Spin.ai

WHITEPAPER

Top 10 Low-Risk Applications and Extensions for Google Workspace

Authors: Davit Asatryan, Vice President of Product, Spin.AI
Sergiy Balynsky, Vice President of Engineering, Spin.AI

Table of Contents

Introduction

Google Workspace is an extremely popular SaaS productivity suite used by millions of organizations today. Companies can also extend its features and capabilities with third-party applications and browser extensions to **achieve an almost limitless set of features in Google Workspace**.

However, **this ability to extend Google Workspace features can quickly become a security liability** as employees may grant access to untrusted third-party apps with their Google credentials without fully understanding the permissions granted or the data they expose with the integration. **Even seemingly harmless and legitimate integrations can pose risks to organizations' most critical data**. So how do you know if your organization has integrated apps and extensions that are low risk or high risk? Let's look at the top 10 most popular low-risk applications and browser extensions as of Q2 2024. And for comparison, let's also take a look at the top 5 most popular, high-risk browser extensions. We will uncover the **risks you should know about related to Google Workspace SaaS data** stored across Gmail, Drive, Shared Drives, Calendar, Contacts, and Google Sites.

Even seemingly harmless and legitimate integrations can pose

RISKS

to organizations' most critical data.

The Explosive Growth of SaaS

SaaS applications and browser extensions are seeing high growth and adoption across the enterprise.

Growth in SaaS Market

The global SaaS industry has seen explosive growth. While the SaaS market was valued at USD 237.48 billion in 2022, it had increased to approximately USD 273.55 billion by the end of 2023. **By 2030, the industry is expected to soar to nearly USD 908.21 billion**.

By 2030, the global SaaS industry is expected to soar to nearly

$908B

Since 2018, SaaS technology adoption has increased

71%

in organizations worldwide.

Adoption Rates

Organizations worldwide have adopted SaaS environments at a rapid pace. An estimated 95% of organizations have adopted SaaS technology by 2023. This has been **a 71% increase in the adoption rate since 2018**.

Future Predictions

By 2025, some 85% of all business applications will be SaaS-based.
This statistic reflects the continuing shift towards cloud-based solutions and away from on-premise deployments.

85%

of all business applications will be SaaS-based by 2025.

Top 10 Low-Risk SaaS Apps

1 LinkedIn | Professional Networking

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	High	Low	Low

Permissions	Why It Matters
This app has permissions to access a user's profile information and email	While LinkedIn is considered low risk, the high business risk reflects its central role in professional networking, where data privacy is crucial

2 Adobe | Creative Software

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Access to profile information and email	Adobe's suite of creative software is essential for many businesses, making its access to user information a point of interest for ensuring data protection

3 Dropbox | File Storage & Collaboration

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Basic operational permissions	As a popular tool for file storage, Dropbox's operational security is crucial for safeguarding sensitive business data

4 Grammarly | Writing & Grammar Checking

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	High	Low	Low

Permissions	Why It Matters
Access to profile information and email	Grammarly helps improve writing quality, but access to sensitive content requires attention to privacy practices

5 Booking.com | Travel

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	High	Low	Low

Permissions	Why It Matters
Profile information and email access	In the context of travel planning, protecting personal and travel-related information is key

6 CloudConvert | File Conversion

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Notifications	CloudConvert's ability to handle diverse file types underlines the importance of secure data handling practices

7 Coursera | Online Learning

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	High	Low	Low

Permissions	Why It Matters
Access to profile and email	Coursera's access to educational materials and user data underscores the need for privacy in online learning

8 Airtable | Database & Organization

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Operational permissions	As a tool for database and organization management, Airtable's security measures are vital for data integrity

9 Bitly | Link Management

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Access to profile information and email	Bitly's link management services necessitate attention to how user data is managed and protected

10 Yelp | Food, Delivery & Reviews

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	High	Low	Low

Permissions	Why It Matters
Access to profile and email	Yelp's access to user information underscores the need for data privacy

Top 10 Low-Risk Browser Extensions

1 Honey: Automatic Coupons & Cash Back | Shopping

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Broad access including scripting, web requests, storage, and cookies on all websites	While aimed at saving money for users, the extensive permissions necessitate a balance between functionality and privacy/security

2 Adblock Plus – Free Ad Blocker | Workflow & Planning

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Can block and manage web content across all websites	Even though it enhances the browsing experience by blocking ads, the control over web requests highlights the need for caution

3 DeepL Translate (Beta Version) | Workflow & Planning

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Access to all URLs for translating text, with additional scripting and storage permissions	Facilitates language translation but requires broad website access, emphasizing the importance of user trust in handling data

4 Tag Assistant Companion | Developer Tools

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Scripting and web navigation across all websites	Helps with managing and verifying website tags, with permissions that could potentially access sensitive website data

5 Floorplanner | Unknown

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Notifications	Assists in designing floor plans with minimal permissions, focusing on a specific functionality with low privacy impact

6 DuckDuckGo Privacy Essentials | Privacy & Security

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Medium	Low

Permissions	Why It Matters
Broad permissions to enhance privacy across all websites, including web request blocking and browsing data management	It aims to improve online privacy, but it requires extensive access to block trackers and secure searches effectively

7 Endpoint Verification | Workflow & Planning

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Involves messaging, data storage, and device information access, focused on verifying device security and compliance	Supports IT in securing endpoints, with permissions that highlight the need for trustworthy security practices

8 Similarweb – Traffic Rank & Website Analysis | Developer Tools

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Web request management and data storage across all websites for analyzing web traffic and metrics	Offers insights into website popularity and user engagement

9 Speechify for Chrome | Education

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Low	Medium	Low

Permissions	Why It Matters
Scripting and storage across all websites for converting text to speech	Enhances accessibility by reading text aloud, necessitating data access that users should be aware of

10 Dark Theme for Google Chrome | Dark & Black

Overall Risk	Business Risk	Security Risk	Compliance Risk
Low	Medium	Low	Low

Permissions	Why It Matters
Minimal, focused on applying a dark theme to web browsing	Improves user experience by offering a visually comfortable browsing mode, with limited privacy or security concerns

Top 5 High-Risk Browser Extensions

1 Docs | Developer Tools

Overall Risk	Business Risk	Security Risk	Compliance Risk
High	High	Medium	High

Permissions	Why It Matters
• Access to specific documentation sites and tab management • Permissions for clipboard writing, downloading, accessing all URLs, storage, and notifications	• Access to tabs and specific URLs creates a risk of data leakage or unauthorized data access, especially if the extension is compromised • The ability to write to the clipboard and download content could be exploited to capture and disseminate sensitive information without proper authorization

2 Adblock for YouTube™ | Workflow & Planning

Overall Risk	Business Risk	Security Risk	Compliance Risk
High	High	Medium	High

Permissions	Why It Matters
Blocking web requests, accessing storage, and permissions for all URLs	While intended to block ads, the extension's capabilities could be misused to block or modify legitimate web requests, potentially leading to data integrity issues

3 QuillBot for Chrome | Communication

Overall Risk	Business Risk	Security Risk	Compliance Risk
High	Medium	High	High

Permissions	Why It Matters
Scripting on specific sites, alarms, storage, cookies, and notifications	The scripting and storage access can be exploited for unauthorized actions within the browser, posing significant security and privacy risks

4 SEO META in 1 CLICK | Developer Tools

Overall Risk	Business Risk	Security Risk	Compliance Risk
High	Medium	Medium	High

Permissions	Why It Matters
Access to the current tab	Access to the current tab can reveal sensitive information about the user's browsing activity and data on visited websites, potentially leading to privacy breaches

5 Edge: The Web Ruler | Productivity

Overall Risk	Business Risk	Security Risk	Compliance Risk
High	High	High	High

Permissions	Why It Matters
Keeping app window always on top and storage access	The ability to keep the app window always on top and access storage poses risks to user privacy and data security, as it could interfere with normal browser operation and access stored data without explicit user consent

Recent Examples of Security Breaches Due to SaaS Apps and Extensions

The real-world implications of SaaS security are far-reaching. Note the following recent examples of SaaS security incidents affecting a large number of users:

Malicious ChatGPT Extensions

A fraudulent extension mimicking "ChatGPT for Google" hijacked Facebook accounts and stole login credentials from at least 6,000 corporate accounts and 7,000 VPN accounts. **The rapid expansion of unregulated ChatGPT extensions poses a growing threat**.

OpenSea API Breach

OpenSea, a leading NFT marketplace, was involved in a security breach through one of its third-party vendors. The breach resulted in the exposure of user API keys. **This exposure allowed unauthorized use of these keys' allocated rate limits, highlighting vulnerabilities in SaaS cybersecurity frameworks**.

Okta Security Breach

A recent incident involving OKTA, a well-known authentication platform, potentially exposed sensitive information of thousands of users across various services. This breach highlights the importance of securing identity and access management platforms and respective SaaS apps, as these are an important part of the security posture of numerous organizations globally. **Such breaches can lead to widespread access to corporate systems, data leakage, and severe consequences to organizational security**.

How Can Organizations Protect Their Data?

Organizations must take a layered approach to secure SaaS environments, encompassing the following strategies:

Inventory

Maintain an up-to-date catalog of all SaaS applications and browser extensions integrated with their SaaS environment. This inventory process allows for understanding the various risks introduced in terms of operations, security, privacy, and compliance.

Continuous Risk Evaluation

Continual risk evaluation is needed for applications and extensions. This helps to understand the changing SaaS landscape and identify and address security vulnerabilities as they arise.

Policy Development and Enforcement

Controls are needed to **enforce policies introduced by third-party risk management frameworks**. These policies consider the evolving nature and operational demands of extensions and applications in the SaaS environment. It also helps to understand their unique business risks and requirements. Automation of these policies not only eases the burden on security teams but also ensures SaaS security is applied consistently and effectively.

Organizations must embrace an end-to-end risk management strategy to protect against ongoing threats posed by SaaS applications and browser extensions.

Organizations must embrace an end-to-end risk management strategy to **protect against ongoing threats posed by SaaS applications and browser extensions**. This strategy includes the initial discovery of all SaaS solutions and extensions within their network, continuing and proactive risk assessments of these apps and extensions, and using automated systems and contemporary cybersecurity technologies.

Spin.AI's Approach to SaaS Risk Assessment

Spin.AI's platform, SpinOne, uses machine learning (ML) technology to gather and evaluate data for the risk assessment of each browser extension and SaaS application.

This evaluation process results in a **comprehensive security score**. The score is created from several factors analyzed in the automated risk assessment. Note the following factors that are analyzed:

- The extent of permissions requested by the extension or application within the cloud environment
- The potential for operational disruptions or risks to business processes
- The security risk introduced by the application or extension
- Compliance and regulatory risk implications

In practical terms, **an extension or application might be deemed high-risk if it displays certain characteristics**, including:

- Requesting broad permissions beyond what its functionality would reasonably require
- Being developed by a limited number of contributors, potentially a single developer, which could increase the risk of unresolved issues due to limited support or development capacity
- Lacking frequent updates, which can leave the application vulnerable to security threats
- Receiving poor feedback or ratings on digital marketplaces or stores
- The developer's failure to submit to an independent security or compliance verification
- Past data breaches associated with the application or extension
- The application or extension is associated with a developer of unknown reputation, possibly identified only by a generic email address

This approach emphasizes the importance of a detailed analysis of several risk factors influencing the risk profile of SaaS applications and browser extensions.

SpinOne is a cybersecurity solution that is flexible, customizable, and versatile for app risk assessment and security automation with robust policies and approval processes.

SpinOne is a cybersecurity solution that is **flexible, customizable, and versatile** for app risk assessment and security automation with robust policies and approval processes. It can adapt to fit the app restriction needs of various organizations. If businesses want to be very conservative and block all SaaS apps and browser extensions, or if they are more open to a wide range of allowed SaaS apps for users, **SpinOne can be tailored to fit any company's security protocols for these scenarios and anything in between**.

Learn More About SpinOne and SaaS Security

With SpinOne, you'll get instant visibility into your environment's third-party applications and browser extensions in a single dashboard.

You'll see each app, the extension's risk score, and all the users accessing these apps. You can allowlist/blocklist using configurable automated policies and customized alerts.

To find out more about Google's integration of the Spin.AI Risk Assessment with the Google Workspace Admin Console, read the Google Cloud Blog article.

For more research from the Spin.AI Research Team, explore the latest reports:

- Spin.AI Application Risk Report
- Spin.AI Browser Extension Risk Report
- ChatGPT or FakeGPT

To learn more, sign up for a free 15-day trial of SpinOne or request a demo.

LEARN MORE

About Spin.AI

Spin.AI is an innovative provider of SaaS security solutions for mission-critical SaaS apps (Microsoft 365, Google Workspace, Salesforce, and Slack). Our all-in-one SpinOne platform helps organizations mitigate risk, save time, reduce downtime, and improve compliance.