMARC configured for all custom domains
- Ensure that DKIM is enabled for all Exchange Online Domains
  DKIM enabled for primary domain

2.2 - Anti-spam policies are configured

- Inbound Anti-Spam Protections SHALL Be Enabled.
  Anti-spam policy detected.

2.3 - Anti-phishing policies are configured

- Ensure that an anti-phishing policy has been created
  Antiphishing policy with targeted user protection found

2.4 - Anti-malware policies are configured

- Zero-hour auto purge (ZAP) for malware SHOULD be enabled in the default antimalware policy and in all existing custom policies.
  Anti-malware policy found with Zap Enabled
- Ensure the Common Attachment Types Filter is enabled
  Anti-malware policy found with Common Attachment filter enabled

2.5 - Automatic forwarding to external domains SHALL be disabled

- Automatic forwarding to external domains SHALL be disabled
  1 Exchange Transport Rule found.

2.6 - Mailbox Auditing SHALL Be Enabled

- Ensure 'AuditDisabled' organizationally is set to 'False'
  Mailbox Logging Enabled.

2.7 - Calendar and Contact Sharing Shall Be Restricted

- Ensure 'External sharing' of calendars is not available
  Sharing policy is not configured to restrict calendar and contact sharing.

2.8 - External Sender Warnings are Implemented

Ensure email from external senders is identified

1 Exchange Transport Rule found.

3 - Teams

3.1 - External User Access SHALL Be Restricted

- Ensure external domains are restricted in the Teams admin center
  Teams Policy misconfigured.

3.2 - External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings

- Ensure external participants can't give or request control
  Teams Policy configured accurately.

3.3 - Anonymous Users SHALL NOT Be Enabled to Start Meetings

- Ensure anonymous users and dial-in callers can't start a meeting
  Teams Policy misconfigured.

3.4 - Automatic Admittance to Meetings SHOULD Be Restricted

- Ensure only people in my org can bypass the lobby
  Teams Policy misconfigured.

3.5 - Unmanaged users SHALL NOT be enabled to initiate contact with internal users.

- Unmanaged users SHALL NOT be enabled to initiate contact with internal users.
  Teams Policy misconfigured.

3.6 - Contact with Skype Users SHALL Be Blocked.

- Ensure communication with Skype users is disabled
  Teams Policy configured accurately.

3.7 - File Sharing and File Storage Options shall be blocked

- Ensure external file sharing in Teams is enabled for only approved cloud storage services
  3rd party file sharing is blocked in Teams

4 - Intune

4.1 - Automated patching is performed on all devices
Patching is enforced using Windows Update Rings or a 3rd party (RMM)

- Windows Update Rings shall be configured for Windows Devices
  4 policies found in Intune. 19 devices that need patching.
- Update Policies shall be configured for Apple Devices
  Update policy found in Intune.

4.2 - Managed devices are enrolled in MDM

- Managed Devices are enrolled in MDM
  Manual

4.3 - Personal Devices should be restricted from enrolling into the MDM solution

- Personal Devices should be restricted from enrolling into the MDM solution
  2 Personal Devices are enrolled into Intune

4.4 - Security Baselines should be configured for Windows Devices

- Security Baselines should be configured for Windows Devices
  Security Baseline policy configured in Intune.

4.5 - Devices compliance policies shall be configured for every supported device platform

- Devices compliance policies shall be configured for every supported device platform
  Device Compliance policies discovered.

4.6 - All devices have drive encryption applied

- Encryption shall be required on all devices
  2 were found that are not encrypted.
  high

4.7 - Lockout screen and password settings shall be configured for each device

- Lockout screen and password settings shall be configured for each device
  Secure Score Controls.

4.8 - App Protection policies should be created for mobile devices

- App Protection policies should be created for mobile devices
  Polices are in Intune for iOS and Android

- [x] **4.9 -** Approved 3rd party applications are deployed and patched
  - [x] Authorized Applications should be deployed to managed devices
    Applications are being deployed through Intune
- [ ] **4.10 -** Local Administrators passwords are managed with LAPS
  - [ ] Enable Microsoft Entra Local Administrator Password Solution (LAPS)
    Manual

5 - SharePoint and OneDrive

- ✗ **5.1 -** Default sharing settings are set for New and Existing Guest
  - ✗ Ensure SharePoint external sharing is managed through domain whitelist/blacklists
    Secure Score Controls.
  - ○ Ensure link sharing is restricted in SharePoint and OneDrive
    Manual.
- ○ **5.2 -** Expiration Dates are set for Anyone links
  - ○ Expiration Date SHOULD Be Set for Anyone Links
    Manual.

6 - Defender

○ **6.1 -** Security Awareness training is conducted at least once per year

  ○ Attack simulations shall be periodically conducted
  Manual

✓ **6.2 -** Anti-virus protections are applied to all devices
Anti-virus protections are configured for Defender or a 3rd party AV

  ✓ Microsoft Defender Antivirus is deployed and managed through Microsoft Intune
  Microsoft Defender Antivirus policy configured in Intune.

✓ **6.3 -** Endpoint detection and response software is running on all devices

  ✓ Devices shall be enrolled for Defender for Business or Defender for Endpoint
  1 enrolled in Defender

✗ **6.4 -** Firewall protections configured on devices

  ✗ Firewall Policies are configured for Windows Devices
  No Windows firewall policy found in Intune.

✓ **6.5 -** Safe Links policies are configured

  ✓ Safe Links policies are configured
  Safe Links Policy Found.

✓ **6.6 -** Safe Attachment policies are configured

  ✓ Ensure Safe Links for Office Applications is Enabled
  Active Safe Attachment policy found

○ **6.7 -** Tamper Protection is configured

  ○ Turn on Tamper Protection
  Manual

✓ **6.8 -** Attack Surface reduction rules are configured

  ✓ Attack Surface Reduction rules shall be configured
  Attack Surface reduction policy configured in Intune.

✓ **6.9 -** Defender for Cloud Apps is configured to monitor applications on the network

  ✓ Cloud App Discovery is configured and apps are periodically reviewed
  Your tenant is licensed for Defender for Cloud Apps

7 - Purview

- **7.1 -** Periodic backups are performed for email, files, and Servers
  - Maintain 3rd party backups of Microsoft 365 data
    Manual
- **7.2 -** Audit Logging SHALL Be Enabled
  - Audit Logging SHALL Be Enabled
    Audit Logging Enabled.
- **7.3 -** Retention Polices are configured
  - Retention Policies shall be configured
    Manual
- **7.4 -** Sensitivity Labels are configured
  - Information Protection Labels shall be configured
    Secure Score Controls.
- **7.5 -** Data Loss Prevention Policies are configured
  - Data loss prevention policies shall be configured
    Secure Score Controls.