GAT labs

Prevent Data Leaks in Google Workspace: A Quick Guide for Admins

Data loss isn't always malicious, it's often accidental. A misdirected email, a wrongly shared file, or an overlooked setting can expose sensitive data. This quick guide outlines what to look for, how to respond, and how GAT+ strengthens your **Data Loss Prevention (DLP) strategy.**

1.What to Watch For:

Common Risk Areas in Google Workspace

- **Gmail:** Unencrypted PII or financial data sent externally
- **Drive:** Sensitive files shared with unauthorized users
- **Chat & Meet:** Confidential info shared in chats or meeting notes
- **Offboarding periods:** File downloads and ownership transfers

Tip: Look for spikes in sharing or downloads from high-risk departments.

2.Best Practices for DLP Admins

Real-World Advice + Use Cases

1.Map your sensitive data

Not all data is equal. Know what you're protecting and where it lives.

Examples by team:

- **HR** → employee records, IDs, contracts
- **Finance** → payroll, invoices, tax data
- **Legal** → NDAs, client agreements
- **Execs** → strategic plans, board decks

Build an inventory of sensitive data types across departments. Start with regulated data (GDPR, HIPAA, etc.) and expand to business-critical documents.

2. Customize Policies by Department Risk

Generic rules don't reflect your org's structure. Tailor rules by unit, risk level, and data type.

Google Workspace tools:

- Predefined detectors (SSNs, credit cards)
- Custom DLP rules + regex for niche patterns
- OU-based policy segmentation

Use Case:

A legal team uses a regex rule to detect case IDs (e.g. "CASE-####") and block sharing with external parties, while the Marketing team can share pitch decks freely — monitored but not blocked.

3. Set Alerts That Teach, Not Just Block

Blocking is necessary, but alerting users with context helps prevent repeat violations.

Smart alerting tips:

- Notify users and admins
- Explain the policy reason in plain English
- Only alert on repeat offenses or high-volume events to reduce noise

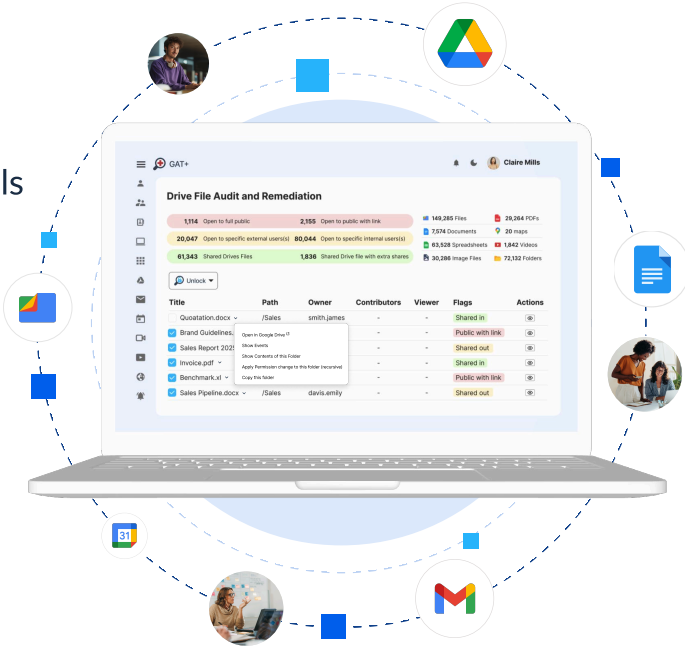
Use Case:

An employee in Sales shares a Google Sheet with external partners. The file contains client emails and SSNs, which match your DLP regex rule.

GAT+ instantly:

- Triggers an alert
- Emails the user with a warning and file details
- Automatically removes the external share
- Notifies Security and the user's manager

Learn more



3.How GAT+ Improves DLP

Why Google Admins Use GAT+ to Go Further

While Google Workspace has strong native DLP, GAT+ adds critical capabilities that save time and reduce blind spots:

GAT Advantage	What it does
Timely alerts	Trigger alerts on download spikes, bulk sharing, or sensitive content matches
Auto-remediation actions	Remove external shares or notify users instantly , no admin action needed
Advanced reporting & audits	Exportable logs of shares, downloads, alerts, and policy violations
Department-level targeting	Apply different policies per department, OU, or group
Full alert visibility	Audit trail available in the Alert tab, with logs, summaries, and action history
Content-aware regex matching	Use predefined or custom regex to detect PII, client data, internal codes
Share-to pattern detection	Alert on shares to personal or suspicious domains

Additional Resources & Deeper Insights:

For admins looking to go beyond theory, these resources offer step-by-step guidance, real alert rule examples, and advanced DLP configurations using GAT+ and Shield. Whether you're just getting started or refining your policies, these links will help you build a stronger, more proactive data protection strategy in Google Workspace.

- A Guide to Data Breach Prevention
- Set up Google Drive DLP Alerts For Shared Out Files
- Powerful SSN Detection Alert for your Enterprise
- Create DLP Alert on Externally Shared Google Docs in Drive
- GAT+ Overview