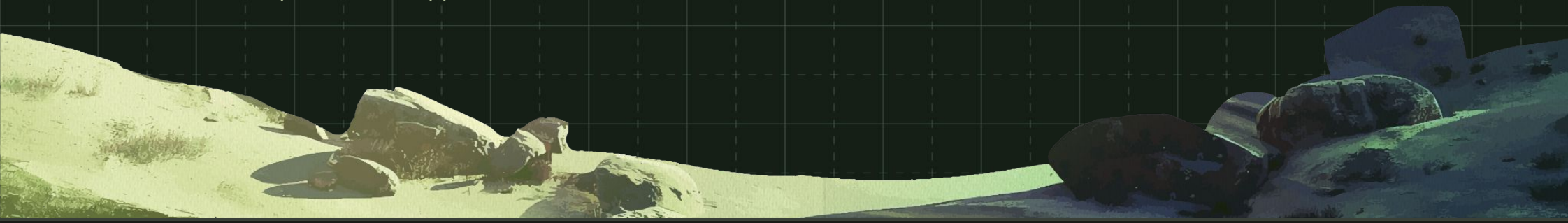
SECURITY RESEARCH REPORT — 2026

OFFROAD

The OAuth Marketplace Verification Blind Spot

An updated audit report on Google Workspace Marketplace and GitHub Marketplace OAuth apps



2,890
public OAuth app listings audited

4.39B
lower-bound reported install footprint

918
apps with at least one structural exposure signal

677
apps with scopes wider than the app's stated function

Marketplace presence makes OAuth feel approved. The data shows a different story: workplace apps can still carry broad scopes, dead publisher infrastructure, external reputation flags, and AI-driven write access that administrators do not see at consent time.

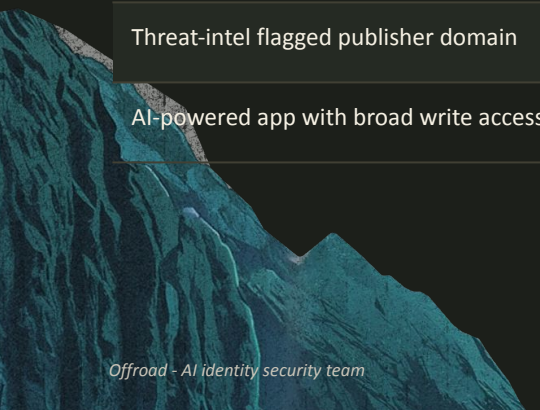
Executive summary

A routine marketplace install can create OAuth access to business systems such as email, files, calendars, repositories, CI workflows, organization settings, and secrets.

The audit covered 2,890 public OAuth app listings: 1,595 on Google Workspace Marketplace and 1,295 on GitHub Marketplace. Their combined reported install footprint is at least 4.39B. Treat that as a lower bound, not a unique-user count, because marketplace install labels use rounded values such as 1M+.

Nearly one in three listings - 918 apps, or 32% of the catalog - carries at least one structural exposure signal: scopes wider than the app's stated function, AI with write access, threat-intel flags, dead publisher websites, buyable or pending publisher domains, or brand-leading app names published by third parties.

Finding	Apps	Lower-bound installs	Why it matters
At least one structural exposure signal	918	1.85B	The marketplace listing does not surface the risk pattern before authorization.
Permissions wider than the app's stated function	677	1.82B	The app can reach data or actions its stated job does not require.
Dead publisher domain	206	20.8M	The accountable party may be unreachable while OAuth grants remain active.
Buyable publisher domain	89	14.4M	Anyone can register the dormant domain and use it to phish under the publisher's identity or trigger account-recovery flows to try to take over the marketplace app.
Threat-intel flagged publisher domain	36	19.3M	Enterprise security products already see suspicious or malicious web infrastructure.
AI-powered app with broad write access	49	81.6M	Autonomous or assisted output can become irreversible mail, file, or repository changes.



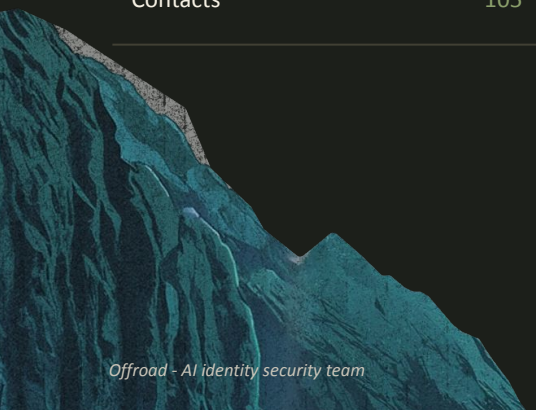
Why this becomes business risk

The business risk comes from the systems these apps can access when installed in workplace environments: email, files, calendars, repositories, CI workflows, organization settings, and secrets.

Google Workspace Marketplace apps attach to Gmail, Drive, Docs, Sheets, Calendar, Contacts, and domain-managed Workspace environments. GitHub Marketplace apps attach to repositories, organization settings, secrets, webhooks, actions, workflows, and runners. The audit found 1,391 Workspace add-ons alone, with a lower-bound install footprint of 3.07B.

Google Workspace surfaces where apps hold broad read, edit, create, or delete access

Surface	Apps	Installs	Relative scale
Drive	281	1.47B	
Docs	125	616.8M	
Sheets	316	1.02B	
Gmail	220	818.2M	
Calendar	167	343.6M	
Contacts	105	347.5M	



Why this becomes business risk

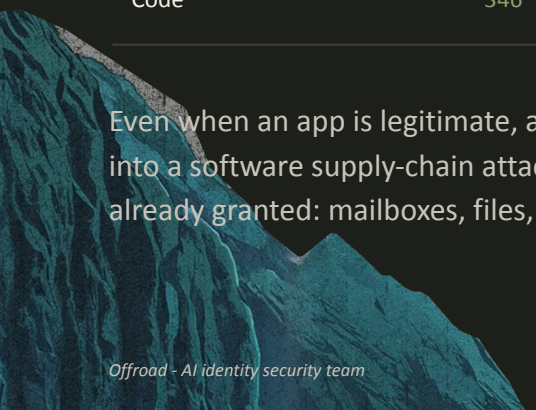
The business risk comes from the systems these apps can access when installed in workplace environments: email, files, calendars, repositories, CI workflows, organization settings, and secrets.

Google Workspace Marketplace apps attach to Gmail, Drive, Docs, Sheets, Calendar, Contacts, and domain-managed Workspace environments. GitHub Marketplace apps attach to repositories, organization settings, secrets, webhooks, actions, workflows, and runners. The audit found 1,391 Workspace add-ons alone, with a lower-bound install footprint of 3.07B.

GitHub surfaces where apps hold read and write access

Surface	Apps	Footprint	Relative scale
Repository administration	96	2.6M	
Organization settings	107	984.2K	
Secrets	46	222.8K	
Actions / workflows / runners	183	7.0M	
Webhooks	138	5.2M	
Code	346	4.8M	

Even when an app is legitimate, a compromise of the publisher or its infrastructure can turn existing OAuth grants into a software supply-chain attack path across many customer environments. The impact depends on the scopes already granted: mailboxes, files, calendars, repositories, CI workflows, organization settings, or secrets.



The permission mismatch

The largest finding by install footprint is the mismatch between what some apps say they do and the high-permission scopes they request

The audit flags 677 apps that request at least one permission exceeding what their stated function requires. Their combined lower-bound reported footprint is 1.82B. The risk does not depend on malicious intent. Once a broad OAuth grant exists, a publisher compromise can turn a legitimate app into a high-impact supply-chain access path across many businesses. The exposure exists as soon as the grant is approved, because a future publisher compromise would inherit the permissions already granted.

Surface with off-purpose high-tier access	App	Lower-bound	Plain-English blast radius
Drive	266	1.26B	Read, edit, create, or delete files beyond the app's stated job
Sheets	161	557.0M	Modify spreadsheets that may contain forecasts, budgets, or customer data.
Docs	73	325.6M	Read or alter documents outside the narrow workflow users expected.
Gmail	70	103.6M	Send or manipulate mail under the user's identity.
Github repositories	97	2.6M	Read and change repository settings, code, branch protection, and other repository-level controls.
GitHub organization settings	107	984.2K	Read and modify org-level settings and policies

The permission mismatch

The largest finding by install footprint is the mismatch between what some apps say they do and the high-permission scopes they request

The audit flags 677 apps that request at least one permission exceeding what their stated function requires. Their combined lower-bound reported footprint is 1.82B. The risk does not depend on malicious intent. Once a broad OAuth grant exists, a publisher compromise can turn a legitimate app into a high-impact supply-chain access path across many businesses. The exposure exists as soon as the grant is approved, because a future publisher compromise would inherit the permissions already granted.

Example app stated use	What the audit found	Why it matters
Multiple-choice form helper	An app with 8M+ installs and off-purpose Drive, Forms, and Sheets scopes.	If the publisher is compromised, the attacker inherits Drive-wide delete, full Sheets edit, and mail-send under the user's identity across 8 million tenants — none of which a radio-button manager needs.
Gmail auto-responder	An app with 60K authorized users and high-risk Drive, Docs, Calendar, and Gmail scopes.	60K users authorized "auto-reply"; the name grant lets a compromised publisher read every Drive file, every Doc, and the entire calendar each user can access — and send mail as them.
URL-to-Drive saver	An app with 3.8M+ installs whose stated function is to save files from URLs into Drive. The OAuth grant lets it see, edit, create, and delete every file in the user's Drive.	The stated save-to-Drive function does not require permission to delete every Drive file the user can access.

The publisher infrastructure gap

OAuth assumes the publisher remains reachable and accountable for as long as the grant survives. The marketplace does not enforce that assumption

The audit identified three overlapping publisher-side gaps: 206 apps with dead publisher domains, 89 apps across 85 distinct publisher domains where the domain is currently available for purchase on a standard registrar, and 36 apps whose publisher domain is flagged on commercial threat-intel blocklists - the same data enterprise security gateways use to block known phishing and malware infrastructure.

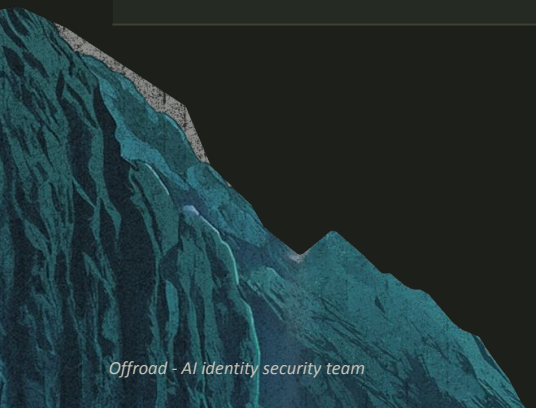
Infrastructure signal	Apps	Lower-bound footprint	Security meaning
Dead publisher domain	206	20.8M	No obvious channel for disclosure, support, rotation, or accountability.
Buyable publisher domain	89	14.4M	Anyone can register the dormant domain at a standard registrar. From there, the buyer can phish under the publisher's identity (using the publisher's real email domain with valid SPF / DKIM / DMARC) or trigger account-recovery flows to try to take over the marketplace app.
Threat-intel flagged publisher domain	36	19.3M	The publisher web surface is already suspect in external security feeds.

The publisher infrastructure gap

OAuth assumes the publisher remains reachable and accountable for as long as the grant survives. The marketplace does not enforce that assumption

The audit identified three overlapping publisher-side gaps: 206 apps with dead publisher domains, 89 apps across 85 distinct publisher domains where the domain is currently available for purchase on a standard registrar, and 36 apps whose publisher domain is flagged on commercial threat-intel blocklists - the same data enterprise security gateways use to block known phishing and malware infrastructure.

Example use cases	Example app the audit found	Why it matters
Single buyable publisher domain shared by multiple apps	One publisher domain, currently available for purchase on a standard registrar, anchors 3 Google Workspace apps with combined 9 million installs.	A single domain purchase gives the buyer the publisher position for all three apps. From there, the buyer can phish under that publisher's identity or try to take over the marketplace apps via account-recovery flows.
Dead publisher domain	An app with 9M+ installs, a dead publisher domain, and a scope that lets the app see, edit, create, and delete every file in the user's Drive.	The publisher domain no longer reachable while the OAuth grant remains valid and with high privilege.
Reputation flagged cluster	A Google Workspace backup product authorized by 180K+ organizations has its publisher domain independently flagged by 5 commercial threat-intel feeds. The same publisher's OAuth grant covers read, edit, and delete authority on every file in those tenants' Drives, every email in their Gmail, every event on every calendar, and the entire contact directory.	A publisher domain that security tools flag as suspicious or malicious can still appear behind a listed OAuth app that users are able to authorize.



AI with write access

AI-powered apps with write access require a different review threshold because they are not deterministic by nature. The issue is not whether the model is malicious. The issue is whether an automated system can write under a user's identity.

The source data marks 49 AI-powered apps with broad write access, representing a lower-bound install footprint of 81.6M. These apps deserve a separate review path because a generated action can become a sent email, edited file, modified spreadsheet, or changed repository state

An AI-powered app with permission to “send email on your behalf” creates a different risk than a traditional app with the same permission. A traditional app usually sends email only after a defined user action, such as clicking send or running a rule. An AI-powered app may decide what to send, when to send it, or who to send it to based on model output.

The consent screen shows the permission, but it does not show how much control the app gives to the model before that permission is used.

49 AI-powered apps with broad write access

81.6M lower-bound reported footprint

127 apps with two or more exposure signals

16 apps with three or more exposure signals

Offroad - AI identity security team

What admins should do now

Administrators should treat OAuth grants as part of identity risk management. High-permission grants should have a business owner, justified scope set, usage monitoring, renewal cadence, and revocation path.

Action	What to look for	Decision rule
Inventory every OAuth grant	Workspace third-party app access and GitHub organization third-party access.	If the owner cannot explain the app, revoke or restrict it.
Monitor OAuth usage continuously	High-privilege actions by third-party apps, including mail sends, file edits or deletes, repository changes, secret access, webhook changes, and CI workflow activity.	Legitimate use should be visible and explainable. Unexplained high-privilege activity should trigger immediate investigation, containment, and revocation if needed.
Prioritize broad write scopes	Drive delete, Gmail send, Docs/Sheets edit, repo administration, org secrets, webhooks, runners.	No broad scope without a business owner and renewal date.
Check publisher infrastructure	Dead websites, parked domains, for-sale domains, missing support channels.	Treat unreachable publishers as rotation candidates.
Separate AI from traditional apps	Any AI app that can write, send, edit, delete, or manage.	Require explicit approval for action- taking AI.
Rotate high-permission grants	The top-risk apps by scope and business surface.	Revoke and re-grant on a fixed

Marketplace listing should not be treated as a substitute for tenant-level security review. Administrators still need to evaluate scope, publisher, purpose, usage, and business owner before approving or retaining high-permission grants, and like other trends in the identity market, move to a continuous monitoring and reviewing instead of periodically.

Methodology and data notes

The findings are based on the audit dataset for publicly listed OAuth apps across GoogleWorkspace Marketplace and GitHub Marketplace. Counts and install-footprint figures were checked for consistency before publication.

This report is based on an audit of 2,890 publicly listed OAuth apps across Google Workspace Marketplace and GitHub Marketplace. Install figures are reported marketplace labels and should be treated as lower- bound footprint indicators, not deduplicated users or tenants. Domain, publisher, and threat-intel signals are point-in-time observations from the audit period

1.

Scopes completely unrelated to the app's stated function - a graphing-calculator app that holds full read-and-delete access to every Google Doc and every Slides presentation, a text-case converter that holds delete access on every Sheet, a Gmail-to-Drive saver that holds full Sheets access. No plausible reading of the listing- described function requires the scope at all.

2.

Scopes that match the function's data class but are broader than the function actually needs, typically because the OAuth provider offers no narrower option. For example, Google does not offer an "edit without delete" scope for Sheets, Docs, or Calendar — an app that legitimately needs to write to a user-selected spreadsheet must take the full Sheets scope, which also grants
delete on every spreadsheet the user can access. Both categories appear in the combined count. The first category is the clearest per-app mismatch. The second category also reflects a structural limitation in the OAuth scope catalog.

OFFROAD

About us

Offroad is an AI identity security team for the modern enterprise. Offroad's agents investigate, govern, remediate, and verify identity risk across human, machine, and AI identities, helping security and identity teams move from visibility to resolution. The company works across existing identity providers, cloud environments, SaaS applications, developer systems, and security tools to reduce identity risk without adding another dashboard. To learn more visit www.offroad.ai.

OhAuth is Offroad's independent research project focused on OAuth marketplace risk and third-party app authorization. For questions about this report, contact info@offroad.ai.