

# Google Workspace Security Posture

saasguardai.com · Scan #68 · Mon, 30 Mar 2026 07:10:47 GMT

RISK SCORE

85

GRADE

B

SCORE DRIFT

▼ -7

## EXECUTIVE SUMMARY

Identity &amp; Access (40%)

100/100

Email Security (20%)

80/100

Data Exposure (20%)

50/100

OAuth / Third-Party Risk (10%)

85/100

Governance &amp; Logging (10%)

100/100

Phase 1 · 5 findings · 2 critical · Generated 3/30/2026

### Top Risks

- Google Drive external sharing unrestricted
- Public link sharing (anyone with the link) enabled
- Automatic email forwarding to external addresses allowed

### Top Quick Wins

- Google Drive external sharing unrestricted
- Public link sharing (anyone with the link) enabled
- Third-party apps with high-risk OAuth scopes detected

## TOP PRIORITY FIXES

### #1 · Google Drive external sharing unrestricted

CRITICAL

All users can share files with anyone outside the org. No domain restriction enforced at admin level.

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Drive and Docs](#) → [Sharing settings](#) → [Sharing outside \[domain\]: OFF or restrict to allowlisted domains.](#)

### #2 · Public link sharing (anyone with the link) enabled

CRITICAL

Files shared via public link are accessible to anyone on the internet — no authentication required.

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Drive](#) → [Sharing settings](#) → [Disable "anyone with the link" for external users.](#)

### #3 · Third-party apps with high-risk OAuth scopes detected

HIGH

Apps with broad scopes (mail.read, drive, admin) can access all org data without ongoing user consent.

[Admin Console](#) → [Security](#) → [API Controls](#) → [Manage Third-Party App Access](#) → [Review each app. Block or restrict apps with overly broad scopes.](#)

### #4 · Automatic email forwarding to external addresses allowed

HIGH

Users forwarding email externally can exfiltrate sensitive data without triggering DLP.

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Gmail](#) → [End User Access](#) → [Disable auto-forwarding to external addresses.](#)

## #5 · DKIM signing not configured

HIGH

Without DKIM, outbound email is not cryptographically signed — vulnerable to tampering and spoofing.

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Gmail](#) → [Authenticate Email](#) → [Generate DKIM key](#) → [Add DNS TXT record](#).

### IDENTITY SNAPSHOT

**Total users:** 1  
**Total admins:** 1  
**Super admins:** 1  
**Dormant users (90d):** 0

**Admin MFA coverage:** 100%  
**User MFA coverage:** 100%  
**Audit logging:** Active / informational  
**Retention check:** Manual verification recommended

### GOVERNANCE EVIDENCE

Audit logging status is verified when recent admin events are visible in Reports API. If no events are found, verify retention and coverage manually in [Admin Console](#) → [Reports](#) → [Audit](#).

### MANUAL VERIFICATION CHECKLIST

#### Standard Verification Items:

- Confirm external email forwarding is disabled for end users.
- Confirm IMAP/POP legacy protocol access is disabled.
- Review Drive external sharing + public link policies.
- Confirm audit log retention meets your compliance window.
- Review OAuth app allowlist in Admin Console.

### DETAILED FINDINGS

#### CRITICAL SEVERITY — 2 FINDINGS

#### Google Drive external sharing unrestricted

Priority 100

▮ PUBLIC FILES DETECTED: 1 file(s) with external access — Fincan\_salary\_2026 (Divij Jawa) - 1 KB

100% IMPACTED 1 IMPACTED CIS 3.2 ISO 27001 A.8

#### IMPACT

All users can share files with anyone outside the org. No domain restriction enforced at admin level.

#### REMEDIATION

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Drive and Docs](#) → [Sharing settings](#) → [Sharing outside \[domain\]: OFF or restrict to allowlisted domains](#).

#### Public link sharing (anyone with the link) enabled

Priority 100

▮ PUBLIC LINK SHARING: 1 file(s) with anyone-with-link access — Fincan\_salary\_2026 (Divij Jawa) - 1 KB

100% IMPACTED 1 IMPACTED CIS 3.2 ISO 27001 A.8

#### IMPACT

Files shared via public link are accessible to anyone on the internet — no authentication required.

#### REMEDIATION

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Drive](#) → [Sharing settings](#) → [Disable "anyone with the link" for external users](#).

## Automatic email forwarding to external addresses allowed

Priority 94

▣ HIGH-RISK EMAIL FORWARDING: Divij Jawa (admin@saasguardai.com) → divijfaridkot@gmail.com

CIS 9.1 DMARC/DKIM/SPF

### IMPACT

Users forwarding email externally can exfiltrate sensitive data without triggering DLP.

### REMEDIATION

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Gmail](#) → [End User Access](#) → [Disable auto-forwarding to external addresses](#).

## Third-party apps with high-risk OAuth scopes detected

Priority 100

▣ HIGH-RISK OAUTH APPS DETECTED: 3 app(s) with dangerous permissions - SaaSGuardAI (This Application): Read all user accounts, Read mobile device info, Read all Drive files, Read all emails | Superhuman: gmail access, Full Drive access | Twilio: gmail access

CIS 16.4 SOC2 CC7

### IMPACT

Apps with broad scopes (mail.read, drive, admin) can access all org data without ongoing user consent.

### REMEDIATION

[Admin Console](#) → [Security](#) → [API Controls](#) → [Manage Third-Party App Access](#) → [Review each app](#). [Block or restrict apps with overly broad scopes](#).

## DKIM signing not configured

Priority 92

No DKIM TXT record found at google.\_domainkey.saasguardai.com. DKIM signing is not configured — outbound email is not cryptographically signed.

CIS 9.4 DKIM

### IMPACT

Without DKIM, outbound email is not cryptographically signed — vulnerable to tampering and spoofing.

### REMEDIATION

[Admin Console](#) → [Apps](#) → [Google Workspace](#) → [Gmail](#) → [Authenticate Email](#) → [Generate DKIM key](#) → [Add DNS TXT record](#).