ADMIN GUIDE

Shadow IT in Google Workspace: How to Detect and Control It

15 MIN READ | FOR ADMINS, SECURITY AND COMPLIANCE TEAMS

GAT labs

Introduction

Shadow IT in Google Workspace is not a single problem with a single fix. It is a category of ongoing risk that grows every time a user connects an app, installs an extension, or transfers data through a channel IT has not reviewed.

This guide gives Google Workspace admins a complete reference: what shadow IT is, where it lives in a Workspace environment, how to detect it using GAT+ and GAT Shield, and how to build the controls and workflows that keep it from growing back.

Section 1:
What Shadow IT Is and What It Is Not

Shadow IT refers to any technology, tool, or service used within an organization without IT's knowledge or approval. The term covers a wide range of behaviors:

- A user connecting a third-party app to Google Drive via OAuth
- A team adopting a SaaS project management tool without submitting a request to IT
- An employee pasting company data into a free AI writing tool
- A user installing a Chrome extension with broad page permissions
- Files being transferred from Drive to a personal cloud storage account via the browser

It is important to understand that shadow IT is rarely malicious. Most users engaging in these behaviors are trying to work faster or solve a problem the approved toolset does not address well. That does not reduce the risk -- but it does inform the right response. A policy built entirely on restriction without an accessible approval alternative tends to push shadow IT underground rather than eliminate it.

What shadow IT is not: it is not just a policy problem. It is a visibility problem. The behaviors above happen whether or not a policy exists. The question is whether you can see them.

Section 2:
Where Shadow IT Hides in Google Workspace

2.1 OAuth-connected apps

When a user authorizes a third-party app to access their Google account, OAuth grants that app a persistent token. Depending on the permissions the user accepted, that token can include full read and write access to Gmail and Drive.

These tokens do not expire automatically. They survive the user leaving the company if the account is not properly off-boarded. They survive the user stopping use of the app. They sit, active and unreviewed, in the background of your domain.

The Admin Console App Access Control view shows you that apps are connected, but getting a complete picture sorted by scope, user, and last activity requires tooling beyond what Google provides natively.

2.2 Chrome browser activity

The browser is where most work happens. It is also where most shadow IT starts. A user visiting an AI tool, uploading a file to a personal account, or installing an extension, all of these happen in Chrome, and all of them are invisible to the Admin Console.

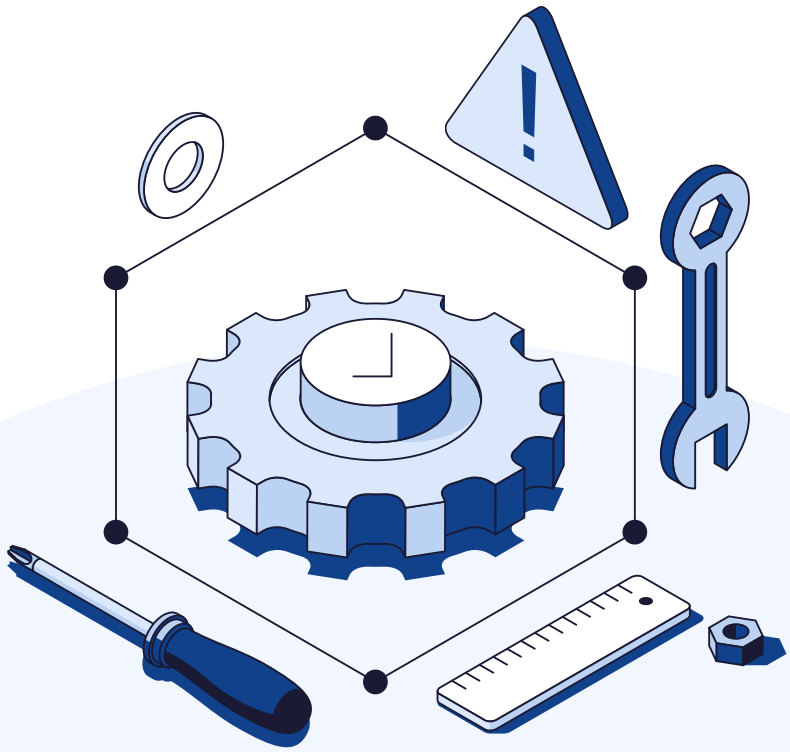
Google's Endpoint Management gives you some visibility into Chrome device policies and can enforce extension restrictions. What it does not give you is a real-time, per-user view of browsing activity, file transfer events, or extension installs across your entire fleet.

2.3 Shared Drive and file transfer risks

When users download files from Shared Drives and move them to personal accounts or unapproved platforms, the download event is logged in Drive. The destination is not. This creates a class of data movement that is genuinely difficult to track without browser-level monitoring.

2.4 Unapproved SaaS adopted by teams

Entire departments can begin using a new tool without IT involvement. The tool gets signed up for with work email addresses, payment goes on a team credit card, and it operates entirely outside your domain management. You may not discover it until an offboarding process reveals data the organization cannot access or a compliance audit asks for a software inventory you cannot produce.



Section 3:
The Compliance and Security Risk

Shadow IT creates three categories of risk for Google Workspace admins:

Data exposure.

Data processed by unapproved tools is processed under their terms, not yours. Personal data pasted into an AI tool, uploaded to an unvetted service, or stored in an unapproved app may be retained, analyzed, or exposed in ways your organization cannot control.

1

Compliance gaps.

Regulations, including GDPR, HIPAA, and ISO 27001 require you to demonstrate where personal data is stored and who has access to it. Shadow IT creates undocumented data flows that make that demonstration impossible. Our GDPR compliance page outlines what this means in practice for Google Workspace environments.

2

Access risk from dormant tokens.

An OAuth token from a tool no longer in use is not a low-risk legacy item. If that app's infrastructure is breached, the attacker inherits the access your user originally granted. With no review process, that token may have been active for years.

3

Related reading: What Is DSPM and Why Every Google Workspace Admin Needs It

Section 4:
How GAT Labs Detects Shadow IT

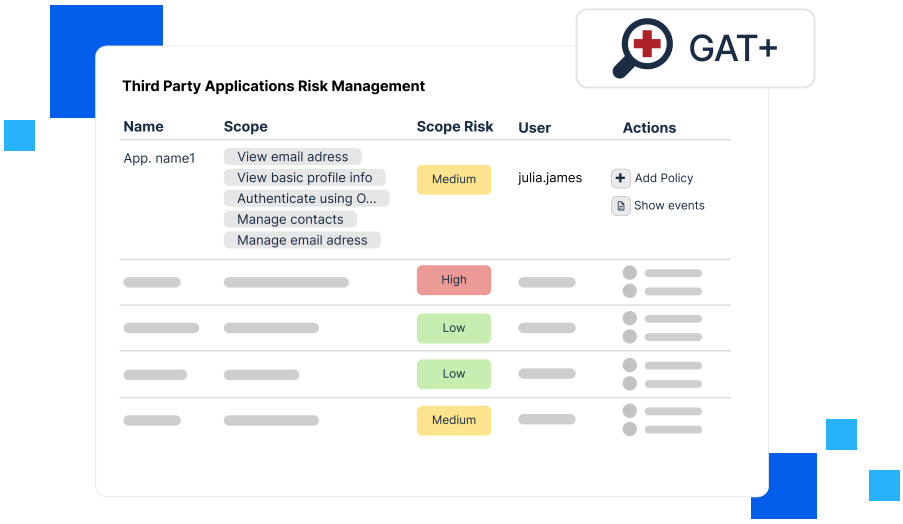
4.1 OAuth app auditing with GAT+

GAT+ gives admins a complete, filterable view of every third-party app connected to your domain. For each app, you can see:

- The full list of OAuth scopes the app holds
- How many users have granted access
- When the token was last active
- A scope risk score calculated from the permissions the app holds

From this view, you can revoke access in bulk, apply ban policies to prevent reconnection, and set trust policies for approved apps so they are not caught by broad restriction rules.

The ban policy mechanism works in real time. When a user attempts to connect a banned app, GAT+ removes the scope access as soon as Google notifies the system. In practice, the user may see a brief login, but the app cannot use any API access after the block takes effect.



Set up walkthrough: Audit and Manage Third-Party Applications in Google Workspace

Policy configuration: Audit and Policy for Google Workspace Apps

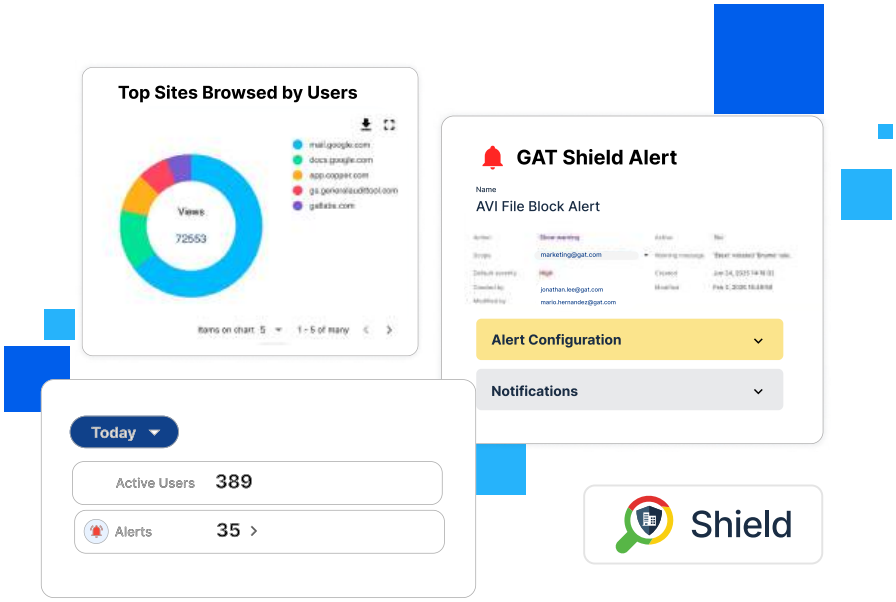
4.2 Browser monitoring with GAT Shield

GAT Shield is a Chrome extension deployed to domain users. It runs locally and sends activity data back to the GAT Shield dashboard in real time. It does not require any infrastructure changes or agent installation outside of Chrome.

From the GAT Shield console, admins can see:

- Full browsing history by user, including time on site and domain visits
- File downloads: what was downloaded, by whom, and when
- File uploads: where files were sent, including external services and AI platforms
- Chrome extensions installed across your fleet, with permission details
- Alerts triggered by custom rules the admin defines

GAT Shield supports custom DLP rules using regex, allowing you to detect sensitive content patterns, credit card numbers, national insurance numbers, specific internal terminology, being typed or pasted into browser fields across any site, not just Google's own apps.



Product overview: GAT Shield

Full DLP capability overview: Google Chrome DLP

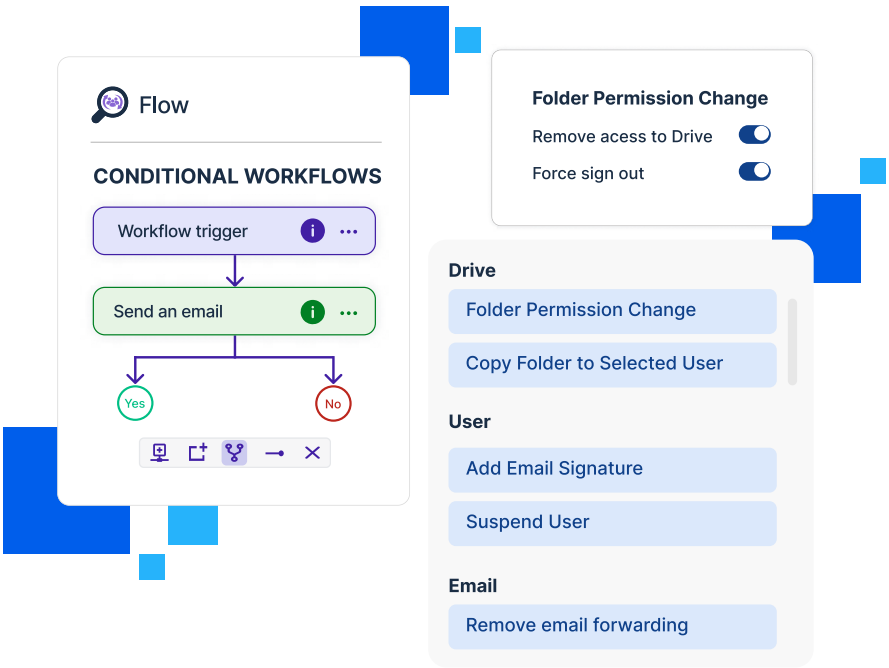
4.3 Automated response with GAT Flow

Detection only matters if you can act on it. GAT Flow works alongside GAT+ alerts and audit insights to help you build structured workflows that guide response and review processes.

Examples:

- **New OAuth app detected:** notify the security team, log the event for compliance tracking, and assign the user account for review
- **Repeated policy violations detected in reports:** trigger an internal review workflow and notify relevant stakeholders
- **High-risk activity identified through audits:** initiate a structured response process with defined approval steps

These workflows support faster response times. You define the trigger and the action, while the admin team remains involved in reviewing and approving actions where needed.



Product overview: GAT Flow

Section 5:
Building a Shadow IT Control Framework

A repeatable control framework for shadow IT in Google Workspace has four components:

Discovery: A scheduled OAuth audit, run at minimum monthly, that reviews all connected apps against an approved list. A Chrome extension review, covering permission scope and install date, for users with access to sensitive data.

Monitoring: Timely alerts in GAT+ for new OAuth connections above a defined risk threshold. Real-time alerts in GAT Shield for file transfer events, new extension installs, and visits to unapproved external services.

Response: Automated workflows in GAT Flow that act on alert triggers without requiring manual intervention for every event. A clear escalation path for alerts that require human review.

Prevention: A lightweight app approval workflow that gives users a fast route to request tools through IT. Clear policy communication that explains why the process exists, not just that it does. Ongoing security awareness training that covers shadow IT risks, including unauthorized apps and external data sharing. A trust list in GAT+ that pre-approves commonly requested tools so users have a visible set of options without waiting for a ticket.

Section 6:
Quick Start Checklist to Audit Shadow IT with GAT

This checklist gives you the highest-impact actions to take in the first two weeks.

Week 1:

- Go to *Security* > *Access and data control* > *API controls* in Admin Console. Export the list of connected apps.

- In GAT+, run the Applications audit. Filter by scope risk score: High. Review every app with Drive or Gmail write access that IT did not approve. Revoke access for anything you cannot justify.

- In GAT Shield, pull the Extensions inventory. Filter for broad permission scope ("Read and change all your data"). Flag anything installed by users with access to regulated data.

- Set up a scheduled report in GAT+ to monitor newly connected OAuth applications. Focus on apps with a higher risk scope, such as Drive or Gmail write access, and review them regularly to identify unapproved access early.

Week 2:

- In GAT Shield, configure download volume alerts. Set a threshold appropriate to your environment; many teams start at 20 files within 30 minutes.

- Configure upload alerts for specific external domains, personal cloud storage, consumer AI tools, and file-sharing platforms outside your approved stack.

- Review your offboarding process. Confirm that departing users have their OAuth tokens revoked as part of the standard checklist.

- Begin documenting your approved app list. This is the foundation of your GAT+ trust policy setup.

Conclusion

Shadow IT in Google Workspace will not go away by itself. It will grow as new AI tools, SaaS platforms, and browser extensions become more accessible and more compelling to use. The right response is visibility and a usable approval process, not blanket restriction.

GAT+ and GAT Shield give you the visibility. GAT Flow gives you the automated response. Together, they give you a shadow IT control framework built specifically for how Google Workspace actually works.

For a live demonstration of what this looks like in a real domain, book a demo with the GAT Labs team.