Spin.ai

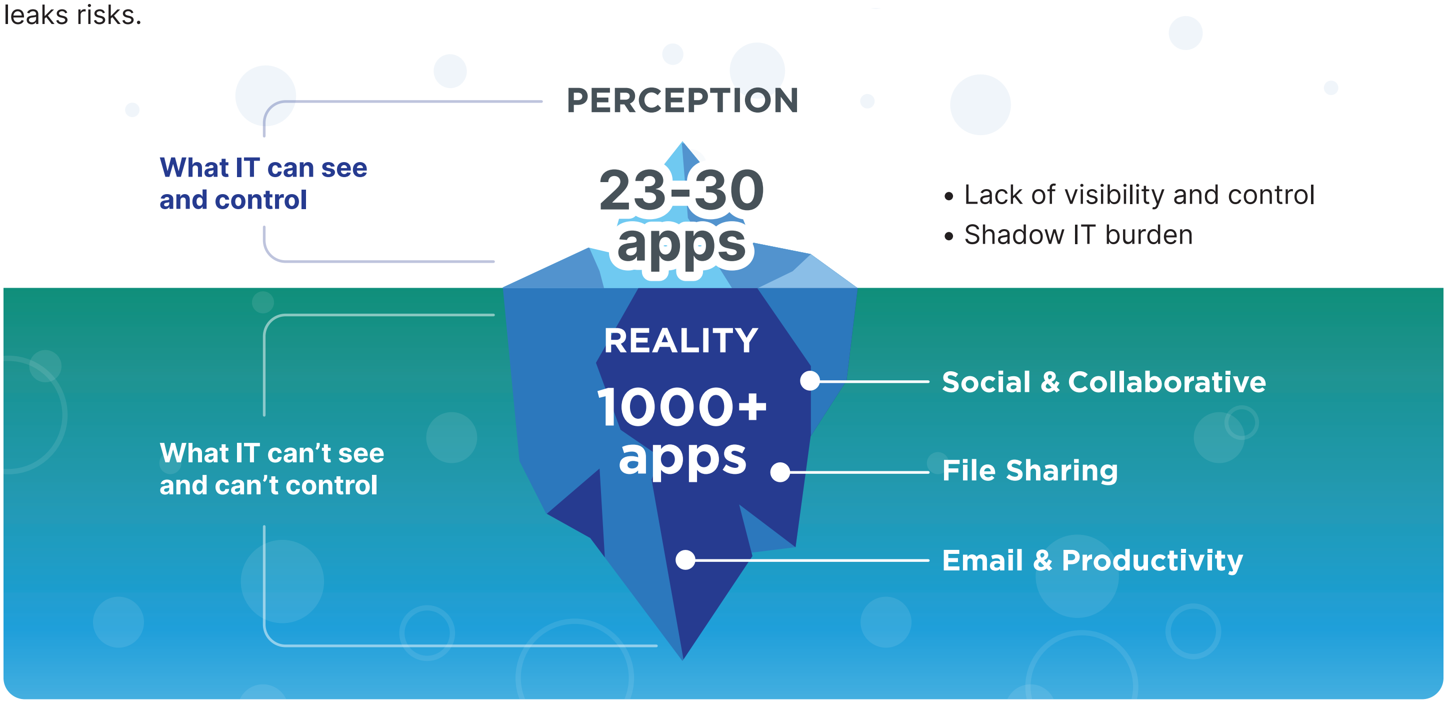
SpinSPM – SaaS Security Posture Management

Get full visibility and fast incident response for misconfigurations, unsanctioned third-party apps, and browser extensions — reduce security, compliance, data loss, and data leak risks.

Challenge

How do organizations manage misconfigurations and access for SaaS apps or browser extensions that have access to business-critical SaaS data?

A perceived 20-30 apps on the surface can, in reality, be thousands of unsanctioned risky apps and browser extensions with dangerous access levels. Lack of visibility leads to security, compliance, data loss, and data leaks risks.



PERCEPTION

What IT can see and control

23-30 apps

- Lack of visibility and control
- Shadow IT burden

REALITY

What IT can't see and can't control

1000+ apps

- Social & Collaborative
- File Sharing
- Email & Productivity

Key Capabilities

Over 80% of organizations have SaaS misconfigurations and risky, third-party applications that lead to immediate security threats. For Security teams who need to reduce risks of misconfigurations and third-party applications, SpinSPM is a SaaS Security Posture Management solution that provides full visibility and automated incident response to save time, reduce security costs, and improve compliance. Unlike other SSPM solutions, SpinSPM provides automated, in-depth risk assessments outlining security and compliance risks by leveraging our unique database of over 300,000 apps and browser extensions assessed by AI algorithms. SpinSPM is recommended and integrated by Google, recognized as a Strong Performer in the Forrester SSPM Wave report, and trusted by 1,500+ organizations worldwide.

Misconfiguration Management

Identify and manage misconfigurations, security drifts, and compliance breaches within your SaaS applications through automated detection and response.

Access Management

Allowlist or blocklist risky applications or browser extensions for everyone or specific organizational units to prevent unauthorized access to your mission-critical SaaS data.

Full Visibility

Inventory and gain visibility of all cloud services, mobile apps, SaaS apps, and browser extensions that have access to your SaaS environment — and understand who has access to these apps.

Automation

Automate access management by creating configurable, granular security policies to monitor, alert, and blocklist/allowlist applications and browser extensions based on set criteria.

Risk Assessment

Leverage 24/7 continuous monitoring and ongoing AI-based risk assessment, taking over 15 risk factors into consideration, to get full visibility into potential business, security, and compliance risks of each application and browser extension.

Fast Incident Response

Get immediate, customizable notifications on detected incidents, misconfigurations, and risk score changes from a single dashboard that includes advanced reporting and integrations with Splunk, ServiceNow, Jira, and Slack.

Integrated by Google

SpinAI was selected by Google to be integrated into the Google Workspace Console to assess the risk of sanctioned and unsanctioned Chrome browser extensions.

SpinSPM is available for

Google Workspace

slack

Microsoft 365

salesforce

Customer Success Stories

Global Automobile Manufacturer Secures Digital Workspace with SpinOne

One of the biggest automobile manufacturers in the world wanted to secure SaaS data in Google Workspace for thousands of employees across multiple departments, factories, and offices in international locations - some even in remote areas. Visibility into all SaaS services they used had become crucial, and so had the safety of all data in those SaaS applications.

The manufacturing company needed a solution that could detect, assess, and manage access for all their third-party OAuth applications and browser extensions. Spin.AI was the only solution that provided an AI-based assessment with no agent required.

With SpinOne, they have reduced the time it took to assess application risk from 2 years manually to 2 months automatically for their 50,000 third party apps, ultimately resulting in millions of dollars of ROI.

Content Delivery Platform Provider Protects Google Workspace Data

An industry-leading content and ads delivery platform lacked visibility into their Google Workspace user activity, third-party apps, and browser extensions — raising the risk of data leak and Shadow IT.

To mitigate this risk and secure employees' data, they consolidated their security efforts onto SpinOne for data leak protection and SaaS security posture management.

Using SpinOne, they have gained full visibility into users and actions across the environment, and created efficiency via policies and approval processes to automatically block high risk apps and extensions.

Recommended by Google Workspace

Microsoft 365 Enterprise 2023-24 DCIG Top 5 SaaS Backup Solutions

Top Infosec Innovator Winner Cyber Defense Magazine 2023

Gartner

Forrester Wave Strong Performer 2023 SaaS Security Posture Management

Global Infosec Awards Winner Cyber Defense Magazine 2023

G2 Users Love Us

See SpinOne in action. Book a free demo today.

REQUEST DEMO

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.