Microsoft Graph permissions statement

Olyteck Cyber — Microsoft 365 security scanner

Version	2.0
Issued	18 August 2026
Status	Final
Applies to	cyber.olyteck.com, all tenants

0. The short version

If you are reviewing this to decide whether a scan may run, these five lines are the whole answer:

1. **The scanner is read-only.** 19 application permissions, every one a `.Read.*`. It holds no write permission of any kind, and it is the only identity that runs unattended.
2. **We read metadata, not content.** No file contents, no message bodies, no attachments. Over-exposure is a property of permissions, not of content.
3. **Changing your tenant is a separate application** that you do not have to enable, that is consented separately, and that can be revoked on its own without affecting scanning.
4. **You can verify all of this in your own tenant**, in about a minute — §1 tells you which two screens.
5. **One click revokes everything**, from your side, without contacting us.

Nothing in this document asks you to take our word for anything you can check yourself in Entra.

1. What this document is

A statement of every Microsoft Graph permission the Olyteck Cyber product requests, why each one is needed, and what it deliberately does not request. Version 2.0 reflects the split of the product into the three separate applications described in §2.

It is written to be relied upon during vendor evaluation and procurement, and a counter-signed copy is provided on request as part of contracting paperwork.

It is also verifiable without trusting us. Two independent checks:

- **In your own Entra tenant** — *Microsoft Entra admin center → Enterprise applications → the app → Permissions*. That list is the authoritative one. If it disagrees with this document, the tenant is right and this document is wrong; tell us and we will correct it.
- **In the product** — *Security Console → Apps & consent*. That panel reads the live grant from Microsoft each time it loads. It is not a stored setting and not marketing copy; it shows what your tenant has actually granted, including anything this document failed to mention.

2. The applications

Olyteck Cyber uses **three separate Entra application registrations**. The separation is the control: a permission granted to one is not available to the others, and each can be revoked independently.

Application	Signs in as	Purpose	Consent
Olyteck Cyber Sign-In	the signed-in user	Authenticates you and reads your own profile	Each user, at first login
Olyteck Cyber Scanner (read-only)	itself, no user	Reads your tenant to produce the findings	One tenant administrator, once
Olyteck Cyber Remediation (opt-in)	**the signed-in user**	Carries out fixes you explicitly request	Separate, optional, revocable

The scanner cannot change anything. It holds no write permission of any kind. It is the application that runs unattended, on a schedule, with no human present — so it is the one that is confined to reading.

Remediation is optional and separate. If you never enable it, the product has no ability to modify your tenant. When you do enable it, it acts **as the person clicking**, using that person's own permissions — it cannot remove something they could not remove themselves in the Microsoft admin portal, and the action is attributed to them in **your own** Microsoft audit log, not only in ours.

3. Sign-In application

Permission	Type	Why
`openid`, `profile`, `email`	Delegated	Standard OpenID Connect sign-in
`User.Read`	Delegated	Your own name, UPN and tenant, to identify you in the product

No application permissions. This registration cannot read anything about any user other than the one signing in.

4. Scanner application — all read-only

Application permissions, granted once by a tenant administrator. Every one is a `.Read.*` permission.

Permission	What it lets us read	Which finding it produces
`Sites.Read.All`	SharePoint site inventory and sharing links	Over-exposed sites and links
`Files.Read.All`	File and folder metadata, and their permissions	Anonymous / external / org-wide sharing
`Group.Read.All`	Microsoft 365 group inventory	Ownerless and stale groups
`GroupMember.Read.All`	Group membership	Who has access via a group
`User.Read.All`	User directory	Guests, dormant accounts, admin sprawl
`Directory.Read.All`	Roles, tenant info, subscribed licences	Admin roles, licence-aware Secure Score
`AuditLog.Read.All`	Sign-in logs, and the authentication-method registration report	Legacy-auth and risky sign-ins; MFA coverage gaps
`Policy.Read.All`	Conditional Access policies	Baseline control scorecard
`Reports.Read.All`	Microsoft 365 usage reports	Copilot and Teams activity
`SecurityEvents.Read.All`	Microsoft Secure Score and its control catalogue	Secure Score, split by what your licences permit
`Application.Read.All`	App registrations and their credentials	Expiring secrets and certificates
`MailboxSettings.Read`	Inbox rules and forwarding settings	Business-email-compromise indicators
`SharePointTenantSettings.Read.All`	Tenant-level sharing policy	Whether the tenant default is permissive
`Team.ReadBasic.All`, `TeamSettings.Read.All`, `TeamMember.Read.All`, `Channel.ReadBasic.All`, `ChannelMember.Read.All`	Teams, their settings and membership	Guest access and channel exposure
`IdentityRiskEvent.Read.All`	Identity Protection risk detections	Risky users (requires Entra ID P1 or P2 in your tenant)

That is **19 application permissions**. Your Entra screen will show **20 rows**: the twentieth is the delegated `User.Read`, which Entra adds to every registration by default and which reads only the profile of whoever is signed in. We mention it so the count matches when you check.

4.1 Two disclosures we make voluntarily

`SecurityEvents.Read.All` is broader than our use of it. The permission also permits reading the legacy `/security/alerts` collection. We call only `/security/secureScores` and `/security/secureScoreControlProfiles`. Microsoft publishes no narrower permission for Secure Score. We would use one if it existed.

`Files.Read.All` sounds broader than it is in practice. We read file and folder *metadata* and *permissions* — names, paths, who has access. We do not download file contents, and no file content is stored in our systems. The scanner's purpose is to find over-exposure, which is a property of permissions, not of content.

---

5. Remediation application — only if you enable it

Delegated permissions, requested at the moment they are first needed, and granted per operator.

Permission	Type	What it permits
`Files.ReadWrite.All`	Delegated	Revoking a sharing link or a direct grant
`Group.ReadWrite.All`	Delegated	Removing a member or **owner** from a group or Team
`GroupMember.ReadWrite.All`	Delegated	Removing a member only — the narrower path, see below
`offline_access`, `User.Read`	Delegated	Keeping the operator signed in for the length of a session, and identifying them

Every permission on this application is delegated. It holds no application permission of any kind — which is what makes property 1 below a fact about the registration rather than a statement of intent.

`Files.ReadWrite.All` is the least-privileged permission Microsoft offers for deleting a sharing permission. For groups there are two, and we request both on purpose:

- **`GroupMember.ReadWrite.All`** is Microsoft's least-privileged permission for removing a *member*. It cannot reach a group's owners, cannot rename a group and cannot delete one.
- **`Group.ReadWrite.All`** is the only permission that reaches the *owners* collection. Microsoft publishes no narrower one.

Requesting both means the narrower permission is available for member removal rather than everything running through the broad one — and it

means **you are asked for consent once.** If we added the narrow permission later, every customer would face a second consent prompt for a capability they had already approved in principle. One prompt, at the start, with the whole picture visible, is the honest version of that trade.

Three properties worth confirming in your own review:

1. **Delegated, not application.** The app can never act without a signed-in person, and never beyond that person's own rights.
2. **No unattended writes.** Scheduled scans run under the scanner identity, which is read-only. Nothing we run on a timer can change your tenant.
3. **Independently revocable.** Removing this registration's consent stops all remediation and leaves scanning untouched.

Until this application is consented, every fix button in the product refuses, explains which permission it would need, and records the refusal in your audit trail.

---

6. Permissions deliberately NOT requested

The scanner application does **not** hold, and does not request:

Not requested	Meaning
`Files.ReadWrite.All` (application)	The unattended scanner cannot modify any file
`Sites.ReadWrite.All`, `Sites.FullControl.All`	It cannot modify or take control of any SharePoint site
`Directory.ReadWrite.All`	It cannot modify any directory object, user, group or role
`Group.ReadWrite.All` (application)	It cannot change any group unattended
`Mail.Read`, `Mail.ReadWrite`	It cannot read or modify the content of any mailbox
`Chat.Read.All`	It cannot read Teams chat messages
Any `*.ReadWrite.*` or `*.FullControl.*` on the scanner	—

> **Verification, in one screen:** *Security Console → Apps & consent* shows the scanner's live permission list and states plainly whether any write permission is present. If one is, that panel says so — it is not able to render this claim when the claim is untrue.

7. Data handling summary

- **No file contents.** Metadata and permissions only.
- **No mailbox contents.** Inbox *rules* and forwarding settings only.
- **No access tokens stored.** Tokens are held in memory for the duration of a request.
- **Sharing URLs** are stored only where a finding is meaningless without them, and are shown only to administrators of that tenant.
- **Revocation** removes our access immediately, from your side, without contacting us.

Full detail: Trust Center → Data handling — https://olyteck.com/trust/cyber

---

8. Reliance and contact

This statement is issued by Olyteck and may be relied upon as-is during evaluation and procurement. A counter-signed copy is provided on request as part of contracting paperwork.

Where this document and your tenant's Enterprise applications screen disagree, **your tenant is authoritative**. Report any discrepancy to security@olyteck.com and we will correct this document and tell every customer holding a copy.

Issued by Olyteck · Version 2.0 · 18 August 2026