SpinOne

Application Security Assessment: How to Protect from Threats in the G Suite Marketplace

- ✓ Security risks from third-party SaaS apps
- ✓ Best G Suite data protection practices
- ✓ What problems security automation can solve

One of the extremely appealing advantages of public cloud SaaS environments is the strong third-party application integration found in the leading public cloud providers such as Google's G Suite and Microsoft's Office 365 environments.

Third-party applications can greatly extend the functionality and capabilities of your public cloud environments; however, they can also introduce potential security implications as well.

Focusing on Google's G Suite environment – how can you solve the security problems involving integrating third-party applications safely and still achieve the value proposition offered to you by G Suite public cloud SaaS? How can your business effectively control third-party apps in the G Suite public cloud and effectively meet G Suite security goals?

SpinOne

Contents

01

THIRD-PARTY APP RISKS

SaaS Data Protection Guide

You are responsible for your data

You only have to browse through the list of productivity apps found in the G Suite Marketplace to see the tremendous amount of applications that are available to extend your G Suite environment and capabilities. There are tools ranging from apps for accounting & finance, administration, ERP & logistics, HR & legal, creative tools, web development, office applications, etc. In fact, there is a good chance if you need a particular application to perform a function in Google's G Suite environment, most likely, there is an application that is available to take care of that process for you.
As with most aspects of the G Suite and other public cloud environments, you must realize you are responsible for your data when it comes to third-party applications and maintaining G Suite security for your data. In fact, Google makes this clear their G Suite Marketplace Terms of Service. This is clearly stated:

"Google is not responsible for any Product on the Market that originates from a source other than Google, and you should ensure that you read and agree to any additional terms that apply to those Products before accessing or using them"

Google recommends that all businesses using G Suite environments evaluate a G Suite Marketplace app and its security before installing and using the app. In regards to the security of G Suite Marketplace apps, Google makes this statement:

You may wonder, why is there a risk from using third-party applications when they may be listed in the G Suite Marketplace? The risk factor from third-party applications comes from two different perspectives:

- The third-party application may directly try to leak your data or have some kind of malicious intent
- The third-party application may be legitimate in nature, but be poorly written. Poorly written applications may introduce G Suite security vulnerabilities that can lead to compromise.

02

HOW TO PROTECT G SUITE FROM MALICIOUS APPS

SaaS Data Protection Guide

While Google has a screening process for developers, as Google's disclaimer mentions, "you are solely responsible for any compromise or loss of data". Businesses must take hard and fast ownership of screening third-party apps for security best practices. What are the best practices that Google outlines for third-party application security?

- Properly evaluate the vendor or application
- Screen gadgets and contextual gadgets carefully
- Use the Security Assessment Program to help gauge whether a vendor or application should be trusted.

Evaluate vendors and/or applications

Google notes that you must evaluate a vendor or application and decide to use it for your G suite environment. To analyze whether or not a vendor or application is acceptable to use from a G Suite security perspective before you install the application:

- Look at reviews left by customers who have downloaded and installed the third-party application. The reviews are listed for all G Suite Marketplace apps
- Look and analyze closely the third-party application vendor's Terms of Service, privacy policy, and deletion policy agreements to ensure there are no unwanted, hidden clauses that may affect the security
- Contact the third-party application vendor directly with questions regarding any grey areas that may be questionable

Screen Gadgets and Contextual Gadgets Carefully

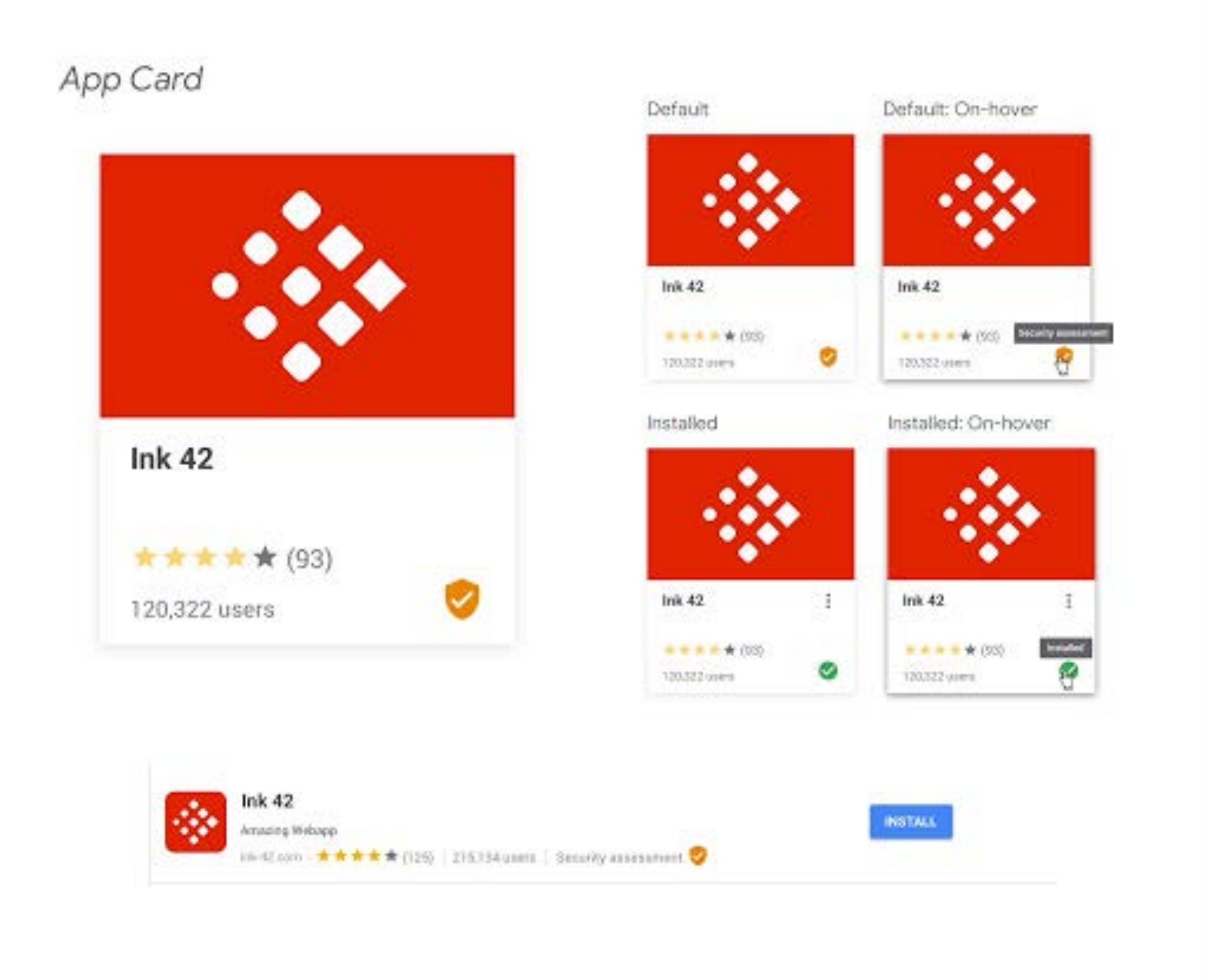
What about third-party gadgets? What are the gadgets? These are full web applications written in HMTL, CSS, and Javascript that can run in the context of the G Suite environment. You can use Gadgets in Gmail, Calendar, Drive, and Sites. What are the security implications?

- A special class of gadget is known as the Gmail contextual gadget. These types of gadgets can extract data from a Gmail message and provide contextually relevant information to you in the message pane.
- Poorly written gadgets by third-party vendors may expose your business to potential risks in the form of phishing attacks and potential data loss or leakage.

Gadgets in general and specifically contextual gadgets should only be installed from vendors that you implicitly trust.

Use the G Suite Security Assessment Program

Google has a G Suite Marketplace Security Assessment Program that allows developers to submit their apps to a third-party security firm which then performs a full security and risk assessment of their application. Once an application has passed the security assessment, the application will be able to display a security badge in the Marketplace listing.



Review G Suite third-party apps for Security assessment badge (Image courtesy of Google)

By following these Google defined best practices for G Suite security, businesses can much better gauge the security of applications that are integrated with the G Suite environment. Another danger when it comes to third-party applications is your end-users. How is this the case?

In general, your typical end-user is very trusting of any application that requests permission to access their data. Most of us are guilty of blindly clicking “Allow” to permissions requests on mobile devices when installing a new third-party application. Do most take the time to consider the security implications of allowing access? For most of your users, the answer is “No”.

Now, think of that same mindset when it comes to accessing sensitive corporate data. Do you want the same type of decision making to happen when deciding whether or not to allow applications to access important business data? This is a very real and present danger in today’s corporate culture of freedom to access business data with mobile devices, including BYOD, from various untrusted networks, etc.
You must have the means in place to keep strict watch over and control of third-party applications to ensure the applications that are granted access to your sensitive corporate data are those that meet the criteria listed above and have all the characteristics of a trustworthy application that is not known for data leak or all-out malicious activity.
How can you successfully meet the ever-increasing demands on IT professionals, not only in the area of operations but now with increasing security complexities?

03

SECURITY AUTOMATION

SaaS Data Protection Guide

Why you need to automate security

With the sheer number of threats, variants, complexities, hybrid networks, BYOD, and many other factors, it is becoming increasingly difficult, if not impossible for you to rely on manual efforts for effective security. Humans are simply not as effective and efficient at parsing logs and manually correlating metrics and activities as “machines” or computers are.

Computers are much better at repetitive tasks that require monotonous activities such as crunching numbers and examining data than humans. Additionally, computers do not “get tired” and can work 24x7x365. Machine Learning is a new type of technology that businesses can make use of that uses powerful and complex mathematical algorithms to “learn” about an environment and determine what normal is and then recognize deviations from this fingerprint of normalcy.

When used with security, machine learning is able to create a baseline of what normal activity is in an environment and build a baseline of activity. If an activity is noticed outside of the normal behavior of both users and applications, this could be a red flag that there may be malicious intent with the new behavior.

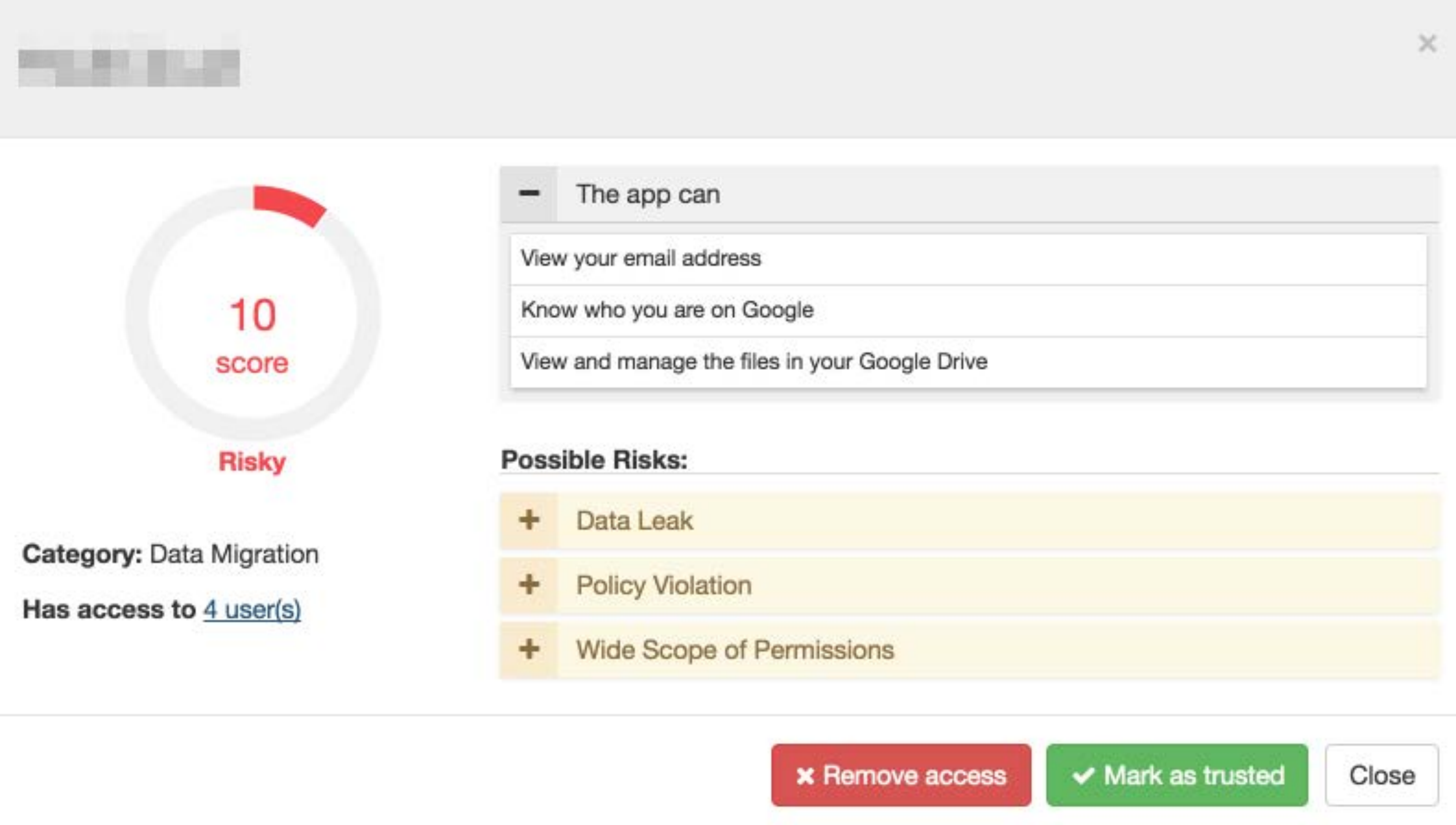
Let’s see how machine learning and intelligent artificial design making can be put to good use to protect the Google G suite environment from G Suite Marketplace security threats, including those that may be posed to your data by third-party applications.

SpinOne – Virtual Security Expert

Imagine if you could have a full-time "expert" security person working to secure your G Suite public cloud SaaS environment. Would you feel more confident about your business-critical data from a security standpoint? Absolutely! You can have such an expert security assistant working to secure your G Suite environment – SpinOne. Using the latest in powerful machine learning algorithms, SpinOne is a virtual security expert scanning the G Suite environment looking and watching for anything that could pose a danger to business-critical data.

SpinOne's API-driven CASB technology integrates with G Suite seamlessly to become a hardened security layer in between corporate data and anyone or any device accessing it. This includes third-party applications that are allowed access to corporate data. Its AI-based approach to analyze third-party apps saves IT personnel and G Suite administrators tremendous amounts of time and energy protecting the G Suite environment.

The SpinOne analytics engine provides unique expertise and fully automated scanning of over 20,000 apps and counting. With new improvements in algorithms and scanning technology implemented on a regular basis, SpinOne is constantly improving the solution to provide the best possible security for businesses utilizing the G Suite environment. The bottom line is SpinOne allows automating the best practices recommended by Google when securing third-party applications.



Category: Data Migration

Has access to 4 user(s)

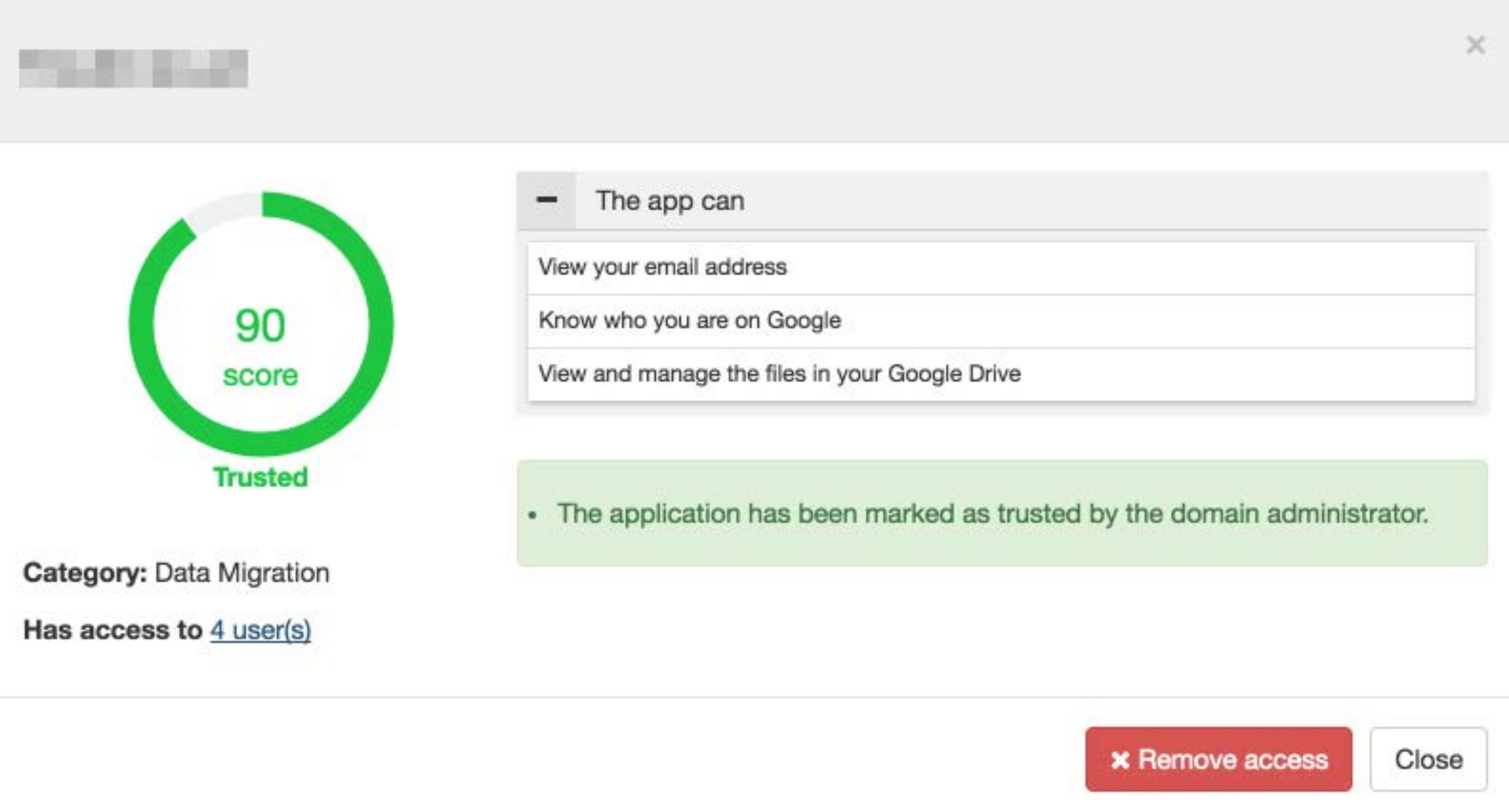
− The app can

- View your email address
- Know who you are on Google
- View and manage the files in your Google Drive

Possible Risks:

- + Data Leak
- + Policy Violation
- + Wide Scope of Permissions

Risky app security assessment in SpinOne


[redacted]

90 score

Trusted

Category: Data Migration

Has access to 4 user(s)

The app can

- View your email address
- Know who you are on Google
- View and manage the files in your Google Drive

- The application has been marked as trusted by the domain administrator.

App security assessment in SpinOne

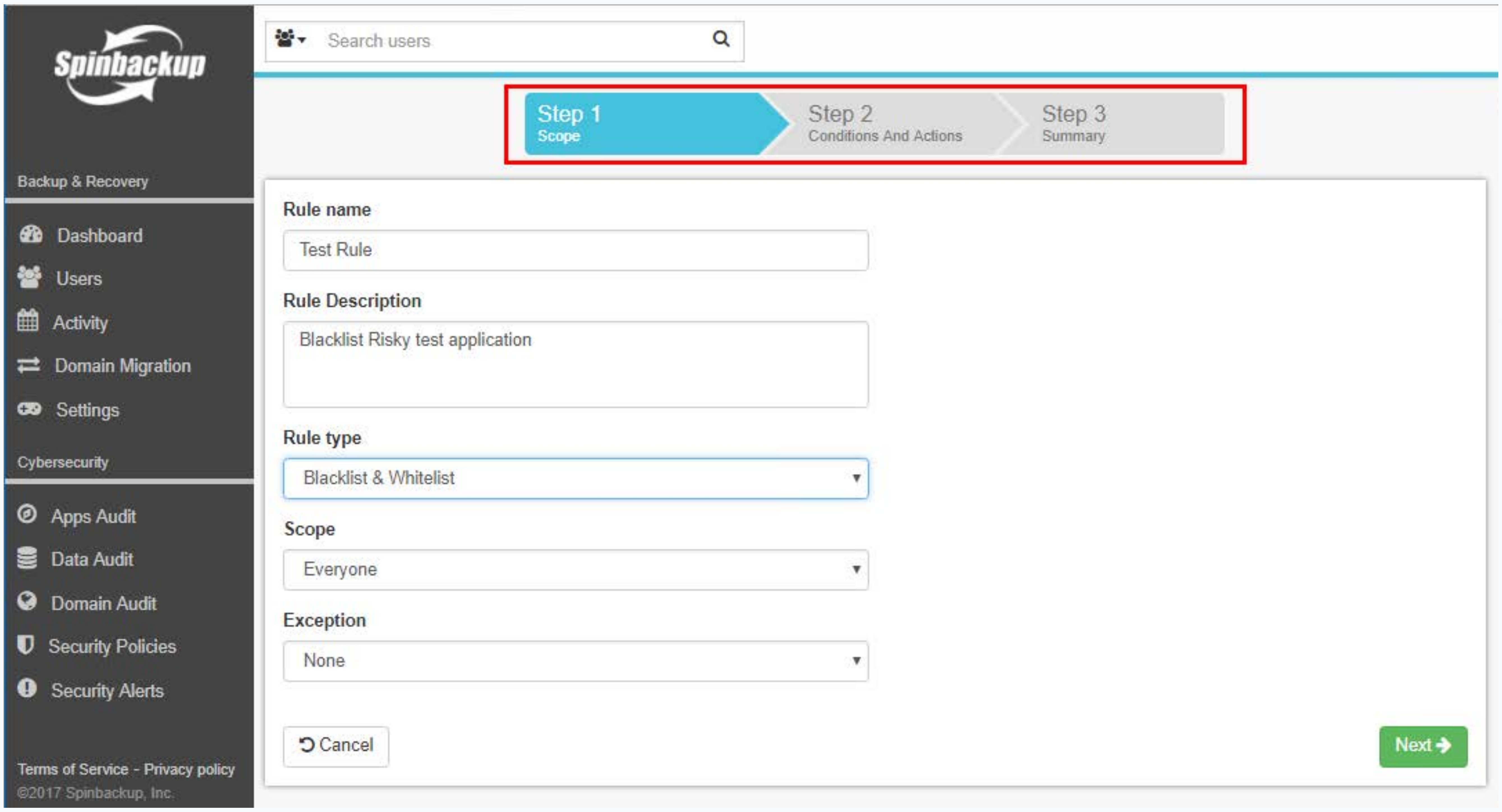
AI-based Third-Party Apps Risk Assessment and Remediation

With the Third-Party Apps protection module and AI-enabled technology, the Apps Audit Policies allow creating effective rules that control how apps are allowed to be installed in the G Suite environment. SpinOne allows creating both a blacklist and whitelist of applications that are allowed or disallowed to access your G Suite environment.

This is a powerful approach that you can use to only allow certain applications to be installed or disallow a list of applications, or a combination of both. Notifications are proactively sent to administrators, notifying them of the event.

Under the Apps Audit Policies, the Blacklist & Whitelist allows configuring the following:

- **Application Name** – This field contains the application's full name, or part of the name, as found in the G Suite Marketplace or in the Apps Audit section.
- **Application Category –** Detects all applications under the defined application category.
- **Application Risk Rate** – Detects all applications under the chosen risk rate.
- **Use Apps Audit Blacklist Check** – If this checkbox is enabled, it will compare detected applications with the blacklist in the Apps Audit section. This rule will be skipped if the blacklist doesn't contain the detected application.
- **Remove Application** – When selected, the application is removed.
- **Send Notification** – Sends notifications.



Rule name: Test Rule

Rule Description: Blacklist Risky test application

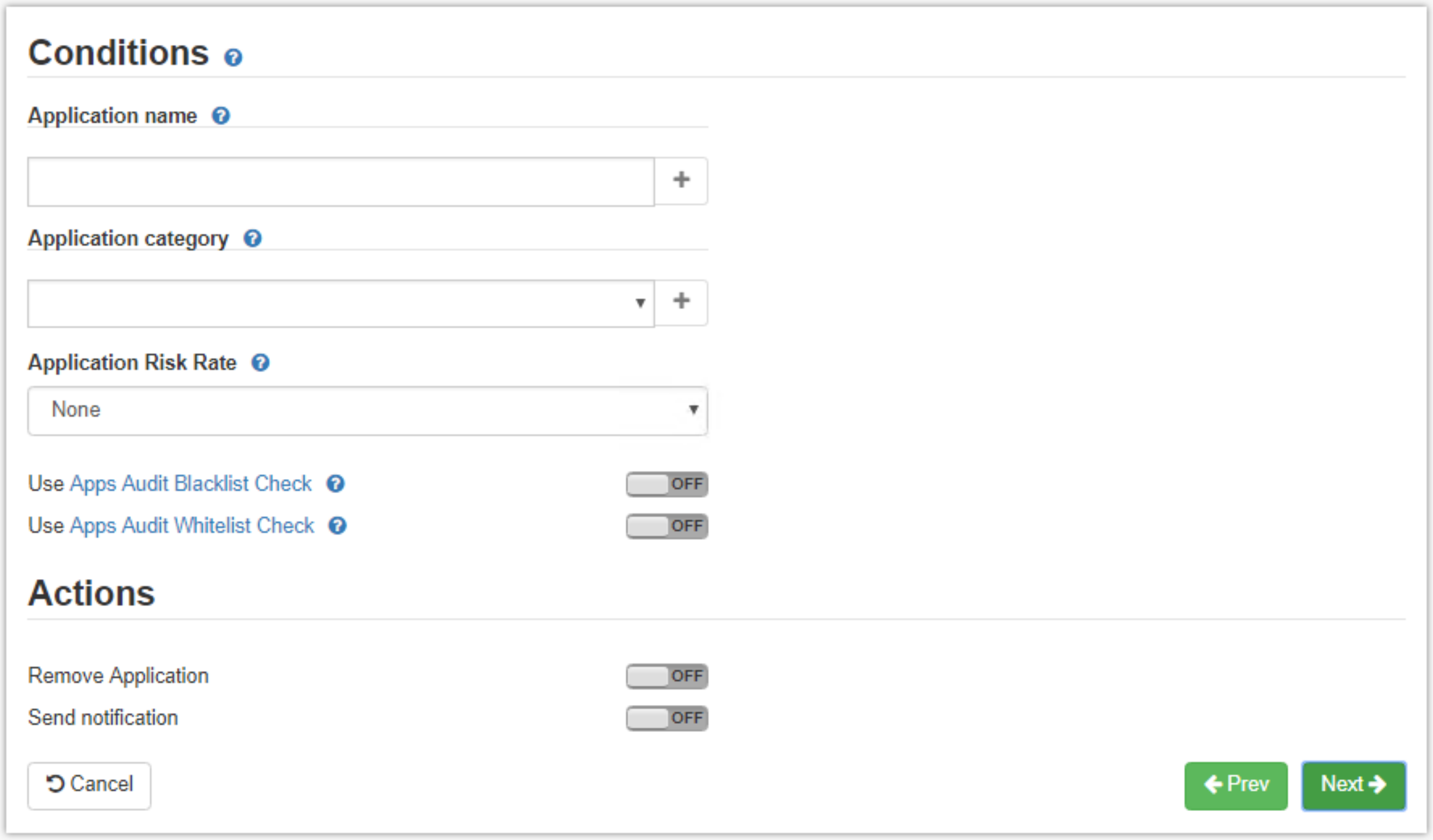
Rule type: Blacklist & Whitelist

Scope: Everyone

Exception: None

Creating a new Rule for Blacklist & Whitelist of applications in Google G Suite

Below, you can configure the Conditions for the Audit Policy Rule applied to the G Suite environment for third-party applications.



Application Risk Rate: None

Use Apps Audit Blacklist Check: OFF

Use Apps Audit Whitelist Check: OFF

Remove Application: OFF

Send notification: OFF

Using Audit Blacklist and Whitelist checks for applications

04

USE CASES

What SpinOne protects your business from

What are some of the common use cases SpinOne's AI-based third-party apps protection module solves for businesses utilizing G Suite SaaS environments?

1. Unsanctioned data download - An employee installs an app that connects to the G Suite environment and starts migrating sensitive data from a corporate account to their personal private cloud storage account. This commonly happens when an employee decides to leave a company.

2. Unsanctioned third-party apps download - An employee installs an app that is not sanctioned for use in the G Suite organization

3. Employee Termination - When a company fires an employee, IT admins usually suspend the user account. When you suspend a G Suite account, all the apps still have access to sensitive data that was accessible by the user. This can be a potential for data breach. SpinOne's third-party app security solution is a must-have tool for HR Departments that have to take care of the most efficient way of OFF-boarding an employee by removing all the Apps that have access to sensitive data through a suspended user account.

4. Compromised third-party apps - An App can be hacked by cybercriminals. Developers may not be able to quickly identify the breach before it starts downloading or migrating an abnormal amount of data or changes the scope of permissions which constitutes abnormal behavior.

05

MAKE THE BEST CHOICE

SaaS Data Protection Guide

Get Automated Intelligence and Security Expertise for Your G Suite Environment

Third-party applications provide tremendous value to your business to extend the capabilities of your G Suite environment. With the capabilities of G Suite Marketplace apps, there are security risks involved.

Google makes it clear that if you decide to utilize third-party apps, you must take ownership of your data and by extension, any data loss that happens due to a risky third-party app. Implementing third-party apps best practices can be involved, and require a lot of manual processes to be effective. To keep pace with the complexity and sheer pace of hybrid environments today, you must make effective use of machine learning and AI to be effective.

SpinOne provides the definitive solution for securing the G Suite environment and making intelligent decisions regarding third-party apps and installation in G Suite. By making use of intelligent AI-based technology, SpinOne is the virtual security expert that constantly watches your G Suite environment and enforcing security 24x7x365.

With Apps Audit and other built-in technologies, SpinOne allows creating blacklists and whitelists of applications for sanctioned use. If the AI-based engine detects that a once-approved third-party app begins demonstrating malicious behavior, SpinOne provides notifications and remediation of the potential security event. SpinOne provides automated intelligence and security expertise to your G Suite environment, seamlessly, and in a way that provides confidence in making use of third-party applications.

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)