Security posture report

Briarfield Group

Prepared by Example Advisory · 28 July 2026 to 26 October 2026 · Generated 26 October 2026 at 10:30



80, capped to Poor: no tenant-wide MFA enforcement in Briarfield Group: Security defaults are off and no Conditional Access policy requires MFA

Security score, the same as on the dashboard

1 critical issue needs action now: High-risk service exposed on remote.briarfield.example. Other gaps are in Microsoft 365 settings and website security settings.

The score rose 9 points, from 71 on 28 Jul 2026 to 80 now.

4 open findings: 1 critical, 2 high and 1 medium. 3 assets monitored, last full assessment 25 October 2026.

Score 80 would be Good. Capped to Poor because:

No tenant-wide MFA enforcement in Briarfield Group: Security defaults are off and no Conditional Access policy requires MFA (caps at Poor).

Why this score: https://securityscore.me/dashboard/why-this-score#band_cap

Top 3 risks

High-risk service exposed

Critical

remote.briarfield.example

A server found during discovery has a database, remote desktop or similar service reachable from the internet. Services like these are a common way into a network.

Microsoft Secure Score is low

High

Briarfield Group

Microsoft's own measurement shows many recommended protections are not in place. The individual actions below show what moves it most.

Security defaults disabled

High

Briarfield Group

Microsoft's free baseline (MFA for everyone, blocking legacy sign-ins) is switched off without equivalent Conditional Access policies taking its place.

What to do first

Close RDP (port 3389) on remote.briarfield.example to the internet.

Critical

High-risk service exposed · remote.briarfield.example · Immediate

How to check: Rescan the asset: the finding closes when the service no longer answers from the internet.

Work through the top Secure Score actions in Briarfield Group.

High

Microsoft Secure Score is low · Briarfield Group · Within 7 days

How to check: Sync the tenant again: the finding closes when Microsoft Secure Score is 50% or higher.

Turn on security defaults or Conditional Access in Briarfield Group.

High

Security defaults disabled · Briarfield Group · Within 7 days

How to check: Sync the tenant again: the finding closes when the next sync no longer reports it.

Publish a Content-Security-Policy that matches the site and test it in report-only mode first.

Medium

Content-Security-Policy header missing · www.briarfield.example · Within 30 days

How to check: Rescan the website: the finding closes when the setting is in the response.

Score trend, last 90 days



First point **71** on 28 July 2026, last point **80** on 26 October 2026.

Findings by area

4 open findings, grouped into 4 issues: the same issue on several assets is listed once.

Area	Score	Assessment	Open findings
Website	78	Assessed	1
Microsoft 365	70	Assessed	2
DNS	92	Assessed	0
TLS	In Website score	Covered by Website scan	0
HTTP headers	In Website score	Covered by Website scan	1
Identity	In Microsoft 365 score	Covered by Microsoft 365 assessment	2
Email security	In DNS score	Covered by Domain scan	0
Cookies	In Website score	Covered by Website scan	0
CORS	In Website score	Covered by Website scan	0

Microsoft 365 2 issues

Microsoft Secure Score is low

High

Briarfield Group · Open since 22 September 2026

What we found

Microsoft Secure Score is 29% (87 of 300).

Why it matters

Microsoft's own measurement shows many recommended protections are not in place. The individual actions below show what moves it most.

What to do

Work through the top Secure Score actions in Briarfield Group.

How to check

Sync the tenant again: the finding closes when Microsoft Secure Score is 50% or higher.

Security defaults disabled

High

Briarfield Group · Open since 22 September 2026

What we found

Security defaults appear to be disabled for this tenant.

Why it matters

Microsoft's free baseline (MFA for everyone, blocking legacy sign-ins) is switched off without equivalent Conditional Access policies taking its place.

What to do

Turn on security defaults or Conditional Access in Briarfield Group.

How to check

Sync the tenant again: the finding closes when the next sync no longer reports it.

Website 1 issue

Content-Security-Policy header missing

Medium

www.briarfield.example · Open since 22 September 2026

What we found

No Content-Security-Policy is sent by www.briarfield.example.

Why it matters

If an attacker manages to inject script into a page (for example through a vulnerable plugin or form), the browser will run it without limits. A CSP is the main safety net that limits the damage of such a flaw.

What to do

Publish a Content-Security-Policy that matches the site and test it in report-only mode first.

How to check

Rescan the website: the finding closes when the setting is in the response.

Exposed services and hosts 1 issue

High-risk service exposed

Critical

remote.briarfield.example · Open since 17 October 2026

What we found

remote.briarfield.example exposes RDP (3389) to the internet.

Why it matters

A server found during discovery has a database, remote desktop or similar service reachable from the internet. Services like these are a common way into a network.

What to do

Close RDP (port 3389) on remote.briarfield.example to the internet.

Evidence

Checked address: 203.0.113.24, port 3389 (RDP)

Checked on: 24 Oct 2026, 11:30

Result: A TCP connection was accepted. Nothing was sent and no banner was read, so the service was not identified: the name is the usual service on this port.

Check: Asset discovery, port test of a discovered host

Confidence: Medium: the port answered from the internet; the service is assumed from the port number.

How to check

Rescan the asset: the finding closes when the service no longer answers from the internet.

Assets

Asset	Type	Score	Last scan
briarfield.example	Domain	92	25 October 2026
www.briarfield.example	Website	78	25 October 2026
Briarfield Group	Microsoft 365	70	25 October 2026

Appendix

How the score is calculated

The security score is the average of the latest complete assessment of each monitored asset, the same score as on the dashboard. An assessment that could not run every check (scan warnings, missing Microsoft 365 permissions) never counts: the asset's last complete assessment counts instead, and an asset without one is left out as limited visibility. Score bands: Excellent from 90, Good from 80, Fair from 60, Poor from 40, Critical below 40. The band is capped when a baseline check fails, while the score itself does not change: at Poor when nothing enforces multi-factor authentication or no user has it set up, and at Fair when admin multi-factor authentication is not enforced, legacy sign-in is not blocked, or a database, remote desktop, secrets or source code on a monitored website is open to the internet. A cap is always named under the score. This is a directional indicator, not a compliance certification.

Scope and disclaimer

Assessed: external website and domain posture where registered, Microsoft 365 where connected, and the scheduled and manual scans of the report period. This report is informational and reflects point-in-time posture scans. It does not guarantee compliance with any framework or eliminate all security risk. This is not a penetration test and not a compliance certification. Findings reflect externally observable posture and connected Microsoft 365 signals available to SecurityScore.me at generation time.

About this sample

All organisations, domains, addresses, scores, dates and findings in this sample are fictional. It was produced by the same report generator as customer reports, from made-up scan results. No customer environment was accessed or assessed.