

WHITEPAPER

# SaaS Application Risk Report

Analysis shows that 75% of SaaS applications pose a high or medium risk to data stored in Google Workspace and Microsoft 365.

---

# Table of Contents

---

Spin.AI released new findings from SpinOne, its SaaS Security platform, analyzing risk from third-party SaaS applications and browser extensions with access to enterprises' Google Workspace and Microsoft 365 environments. The findings emphasize the need for enterprises to have visibility into all applications connected to their environments, and the potential security risks these applications pose to their critical SaaS data.

This report provides detailed background and analysis on the following topics:

<b>The modern SaaS environment</b>	<b>01</b>
<b>How risky are the SaaS applications I use?</b>	<b>02</b>
<b>What types of access do applications have to my data?</b>	<b>04</b>
<b>Examples of low and high risk applications</b>	<b>05</b>
<b>What damage can a high-risk SaaS application cause?</b>	<b>07</b>
<b>Four questions to ask yourself about SaaS application risk</b>	<b>08</b>
<b>How Spin.AI evaluates SaaS application risk</b>	<b>09</b>

# The Modern SaaS Environment

SaaS applications provide users with modern productivity, communication, and collaboration tools regardless of location. This flexibility has increased efficiency, accelerating the cloud journey for organizations worldwide. The sheer number of SaaS applications in the enterprise reflects this transition.

For example, large organizations can have **thousands of SaaS applications with OAuth permissions** to Google Workspace or Microsoft 365, including both native SaaS applications (those provided by the cloud vendor) and third-party SaaS applications.

**OAuth** allows users to easily login to third-party and native applications using access tokens, but it can put SaaS data at risk depending on the type and level of access granted to the application. Attackers can abuse applications with high permissions by deleting, encrypting, leaking, or changing SaaS data.

SaaS applications are typical in the modern hybrid workforce, but their adoption requires organizations to carry out a proper risk assessment of each SaaS application accessing the data in these environments.

SecOps teams can take up to

# 2 WEEKS

per application to conduct a manual risk assessment which can be time consuming and non-repeatable.

When you have a lot of apps connected to your mission-critical SaaS data in Google Workspace or M365 automation is an important consideration.



# How risky are the SaaS applications I use?

While SaaS applications enable collaboration and efficiency, this new level of accessibility is also a double-edged sword. Risky applications introduce Shadow IT - putting critical data at risk with malicious apps and browser extensions, data leaks, and even ransomware attacks.

Analysis of SaaS applications shows that risky applications are far more common than one might think. Note in figure 1 below the average risk levels of SaaS applications with OAuth access to mission critical SaaS data.

When you factor in both high and medium risk, the analysis shows that more than

# 75%

of SaaS applications pose a high or medium risk to data stored in Google Workspace and Microsoft 365.

On average, a surprising 35% of apps with OAuth permissions to Google Workspace or Microsoft 365 are classified as high risk, with 24% of apps being high risk for Microsoft and 35% being high risk for Google environments.

Figure 1. Risk Levels for SaaS Applications With OAuth Permissions to Microsoft 365 and Google Workspace

	High Risk %	Medium Risk %	Low Risk %
All apps	34.63	41.11	24.26
All apps for large organizations (>2000 users)	56.91	26.46	16.63
All apps for small organizations (<2000 users)	27.39	20.24	22.37
Google OAuth	34.60	41.53	23.87
Microsoft OAuth	24.21	12.16	63.63

---

We believe that there are several factors that are driving high levels of application risk.

### 1 Assessment

The first and most significant factor is that within the enterprise, there is a difficulty to inventory, assess, and control the sprawl of these applications. An assessment cannot be a point-in-time view as applications may become more hardened or vulnerable to attack over time. Having the ability to track those changes and control access to them is a significant challenge and blind spot for enterprises not equipped to tackle this challenge at scale.

### 2 OAuth abuse

A second factor contributing to application risk is OAuth abuse. Because OAuth tokens do not require knowledge of a user's password, malicious applications can pose as legitimate applications to gain high access levels that allow them to steal or manipulate data.

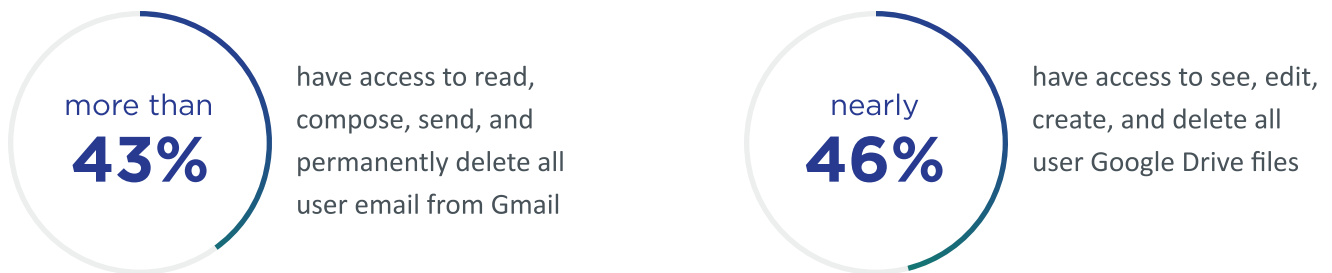
### 3 Assumption

A third factor is the assumption by many organizations that tools such as Microsoft Defender are assessing all application risk to Microsoft environments, when in fact, these tools may assign the same risk for different application permissions, leaving security gaps for risky applications to exploit.



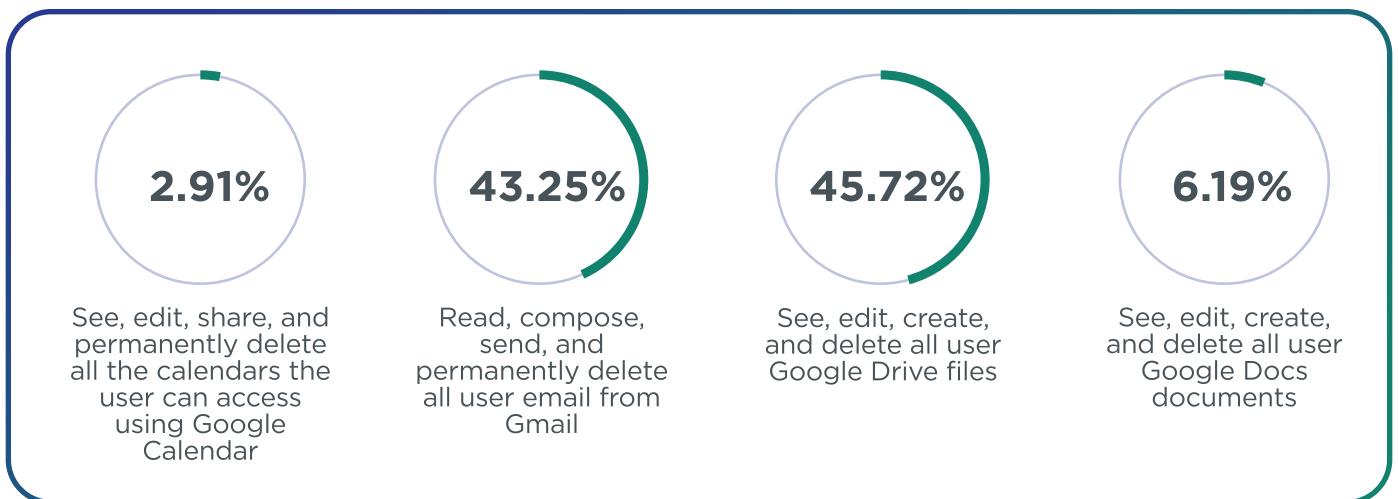
# What types of access do applications have to my data?

The analysis in figures 2 below provides examples of the types of access that various applications can have to SaaS data in Google Workspace environments. Some of the percentages are low which we believe shows that organizations are actively managing configurations and that application marketplaces are helping enterprises determine the risk of an application. But some applications have surprisingly high levels of access. For example:



The reason so many applications have high Gmail permissions is that many of the most popular Google Workspace applications are extensions of Gmail functionality, including assisting with personalization, tracking, collaboration, and routing. Those applications are commonly installed by end users and require extensive permissions.

Figure 2. Percent of Applications with OAuth Permissions to Google Workspace Data



# Examples of low and high risk applications

With nearly **5,300 applications** in the Google Workplace Marketplace and **15,000 applications in the Microsoft Azure Marketplace**, the options are endless for users. Here are examples of popular applications in use at many organizations today, and their related risk levels.

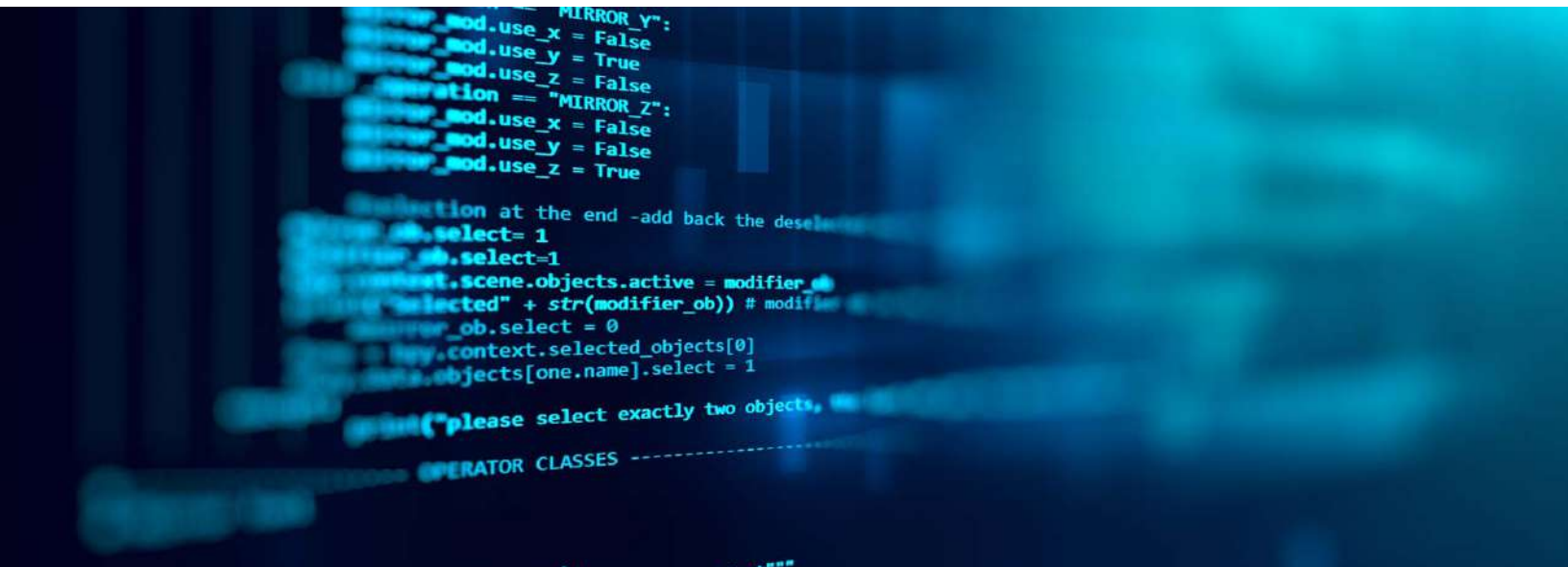
## Low Risk

A graphic design application does not want risky permissions and can be considered as lower risk to install and use.

## High Risk

A project management application has the following dangerous permission scopes requested that may affect the security and privacy status of your data:

- See and download all your Google Drive files which may result in classified information disclosure that may include sensitive data such as financial records, medical reports, photos, or tax information, as well as the names of people these files are shared with
- See, edit, download, and permanently delete your contacts which may result in disclosing contact information including names, phone numbers, addresses, notes, and other information about the people you know



---

SaaS applications have long been the target of attackers and provide a dangerous entrypoint to business-critical SaaS data. Note the following SaaS application breaches that led to otherwise lower risk SaaS apps becoming high risk apps overnight:

## LinkedIn

In April 2021, a database containing the personal information of 500 million LinkedIn users was posted for sale on a hacker forum. The data had **reportedly been scraped from LinkedIn's systems**.

## HubSpot

On March 21, 2022, HubSpot **reported a breach** which happened on March 18. Malicious actors compromised a HubSpot employee account that the employee used for customer support. This allowed malicious actors the ability to access and export contact data using the employee's access to several HubSpot accounts linked to top cryptocurrency firms.

## {okta}

On March 22, 2022, DEV-0537, which is more commonly known as LAPSUS\$, **compromised approximately 2.5% of Okta** customers.

## LastPass

On December 22, 2022, LastPass disclosed that a security incident in August had led to a **data breach** of customer account information.



# What Damage Can a High-Risk SaaS Application Cause?

A high-risk application can damage your data, steal your data, delete your data, damage your reputation, and reduce customer confidence, leading to irreparable consequences - including loss of revenue, compliance fines, and litigation.

An all-out malicious application containing cloud ransomware can encrypt, change, or delete your data. "Leaky" SaaS applications can lead to compliance and privacy risks and result in high costs from a data breach.

IBM's [Cost of a Data Breach Report 2022](#) notes the following average costs across the landscape of business sectors:



Average total cost of a data breach globally



Average cost of a ransomware attack



Average cost of a data breach in the United States



Average cost of a data breach in healthcare



# Four Questions to Ask Yourself About SaaS Application Risk

With the mounting risk that SaaS applications can pose to mission-critical data, businesses need to consider these essential questions:

1. Which SaaS applications are installed and have access to my SaaS data?
2. What specific data do these applications access?
3. What risks are posed by the applications integrated with the SaaS environment?
4. How do I inventory, assess risk, and control these applications?
5. How do I re-assess risk and manage access for applications every time when there is an update?

**Mature organizations typically employ a comprehensive approach to assessing the security of third-party SaaS applications. What does this include?**

## Application Inventory

Maintaining an inventory of applications and extensions that have access into your environment, and flagging in real time when they are granted OAuth permissions, is vital to understanding the operations, security, privacy, and compliance risks they present.

## Risk assessments and re-assessment

Ongoing risk assessments are critical in the overall strategy to secure SaaS applications and identify potential security risks. Data should be identified that will be processed, stored, or transmitted through the application and any associated risks. Maintaining ongoing assessments is vital to understanding how apps have either become more vulnerable or hardened against operations, security, privacy, and compliance risk.

## Policies




Policies based on your third party risk management frameworks should be established and enforced. These policies should be attributable to SaaS application factors and consider their dynamic nature, their operational use, and the risks and needs of the business.

## Controls

Automated controls that can allow or block applications based on your organizational policies are vital for alleviating the workload of security resources, especially when considering the number of SaaS applications installed within organizations.

# How Spin.AI evaluates SaaS application risk

Spin.AI's platform, SpinOne, uses machine learning (ML) to collect and analyze data to assess each SaaS application's risk. From this analysis, an overall security score is generated based on the results of the automated risk assessment. The overall risk score is comprised of several key components, including:

-  Scope of the Permissions
-  Business Operation Risk
-  Security Risk
-  Compliance Risk

For example, a risky application may have the following characteristics:

- It requests high levels of permissions to the SaaS environment, regardless of the need
- It may have very few or a single developer, leading to an increased risk of business continuity issues related to application bugs or security concerns
- It may not have regular updates which can lead to a vulnerable application
- It may have poor reviews on the cloud marketplace, Microsoft Azure or Google Workspace Marketplace
- Its developer may not disclose or undergo a third-party security or compliance audit, leading to increased risks of improper security controls
- It may have recently been subject to a data breach

Our findings show that nearly

# 56%

of high risk applications have high levels of permissions and nearly 39% have poor reviews on marketplaces.

Businesses must continuously evaluate SaaS applications and the risks they pose in the environment, as risk scores can change over time. For example, many organizations are reevaluating the use of LastPass by employees due to the [recent data breach](#).

Using the SpinOne automated risk assessment and an organization's security policies, SaaS applications can be allowed or blocked based on the risk score that best aligns with a company's security policies and business needs. SecOps teams can use SpinOne to reduce application risk assessment time from two weeks manually, to five minutes automatically.



---

SpinOne is an all-in-one SaaS security solution that protects SaaS data for mission critical apps so that enterprises can mitigate risk, save time, reduce downtime, and improve compliance. Spin.AI SaaS Security Posture Management (SSPM) solutions leverage the power of machine learning (ML) to perform the heavy lifting, so IT security and operations teams have the visibility and controls needed to protect the environment from risky SaaS applications. The findings in this report encompass the anonymized data of over 750 Spin.AI clients using the SpinOne platform.

Get full visibility into third party SaaS apps and Browser Extensions that have access to your mission-critical SaaS data.

**REQUEST A FREE SAAS APPLICATION  
RISK ASSESSMENT TODAY**

**Spin.ai**

@ info@spin.ai

📞 1 888-883-2993

## About **Spin.AI**

Spin.AI is an innovative provider of SaaS security solutions for mission critical SaaS apps. Enterprises use the all-in-one SpinOne platform to mitigate risk, save time, reduce downtime, and improve compliance.