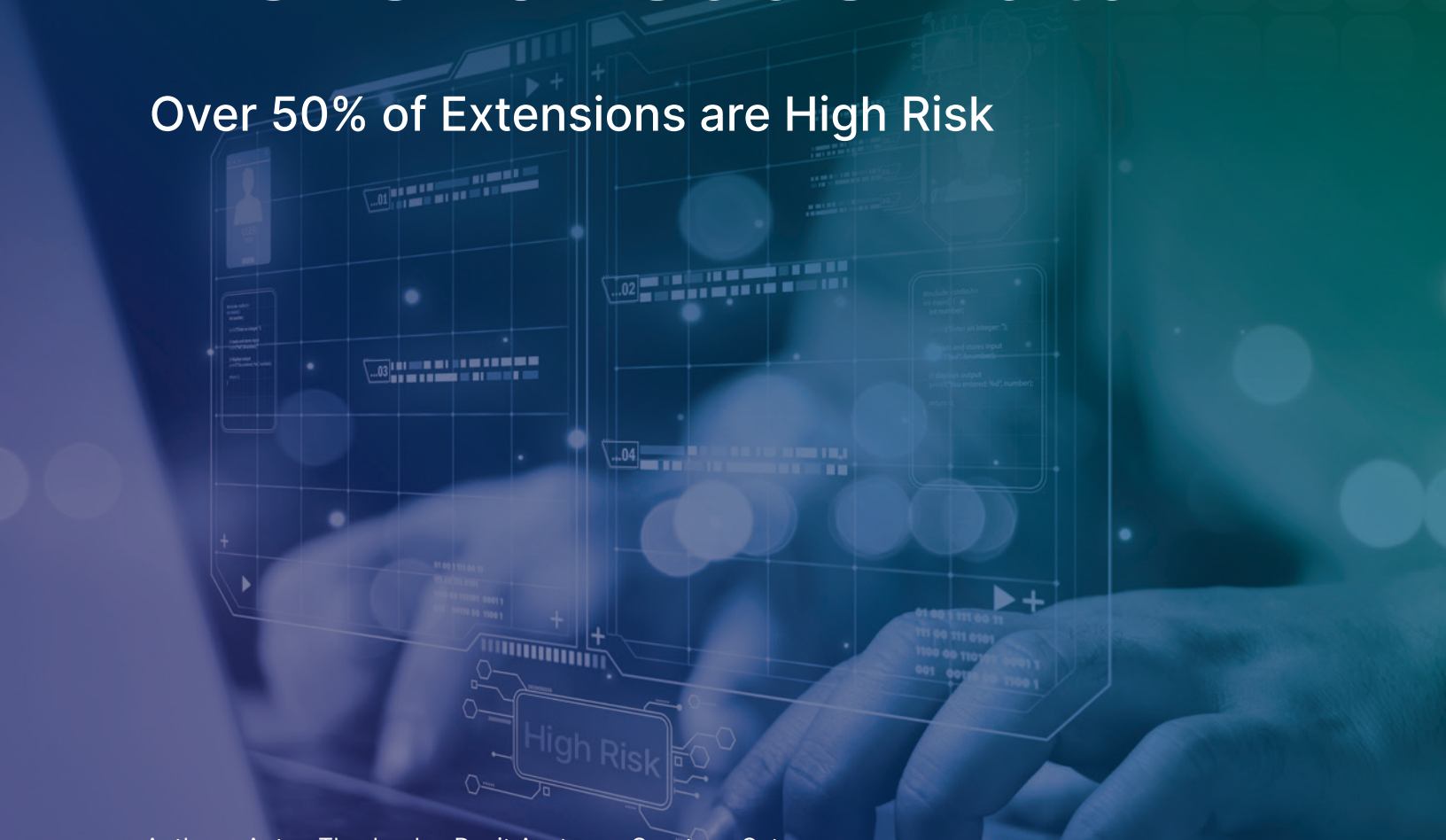
Spin.ai

WHITEPAPER

Browser Extension Risk Report: High Risks for SaaS Data

Over 50% of Extensions are High Risk



Authors: Anton Tkachenko, Davit Asatryan, Courtney Ostermann

Table of Contents

Introduction

The transition towards an increasingly digital workspace in the last decade has seen a colossal rise in Software-as-a-Service (SaaS) applications. From small-scale startups to multinational corporations, businesses everywhere leverage SaaS for increased productivity, enhanced customer engagement, and support of the hybrid workforce. However, with the digital revolution generating vast amounts of SaaS data, there is a downside — increased cybersecurity risk.

Recently, Spin.AI released the *SaaS Application Risk Report* analyzing the risk associated with SaaS applications. The report showed that 75% of SaaS applications pose a high or medium risk to data stored in Google Workspace and Microsoft 365. In this article, we'll take a similar approach with a deeper look into the risk associated with browser extensions in 2023.

The Browser Extension Landscape

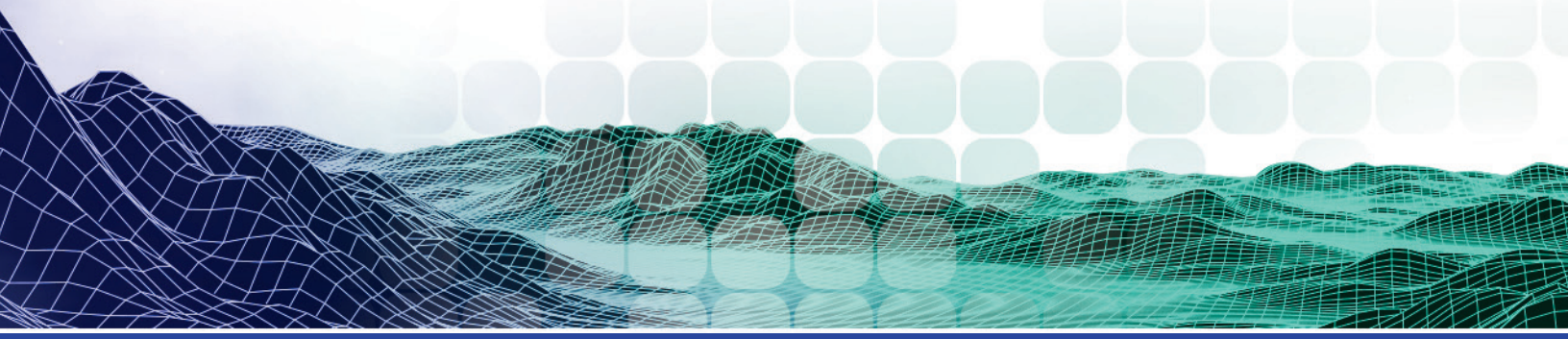
A key risk factor connected with SaaS data in mission-critical SaaS applications such as Google Workspace and Microsoft 365 involves browser extensions. These have become commonplace, offering various features to enhance user experience and productivity. Spin.AI has visibility into this large landscape, having used its AI algorithms to discover and assess over 300,000 browser extensions and third-party OAuth applications.

Google states that there are 250,000 extensions in the Chrome Web Store, but this doesn't account for extensions available outside the official marketplace. For example, Spin.AI has already uncovered more than 2,000 extensions outside of the marketplace which are used by our customers. The browser extension landscape is broad and growing.

Anonymous extension authors

Interestingly, our research team found that many extensions — 42,938 to be precise — have unknown authors. This statistic is especially concerning as it underscores the significant risk to companies using apps from unknown or untrusted developers, given that anyone with malicious intent can publish an extension in the marketplace.

In addition, the average number of extensions installed in a company with over 2,000 employees is 1,454 extensions. Combining the number of extensions used by unknown or untrusted developers with the sheer number of extensions and apps in use across most organizations today paints a worrisome picture of the potential security vulnerabilities lurking in these extensions.

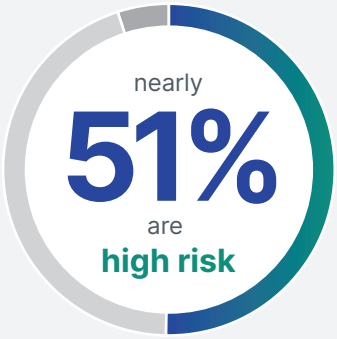


Browser extension risk factors

To understand the risk extensions pose, Spin.AI has classified them into high, medium, and low-risk categories. Extensions are evaluated by the SpinOne platform on the operational, security, privacy, and compliance risks they pose.

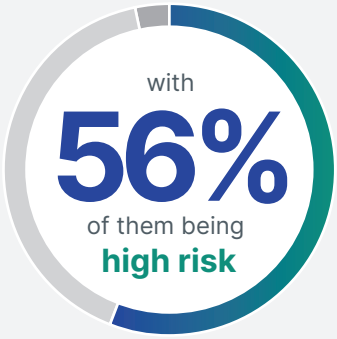
Here are the statistics for risk categories distributed across company size and extension categories. Note:

Of **all extensions** installed



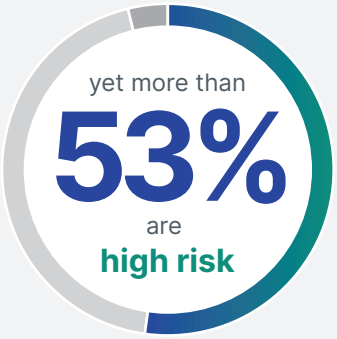
(See Figure 1 below)

Developer tool extensions are the **highest risk**



(See Figure 2 on page 6)

Productivity extensions are the **most installed**



(See Figure 2 + 3 on page 6)

Dimension	High Risk %	Medium Risk %	Low Risk %
Total	50.53	44.50	4.97
< 2000 users company size	27.49	49.69	22.82
> 2000 users company size	35.01	48.62	16.37

Figure 1: Browser extension risk scores overall and by company size

The prevalence of high-risk extensions can be attributed to various factors like the difficulty of assessing risk, the economics of cybercrime, and misconceptions about what vendors like Google and Microsoft protect. However, medium or high-risk extensions pose serious threats.

Extension Category	High Risk %	Medium Risk %	Low Risk %
Accessibility	52.84	44.66	2.49
Developer Tools	56.07	40.78	3.15
Productivity	52.35	43.9	3.75
Search Tools	46.22	49.16	4.62
Themes	1.29	63.79	34.91

Figure 2: Browser extension risk scores for the top 5 categories of extensions according to volume installed

Medium and high-risk apps have access to high levels of content, allowing them to capture data or run potentially malicious JavaScript. Furthermore, B2C developers (generally writing a large percentage of browser extensions) don't consider compliance factors, further enhancing the risk.

This report helps to highlight that browser extensions can pose the same and even higher risks than third-party SaaS applications to business-critical data, underscoring the unique risk posed by browser extensions. It emphasizes the importance of proactively managing and mitigating these risks within your organization.

Note the following most popular categories of extensions installed, with examples from each, indicating the diverse range of needs that extensions cater to within organizations.

Extension Category	Average per Organization	Example
Accessibility	17	Dark Reader
Developer Tools	51	Copilot
Productivity	97	Grammarly
Search Tools	14	Norton Safe Search
Themes	27	Morpheon Dark

Figure 3: Average number of extensions installed per organization for the top 5 categories

Extension Data Access Levels

Extensions have diverse permissions, each presenting different risk levels — high, medium, and low. Specific characteristics, such as the extent of access to data and the potential for malicious activity distinguish these levels of risk.

Extensions may acquire this information through various permissions granted by a user. Understanding permissions granted to extensions is crucial for a few reasons:

- **An extension could be harmful from inception but may also become malicious through updates throughout the supply chain.** Extensions automatically update, and an attacker can transform a benign extension into a hostile one without the user's knowledge. Additionally, a legitimate developer's account could be compromised, resulting in malicious updates appearing in the official store under the developer's name.
- **Developers may also sell their extensions to companies offering attractive sums.** These companies may then update the extension with malicious features. Extensions can be challenging to monetize, making the offers for purchase enticing to developers.
- **Many extensions possess the capability to gather extensive user data.** Some developers sell anonymized data to third parties to generate income, leading to compliance risks without the knowledge of users or businesses.

Users may encounter two primary issues concerning extensions:

1. **Unauthorized actions by a malicious application**, such as manipulating "like" buttons to increase subscriptions or traffic, commonly a paid service. Security researchers and platforms like Google regularly detect and neutralize such applications.

2. More ominously, **an extension may gather sensitive information**, such as Internet banking details, login credentials, and authentication tokens. As information is a valuable commodity, these extensions present a higher risk.

More importantly, permissions can also be used together in a way that leads to greater security or compliance risks (see figures 4 + 5 on page 8). For example, an extension could obtain "identity" permission and then use the "webRequest" permission to send this information to a third party. Closely monitoring SaaS app permissions and understanding their potential combinations are vital in mitigating the risks associated with extensions.

High-risk extensions can cause extensive damage. For example, recently, a fraudulent extension posing as a legitimate Chat GPT Chrome browser extension was installed by over 9,000 users. Advertised on Facebook as a tool to help users enhance their search engine with ChatGPT, the extension instead acted as a Trojan horse and hijacked Facebook accounts undetected. The extension was quickly removed from the storefront — but not before stealing login credentials of at least 6,000 corporate accounts and 7,000 virtual private network accounts. Unregulated ChatGPT extensions are cropping up faster than they can be taken down. Spin.AI's security researchers reviewed the Chrome Web Store and discovered that in May, there were only 11 extensions for ChatGPT: today, there are over 200 and counting.

The list of Google extension permissions from the Chrome Web Store includes the following notable permissions which can lead to security and compliance violations and must be monitored:

Google Extension Permission	High Risk %	Medium Risk %	Low Risk %
webRequest	4.3	2.3	0.3
cookies	1.8	1.8	0.2
identity	1.6	1.0	0.1
scripting	1.5	1.4	0.2
desktopCapture	0.9	1.4	0.2
clipboardRead	0.6	0.3	0

Figure 4: Sampling of Google extension permissions and related risk scores

Examples of Microsoft extension permissions from Microsoft Edge Add-Ons that organizations need to monitor:

Microsoft Extension Permission	High Risk %	Medium Risk %	Low Risk %
cookies	9.8	24.0	0
webRequest	9.8	20.0	0
scripting	4.9	9.8	0
desktopCapture	2.4	0	0
identity	2.4	0	0
clipboardRead	2.4	0	0

Figure 5: Sampling of Microsoft extension permissions and related risk scores

Note that although more Microsoft extension permissions were seemingly rated high-risk and medium-risk as compared to Google permissions the difference is in fact due to the larger number of Google extensions in use within our customer base as compared to Microsoft extensions (i.e. more extensions means lower percentages).

How to Disrupt Extension Risks

Mature organizations adopt a comprehensive approach to SaaS security, which includes:

Inventory

Maintain a real-time inventory of extensions and SaaS applications with access to your environment to understand the operational, security, privacy, and compliance risks they pose.

Risk Assessments

Conduct ongoing assessments to secure extensions and applications, and identify potential security risks.

Policies

Establish and enforce policies based on third-party risk management frameworks, considering extension and applications' dynamic nature, operational use, and business risks and needs.

Controls

Implement automated controls to allow or block extensions and applications based on organizational policies, reducing the workload of security resources and managing the numerous SaaS applications used within organizations.

To effectively mitigate extension and SaaS app risks, **businesses must adopt a comprehensive approach to manage the entire risk lifecycle**. It involves effectively discovering all extensions and SaaS applications connected to the environment and which can access which data. It also involves proactive, continuous risk assessments of all connected extensions and SaaS apps. Finally, as risk may change over time, organizations must leverage automated risk assessments and modern cybersecurity tools to eliminate the threat.

How Spin.AI Evaluates Extension Risk

Spin.AI's platform, SpinOne, uses machine learning (ML) to collect and analyze data to assess each extension and 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:

For example, a risky extension or 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 concern
- It may **not have regular updates** which can lead to a vulnerable application
- It may have **poor reviews** on a store or marketplace
- Its developer may **not disclose or undergo a third-party security or compliance audit**, leading to increased risks of improper security control
- It may have recently been **subject to a data breach**
- The developer of the extension can be a **no-name individual** with a gmail.com address

Conclusion

The research in this report encompasses the anonymized data of clients using the SpinOne platform and the anonymized data of extensions assessed and discovered through our integration with Google. The findings reveal that businesses must continuously evaluate extensions and 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 the LastPass extension and application by employees due to the 2022 breach. Using the SpinOne automated risk assessment and an organization's security policies, extensions and 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.

Request a demo of Browser Extension Risk Assessment today.

BOOK A DEMO