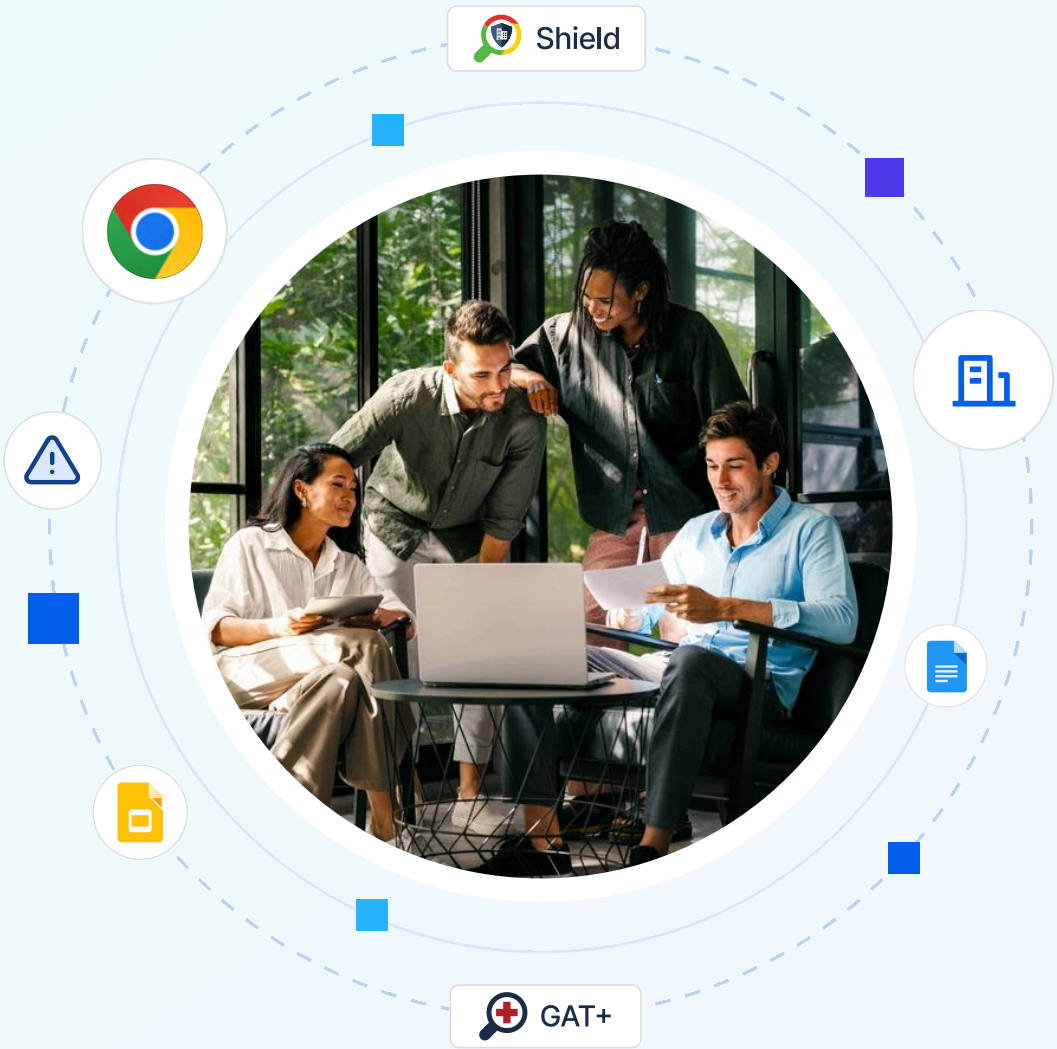
ADMIN GUIDE

The Google Admin's Guide to Data Discovery and DSPM

A practical framework for finding sensitive data across your Google Workspace domain, assessing your exposure, and keeping it under control.

15 MIN READ | FOR ADMINS, SECURITY AND COMPLIANCE TEAMS



GAT labs

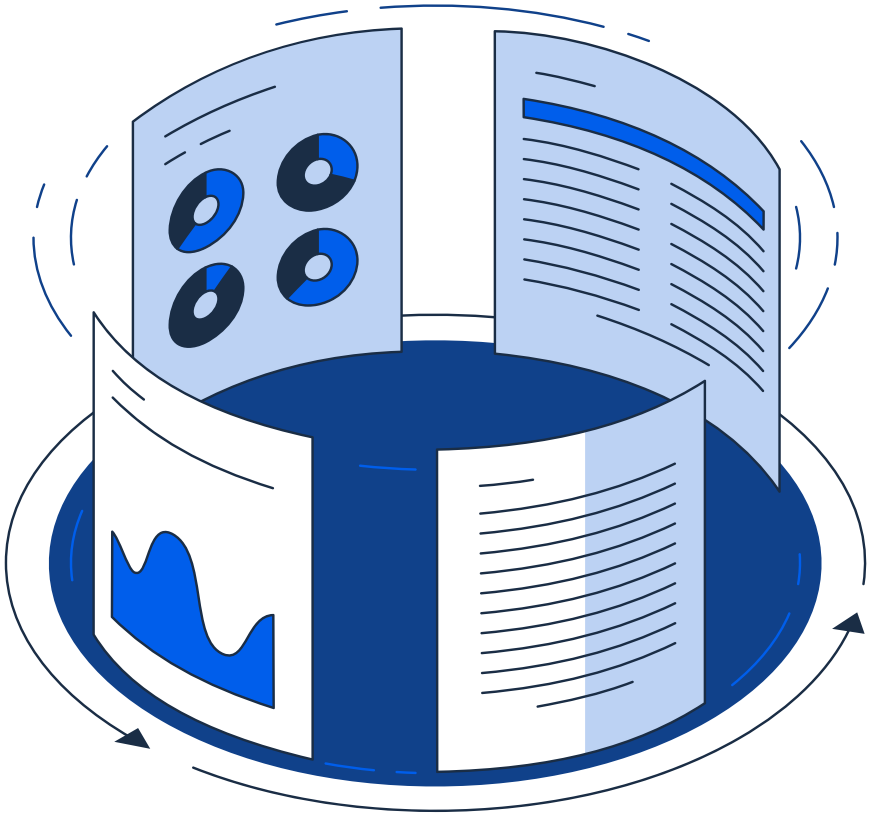
THE PROBLEM

Most admins find out about their data exposure the hard way

Not from an audit. From an incident, a compliance request they cannot answer quickly, or a DSAR that takes three weeks to piece together. By then, the exposure has already happened.

Google Workspace makes collaboration effortless. That same effortlessness means files spread, permissions drift, and staff leave data behind (continuously, and mostly without admin visibility). The native admin console was not built to surface all of this at the depth and scale that security and compliance teams need.

> The question is not whether your domain has exposed sensitive data. It almost certainly does. The question is whether you know about it.



Five data risks specific to Google Workspace

1. Uncontrolled external sharing

Files set to "Anyone with the link" accumulate silently over months and years. PII, financial records, and confidential documents end up accessible to people outside your organisation with no admin aware it is happening.

2. Orphaned data from former employees

When someone leaves, their Drive files stay. Without proactive ownership transfer at offboarding, sensitive data sits in inactive accounts with no governance and no clear owner.

3. Third-party OAuth app access

Every connected app may hold ongoing Drive or Gmail permissions. Most organisations have dozens of apps they are no longer actively using, still sitting on access nobody has reviewed.

4. Sensitive data in the wrong places

Payroll spreadsheets in a team Drive. HR documents in a folder accessible to all staff. Customer contracts shared to the wrong group. Identifying these requires content-aware scanning, not just permission auditing.

5. GDPR and DSAR exposure

Under GDPR, organisations must respond to Data Subject Access Requests and report breaches within 72 hours. Neither is realistic without a reliable, current view of where personal data lives across the domain. For more on handling DSARs specifically, see the Google Admin's Playbook for DSAR.

How to prioritise: the exposure risk matrix

Not all data carries the same risk. Prioritise based on the combination of how sensitive the data is and how broadly it is exposed.

Exposure Risk Matrix — Sensitivity vs Access Level

SENSITIVITY	INTERNAL ONLY	EXTERNAL (NAMED)	PUBLIC / ANYONE WITH LINK
	Low Product docs, public comms	Low	Low
	Medium	Medium Internal reports, team data	Low
	Medium	High	High PII, payroll, contracts
Medium	High	Critical	

The four-phase data discovery framework

Effective data discovery and DSPM in Google Workspace follows a clear structure, regardless of what tooling you use.

1

Inventory

Build a complete picture of every file, share, external collaborator, and OAuth app across the domain.

2

Risk Score

Assess each element using the sensitivity vs exposure matrix. Focus on Critical and High first.

3

Remediate

Act in bulk. Revoke shares, transfer ownership, remove inactive collaborators, document every change.

4

Monitor

Set real-time alerts, schedule recurring reports, and review your posture regularly. This is ongoing, not quarterly.

REAL-WORLD SCENARIO

A team member left three months ago. Here is exactly what to do.

This is one of the most common situations that creates lasting exposure in enterprise Google Workspace environments. Here is the step-by-step process.

1. **Find all files owned by the departed user**
   Search your domain Drive inventory filtered by owner email. Include My Drive, all Shared Drives, and any folders they had edit access to.

2. **Identify which of those files have active external shares**
   Cross-reference ownership with sharing status. Any file owned by an inactive account with external access is a Critical risk item.

3. **Revoke public and external shares on high-sensitivity files immediately**
   Do not wait for ownership transfer to complete. Revoke risky access first, then sort governance. Prioritise files containing PII, financial data, or contractual information.

4. **Transfer file ownership in bulk to an active team member or manager**
   Assign a clear owner for every file. Ungoverned data stays ungoverned regardless of who can technically access it.

5. **Revoke any OAuth app tokens associated with the departed user**
   Retained OAuth tokens can allow continued access to Drive or Gmail after an account is suspended. Review and revoke all connected apps on the account.

6. **Document every action taken with timestamps for your audit trail**
   In the event of a GDPR inquiry or breach notification, having a clear record of remediation actions taken and when is essential.

Google Workspace Security: Typical vs Well-Governed Domain

Here is the difference between a typical domain and a well-governed one across the metrics that matter.

TYPICAL DOMAIN

✗ Hundreds of "Anyone with the link" files, many unreviewed for over a year

✗ Former employee Drive files with no owner and active external shares

✗ DSAR response takes 2 to 3 weeks and requires manual cross-department searches

✗ OAuth app inventory unknown, permissions not reviewed

✗ No real-time alerting, exposures discovered reactively

WELL-GOVERNED DOMAIN

✓ External sharing audited monthly, public links reviewed and removed on schedule

✓ Offboarding includes ownership transfer and external share revocation as standard steps

✓ DSAR response completed in hours with a documented, repeatable workflow

✓ OAuth app inventory reviewed quarterly, inactive apps revoked

✓ Real-time alerts fire when sensitive data is shared outside policy

HOW GAT HELPS

For admins using GAT: what each product does here

GAT is the only full-stack audit and security platform built specifically for Google Workspace. Here is how each product maps to the data discovery and DSPM framework above.

GAT+

DATA DISCOVERY AND AUDIT

Scans every Drive file, Shared Drive, and Gmail inbox across the domain. Surfaces sharing configurations, file ownership, external collaborators, and sensitive content that Google's own tools do not expose. Supports bulk remediation across thousands of files in one operation.

Shield

BROWSER-LEVEL COVERAGE

Extends visibility to Chrome. Monitors downloads, visited sites, and session activity across managed users. Block pages or downloads in real time and set alerts for risky browser behaviour such as file uploads to external services.

Unlock

SECURE INVESTIGATIONS

Provides accountable, approval-gated access to user Gmail and Drive content for investigations or DSAR response. Every request requires a second approver and leaves a full audit trail. No uncontrolled access, no privacy risk.

Flow

USER AUTOMATION

Automate your onboarding, offboarding and modifying Google Workspace users chores seamlessly. Signature management, Email and File Migration, and much more!

For step-by-step guidance on specific tasks, visit the Google Drive Management knowledge base or the GDPR compliance tech tips.

QUICK-START CHECKLIST

Your data discovery action plan

Use this as your starting point. Work through it in order, each phase builds on the one before.

PHASE 1: INVENTORY

- [ ] Generate a full list of all files shared externally across the domain, filterable by owner and date
- [ ] Identify all files owned by former or inactive employees
- [ ] List all Shared Drives with external membership
- [ ] Inventory all third-party OAuth apps and their Drive permissions

PHASE 2: RISK ASSESSMENT

- [ ] Identify all files shared with "Anyone with the link" — prioritise those containing sensitive data
- [ ] Flag all files owned by former employees with active external shares (Critical risk)
- [ ] Review Shared Drive membership for accuracy and necessity
- [ ] Flag OAuth apps not accessed in the last 90 days for review

QUICK-START CHECKLIST

PHASE 3: REMEDIATION

- [ ] Revoke public link access on all Critical and High risk files immediately
- [ ] Transfer ownership of orphaned files from former employees
- [ ] Remove inactive external collaborators from files and Shared Drives
- [ ] Revoke OAuth app permissions for apps no longer in active use
- [ ] Document every change with timestamp and scope for your audit trail

PHASE 4: ONGOING MONITORING

- [ ] Set real-time alerts for any new external sharing of sensitive content
- [ ] Schedule monthly audit reports on sharing activity and external collaborators
- [ ] Define who receives alerts, who acts on them, and what the response SLA is
- [ ] Schedule a quarterly data posture review with your security or compliance team

FURTHER READING

Related guides and resources

- → The Google Admin's Playbook for DSAR
- → File Sharing Governance Guide
- → Data Discovery and DSPM for Google Workspace
- → GDPR Compliance for Google Workspace