Astrix

# Google Workspace Security - Minimizing Supply Chain Risks

**Do you really know how many applications employees have connected to your organization's Google Workspace account?**

Google Workspace is a core productivity engine for many businesses. But from a security perspective, it significantly increases an organization's attack surface through its third-party integrations and add-ons. Employees are increasingly connecting third-party applications (like Zoom/Calendly/Grammarly) into their Google Email, Calendar, Docs, and Drive (and more) in a bid to increase productivity. These connections are also created when users sign in to third-party apps using the Google Single Sign-On feature. Many of these third-party apps and add-ons (connected via OAuth tokens, and sometimes even service accounts) are not vetted by security teams. They are often also published by untrusted vendors, are over-privileged or were connected by users who have since left the company.

These unmonitored connections to your Google Account (of which there could be thousands) create a new ecosystem of supply chain dependencies that expand your attack surface and expose your organization to supply chain attacks, compliance violations, and unauthorized access. This is because even if Google Workspace itself is innately secure, the more than 5,000 third-party integrations that users can connect to it may not be. And this is just counting the actual marketplace for Google Workspace apps, not the vast ecosystem of non-native apps that can and and are actively integrated all the time. This risk may apply to your company's Google Cloud Platform (GCP) environment, due to the way these environments are connected to each other.

## The threat is real

# Attacks against Google Workspace users via third-party applications

Recent high-profile attacks targeting Github, Microsoft and Mailchimp, reveal a new generation of supply chain attacks, in which attackers take advantage of access granted to third-party applications as a backdoor into organizations' core systems.

In environments like Google and Microsoft 365, attackers are not just using stolen OAuth tokens to penetrate organizations, but launching sophisticated 'consent phishing' campaigns to trick users to granting access to malicious third-party apps.

- In an OAuth phishing campaign, attackers used a fake service called "Google Apps" to trick users into granting them access to their email account, contacts and other online documents. The attack ultimately resulted in tens of thousands of dollars in losses for the state of Minnesota. Russian hackers (Fancy Bear) were using a similar method to carry out their own set attacks with a fake malicious app called Google Defender.

- In January 2022, Office 365 customers received phishing emails that aim to trick them into giving OAuth permissions to a bogus app that then lets attackers read and write emails. This exact same attack could also happen within Google Workspace.

- Researchers found OAuth flaws in Google's Single Sign-On service, allowing attackers to bypass phishing detection and email security solutions, and at the same time, gives phishing URLs a false sense of legitimacy to victims.

# Google Workspace security risks found in real organizations’ environments

Using the Astrix Security platform, our customers discovered that their Google environment is far more exposed to third-party applications than they thought, with the average number of connections 10x more than the estimated number.

From our research among organizations of over 1,000 employees, we discovered Google environments have:

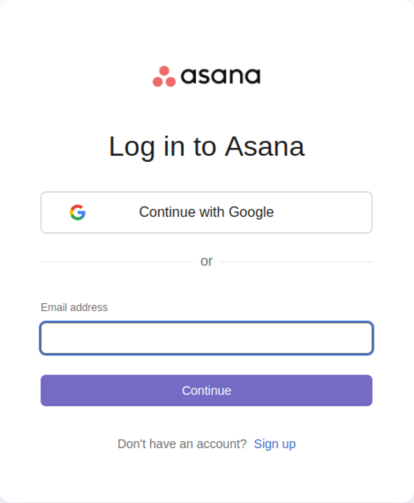
- Thousands of connections to third-party applications and Add-ons
- On average, 4-5 new integrations are added on a weekly basis

As a result, there is simply too much data for security teams to review to ensure that all Google integrations are secure.

The troubling findings include:

- **Over-privileged apps due to Google Single-Sign-On (SSO):** SSO means that an employee can login once, then implicitly grant access to his or her entire Google Workspace account – along with any assets shared with the account. This is often done by non-security personnel who don’t pay attention (or are not aware of) to the security risks the permissions granted to such apps provides. And the fact that almost every app in Google Workspace supports single sign-on exacerbates this issue.

Image A



asana

Log in to Asana

Continue with Google

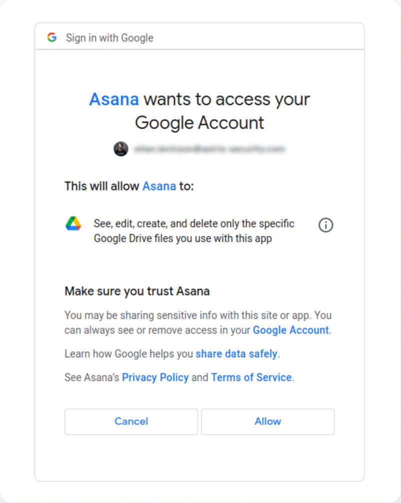
or

Email address

Continue

Don't have an account? Sign up

Image B



Sign in with Google

Asana wants to access your Google Account

[redacted]

This will allow Asana to:

See, edit, create, and delete only the specific Google Drive files you use with this app

Make sure you trust Asana

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

Learn how Google helps you share data safely.

See Asana's Privacy Policy and Terms of Service.

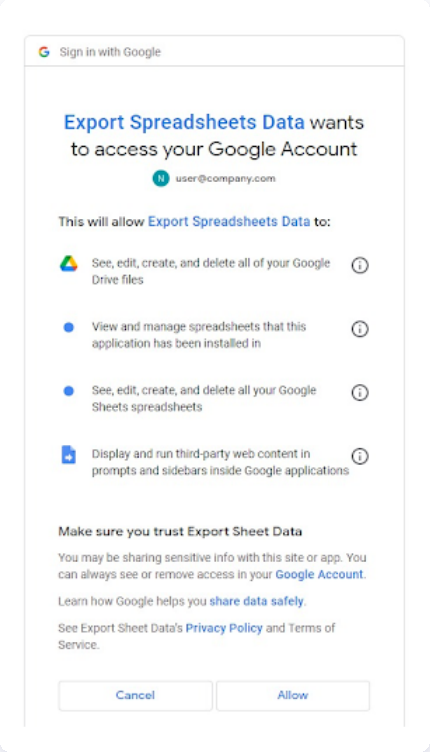
Cancel | Allow

In image A we can see the SSO option for Asana allowing users to login with one-click using their Google credentials. In image B we can see the permissions granted when signing up - Note the high level of access granted to the app (beyond the identity credentials). While the Asana application is published by a trusted vendor, there are likely thousands of third-party applications that are published by individuals that are not necessarily trustworthy, which offer the same SSO functionality.

- **Over-privileged apps published by untrusted vendors:** Astrix Security platform has found apps in Google Workspace environments that were granted with excessive permissions such as the ability to ***see, edit, create and even delete information*** contained in the drive, even though the apps did not require such permissions to perform their functionality. Many of these apps also come from untrusted individual vendors (as opposed to companies) that have a poor security reputation.

- **Mix of personal and corporate Google environments:** Astrix Security platform found incidents where poorly misconfigured connections with calendar, email & photo synchronizing apps have unintentionally created a mix between users' personal and corporate accounts and a leakage of corporate data to users' personal environment.

- **Malicious insider threats:** Astrix Security platform also found an incident where an employee (right before leaving the company) extracted sensitive information like customer records using a third-party application.



Sign in with Google

Export Spreadsheets Data wants to access your Google Account

user@company.com

This will allow Export Spreadsheets Data to:

- See, edit, create, and delete all of your Google Drive files
- View and manage spreadsheets that this application has been installed in
- See, edit, create, and delete all your Google Sheets spreadsheets
- Display and run third-party web content in prompts and sidebars inside Google applications

Make sure you trust Export Sheet Data

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

Learn how Google helps you share data safely.

See Export Sheet Data's Privacy Policy and Terms of Service.

This is an example of a third-party app published by an untrusted vendor, which asks for a high level of permissions and access to users' Google Drive.

## Existing security solutions fail to protect your Google Workspace from third-party integrations

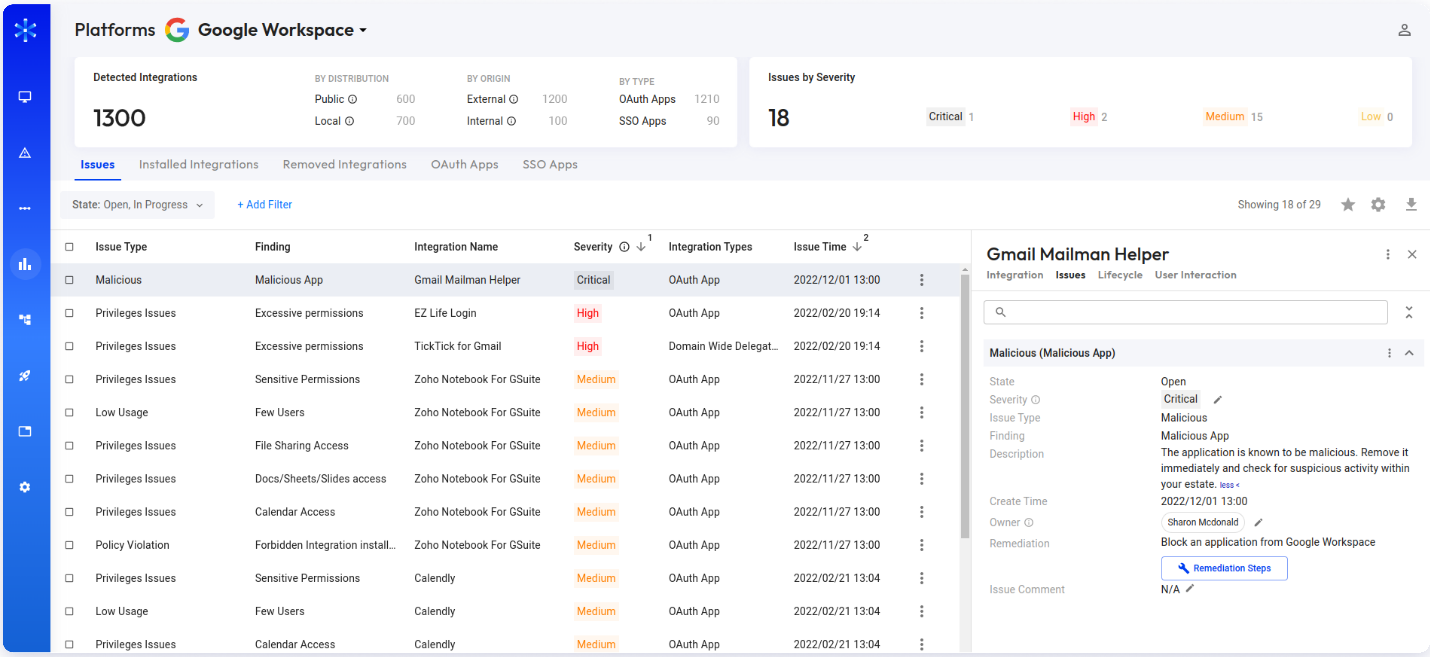
Most security solutions (Like CASB, IAM, MFA and SSO) focus on ensuring that users securely connect to Google Workspace, authenticating them and protecting their user credentials. However, such solutions don't ensure your Google Workspace is connected securely to third-party applications. Organizations should protect their access tokens (API keys, OAuth, webhooks and service accounts) as vigorously as they protect their passwords. This is because leaking an access token can be more consequential than leaking a username and password login since logins are often protected by two-factor authentication nowadays, whereas access tokens keys are not.

And if you think that monitoring for apps known to connect to Google Workspace is enough, think again. Not all apps or integrations that are compatible with Workspace are listed in central repositories, like Google Marketplace. Others can be integrated directly from websites, or from third-party marketplaces that are not monitored by Google, greatly extending the number of entry points for hackers.

# How does Astrix Secure Google Workspace?

Astrix Security Platform allows Google Workspace users to be productive while also ensuring robust supply chain security by delivering:

- **Holistic visibility:** By comprehensively identifying third-party integrations in use within your business, Astrix provides a holistic, consolidated view of all internal and external connections with your Google Workspace domain – including ones that your security and IT teams may not even know about. You can also see which access permissions users have configured for each integration.



Platforms Google Workspace

Detected Integrations
1300

BY DISTRIBUTION: Public 600, Local 700
BY ORIGIN: External 1200, Internal 100
BY TYPE: OAuth Apps 1210, SSO Apps 90

Issues by Severity
18
Critical 1 High 2 Medium 15 Low 0

State: Open, In Progress

Showing 18 of 29

| Issue Type | Finding | Integration Name | Severity | Integration Types | Issue Time |
|---|---|---|---|---|---|
| Malicious | Malicious App | Gmail Mailman Helper | Critical | OAuth App | 2022/12/01 13:00 |
| Privileges Issues | Excessive permissions | EZ Life Login | High | OAuth App | 2022/02/20 19:14 |
| Privileges Issues | Excessive permissions | TickTick for Gmail | High | Domain Wide Delegat... | 2022/02/20 19:14 |
| Privileges Issues | Sensitive Permissions | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Low Usage | Few Users | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Privileges Issues | File Sharing Access | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Privileges Issues | Docs/Sheets/Slides access | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Privileges Issues | Calendar Access | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Policy Violation | Forbidden Integration install... | Zoho Notebook For GSuite | Medium | OAuth App | 2022/11/27 13:00 |
| Privileges Issues | Sensitive Permissions | Calendly | Medium | OAuth App | 2022/02/21 13:04 |
| Low Usage | Few Users | Calendly | Medium | OAuth App | 2022/02/21 13:04 |
| Privileges Issues | Calendar Access | Calendly | Medium | OAuth App | 2022/02/21 13:04 |

Gmail Mailman Helper

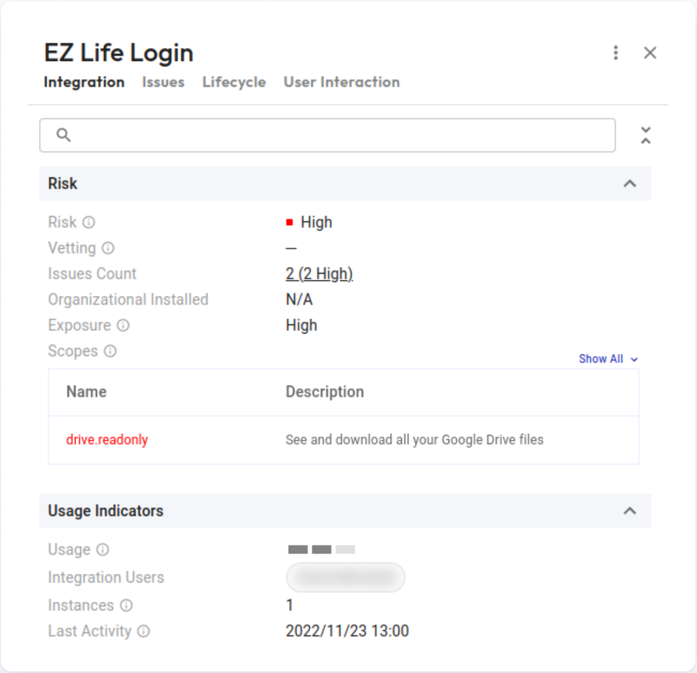
Malicious (Malicious App)

| | |
|---|---|
| State | Open |
| Severity | Critical |
| Issue Type | Malicious |
| Finding | Malicious App |
| Description | The application is known to be malicious. Remove it immediately and check for suspicious activity within your estate. less < |
| Create Time | 2022/12/01 13:00 |
| Owner | Sharon Mcdonald |
| Remediation | Block an application from Google Workspace<br>Remediation Steps |
| Issue Comment | N/A |

Here, the Astrix Security Platform pinpoints the most critical integration issues. One of the issues highlighted here is a critical-risk integration identified as being malicious, and should be removed immediately. Astrix provides quick and easy-to-follow steps to remediate the issue as fast as possible.

- **Real-time threat detection:** Our threat detection engine uses three layers of context to identify and prioritize integration risks as soon as they emerge. We help you focus on the 5% integration risks that matter the most. Astrix automatically identifies malicious third-party integrations, anomalous behavior (like suspicious source IPs and irregular activity), overly permissive integrations, redundant applications and applications developed by non-trustworthy individuals.

Using this context, security practitioners can make informed decisions about which Google Workspace integration risks to remediate first.



EZ Life Login

**Risk**

| | |
|---|---|
| Risk ⓘ | ■ High |
| Vetting ⓘ | – |
| Issues Count | 2 (2 High) |
| Organizational Installed | N/A |
| Exposure ⓘ | High |
| Scopes ⓘ | |

| Name | Description |
|---|---|
| drive.readonly | See and download all your Google Drive files |

**Usage Indicators**

| | |
|---|---|
| Usage ⓘ | ▬▬▬ |
| Integration Users | [redacted] |
| Instances ⓘ | 1 |
| Last Activity ⓘ | 2022/11/23 13:00 |

Here, the Astrix Security Platform enables you to deep-dive into a specific connection (integration). In this example, we see a high risk integration with read access to the entire Google Drive the installing user has access to. The Astrix platform shows data about the usage and API access of the integration, to help mitigate the risks imposed by the high-privileged access granted to it.

- **Rapid remediation:** We take the load off the security team by automating remediation workflows, integrating with your daily IT service management tools, and enabling end-users to resolve security issues in the process.

- **Lifecycle Management:** Monitor every third-party app from the moment it connects to your systems and automatically adapt security controls.

## Summary

For almost every service, you can sign in with Google. And once you do so, you give access to the data that the service requires. Non-security minded employees don't realize the risks associated with this, meaning that businesses with thousands of users in the workspace have a high risk that their data can be breached by malicious third-parties. Such integrations also greatly expand the attack surface further increasing the risk of data leakage, compliance violations and supply chain attacks.

Stay up-to-date with the latest in third-party integration threat prevention by downloading our free eBook, “The Ultimate Guide to Securing App-to-App Integrations" or, contact us to discuss your business’s Google Workspace security risks and how Astrix can solve them.