ENTERPRISE RESOURCES

How Can GAT Help With OAuth App Security

GAT labs

Modern attacks are increasingly focused on the permissions your users have already granted to third party apps and browser extensions. Dormant OAuth tokens provide silent, high privilege access that often goes unnoticed and create invisible backdoors into your Google Workspace environment.

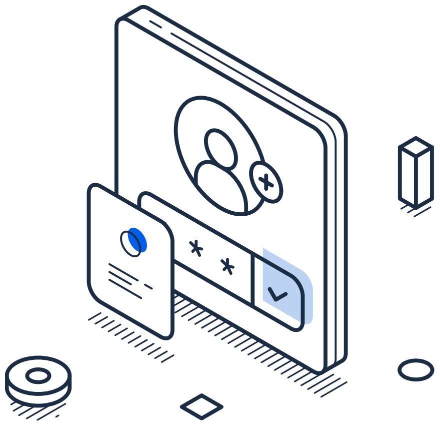
This guide shows how GAT Labs gives you the visibility, control, and automation to secure your Workspace environment against these hidden risks.

Understanding OAuth and Why Scope Permissions Matter

OAuth allows apps to request permission to read or modify Google Workspace data. These permissions are defined as scopes. Some scopes provide limited access. Others provide very broad access, such as reading every file in Drive or modifying any Gmail message.

Examples of high-risk scopes include:

- Gmail modify
- Gmail send
- Drive readwrite
- Drive metadata
- Admin directory access



Attackers increasingly target these token-based permissions because they bypass passwords and MFA.

1. Complete OAuth Visibility

GAT eliminates blind spots by giving you full visibility into every connected application across your domain.

What you can view in seconds:

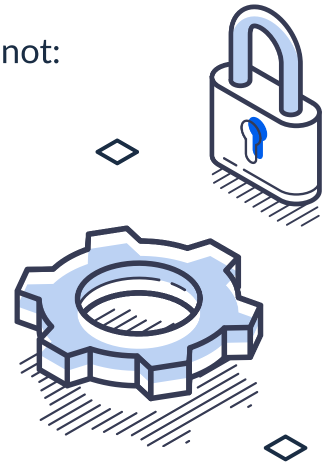
- **Full App Inventory:** See every third-party app and Chrome extension authorized by your users.
- **Detailed Permission Scopes:** Understand what data each app can access, modify, or delete.
- **Scope Risk Scoring:** GAT+ ranks apps by risk level based on the permissions they request.
- **Last Used Date:** Identify dormant apps that still hold active tokens but have not been used recently.
- **User-Level Reports:** View connected apps per user, group, or OU to apply targeted policies.

This level of visibility allows you to locate risky apps, inactive access, and potential compliance issues quickly.

What Admin Console Cannot Show

Google Admin Console provides basic app visibility, but it does not:

- show all OAuth scopes per user
- flag dormant apps with active keys
- auto-revoke tokens
- enforce persistent ban or trust rules
- show all Chrome extensions with OAuth permissions



This gap is where most hidden risks develop.

2. Enforce Automated App Policies

Manual OAuth cleanup is nearly impossible to maintain. GAT replaces it with automated, continuous enforcement.

App Banning and Trust Policies

GAT+ uses a proactive, real-time blocking mechanism to make banned apps unusable, even if a user tries to re-grant access

Policy Type	Function	Precedence Rule
Ban Policy	Revokes an app's permissions in real-time. Prevents the app from accessing any domain data.	The Ban rule will be skipped if a Trust policy is applied to the same user.
Trust Policy	Whitelists an approved app. Always takes precedence over a Ban policy.	If a user is part of a Banned group but is explicitly Trusted, the Ban will not apply to them.

When to Use Ban or Trust

- **Ban Example:** A browser extension that reads page content and sends it to external servers.
- **Trust Example:** A document signing app required by HR or Legal.

How it works:

1. An admin applies a Ban policy to an app.
2. GAT+ immediately revokes its permissions.
3. If a user tries to reconnect it, GAT+ detects and revokes it again automatically.

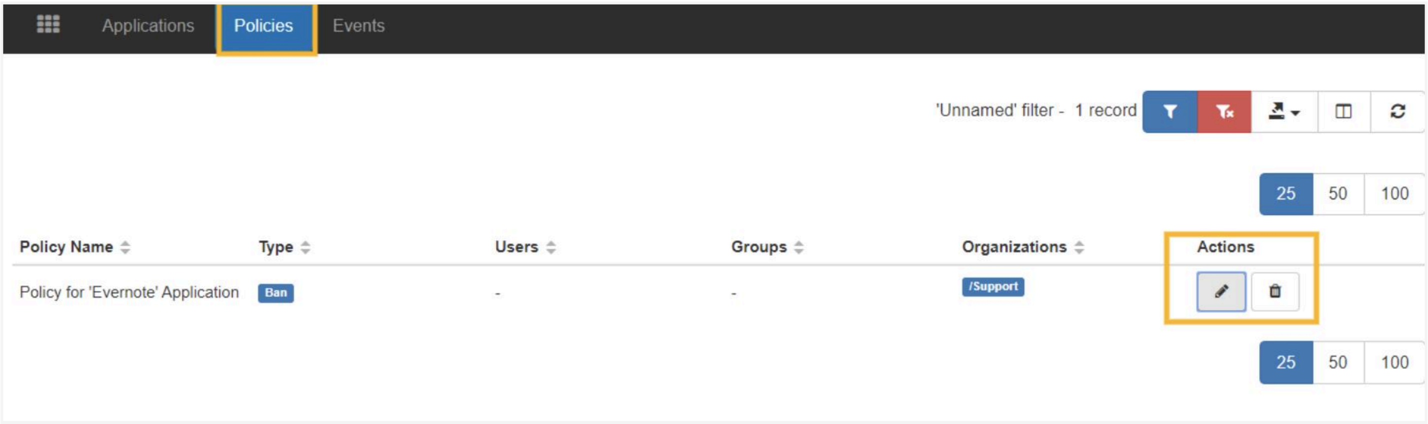
This loop ensures banned apps remain locked out, even if users try to reinstall them.

Steps to Create a Real-Time Ban Policy

1. **Find the Applications:** Navigate to *GAT+ → Applications → Apply custom filter* and search for the application(s) you want to manage.
2. **Set up Policy:** Click the + sign button under Actions next to the application name.
3. **Define the Policy:**

- Set the Policy type to Ban or Trust.
- Select the users whom the policy will affect (by User, Group, or Org. Unit).
- Click the Save button to enable the policy.

4. **Review and Manage:** Use the Policies tab at the top to view, edit, or delete all applied policies for the applications in your domain.



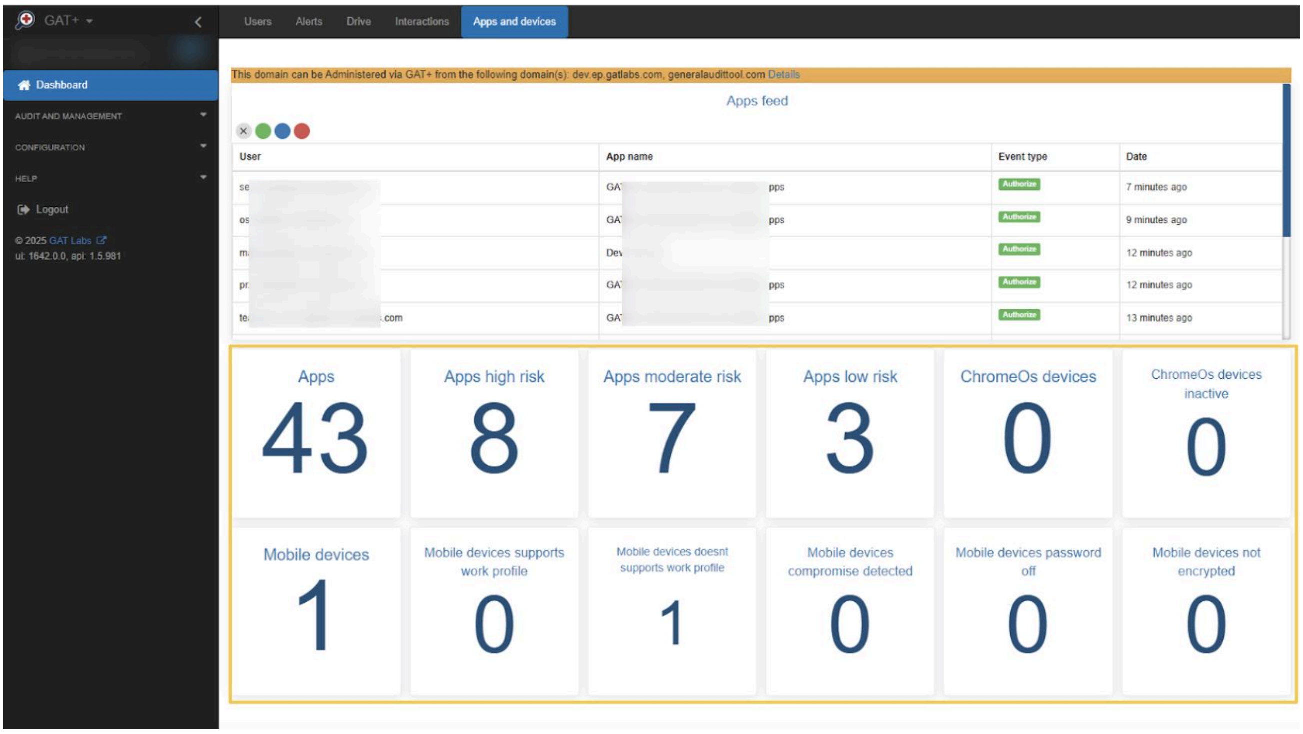
Policy Name	Type	Users	Groups	Organizations	Actions
Policy for 'Evernote' Application	Ban	-	-	/Support	

Related Articles: [Audit and manage third-party Applications in Google workspace]

3. Continuous Monitoring and Audit Support

Once policies are set, GAT+ keeps monitoring everything automatically.

- **Apps Auditing:** GAT+ continuously audits app behavior. If new apps are installed or permissions change, you receive instant visibility in the dashboard and via custom alerts.



© 2025 GAT Labs
ui: 1642.0.0, api: 1.5.981

This domain can be Administered via GAT+ from the following domain(s): dev.ep.gatlabs.com, generalaudittool.com Details

Apps feed

User	App name	Event type	Date
se[redacted]	GA[redacted]pps	Authorize	7 minutes ago
os[redacted]	GA[redacted]pps	Authorize	9 minutes ago
m[redacted]	Dev[redacted]	Authorize	12 minutes ago
pr[redacted]	GA[redacted]pps	Authorize	12 minutes ago
te[redacted].com	GA[redacted]pps	Authorize	13 minutes ago

Apps	Apps high risk	Apps moderate risk	Apps low risk	ChromeOs devices	ChromeOs devices inactive
43	8	7	3	0	0

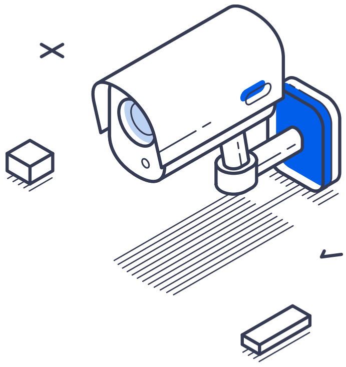
Mobile devices	Mobile devices supports work profile	Mobile devices doesnt supports work profile	Mobile devices compromise detected	Mobile devices password off	Mobile devices not encrypted
1	0	1	0	0	0

- **Alerts:** Set up alerts to notify admins immediately if a new, unauthorized app is installed or if an app requests a high-risk permission scope.
- **Events Tab:** Admins can use the Events tab to check and search by User, viewing the data on which applications had access granted to an API and when that access was authorized or revoked.
- **Compliance and Reporting:** Generate on-demand reports that provide a Full App Inventory with Permissions, User Installation Logs, and Risk Categorization Summaries to verify adherence to internal policies and satisfy external compliance reviews.

4. Monthly Governance Checklist

A simple recurring review helps reduce long-term token exposure. Recommended monthly tasks:

- ✓ Review all apps with high-risk scopes
- ✓ Check apps unused for more than 60 days
- ✓ Review newly installed apps
- ✓ Check apps installed by high-risk groups
- ✓ Review alerts triggered since last month



This routine helps reduce silent access over time.

5. The Shift: From Reactive Cleanup to Proactive Security

Using GAT+ for OAuth security fundamentally changes the security stance of your Google Workspace domain.

Old Security Posture (Reactive)	New Security Posture (Proactive With GAT+)
Blind Spot: Don't know which apps have access or what permissions they hold.	**Full Visibility:** Detailed inventory, risk scoring, and last used dates for all OAuth tokens.
Token Decay: Dormant, unused tokens remain valid indefinitely, posing a persistent risk.	**Zero Trust:** Auto-revoke tokens for unused apps, constantly minimizing the attack surface.
Policy Failure: Rely on manual review or one-time cleanups after a security event.	**Real-Time Governance:** Automated Ban and Trust policies enforce rules instantly and persistently, even if the user attempts to bypass them.

Final Takeaway

Dormant OAuth tokens and unmonitored app permissions represent one of the biggest hidden risks in Google Workspace.

GAT helps you take back control with full visibility, automated policies, and continuous protection that keeps your Workspace secure and compliant.

Your greatest security risk may not be an attacker breaking in, but a forgotten permission that already grants them access. Reviewing OAuth activity today reduces the chance of an invisible breach tomorrow.

Book A Demo Today