

AUGUR Assessment Report

Prepared for Contoso

ASSESSMENT DATE 2026-06-23 19:15 UTC
PREPARED BY Ironwright Labs

METHODOLOGY AUGUR v1.8.1
ASSESSMENT ID f0d9e473-5d19-45c0-88da-b5fac89f3f87

CLIENT EXPOSURE LEVEL	1	0	9	24
Critical	CRITICAL PRINCIPALS	HIGH PRINCIPALS	PRINCIPALS ASSESSED	FINDINGS

1 Scope & Limitations

This assessment reads tenant configuration only. Message content, file content, and email body text are never inspected. Conditional Access policies are not evaluated and do not raise or lower scores. Power Automate trigger-to-action paths are not fully parsed; flow findings are presence flags requiring manual review. SharePoint effective permissions are approximated through the identity layer; per-site permission inheritance is not enumerated. Severity reflects structural exposure at the time of assessment. Configuration changes between assessment runs are not visible until the next run.

2 Principal Heatmap

PRINCIPAL	DATA ACCESS	INBOUND SURFACE	OUTBOUND ACTION	RATING	FINDINGS
Tenant	● Path	● Path	● Direct	Critical	6
jackie@contoso.onmicrosoft.com	● Path	● Presence	—	Elevated	4
21815124-4742-47f0-9ee5-6a9426c07cdd	● Direct	—	—	Low	1
61d26025-bd7d-406b-8652-8c6b46e2f9e2	● Direct	—	—	Low	1
8a7bb3aa-9edb-40af-b95a-013fe4b0c34e	● Direct	—	—	Low	1
admin@contoso.onmicrosoft.com	—	● Presence	—	Low	3
morgan@contoso.onmicrosoft.com	—	● Presence	—	Low	3
jane@contoso.onmicrosoft.com	—	● Presence	—	Low	3

PRINCIPAL	DATA ACCESS	INBOUND SURFACE	OUTBOUND ACTION	RATING	FINDINGS
john@contoso.onmicrosoft.com	—	● Presence	—	Low	2

3 Findings by Principal

Critical Tenant

● Direct OutboundAction.McpConnector.HighImpact

OUTBOUND ACTION

App:Nomad - SharePoint Migration (b9b4cdfe-6397-4186-802f-6684cb07f715): Files.ReadWrite.All, Sites.ReadWrite.All, User.Read

Service principal 'Nomad - SharePoint Migration' is an unrecognized publisher (AI attribution unconfirmed) holding delegated consent for scope(s) 'Files.ReadWrite.All, Sites.ReadWrite.All, User.Read'. An AI assistant invoking this connector could act with these permissions, with no per-request approval step.

RECOMMENDATION

Confirm 'Nomad - SharePoint Migration' is an authorized AI tool connector and that its delegated scopes are the minimum required. Revoke unused consents. Treat any write/send scope as an injection-to-action path.

● Path InboundSurface.GuestSharing

INBOUND SURFACE

SharePoint.sharingCapability=externalUserAndGuestSharing

SharePoint tenant sharing capability is set to 'externalUserAndGuestSharing'. External users may share files with principals in this tenant, creating an inbound content surface.

RECOMMENDATION

Set SharePoint sharing to the most restrictive level that meets business requirements. Review per-site sharing settings. Anonymous sharing (AnyoneCanShare) should be disabled unless explicitly required.

● Path DataAccess.Files.BroadPermission

DATA ACCESS

SharePoint.sharingCapability=externalUserAndGuestSharing

SharePoint tenant sharing capability 'externalUserAndGuestSharing' permits external access to files. Per-site enumeration of effective permissions is out of scope for this assessment; this finding reflects the tenant-level policy floor.

RECOMMENDATION

Audit SharePoint site collection permissions. Disable anonymous links. Review Files.ReadWrite.All application permissions in DataAccess findings.

AuthorizationPolicy.AllowInvitesFrom=everyone

Guest invitation policy allows 'everyone' to invite external users to the tenant. Non-administrative users can introduce external identities into the tenant.

RECOMMENDATION

Restrict AllowInvitesFrom to 'adminsAndGuestInviters' or 'adminsOnly' to limit who can introduce external guest accounts.

MicrosoftForms

Microsoft Forms is enabled tenant-wide. Forms collect untrusted external input that can flow into files, lists, or email that an AI assistant later reads and acts on, creating a prompt-injection path. Microsoft exposes no Graph or admin API to enumerate forms or their configuration, so this surface cannot be measured programmatically. This is a presence / manual-audit stub, not a measured finding.

RECOMMENDATION

Manually audit Microsoft Forms at admin.microsoft.com -> Settings -> Org settings -> Microsoft Forms. Review External sharing (four options, all enabled by default) and restrict external form sharing and response collection unless required. Confirm internal phishing protection is enabled. Review the "record names of people in your org" setting. There is no programmatic API for these controls; this audit is manual.

TransportConfig

Organization is configured to accept inbound email from external senders. This is the default state and applies to all mailboxes not individually restricted.

RECOMMENDATION

Confirm inbound external email is intentional for all recipient mailboxes. Review per-mailbox RequireSenderAuthenticationEnabled settings via Get-InboundSurfaceFindings.

Elevated

jackie@contoso.onmicrosoft.com

● Path

DataAccess.Mailbox.Delegated

DATAACCESS

jackie@contoso.onmicrosoft.com -> testmc@contoso.onmicrosoft.com

Delegated FullAccess granted from mailbox 'jackie@contoso.onmicrosoft.com' to 'testmc@contoso.onmicrosoft.com'. The delegate can read and manage all mail in this mailbox.

RECOMMENDATION

Review whether 'testmc@contoso.onmicrosoft.com' requires FullAccess to 'jackie@contoso.onmicrosoft.com'. Remove delegated access that is no longer required. Consider whether this mailbox is a target for AI-assisted triage.

● Presence

InboundSurface.ExternalEmail

INBOUNDSURFACE

jackie@contoso.onmicrosoft.com mailbox

Mailbox 'jackie@contoso.onmicrosoft.com' accepts inbound email from external (unauthenticated) senders (RequireSenderAuthenticationEnabled = False). External parties can deliver content to this mailbox.

RECOMMENDATION

This is the default state for user mailboxes and is usually intentional. If this mailbox is a high-value target or attached to an AI assistant, consider enabling RequireSenderAuthenticationEnabled or adding transport rules to tag or quarantine external mail.

● Presence

InboundSurface.GuestSharing

INBOUNDSURFACE

jackie@contoso.onmicrosoft.com SharePoint/OneDrive

User 'jackie@contoso.onmicrosoft.com' has a Microsoft 365 license that includes SharePoint/OneDrive. External users may share files with this principal via guest sharing links if tenant sharing policy permits (see Tenant findings).

RECOMMENDATION

Review tenant-level SharePoint sharing policy in DataAccess.Files.BroadPermission and InboundSurface.GuestSharing Tenant findings. Restrict sharing to known external users or disable external sharing for high-value principals.

jackie@contoso.onmicrosoft.com Teams presence

User 'jackie@contoso.onmicrosoft.com' is a Teams-capable account. If tenant-level external federation is enabled (see Tenant findings), external parties may initiate Teams messages to this user. Per-user policy granularity was not collected in this run (MicrosoftTeams module or connection unavailable).

RECOMMENDATION

Review tenant-level Teams federation in InboundSurface.TeamsExternal Tenant findings. To assess per-user policy, install the MicrosoftTeams module and re-run, or run Get-CsExternalAccessPolicy / Get-CsOnlineUser manually.

Low 21815124-4742-47f0-9ee5-6a9426c07cdd

Ironwright-AUGUR-Assessment (a8c02843-018d-4ccf-8c2e-98a20212c468): Mail.Read

Service principal 'Ironwright-AUGUR-Assessment' holds Graph application permission(s) 'Mail.Read'. Application permissions grant tenant-wide mailbox read access with no per-mailbox boundary.

RECOMMENDATION

Verify 'Ironwright-AUGUR-Assessment' requires tenant-wide mailbox access. If read access is needed for a single mailbox only, implement resource-specific consent (RSC) to scope the permission. Remove unused application permissions.

Low 61d26025-bd7d-406b-8652-8c6b46e2f9e2

Nomad - SharePoint Migration (b9b4cdfc-6397-4186-802f-6684cb07f715): Files.ReadWrite.All

Service principal 'Nomad - SharePoint Migration' holds Graph application permission(s) 'Files.ReadWrite.All'. Application permissions grant tenant-wide file access across all SharePoint sites and OneDrive accounts.

RECOMMENDATION

Verify 'Nomad - SharePoint Migration' requires tenant-wide file access. Scope permissions using site-specific app registration where possible. Remove unused application permissions.

Low

8a7bb3aa-9edb-40af-b95a-013fe4b0c34e

● **Direct** **DataService.Graph.FilesRead**

DATAACCESS

Nomad-BenchTest (7b5d7693-5e66-43d3-8a77-9a35f78e8ff2): Files.ReadWrite.All

Service principal 'Nomad-BenchTest' holds Graph application permission(s) 'Files.ReadWrite.All'. Application permissions grant tenant-wide file access across all SharePoint sites and OneDrive accounts.

RECOMMENDATION

Verify 'Nomad-BenchTest' requires tenant-wide file access. Scope permissions using site-specific app registration where possible. Remove unused application permissions.

Low

admin@contoso.onmicrosoft.com

● **Presence** **InboundSurface.ExternalEmail**

INBOUNDSURFACE

admin@contoso.onmicrosoft.com mailbox

Mailbox 'admin@contoso.onmicrosoft.com' accepts inbound email from external (unauthenticated) senders (RequireSenderAuthenticationEnabled = False). External parties can deliver content to this mailbox.

RECOMMENDATION

This is the default state for user mailboxes and is usually intentional. If this mailbox is a high-value target or attached to an AI assistant, consider enabling RequireSenderAuthenticationEnabled or adding transport rules to tag or quarantine external mail.

● **Presence** **InboundSurface.GuestSharing**

INBOUNDSURFACE

admin@contoso.onmicrosoft.com SharePoint/OneDrive

User 'admin@contoso.onmicrosoft.com' has a Microsoft 365 license that includes SharePoint/OneDrive. External users may share files with this principal via guest sharing links if tenant sharing policy permits (see Tenant findings).

RECOMMENDATION

Review tenant-level SharePoint sharing policy in DataService.Files.BroadPermission and InboundSurface.GuestSharing Tenant findings. Restrict sharing to known external users or disable external sharing for high-value principals.

admin@contoso.onmicrosoft.com Teams presence

User 'admin@contoso.onmicrosoft.com' is a Teams-capable account. If tenant-level external federation is enabled (see Tenant findings), external parties may initiate Teams messages to this user. Per-user policy granularity was not collected in this run (MicrosoftTeams module or connection unavailable).

RECOMMENDATION

Review tenant-level Teams federation in InboundSurface.TeamsExternal Tenant findings. To assess per-user policy, install the MicrosoftTeams module and re-run, or run Get-CsExternalAccessPolicy / Get-CsOnlineUser manually.

Low morgan@contoso.onmicrosoft.com

morgan@contoso.onmicrosoft.com mailbox

Mailbox 'morgan@contoso.onmicrosoft.com' accepts inbound email from external (unauthenticated) senders (RequireSenderAuthenticationEnabled = False). External parties can deliver content to this mailbox.

RECOMMENDATION

This is the default state for user mailboxes and is usually intentional. If this mailbox is a high-value target or attached to an AI assistant, consider enabling RequireSenderAuthenticationEnabled or adding transport rules to tag or quarantine external mail.

morgan@contoso.onmicrosoft.com SharePoint/OneDrive

User 'morgan@contoso.onmicrosoft.com' has a Microsoft 365 license that includes SharePoint/OneDrive. External users may share files with this principal via guest sharing links if tenant sharing policy permits (see Tenant findings).

RECOMMENDATION

Review tenant-level SharePoint sharing policy in DataAccess.Files.BroadPermission and InboundSurface.GuestSharing Tenant findings. Restrict sharing to known external users or disable external sharing for high-value principals.

morgan@contoso.onmicrosoft.com Teams presence

User 'morgan@contoso.onmicrosoft.com' is a Teams-capable account. If tenant-level external federation is enabled (see Tenant findings), external parties may initiate Teams messages to this user. Per-user policy granularity was not collected in this run (MicrosoftTeams module or connection unavailable).

RECOMMENDATION

Review tenant-level Teams federation in InboundSurface.TeamsExternal Tenant findings. To assess per-user policy, install the MicrosoftTeams module and re-run, or run Get-CsExternalAccessPolicy / Get-CsOnlineUser manually.

Low jane@contoso.onmicrosoft.com

jane@contoso.onmicrosoft.com mailbox

Mailbox 'jane@contoso.onmicrosoft.com' accepts inbound email from external (unauthenticated) senders (RequireSenderAuthenticationEnabled = False). External parties can deliver content to this mailbox.

RECOMMENDATION

This is the default state for user mailboxes and is usually intentional. If this mailbox is a high-value target or attached to an AI assistant, consider enabling RequireSenderAuthenticationEnabled or adding transport rules to tag or quarantine external mail.

jane@contoso.onmicrosoft.com SharePoint/OneDrive

User 'jane@contoso.onmicrosoft.com' has a Microsoft 365 license that includes SharePoint/OneDrive. External users may share files with this principal via guest sharing links if tenant sharing policy permits (see Tenant findings).

RECOMMENDATION

Review tenant-level SharePoint sharing policy in DataAccess.Files.BroadPermission and InboundSurface.GuestSharing Tenant findings. Restrict sharing to known external users or disable external sharing for high-value principals.

● Presence

InboundSurface.TeamsExternal

INBOUNDSURFACE

jane@contoso.onmicrosoft.com Teams presence

User 'jane@contoso.onmicrosoft.com' is a Teams-capable account. If tenant-level external federation is enabled (see Tenant findings), external parties may initiate Teams messages to this user. Per-user policy granularity was not collected in this run (MicrosoftTeams module or connection unavailable).

RECOMMENDATION

Review tenant-level Teams federation in InboundSurface.TeamsExternal Tenant findings. To assess per-user policy, install the MicrosoftTeams module and re-run, or run Get-CsExternalAccessPolicy / Get-CsOnlineUser manually.

Low

john@contoso.onmicrosoft.com

● Presence

InboundSurface.GuestSharing

INBOUNDSURFACE

john@contoso.onmicrosoft.com SharePoint/OneDrive

User 'john@contoso.onmicrosoft.com' has a Microsoft 365 license that includes SharePoint/OneDrive. External users may share files with this principal via guest sharing links if tenant sharing policy permits (see Tenant findings).

RECOMMENDATION

Review tenant-level SharePoint sharing policy in DataAccess.Files.BroadPermission and InboundSurface.GuestSharing Tenant findings. Restrict sharing to known external users or disable external sharing for high-value principals.

● Presence

InboundSurface.TeamsExternal

INBOUNDSURFACE

john@contoso.onmicrosoft.com Teams presence

User 'john@contoso.onmicrosoft.com' is a Teams-capable account. If tenant-level external federation is enabled (see Tenant findings), external parties may initiate Teams messages to this user. Per-user policy granularity was not collected in this run (MicrosoftTeams module or connection unavailable).

RECOMMENDATION

Review tenant-level Teams federation in InboundSurface.TeamsExternal Tenant findings. To assess per-user policy, install the MicrosoftTeams module and re-run, or run Get-CsExternalAccessPolicy / Get-CsOnlineUser manually.

4 Remediation Priority

Address Critical principals first, then High, then by finding count.

1

Critical

Tenant

6 findings

2	Elevated	jackie@contoso.onmicrosoft.com	4 findings
3	Low	21815124-4742-47f0-9ee5-6a9426c07cdd	1 finding
4	Low	61d26025-bd7d-406b-8652-8c6b46e2f9e2	1 finding
5	Low	8a7bb3aa-9edb-40af-b95a-013fe4b0c34e	1 finding
6	Low	admin@contoso.onmicrosoft.com	3 findings
7	Low	morgan@contoso.onmicrosoft.com	3 findings
8	Low	jane@contoso.onmicrosoft.com	3 findings
9	Low	john@contoso.onmicrosoft.com	2 findings

5 Appendix — Full Finding List

FINDINGID	SEV	AXIS	PRINCIPAL	RESOURCE
OutboundAction.McpConnector.HighImpact	● Direct	OutboundAction	Tenant	App:Nomad - Share 802f-6684cb07f715 Sites.ReadWrite.A
DataAccess.Graph.MailRead	● Direct	DataAccess	21815124-4742-47f0-9ee5-6a9426c07cdd	Ironwright-AUGUR-98a20212c468): Ma
DataAccess.Graph.FilesRead	● Direct	DataAccess	61d26025-bd7d-406b-8652-8c6b46e2f9e2	Nomad - SharePoint (6684cb07f715): Fi
DataAccess.Graph.FilesRead	● Direct	DataAccess	8a7bb3aa-9edb-40af-b95a-013fe4b0c34e	Nomad-BenchTest (Files.ReadWrite.A
InboundSurface.GuestSharing	● Path	InboundSurface	Tenant	SharePoint.sharin
DataAccess.Files.BroadPermission	● Path	DataAccess	Tenant	SharePoint.sharin
InboundSurface.GuestSharing	● Path	InboundSurface	Tenant	AuthorizationPoli
DataAccess.Mailbox.Delegated	● Path	DataAccess	jackie@contoso.onmicrosoft.com	jackie@contoso.on testmc@contoso.on

FINDINGID	SEV	AXIS	PRINCIPAL	RESOURCE
InboundSurface.TeamsExternal	● Presence	InboundSurface	jackie@contoso.onmicrosoft.com	jackie@contoso.on
InboundSurface.TeamsExternal	● Presence	InboundSurface	john@contoso.onmicrosoft.com	john@contoso.onmi
InboundSurface.TeamsExternal	● Presence	InboundSurface	morgan@contoso.onmicrosoft.com	morgan@contoso.on
InboundSurface.TeamsExternal	● Presence	InboundSurface	jane@contoso.onmicrosoft.com	jane@contoso.onmi
InboundSurface.GuestSharing	● Presence	InboundSurface	admin@contoso.onmicrosoft.com	admin@contoso.onm
InboundSurface.GuestSharing	● Presence	InboundSurface	jackie@contoso.onmicrosoft.com	jackie@contoso.on
InboundSurface.GuestSharing	● Presence	InboundSurface	john@contoso.onmicrosoft.com	john@contoso.onmi
InboundSurface.ExternalEmail	● Presence	InboundSurface	jackie@contoso.onmicrosoft.com	jackie@contoso.on
InboundSurface.GuestSharing	● Presence	InboundSurface	jane@contoso.onmicrosoft.com	jane@contoso.onmi
InboundSurface.ExternalEmail	● Presence	InboundSurface	admin@contoso.onmicrosoft.com	admin@contoso.onm
InboundSurface.TeamsExternal	● Presence	InboundSurface	admin@contoso.onmicrosoft.com	admin@contoso.onm
InboundSurface.ExternalEmail	● Presence	InboundSurface	morgan@contoso.onmicrosoft.com	morgan@contoso.on
InboundSurface.ExternalEmail	● Presence	InboundSurface	jane@contoso.onmicrosoft.com	jane@contoso.onmi
InboundSurface.ExternalEmail	● Presence	InboundSurface	Tenant	TransportConfig
InboundSurface.GuestSharing	● Presence	InboundSurface	morgan@contoso.onmicrosoft.com	morgan@contoso.on

FINDINGID	SEV	AXIS	PRINCIPAL	RESOURCE
InboundSurface.Forms.Present	● Presence	InboundSurface	Tenant	MicrosoftForms