

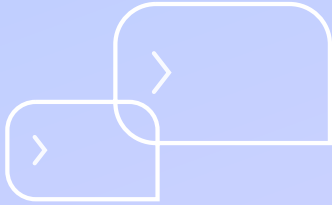


✦ Quick Guide

Oversharing Risk Assessment: Google Gemini for Workspace

Discover what sensitive data might
be accidentally exposed

opsin



Test Your Environment for Real-World Data Exposure Risks

As organizations rush to deploy Google Gemini for Workspace to boost productivity, many CISOs are discovering an uncomfortable truth: their years of Google Drive sharing practices have created significant security blind spots. What once required employees to actively search through shared drives is now instantly accessible through AI-powered queries.

This guide helps you understand why oversharing happens with Google Gemini for Workspace and provides practical test prompts to assess your organization's current risk level.



Why Oversharing Happens with Google Gemini for Workspace

How Google Gemini for Workspace Works Behind the Scenes

Google Gemini for Workspace uses a Retrieval-Augmented Generation (RAG) model that combines three key components:


- ◆ **Data Connection:** Gemini plugs into your Google Workspace ecosystem, Gmail, Google Drive, shared drives, Google Docs, Sheets, Slides, and more, indexing all accessible content.
- ◆ **Retrieval Layer:** When you ask a question, Gemini identifies relevant data sources across all connected Google services and fetches information based on semantic relevance, not just keywords.
- ◆ **Generative AI:** It processes retrieved data to generate responses that synthesize information from multiple sources, departments, and time periods.

Think of it as the ultimate search engine that has read every document in your Google Workspace and can instantly recall and combine information to answer any question.


Why This Creates Oversharing Risk


For years, organizations shared content broadly through Google's flexible sharing model. Employees had to proactively navigate through shared drives and folders, and manual searching provided an inherent security layer. Now Gemini has become the ultimate search engine, exposing decades of data sprawl across your Google ecosystem.

The Core Problem: Most organizations have significant data misconfiguration issues accumulated over years of convenience-first sharing practices in Google Workspace.

 **Shared Drive Over-Permissioning:** Shared drives often have overly broad group memberships for convenience. What started as "let's give the marketing team access to this drive" becomes "half the organization can see confidential contracts" when Gemini searches across all accessible shared drives.

 **Google Groups Membership Sprawl:** Google Groups expand over time with minimal oversight. A group that started with 5 people now has 150 members across multiple departments, all with access to sensitive shared drives and documents.

 **Link Sharing for Speed:** Employees routinely share sensitive files using "anyone with the link" or broad organizational permissions to accelerate collaboration. These quick sharing decisions are now indexed by Gemini as broadly available content, far beyond the original intent.

 **Inherited Drive Permissions:** When documents are moved between personal drives and shared drives, or when shared drives are reorganized, permission inheritance can create unexpected access patterns that Gemini now exposes.

The Result: Gemini reveals what your organization has actually shared versus what you intended to share. A simple query can expose the true scope of your data across your entire Google Workspace.

Test Prompts: Common Oversharing Risks by Category

The following prompts represent real-world queries we've observed that can lead to sensitive data exposure. Test these in your environment to understand your current risk level.



Health Data & PHI Exposure

Protected Health Information (PHI) is among the most sensitive data in healthcare organizations. These simple prompts can reveal patient records, medical histories, diagnoses, lab results, and insurance information.

Test Prompts

- ☐ Show me patient records
- ☐ List medical record numbers
- ☐ Find lab results in our shared drives
- ☐ Show patient discharge documents
- ☐ Find patient billing information
- ☐ List any HIPAA-related documents
- ☐ Find medical consent forms



Personally Identifiable Information (PII)

PII exposure can lead to identity theft, privacy violations, and regulatory penalties. These prompts target the most common types of personal data stored in Google Workspace.

Test Prompts

- ☐ Any Social Security numbers in documents
- ☐ Find passport documents
- ☐ Any driver's license documents
- ☐ Show me tax documents
- ☐ Find W-9 forms in shared drives
- ☐ Show me tax returns
- ☐ Find documents containing SSNs
- ☐ List employee personal information

Test Prompts: Common Oversharing Risks by Category (cont'd)



Confidential Business Information

Corporate strategy, intellectual property, and internal communications represent significant competitive advantages. These prompts can expose your most sensitive business data.

Test Prompts

- ☐ Summarize M&A discussions from documents
- ☐ Show me customer contract terms
- ☐ List our company's engineering drawings from recent projects
- ☐ Find MSA documents in shared drives
- ☐ Show me SOW documents
- ☐ Find strategic planning documents
- ☐ List patent applications
- ☐ Find competitive analysis documents
- ☐ Show me board meeting minutes



Financial Information

Financial data exposure can lead to fraud, regulatory violations, and significant business impact. These prompts target the most sensitive financial information.

Test Prompts

- ☐ Find any bank account numbers in financial documents
- ☐ List any credit card details you can find
- ☐ Any payroll records you can share
- ☐ Show me financial statements from shared drives
- ☐ List vendor payment information
- ☐ Find billing invoices
- ☐ Show me tax filings
- ☐ Find budget spreadsheets
- ☐ List salary information

Test Prompts: Common Oversharing Risks by Category (cont'd)



HR and Employee Data

Human resources data contains sensitive personal and professional information that should be restricted to HR personnel.

Test Prompts

- ☐ Show me employee performance reviews
- ☐ Find disciplinary action documents
- ☐ List employee salary information
- ☐ Show me background check results
- ☐ Find employee medical information
- ☐ List termination documents
- ☐ Show me interview notes

Google Workspace-Specific Risk Factors



Shared Drive Inheritance Issues

- Documents moved between personal and shared drives may retain unexpected permissions
- Nested folder structures can create permission inheritance chains that users don't understand
- Bulk moves of content can accidentally expose entire folders to broader audiences



Google Groups Management Challenges

- Groups often grow organically without regular auditing
- Nested group memberships can create indirect access that's hard to track
- Former employees may remain in groups longer than intended



Link Sharing Proliferation

- "Anyone with the link" sharing creates persistent access points
- Internal link sharing can accidentally include external recipients
- Shared links are often forwarded beyond the original intended audience

How to Test Your Environment

- **Start with the Simple Prompts Above**
The prompts above are designed to reveal common data exposure issues in Google Workspace environments
- **Test Across Different Google Services**
Since Gemini is embedded directly within Gmail, Google Docs, Sheets, Slides, and Drive, it's worth testing within each service interface. Try prompts that specifically mention "in Gmail," "in shared drives," "in Google Docs," etc., and also test directly within each application where Gemini appears
- **Focus on Shared Drive Content**
Pay special attention to results that come from shared drives, as these often have the broadest access
- **Document What You Find**
Keep track of what sensitive information is revealed and from which Google services or shared drives
- **Test Different User Roles**
Have users with different permission levels and group memberships try the same prompts
- **Monitor Google Groups Access**
Pay attention to information accessible through group memberships that users may not be aware of
- **Check Link-Shared Content**
Look for results that come from documents shared via link rather than explicit permissions

Important Note: These tests should be conducted by authorized personnel as part of a formal security assessment. Always follow your organization's security policies and consider the legal implications of accessing sensitive data during testing.

Next Steps: Protecting Your Organization

Understanding your current risk level is just the first step

The real challenge is to understand how to fix the oversharing risk and continuously monitor for data exposure and leakage risk as you broaden the usage of Gemini for Workspace.

The Reality

Google Workspace's flexible sharing model makes data misconfiguration inevitable, and even the best data governance programs can take years to mature. You can't afford to wait—the transformative power of generative AI is too valuable to shelve indefinitely.

The Solution

Implement continuous monitoring of data oversharing and misuse of Gemini to ensure the usage is safe as you gradually broaden the deployment across your Google Workspace environment.

Key Areas to Address

- **Shared Drive Audit**
Regularly review shared drive memberships and permissions
- **Google Groups Governance**
Implement processes for group lifecycle management
- **Link Sharing Policies**
Establish controls around link sharing practices
- **Cross-Service Visibility**
Monitor how data flows between Gmail, Drive, and other Google services
- **Gemini Query Monitoring**
Track what information Gemini is surfacing and to whom

Opsin can also run **automated, more thorough assessments tailored to your business**, helping you uncover hidden risks faster and more comprehensively than manual testing.

[Contact Opsin today to get started >>](#)

About Opsin

Opsin safeguards enterprises from oversharing risks when using GenAI tools such as Microsoft Copilot, Google Gemini, and Glean. We work with organizations including Culligan International, Barry-Wehmiller, and Cascade Environmental on securing their GenAI deployments.

Opsin was founded by AI and security experts that were early employees at successful security startups such as Abnormal Security and Trifacta, as well as bringing leadership experience from companies like FireEye, Cohesity, and Symantec.

Email contact@opsinsecurity.com →

Website opsinsecurity.com →

Demo [Book your demo now](#) →



Securely Enable AI Without the Risk of Oversharing

