

Control Access, Catch Misconfigurations, and Secure Google Workspace

The Challenge

Google Workspace powers daily collaboration across enterprises, but its flexible, open design can introduce security risks if left unchecked. Broad file sharing, unmanaged OAuth apps, and user sprawl can create security gaps for security teams—especially when configurations drift or MFA isn't enforced.

The Solution

AppOmni secures Google Workspace by continuously monitoring configurations, access permissions, and app integrations. Our platform evaluates posture against internal policies and best practices, identifies inactive or over-permissioned users, flags risky OAuth scopes, and detects drift from your security baseline.

With policy-based enforcement and automation, security teams can detect and fix issues before they lead to exposure or compliance gaps, without slowing down productivity. AppOmni also helps organizations align to industry and government frameworks by providing comprehensive insight into identity, configuration, and app-to-app risk.

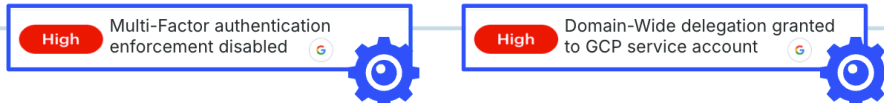
Prevent SaaS Breaches

Attackers are increasingly targeting SaaS platforms like Google Workspace using common entry points, such as weak MFA, inactive accounts, and high-risk third-party apps. AppOmni helps organizations close these gaps before they can be exploited. The following breaches show how these risks play out in the real world.



The Hacker News

Design Flaw in Google Workspace Could Let Attackers Gain Unauthorized Access



THE BENEFITS

- **Continuous visibility** into user access, app integrations, and Google Workspace posture
- **Misconfiguration detection** to identify policy drift and gaps that increase risk
- **MFA and identity enforcement** to address inactive accounts, missing authentication, and excessive permissions
- **OAuth risk control** to detect unvetted third-party apps and excessive scope permissions
- **Compliance monitoring** to support internal policies and frameworks like NIST and ISO 27001



KEY USE CASES

- Posture & Permissions Monitoring
- Identity & Access Control
- Threat & Anomaly Detection
- Third-Party Risk Management
- Compliance & Policy Enforcement

How AppOmni Prevents Google Workspace Breaches

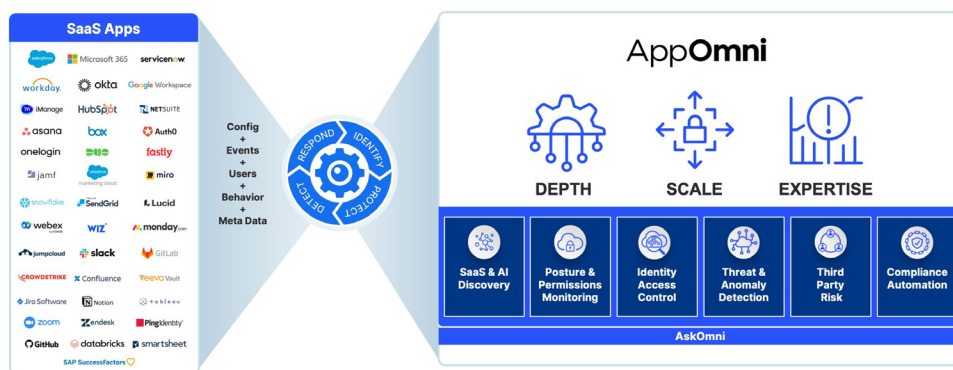
AppOmni continuously monitors Google Workspace for risky settings, unapproved app access, and identity weaknesses. By flagging issues like unprotected accounts, high-risk OAuth scopes, and suspicious user activity, we help teams stay ahead of threats and secure their collaboration environment.

The examples below highlight how AppOmni enhances Google Workspace security across multiple domains.

Use Case	How To Use It	Security Impact
Posture & Permissions Monitoring	Continuously assess Workspace org-level and app-specific settings, including file sharing defaults, calendar visibility, and access control for external domains.	Reduce risk from permissive configurations and maintain consistent security posture.
Identity & Access Control	Identify inactive users, accounts without MFA, and over-permissioned roles across Gmail, Drive, and Admin Console.	Enforce least privilege and prevent credential-based threats.
Threat & Anomaly Detection	Monitor user activity and behavioral patterns to surface signs of compromise or misuse.	Accelerate response to unusual behavior before it leads to exposure.
Third-Party Risk Management	Evaluate connected apps based on OAuth scopes, inherited access, and user connections.	Prevent data exposure through unvetted or overly permissive integrations.
Compliance & Policy Enforcement	Ensure security posture aligns to organizational controls and frameworks like NIST and ISO 27001.	Simplify audits and enforce policy across identity, configuration, and access.

Achieve Effective SaaS Security for Google Workspace

AppOmni helps security teams close critical gaps in Google Workspace—before attackers find them. From posture to third-party risk, our platform delivers deep visibility, actionable insights, and automated enforcement to protect collaboration data at scale.



“AppOmni will help you solve the risks you never knew about that could result in a breach or data exposure. The AppOmni platform solves this in a painless, efficient, and programmatic lifecycle way.

Advisory CISO, Trace3

See AppOmni in Action

Discover how AppOmni secures Google Workspace with policy enforcement, OAuth control, and access visibility. [Get a demo](#)

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by the world's largest enterprises, AppOmni specializes in securing diverse SaaS environments. Learn more at appomni.com. © 2025 All Rights Reserved