



Microsoft 365 Security Assessment

Searchcore Ltd (fictional sample) · searchcore.example · Sign-in history: last 30 days · Entra ID P1 detected (no P2)

Summary

OVERALL RISK

Critical

3

CRITICAL

6

HIGH

9

MEDIUM

4

LOW

The most urgent problem: **1 admin account can sign in with a password alone**. The findings below are in order of urgency; fixing the Critical and High items closes the most likely ways into the business.

What we checked

AREA	RESULT	QUESTION
Microsoft Secure Score	1 finding	How does Microsoft score your setup, compared with similar organisations, and what would raise it most?
MFA registration	2 findings	Which accounts, especially admins, can still sign in with just a password?
Sign-in protection	2 findings	Is MFA actually enforced, by Conditional Access policies or by Microsoft's Security Defaults?
Admin accounts	1 finding	Are admin rights limited to the right people, on accounts built for the job?
Unused accounts	1 finding	Which enabled accounts has nobody signed in to for 90 days or more?
App consents	3 findings	Which third-party apps has someone allowed to read mail or files on their behalf?
Guest access	2 findings	Who can invite outsiders in, how much can guests see, and are old guests still active?
External sharing	2 findings	How far can files in SharePoint and OneDrive be shared outside the business?
Mailbox rules	3 findings	Are any inboxes silently forwarding mail outside the business, or hiding replies?

AREA	RESULT	QUESTION
Sign-in history	4 findings	Signs of password guessing, logins from unexpected countries, or impossible travel.
Recent admin changes	1 finding	In the last 30 days, were admin rights granted, protections weakened, or app credentials added?
Risky users	Not on your licence	Accounts Microsoft has already flagged as at risk.

Findings and fixes

Critical 1 · MFA registration

1 admin account can sign in with a password alone

An admin account is the master key to the tenant. With only a password, one phishing email or one reused password hands an attacker control of every mailbox and file.

EVIDENCE

- admin@searchcore.example (Global Administrator)

Fix: Register an authenticator app or security key for each account today, then require MFA for every admin (Security Defaults or a Conditional Access policy).

Critical 2 · Sign-in protection

Nothing forces anyone to use MFA when they sign in

Even users who have registered MFA can be signed in with just a password if nothing requires the second step. This is how most Microsoft 365 takeovers happen.

EVIDENCE

- Security Defaults is switched off.
- No switched-on Conditional Access policy requires MFA.

Fix: Create a Conditional Access policy requiring MFA for all users (exclude one break-glass account), or switch on Security Defaults.

Critical 3 · Mailbox rules

1 inbox rule forwards mail outside the business

A forwarding rule is the classic sign of a taken-over mailbox: the attacker reads every message, including invoices they can later fake.

EVIDENCE

- sam@searchcore.example: rule 'Sync' sends mail to sam.archive2024@webmail.example.net

Fix: Confirm with each person whether they set this up. If not: delete the rule, reset their password, sign them out everywhere, and check their recent sign-ins. Then block automatic external forwarding in Exchange (outbound spam policy).

High 4 · App consents

1 app can read or change data for the whole organisation

A malicious app with these permissions keeps reading mail even after passwords are changed, because it never needs the password again.

EVIDENCE

- PDF Converter Pro (unverified publisher): Mail.Read (approved for everyone)

Fix: Confirm each app is one you use and trust. Revoke any you don't (Entra admin centre > Enterprise applications > the app > Permissions), and stop users approving apps themselves.

High 5 · Mailbox rules

1 inbox rule hides messages about payments

Attackers hide replies about invoices so the victim never sees the customer asking about changed bank details.

EVIDENCE

- sam@searchcore.example: rule '.' moves and marks as read mail mentioning "invoice", "bank details"

Fix: Check with each person. Unexplained rules like this should be deleted and the account treated as compromised.

High 6 · Sign-in history

Password guessing against 1 account

Repeated failures from outside are someone trying passwords. It only takes one to work.

EVIDENCE

- phil@searchcore.example: 412 wrong-password attempts from 6 IP addresses

Fix: Make sure each account has MFA registered and enforced, and that old sign-in methods are blocked. A long unique password stops guessing; MFA stops a leaked one.

High 7 · Sign-in history

1 account still signs in with old methods that bypass MFA

Old protocols like IMAP, POP and basic SMTP cannot ask for MFA, so a stolen password is enough.

EVIDENCE

- lee@searchcore.example: IMAP4 (1 sign-in)

Fix: Move these devices or apps to modern sign-in (current Outlook / mobile mail apps), then block legacy authentication (Security Defaults does this, or a Conditional Access policy).

High 8 · Sign-in history

Impossible travel on 1 account

Two successful sign-ins from countries too far apart to travel between usually means two different people.

EVIDENCE

- sam@searchcore.example: GB then NG 60 minutes apart (5,269 km), 5 Oct 04:43 UTC

Fix: Unless the person uses a VPN, treat the account as compromised: reset the password, revoke sessions, and check mailbox rules and app consents.

High 9 · Recent admin changes

Admin rights were granted (1 change in 30 days)

Attackers who get in quietly give themselves admin rights, weaken protections or plant app credentials so they keep access after a password reset.

EVIDENCE

- 5 Oct 05:43 UTC · Privileged role granted – Global Administrator (Add member to role) · by sam@searchcore.example

Fix: Confirm each change with the person who made it. Anything nobody recognises should be reversed and treated as a possible compromise of the account that made it.

Medium 10 · Microsoft Secure Score

Secure Score is 34%, below similar organisations (48%)

Secure Score is Microsoft's own measure of how well the protections you already pay for are switched on.

EVIDENCE

- Ensure multifactor authentication is enabled for all users in administrative roles (+10 points)
- Enable Conditional Access policies to block legacy authentication (+8 points)
- Ensure multifactor authentication is enabled for all users (+5 points)
- Enable self-service password reset (+1 points)

Fix: Work through Microsoft's top recommendations (listed as evidence) in the Microsoft Defender portal > Secure Score > Recommended actions. Many take minutes and cost nothing.

Medium 11 · MFA registration

4 of 12 users have no MFA method registered

Accounts without MFA are the ones attackers take over with guessed or leaked passwords.

EVIDENCE

- admin@searchcore.example
- lee@searchcore.example
- mo@searchcore.example
- test@searchcore.example

Fix: Ask each person to register the Microsoft Authenticator app (aka.ms/mfasetup), then enforce MFA so nobody can skip it.

Medium 12 · Sign-in protection

2 Conditional Access policies only report and do not protect

A report-only policy records what it would have blocked, but blocks nothing.

EVIDENCE

- 'Require MFA for all users' is in report-only mode
- 'Block legacy authentication' is in report-only mode

Fix: Check each policy's report-only results, then switch it to On (start with a pilot group if unsure).

Medium 13 · Unused accounts

2 enabled accounts unused for 90+ days

Nobody notices when an unused account is taken over, which makes leavers' accounts a favourite way in.

EVIDENCE

- `test@searchcore.example`: last signed in 14 Mar 2026 (licensed)
- `dana@searchcore.example`: last signed in 5 Jun 2026 (licensed)

Fix: Confirm each with its manager. Disable accounts for people who have left, and remove their licences (licensed ones are also costing you money). Shared mailboxes don't need sign-in at all; block sign-in on them.

Medium 14 · App consents

1 app holds high-risk permissions for individual users

"Consent phishing" tricks one person into approving a fake app, which then reads their mail silently.

EVIDENCE

- `QuickNotes Sync: Files.Read.All` (1 user)

Fix: Review each app with the people who approved it, and revoke any nobody recognises.

Medium 15 · App consents

Staff can approve any app's access to their data

This is how consent phishing works: one click by one person gives an attacker's app lasting access.

EVIDENCE

- User consent is set to 'Allow user consent for apps' (all apps, any publisher).

Fix: Limit it to 'apps from verified publishers, for low-risk permissions', or require admin approval, with an approval workflow so staff can still ask: Entra admin centre > Enterprise applications > Consent and permissions.

Medium 16 · Guest access

Anyone, including existing guests, can invite more guests

A guest who can invite other guests can bring outsiders into your files and Teams without anyone at your business deciding.

EVIDENCE

- Entra setting 'Guest invite restrictions' allows everyone (the Microsoft default).

Fix: Restrict invitations to admins and the Guest Inviter role, or at least to staff (not guests): Entra admin centre > External Identities > External collaboration settings.

Medium 17 · External sharing

Files can be shared with 'anyone' links that need no sign-in

An 'anyone' link works for whoever has it: forwarded, posted or leaked, and there's no record of who opened it.

EVIDENCE

- SharePoint external sharing is set to 'Anyone'.

Fix: Change it to 'New and existing guests' so people outside must sign in, or keep 'Anyone' but set those links to expire and to view-only: SharePoint admin centre > Policies > Sharing.

Medium 18 · Sign-in history

Successful sign-ins from outside GB

A successful sign-in from an unexpected country is the most common sign a password has been stolen.

EVIDENCE

- sam@searchcore.example: 1 sign-in(s) from NG, last 5 Oct

Fix: Confirm each was a trip or a known remote worker. Any that weren't: reset the password, revoke sessions, and check the account's mailbox rules.

Low 19 · Admin accounts

3 admin accounts are also used for everyday email

Everyday accounts read email and browse the web, which is where phishing lands. An admin role on that same account makes one click far more damaging.

EVIDENCE

- admin@searchcore.example
- jo@searchcore.example
- sam@searchcore.example

Fix: Give admins a separate, unlicensed admin account and keep their everyday account (email, Teams) unprivileged.

Low 20 · Guest access

1 guest unused for 90+ days

Old guest accounts keep access to whatever they were shared, long after the project ended.

EVIDENCE

- accountant_partner.example#EXT#@searchcore.onmicrosoft.com: last signed in 9 Sep 2025

Fix: Remove guests who no longer need access, and consider Entra access reviews for guests (needs P2) or a quarterly manual check.

Guests can re-share your files with other people

Once a guest can re-share, you no longer control who outside the business ends up with your files.

EVIDENCE

- 'Allow guests to share items they don't own' is switched on.

Fix: Switch it off: SharePoint admin centre > Policies > Sharing > More external sharing settings.

1 inbox rule deletes or hides incoming mail

Rules that silently hide mail are also a common attacker trick, so it is worth a quick check.

EVIDENCE

- tom@searchcore.example: rule 'Newsletters' deletes incoming mail

Fix: Usually harmless (newsletters, alerts), but confirm each person recognises their rule.

Detail by area

Microsoft Secure Score	• Score 142 of 412 (34%), as calculated by Microsoft on 2026-10-12. • Organisations of a similar size average 48%.
MFA registration	• 12 user accounts checked; 8 have MFA registered (66%). • 3 accounts hold an admin role; 1 without MFA.
Sign-in protection	• Security Defaults is OFF. • 2 Conditional Access policies: 0 on, 2 report-only, 0 off.
Admin accounts	• 3 accounts hold an admin role; 2 are Global Administrators.
Unused accounts	• 12 enabled member accounts checked against their last successful sign-in.
App consents	• 2 app permission grants reviewed.
Guest access	• 1 guest accounts (1 enabled).
External sharing	Checked.
Mailbox rules	• 12 mailboxes checked; 3 inbox rules reviewed.
Sign-in history	• 715 sign-ins over 30 days: 303 succeeded, 412 rejected for a wrong password or username, 0 stopped by a control (e.g. an MFA prompt or a block). • Most sign-ins come from GB.

Recent admin changes

- 1 admin and configuration changes reviewed over 30 days.

Risky users

Microsoft's risky-user verdicts need Entra ID P2 (e.g. Microsoft 365 E5).

How this assessment was done

Kempcore read your Microsoft 365 settings and logs on 14 October 2026 through a read-only app approved by your administrator. The app could read settings and logs only; it could not change, send or delete anything. Every finding was reviewed by a person before this report was issued.

Permissions used (all read-only): Organization.Read.All, User.Read.All, Directory.Read.All, Policy.Read.All, AuditLog.Read.All, UserAuthenticationMethod.Read.All, MailboxSettings.Read, IdentityRiskyUser.Read.All, SecurityEvents.Read.All, SharePointTenantSettings.Read.All.

This report reflects your tenant on the date above. It reduces risk but cannot guarantee that no attack will succeed. Out of scope: devices, on-premises servers, firewalls, email filtering and phishing tests. Collected data is deleted within 30 days of delivery.