Spin.ai

PLAYBOOK

Professional Services Playbook

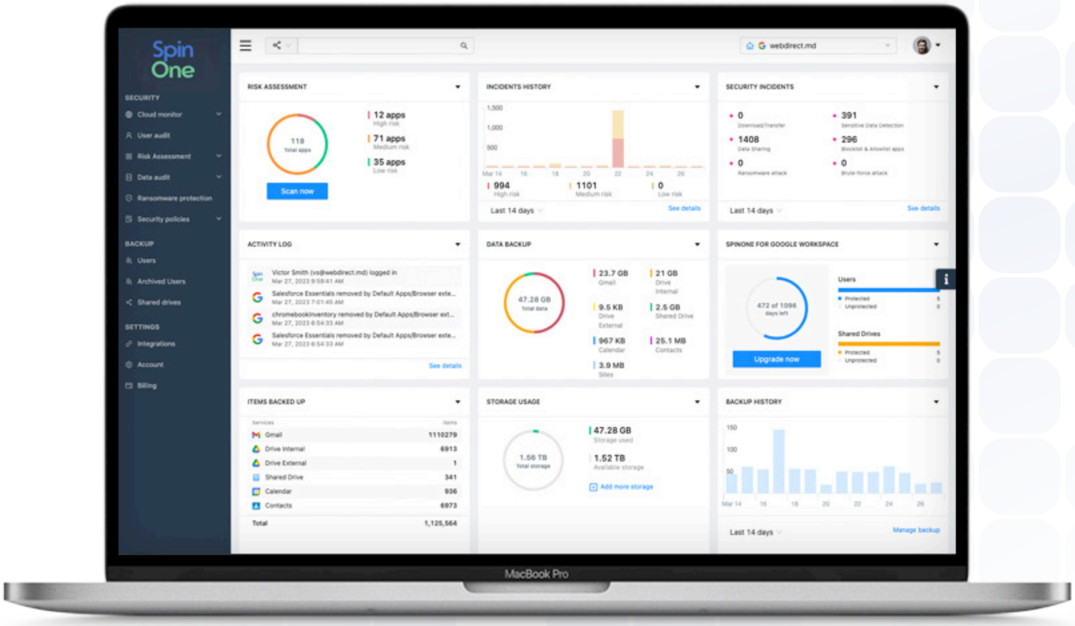
Table of Contents

About Spin.AI

Spin.AI is a SaaS security company protecting enterprises against the risk of shadow IT, data leaks, data loss, ransomware, and non-compliance. SpinOne, the all-in-one SaaS security platform for mission-critical SaaS apps, protects SaaS data for Google Workspace, Microsoft 365, Salesforce, and Slack. SpinOne provides SSPM, SaaS DLP/DSPM, SaaS ransomware protection, and SaaS backup for more than 1,500 organizations worldwide to enhance cyber resilience, streamline security operations, and reduce security costs. For more information, please visit Spin.AI.

Our Platform

SpinOne is an all-in-one SaaS security platform that protects your SaaS data across multiple environments including Google Workspace, Microsoft 365, Salesforce, and Slack. SpinOne provides robust solutions for SaaS security posture management, app risk assessment, data leak prevention and data loss protection, ransomware protection, and SaaS backup and recovery. It integrates with business-critical apps to deliver seamless work for Security professionals aiming to save them time and budget.



ACTIVITY LOG

Victor Smith (vs@webdirect.md) logged in
Mar 27, 2023 9:59:41 AM

Salesforce Essentials removed by Default Apps/Browser exte...
Mar 27, 2023 7:01:45 AM

chromebookinventory removed by Default Apps/Browser ext...
Mar 27, 2023 6:54:33 AM

Salesforce Essentials removed by Default Apps/Browser exte...
Mar 27, 2023 6:54:33 AM

ITEMS BACKED UP

Services	Items
Gmail	1110279
Drive Internal	6913
Drive External	1
Shared Drive	341
Calendar	936
Contacts	6973
Total	1,125,564

Partner Led Professional Services

Today, clients are more likely to pick a software platform they want to invest in, then seek a services partner to help them implement it. In effect, when consulting firms are hired, the responsibility has shifted to the right in a quasi-linear buying process. The technology decision has already been made. Now, the client is looking for a partner to help implement the solution as quickly and effectively as possible.

As a result, many of today's fastest growing consulting firms are fixtures in the partner ecosystems of today's fastest growing software companies, like Spin.AI.

General Values

Multi-Tenant

Manage all your customers from the Partner portal, easily accessing each environment as a Shadow Administrator.

Automated Detection & Response

Adds an additional layer of value for MSPs by responding quickly as the first layer, and providing insightful reporting for you to take action.

All-in-One

Instead of managing 4 different solutions (Backup, Ransomware, DLP, SSPM), you can easily provide all services from one dashboard.

Customizable Policies & Reporting

Flexibility in creating security policies based on individual customers, and directing notifications to Jira/ServiceNow/Slack/Teams to aggregate all alerts in one area.

Multi-SaaS

Protect your customers' Google Workspace, Microsoft 365, Salesforce & Slack environments using one platform.

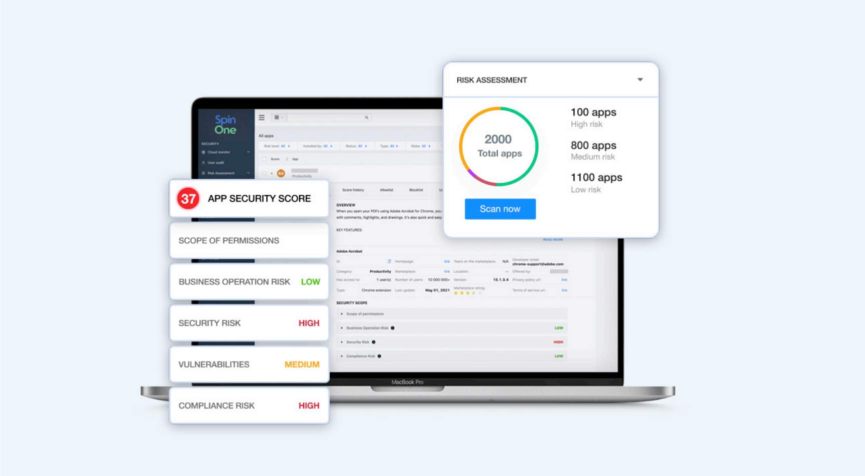
Training & Support

Even though the SpinOne platform is extremely easy to use and manage, SpinOne will provide 24/7 support to you, along with training sessions to ensure up to date product knowledge.

Pre-Sales Services

Risk & Compliance Audit

As the number of SaaS applications used by organizations increases, so does the risk of misconfiguration and non-compliance. Misconfigurations can expose sensitive data and open vulnerabilities, which can result in data breaches or ransomware attacks. According to Gartner, more than **60% of security incidents will be traced to misconfigured security controls by 2029**.



Service Offering

Utilizing Spin.AI's SSPM solution (SpinSPM), partners can offer a Risk & Compliance Audit, providing full visibility into unsanctioned apps, potential data exposure risks, browser extensions, and misconfigurations, further reducing clients exposure to non-compliance and potential risk. The Risk & Compliance Audit can be offered standalone or in addition to existing partner services.

Service Days

A typical Risk & Compliance Audit will take 1-2 service days.

Day 1 – Environment Assessment: Utilize SpinSPM to bring full visibility to client environments, exposing potential unsanctioned apps, potential data exposure, browser extensions, and misconfigurations. The assessment will consist of real time analysis and reporting, not only on potential application risks, but also sensitive data sharing. Partners can add additional services as needed, but provide a baseline to introduce SpinSPM to not only fix, but manage these associated risks and data exposure in the future.

Day 2 – Best Practices: After exposing potential unsanctioned apps, browser extensions, and misconfigurations with SpinSPM, partners can offer clients a one-time best practices implementation by creating an Application Policy to take action on the presented audit risks. Partners can further configure Application Risk Heatmap to show clients potential compliance risks. These services are designed to provide visibility of potential risks, but it is suggested to offer clients a one-month no cost POC so they can realize the value of SpinSPM in their environment. Partners can offer implementation and training (see Implementation and Training below) services for those clients that choose to proceed with a one month SpinSPM no cost POC.

Environment Assessment

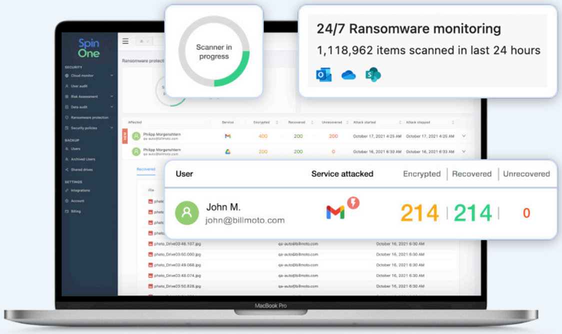
- Automated and continuous (1) inventory, (2) assessment and (3) reassessment of OAuth Apps & Browser Extensions.
- Executive overviews by compliance, by scope of permissions, by category and by type.
- Customizable heatmaps for personalized risk overview.
- Visibility into overall security posture along with executive reports.
- Visibility into the compliances of OAuth Apps & Browser Extensions.
- Measurable compliance support for widely recognized benchmarks, frameworks, and best practices.
- Visibility and risk assessment of high risk users and their activities.

Best Practices

- Periodically generate and review reports on the SpinOne platform of **All Apps** to get an understanding of all applications that have access to sensitive data.
    - Creating an **Application Policy** to identify and take action on risky OAuth applications and browser extensions. This policy is extremely configurable and can be set to alert, to Blocklist/Allowlist, and to even revoke access.
- Periodically review SpinOne overviews of applications to understand if they are compliant, if they request specific scopes.
- Configure the **Apps Risk Heatmap** to a specific customer's requirements in order to personalize and identify risky applications specifically for them. This will lay out High vs Medium vs Low risk applications.
- Periodically monitor the **User Audit** to review the high risk users of a specific customer. Configure the **User Audit** scoring in order to personalize user risk scores according to that customer's requirements.

Disaster Recovery Audit

Ransomware WannaCry, CryptoLocker, Jigsaw, Petya — there are many names for the various strains of ransomware, but at their core, they all threaten to publish the victim's data or perpetually block access to it unless a ransom is paid. Despite the funny names of these attacks, the ransoms are no laughing matter. While the **cost of these attacks** today may make your jaw drop, surpassing $7.5 billion, they **are estimated to jump up to $21 billion**.



Scanner in progress

24/7 Ransomware monitoring

1,118,962 items scanned in last 24 hours

User	Service attacked	Encrypted	Recovered	Unrecovered
John M. john@billmoto.com	M	214	214	0

Service Offering

Utilizing SpinRDR, partners can offer a Disaster Recovery Audit, whereas a simulated ransomware attack on their SaaS environment will test their current remediation plan, RTO (recovery time objective) and RPO (recovery point objective). The Disaster Recovery Audit can be offered standalone or in addition to existing partner services.

Service Days

A typical Disaster Recovery Audit will take 1 service day.

Day 1 – Setup and run Ransomware simulator on client's environment: Utilizing SpinRDR partners can test clients' SaaS environments for fidelity on RTO and RPO goals, illustrating potential issues with their current disaster recovery plan. Partners can add additional services as needed, but provide a baseline to introduce SpinRDR for ongoing Ransomware remediation and recovery. This service is designed to evaluate current disaster recovery goals, but it is suggested to offer clients a one-month no cost POC so they can realize the value of SpinRDR in their environment. Partners can offer implementation and training (see Implementation and Training below) services for those clients that choose to proceed with a one month SpinRDR no cost POC.

Ransomware Simulation

- 2 Hour Recovery SLA.
- No human factor, fully automated Monitoring, Detection, Stop & Recovery.

Best Practices

- Prepare a test user within the environment that will be attacked.
- Provide Spin.AI partner team with the email addresses of the users that will participate in the simulation (attacker & victim).
- Begin uploading test files that will be attacked in the scope of this simulation.
- Backup the files on the SpinOne platform and wait for a minimum of 15 minutes.
- Start the encryption process from Spin.AI's Ransomware simulator to see the automated ransomware protection in action.

Post-Sale Services

Implementation

Service Offering

For no cost POC and licensed customers. Partners will be trained and certified to set up and implement SpinOne products per best practices. Each product will require different configuration and setup, which will dictate the number of service days required.

Service Days

A typical SpinOne implementation will take 2-3 service days.

Day 1: Initial installation of the SpinOne application to the customer's tenant.

Day 2: Configuring the platform according to the customer's needs. Configurations include but are not limited to:

- Automating onboarding / offboarding.
- Security workflows for SSPM & DSPM (if applicable).
- Setting up integrations (Email, Jira, ServiceNow, Slack, Teams) & reporting.

Day 3: Review and fine-tune automation as needed.

Admin Training

Service Offering

For no cost POC and licensed customers. Partners will need to complete a "Train-the-trainer" course and become certified. Each product will require different admin training, which might require more service days.

Service Days

Admin training will typically take 1 service day.

Day 1: Full day (onsite or remote) training of the SpinOne platform.

For more information, contact your partner manager.

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.