ADAPTIVE SHIELD

2023 SaaS-to-SaaS Access Report

Uncovering the Risks & Realities of Third-Party Connected Apps

Executive Summary

Any app that can improve business operations is quickly added into the SaaS stack. However, employees don't realize that this SaaS-to-SaaS connectivity, which typically takes place outside the view of the security team, significantly increases risk.

Whether employees connect through Microsoft 365, Google Workspace, Slack, Salesforce, or any other app, security teams have no way to quantify their exposure. These 'secondary' apps can be requesting an intrusive set of permissions or be malicious. Every click authorizing access may grant the right to edit or delete company files, send emails on behalf of the user, create new files, or otherwise handle data in a way that poses a profound threat to the organization's security.

In an effort to better understand this challenge, Adaptive Shield's researchers analyzed anonymized data from hundreds of tenants to discover the current state of SaaS-to-SaaS access.

In this research, we focused on three core questions:

1

On average, how many SaaS apps are being connected to the core SaaS stack?

2

What type of permissions are being granted to these applications?

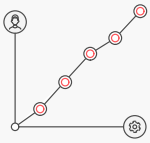
3

How high a risk are the apps that are being connected?

Our research uncovered some shocking facts

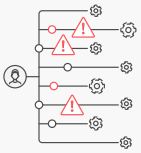
Organizations Have Thousands of Connected Apps

Organizations with 10,000 SaaS users that use M365 and Google Workspace average over 4,371 connected apps beyond the view of the security team.



The More Employees, The More Connected Apps

The number of connected apps increases significantly in relation to the number of employees.



High Level of Risk for Connected Apps

39% of apps connected to M365 and 11% to Google Workspace have ‘high-risk’ permission access.

The number of connected apps, their permissions, and the lack of visibility to app access and activity pose an increased security, privacy, and operational risk to all business operations. This report takes a deep dive into the SaaS-to-SaaS landscape, from the high-risk permissions found in the leading workspaces (M365 and Google) to exploited permissions and SaaS-to-SaaS breaches. Armed with this report, security teams can more deeply understand the risks and take the steps necessary to better protect their organizations.

Contents

The Challenges of SaaS-to-SaaS App Access

SaaS-to-SaaS app integrations are designed for easy self-service installations, boosting efficiency and functionality. However, these features pose a security nightmare. SaaS-to-SaaS app access takes place beyond the sight of security teams, and employees don't realize the risk inherent in the permissions that they are granting.

Most employees are unable to discern whether an app they would like to connect to their SaaS stack is malicious or legitimate. Furthermore, they don't realize that by granting an app read/write permissions, it now has the capacity to either inadvertently or maliciously damage the data within the original application.

As part of a zero-trust cybersecurity approach, the security team must be able to monitor all apps and access points to determine vulnerability and risk. Unfortunately, they are ill-equipped to measure or mitigate the risk associated with SaaS-to-SaaS access.

SaaS Security Posture Management (SSPM) provides visibility into third-party applications. It captures each added application as it's connected, and alerts security teams to the permission scopes being granted and the level of risk posed by the application.

Lack of Common Frameworks

There is no common framework or standard that defines the level of risk for each scope across different providers. Google Workspace has restricted / sensitive / not sensitive, while the basic M365 bundle has a no scope/risk definition. Security teams struggle to create a security policy that aligns all SaaS-to-SaaS risks across the different platforms.

SSPMs provide context to each scope and help define the level of risk. This allows security professionals to easily create a security policy that can be overlayed across the entire SaaS stack.

Inconsistent Terminology & Controls

The built-in controls within each SaaS platform not only vary greatly but use significantly different terminology. While different terms may mean the same thing, most users may not understand what they are authorizing. This makes it difficult for users to make consistent choices when authorizing permissions with different SaaS apps.

Using an SSPM allows security teams to use a common language across the SaaS stack. It maps out all security controls, making it possible to manage the security settings for all the organization's SaaS applications.

The Codecov Breach

Codecov is an automated code coverage tool that allows developers to detect untested code. In late January 2021, Codecov experienced a supply chain attack that threatened nearly 23,000 customers' networks. Malicious actors were able to update the bash uploader script by utilizing credentials that they had exported from a docker image. From January until April 1, attackers squatted inside Codecov and accessed sensitive data from Codecov's customers, including environment variables such as tokens, API keys, and read access to source codes.

As a SaaS app, Codecov integrates with GitHub to offer developers an open source for their projects. The integration allows developers using Github to utilize Codecov's testing functionally for their applications. As more users adopt open source tools, the more attackers see it as a new tool for exploitation.

Research Methodology

From across 200+ tenants, Adaptive Shield's researchers aggregated and anonymized data to uncover the current state of SaaS-to-SaaS access.

Our researchers focused on the apps connected to M365 and Google Workspace, the two most dominant workspaces in today's business environment. They analyzed the different types of SaaS apps connected, risk levels, scopes and permissions granted.

Data came from a number of industries, including financial services, insurance, retail, tech, security, e-commerce, telecommunications, transportation, and healthcare.

Diving into the SaaS-to-SaaS Data

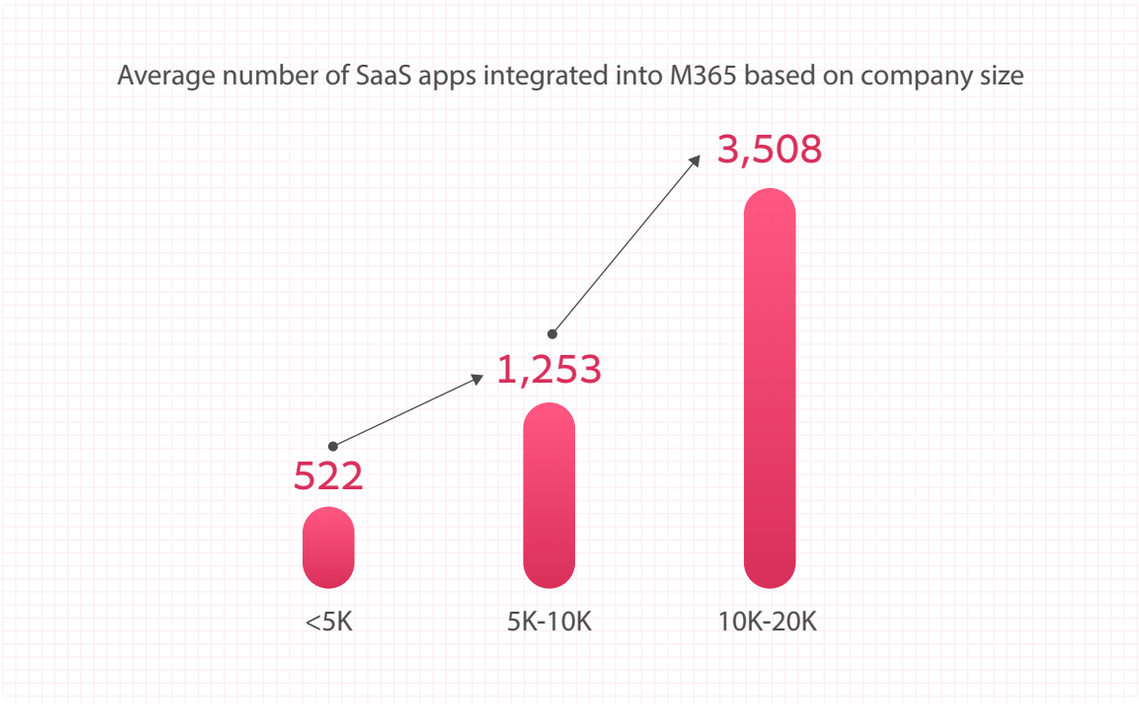
Connected Third-Party Applications

The first step in understanding the attack surface exposed by SaaS-to-SaaS access is to look at the number of apps that are typically connected to a workspace. On average, the typical company using Microsoft 365 has 0.2 connected apps per SaaS user, while companies using Google Workspace average 0.6 apps per SaaS user.

Microsoft Third-Party Connected Apps

Companies with 10,000 SaaS users average 2,033 applications connected to M365.

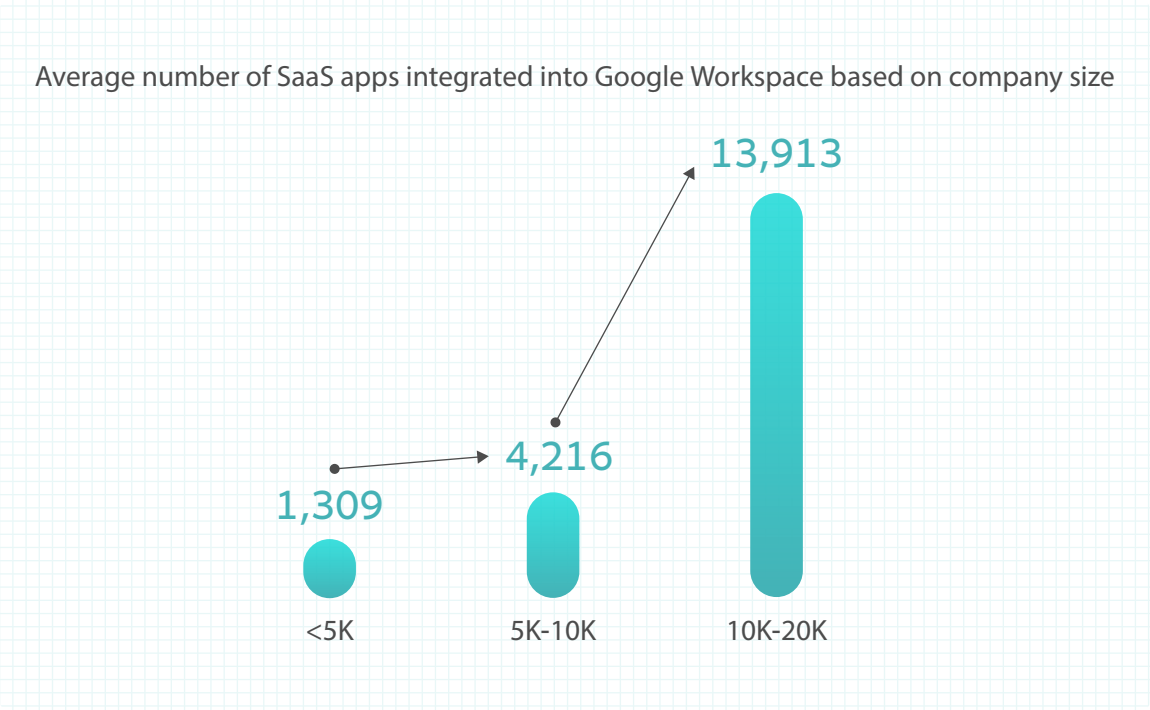
That number changes as the organization's size increases. Companies with 10,000-20,000 SaaS users average about 3,500 integrated SaaS apps. Even smaller organizations with fewer than 5,000 SaaS users have an average of 500 third-party SaaS applications connected to their core hub, all beyond the watchful eyes of the security team.



Google Third-Party Connected Apps

Companies with 10,000 SaaS users average 6,710 applications connected to Google Workspace.

Companies with 10,000-20,000 SaaS users have an average of 14,000 connected applications. Even small organizations with fewer than 5,000 SaaS users have over 1,300 different applications connected to their workspace.



Salesforce & Slack

Organizations use many business-critical apps, from M365 and Google Workspace to Slack, Salesforce and more. The numbers listed above are just the starting point.

In addition to the high average of apps connected to M365 and Google Workspace, organizations have an average of 222 connected SaaS apps for Slack. Salesforce, an app used by only a small portion of the workforce, averaged 41 apps per instance.

These numbers are impacted based on the size of the organization and the number of core apps used.

Connected SaaS Apps by Category

The most frequently connected apps are divided into 10 categories, as seen in Figure 4. By far, email applications are the most frequently connected apps, using email add-ons and email client SaaS applications. Next are apps related to file and document management.

Figure 4.
Top 10 SaaS-to-SaaS Apps by App Category

1. Email Clients
2. Files and Documents
3. Communications and Meetings
4. Calendar and Scheduling
5. Data and Analytics
6. Content Management
7. Productivity and Project Managment
8. Security
9. Images and Videos
10. Marketing tools

Takeaway

While both Microsoft 365 and Google Workspace organizations have a large number of connected apps, organizations using Google tend to connect with more third-party applications. This is most likely due to:

- The wide offering of apps available in the Google ecosystem
- Google Workspace's app-friendly design

When hardening your SaaS security, the first step is identifying the number of apps that your core SaaS stack is connected to.

An SSPM solution provides your security team with insight into the apps connected to your core stack.

Risk Levels & Permission Type Breakdown

After identifying the third-party SaaS applications connected to a SaaS stack, security teams need to understand the types of permissions being granted to these applications. The scopes being granted to applications in both Microsoft 365 and Google Workspace were analyzed.

Microsoft 365 Permission Scopes

The two most common high-risk scopes within the Microsoft 365 ecosystem grant the app the ability to read, create, update and delete data. Together, they make up 27% of all high-risk scopes being granted.

Top high-risk scopes and the frequency with which they appear

Scope Requested	Percentage of Time Scope is Requested
Allows the app to read, create, update and delete all files that you can access.	15%
Allows the app to read, update, create and delete email in your mailbox. Does not include permission to send mail.	12%
Allows the app to send mail as you.	10%
Allows the application to have full control of all site collections on your behalf.	8%
Allows the app to have the same access to information in your work or school directory as you do.	7%
Allows the app full access to your mailboxes on your behalf.	4%
Allows the app to create, read, update and delete applications and service principles on your behalf. Does not allow the management of consent grants.	4%
Allows the app to read, create, update, and delete your files.	4%
Allows the application to edit or delete documents and list items in all site collections on your behalf.	4%
Allows the app to read, update, create, and delete your mailbox settings.	2%

Figure 5. High-Risk Scope Requests in M365

A Dangerous Loophole in Microsoft

Recently, a team of **researchers** discovered a standard functionality in Microsoft 365 with the potential to allow ransomware to encrypt files stored in SharePoint and OneDrive so that they would be completely unrecoverable without dedicated backups or a decryption key.

In order to exploit this loophole, the attacker must gain initial access to either SharePoint or OneDrive. Such access can be gained through a SaaS-to-SaaS app with access to SharePoint or OneDrive using a “Files.ReadWrite” or "Sites.ReadWrite.All" permission scope. While this type of attack has yet to be reported, it highlights how vulnerable organizations are to SaaS-to-SaaS access.

Google Workspace Permission Scopes

The top three high-risk permission sets requested (78%) the ability to see, edit, create, and delete any or all Google Drive files, emails, and docs.

Top restrictive (high-risk) scopes in Google Workspace applications, listed in order of frequency

Top Restrictive Scopes	Frequency Requested
See, edit, create, and delete all of your Google Drive files.	40%
Read, compose, send, and permanently delete all your email from Gmail.	24%
See and download all your Google Drive files.	14%
View your email messages and settings.	5%
Read, compose, and send emails from your Gmail account.	3%
See, edit, create, or change your email settings and filters in Gmail.	2%
See information about your Google Drive files.	2%
Manage drafts and send emails.	2%
Use Google Fit to see and store your physical activity data.	2%
See your Google Fit speed and distance data.	1%

Figure 6. Restrictive (High) Scope Requests

Figure 7 shows the top sensitive (medium risk) scopes. They have diverse requested permissions, from "Allow this application to run when you are not present" to "Manage your AdWords campaigns." Interestingly, Google has isolated the ability to see, edit, create, and delete Sheets as a sensitive scope and takes up the majority of medium severity scopes at 36%.

Top Sensitive (medium risk) Scopes

Top Medium Scopes	Frequency Requested
See, edit, create, and delete all your Google Sheets spreadsheets.	36%
View and manage your data in Google BigQuery and see the email address for your Google Account.	25%
Connect to an external service.	5%
Display and run third-party web content in prompts and sidebars inside Google applications.	3%
Send email as you.	3%
View your data in Google BigQuery.	3%
See, edit, share, and permanently delete all the calendars you can access using Google Calendar.	2%
Allows this application to run when you are not present.	2%
See and download any calendar you can access using your Google Calendar.	1%
See, edit, create, and delete all your Google Docs documents	1%

Figure 7. Sensitive (Medium) Scope Requests

Takeaway

Organizations are frequently being asked to hand over high-risk permissions to third-party applications regardless of whether they use Microsoft 365 or Google Workspace. Having the insight from your SSPM into the granted scopes enables the security team to close loopholes within the SaaS applications and protect data from being deleted or exposed.

GitHub's Bug

GitHub, a repository hosting and management service, **disclosed** that over a 5-day period in June a bug in GitHub's app marketplace enabled an escalation of already granted permissions to third-party applications.

An app originally granted any "read" permissions during that time period could have generated new tokens with elevated "write" permissions. For example, permission to read workflows in GitHub could be elevated to permission to manage workflows. Had an attacker been aware and taken advantage of this bug, it could have led to major security issues, including data loss, exposure of company IP, and compromised login credentials.

Risk Levels by Environment

After identifying the volume of connected applications and looking at the scopes being requested, security teams need to understand the level of risk inherent within a scope request.

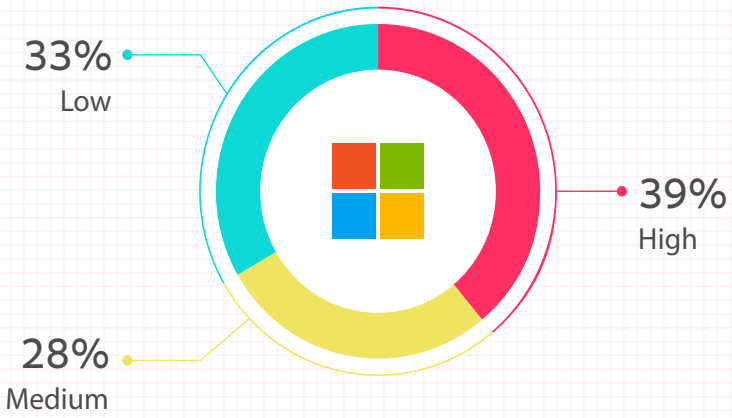
The Risk Levels for Permissions in Microsoft 365

The basic M365 bundle does not have a built-in classification method for the scopes being accessed by SaaS-to-SaaS apps. The low, medium, and high-risk scopes requested in Microsoft were categorized by Adaptive Shield based on thorough research and cyber expertise.

These assessments evaluate risk factors such as the type of the scope, its read versus write permissions, and the resources the app is accessing (e.g., directory, files, emails, printers, calendars).

The level of scopes requested by each app are categorized by their level of severity, as seen in Figure 8. SaaS apps given access to M365 accounts are distributed with 39% high risk, 28% medium, and 33% low severity levels.

Figure 8.
Distribution of Microsoft 365 SaaS-to-SaaS app by the level of risk

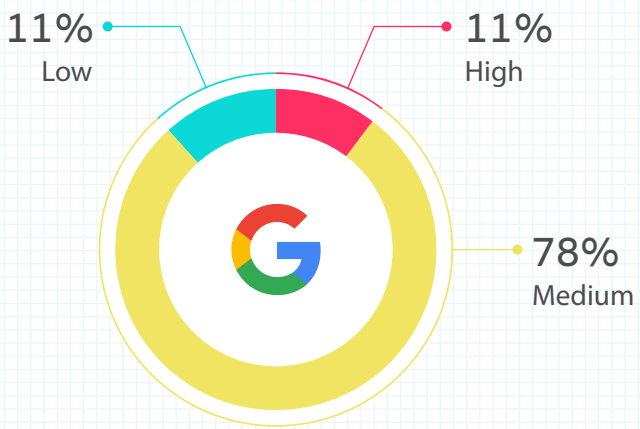


The Risk Levels for Permissions in Google Workspace

Google developed its own definition of scope severity and categorized them into Restricted (high), Sensitive (medium), and Non-Sensitive (low). Google sets specific requirements and conducts assessments in order to define scopes in these categories.

In order to define a scope as Restricted, Google states it must meet the **Additional Requirements for Specific Scopes** and an independent **third-party security assessment**. Figure 9 shows the distribution of apps by severity level, with nearly 80% considered medium severity risk – and more than one in ten poses a high risk.

Figure 9.
Distribution of SaaS-to-SaaS Permissions by Severity



Takeaway

High-risk scopes can result in intrusive permissions that lead to data loss in the event of bugs or a malicious takeover attack. Security teams need to identify all high-risk scopes and conduct a risk-benefit analysis to determine whether the added functionality is worth the risk. Additionally, compliance scores (GDPR, SOC 2, HIPAA, etc.) can be affected if the scopes granted impact the company's security posture.

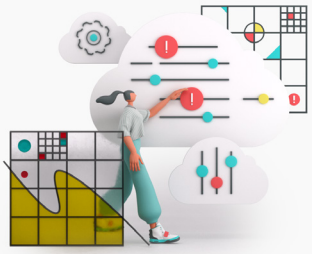
SSPM solutions can assist security teams in identifying and closing risks emanating from a third-party application in real time. They ensure that the security team is aware of the expanded attack surface, and can make the necessary adjustments to limit exposure.

Insights & Conclusion

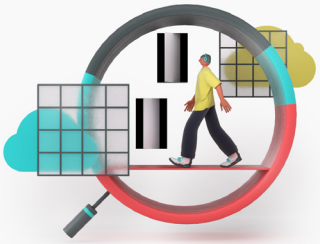
A cursory glance at all this data might lead one to think that the Microsoft environment has less cause for concern due to fewer connected applications. However, that is not the case.

While there are more third-party applications typically connected to the Google Workplace (on average 6,710 in Google Workspace compared to 2,033 in M365), 40% of Microsoft permission requests are high risk. This is significantly higher than Google. When running the numbers, the amount of oversight and control needed by the security team working with Microsoft and Google to secure the connected apps are on a similar scale.

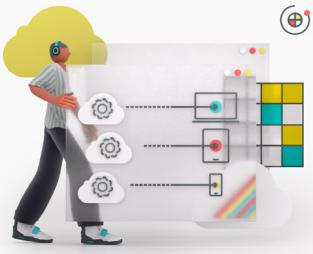
An SSPM platform is equipped to identify third-party application risk and detect threats from malicious third-party SaaS applications. In addition to SaaS-to-SaaS, SSPMs manage the entire SaaS ecosystem's security including:



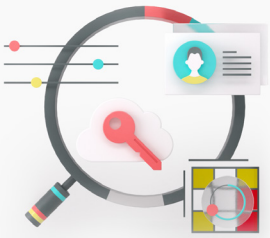
SaaS Misconfigurations



Identity & Access Governance



Device-to-SaaS User Risk Management



Identity Threat Detection & Response (ITDR)

About Adaptive Shield

Adaptive Shield enables security teams to start securing their entire SaaS ecosystem's security by strengthening the organization's SaaS posture, and detecting and responding to SaaS threats. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and has been named Gartner® Cool Vendor™ 2022.

For more information, visit us at www.adaptive-shield.com or follow us on LinkedIn.

www.adaptive-shield.com

Follow us on LinkedIn

Research Team

Led by Eliana Vuijsje, Marketing Director
Lilit Grigorian, Product Manager
Zehava Musahanov, Content Manager
Arye Zacks, Sr. Technical Content Specialist