SpinOne

G Suite Security: a Checklist for Admins

- 7 steps to admin Google G Suite

As a G Suite admin, you have to make your company's data secure. G Suite is a collection of Google cloud computing apps and tools to help you. In this 7-step guide, we will show you how to admin Google G Suite in a secure and effective way.

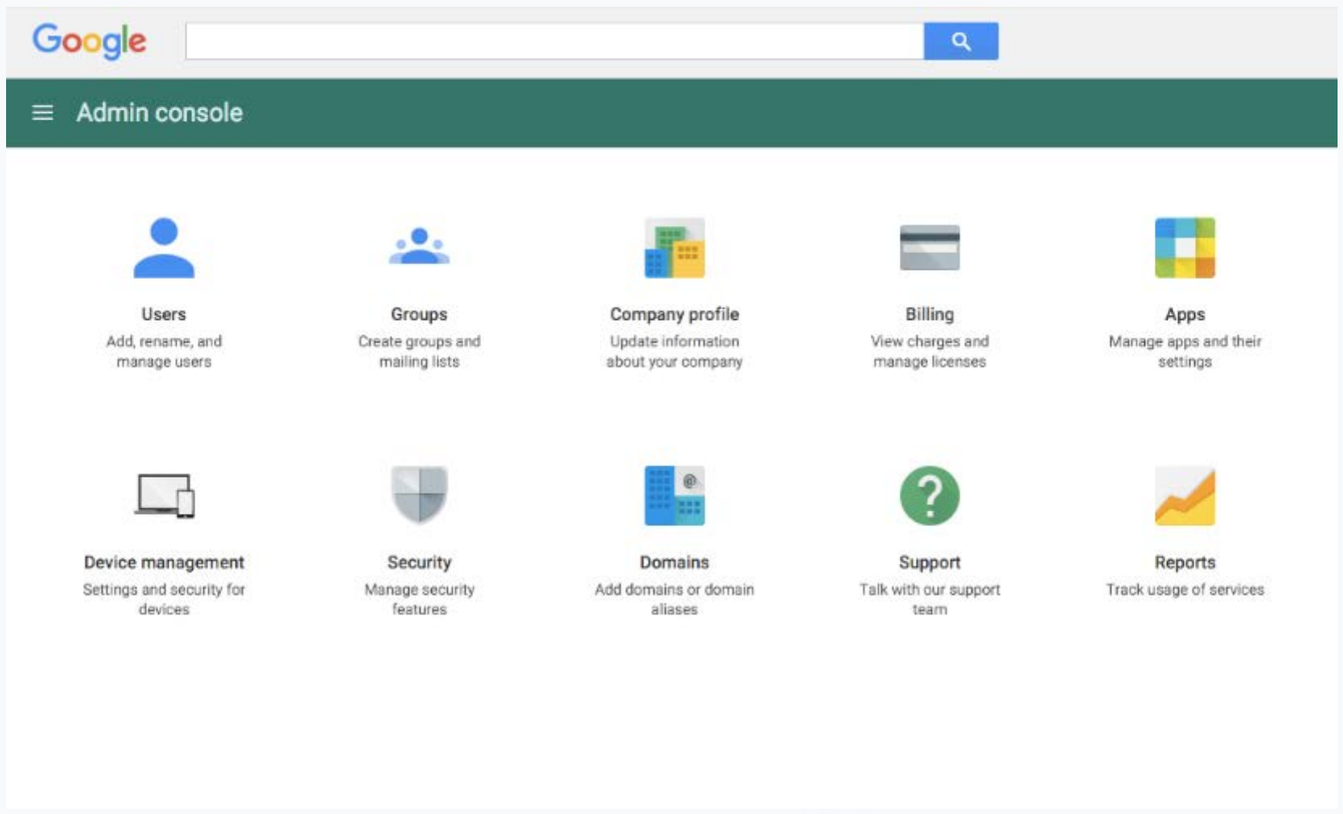
SpinOne

Contents

1.

Manage G Suite with Google Admin Console

SaaS Data Protection Guide



You, as an admin, handle a significant amount of vital information daily. Correct data management will help you save your time and get a more complete understanding of your company's data.

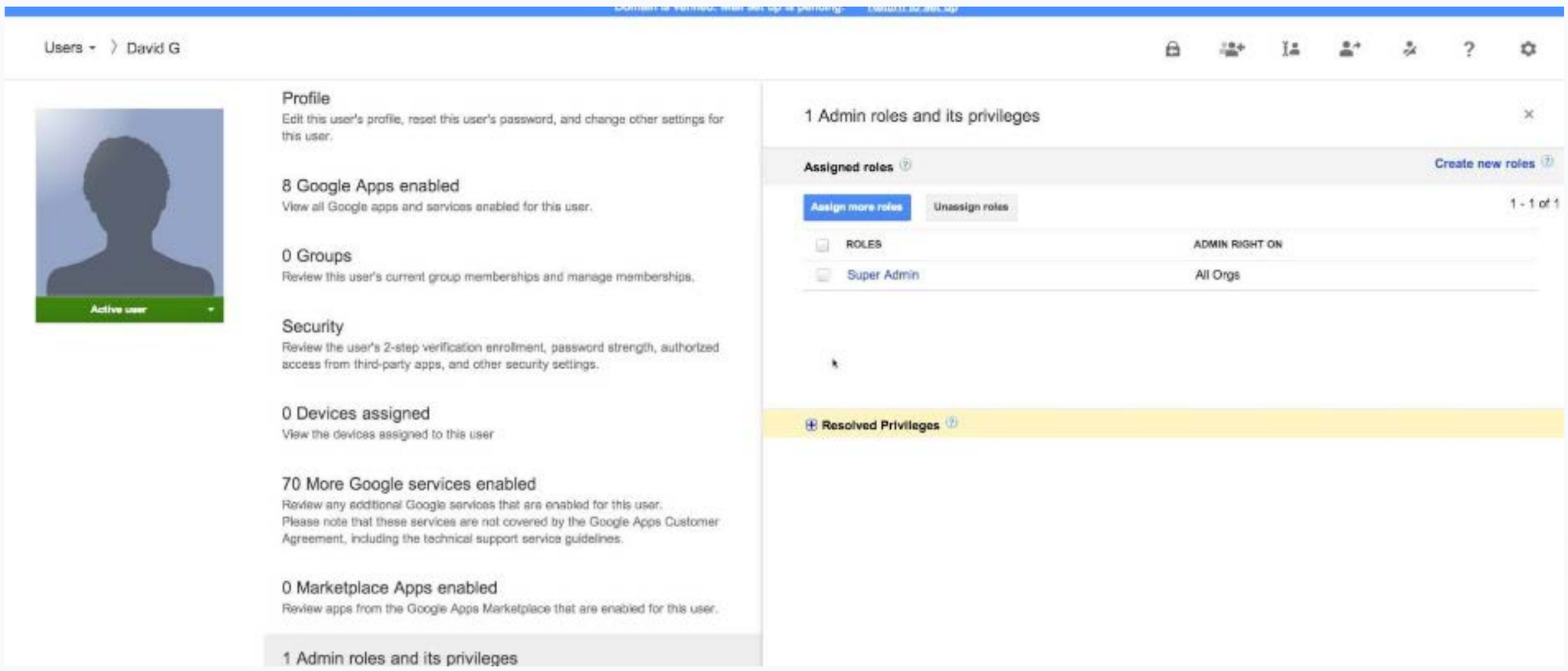
The Admin Console for G Suite is an extremely useful tool for corporate data management. The Google Admin Console allows accessing and managing information about various aspects of G Suite. The features Admin Console gives access to are Apps, Billing, Users, Security, and more.

A must-have for a perfect G Suite admin is the understanding of interactions between users/apps and the G Suite Business account. The admin console will help you to get regular reports on these interactions.

Using the information provided in the Admin Console, you can monitor every aspect of the G Suite domain. The console's report offers major metrics such as:

- Usage
- User status
- Storage
- Security
- File sharing

To monitor user behavior, you should click on Users in the G Suite admin panel.



How is it possible for file encryption to be used on your own data without your consent?

Under normal circumstances, file encryption is a security operation implemented by a trusted system administrator to protect access to business-critical or sensitive data.

Ransomware uses this legitimate security tool against you. It is malicious software that infects an end-user, often under the guise of legitimate software installation, that assumes the permissions and rights of the user and encrypts all files the user has access to. Once user permissions are “hi-jacked”, it allows ransomware to encrypt files that are stored locally, on a network share, and even cloud storage, all without the consent of the end-user.

2.

Enable 2-Step Verification

SaaS Data Protection Guide

Preventing unauthorized access to the system is among the key admin responsibilities. Insufficient security measures may lead to a data breach, a situation of a company’s data being lost or stolen by hackers. As a result of a data breach, a business suffers severe damage, both financial and reputational.

A good security practice is to enable Google 2-Step Verification. With 2-step verification, you can protect an account using both a password and a mobile phone. The Verification enables additional security.

Why is the 2-Step Verification effective? It’s quite simple. A password is required to log in. When you enable Google 2-Step Verification, you also need to input the security code that arrives at your phone via an SMS. So even if your password is compromised, your account is still under your control.

For robust access control, an admin should ensure there’s a 2-step verification, and all employees use it no matter what. Accessing the account through a 2-step verification assures that there will be no unauthorized access to data and information.

Moreover, reinforced access increases the level of authentication. You can verify security processes through the Users link in the admin panel. Reports from the admin console display specific users who have not used a 2-step verification. Through this report, you can ensure that everybody in your organization is going through a 2-step verification process when accessing their corporate accounts.

3.

Check Third-Party Apps

SaaS Data Protection Guide

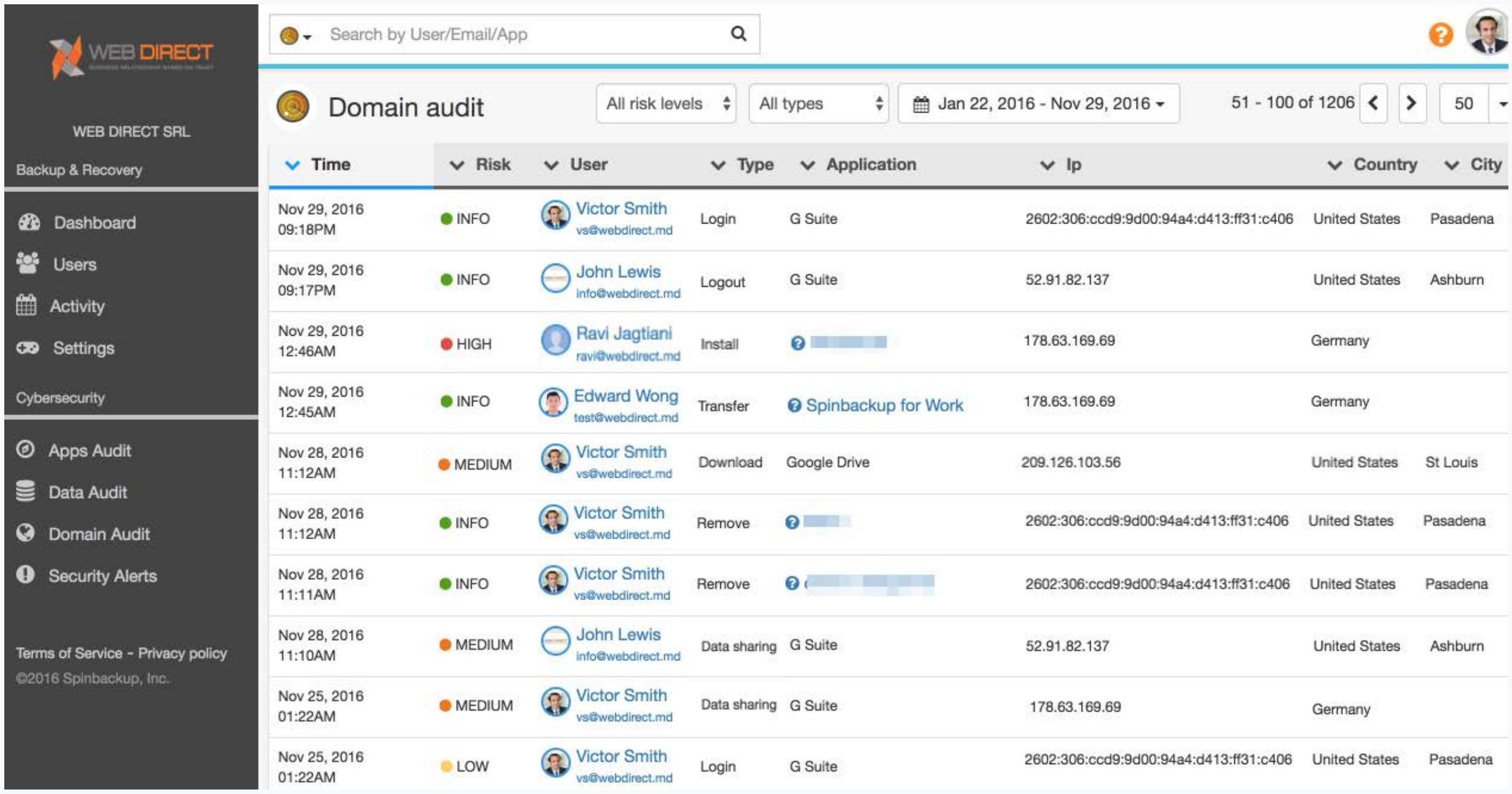
Some third-party apps have access to corporate data. Using such apps might involve risks. For example, your sensitive data might be stolen or altered.

The sad truth is that many apps have embedded Trojan codes within. Giving a malicious app access to your data may result in a major data breach.

A good admin understands these possible risks and takes measures.

A G Suite admin should regularly audit all third-party apps installed by users and allow or deny their access. The audit ensures transparency of the apps and allows you to mitigate or avoid risks permanently. You can perform the audit through the Security, Apps and Device management links in the admin console. However, a manual audit is time-consuming.

With SpinOne’s 3rd-party apps audit, you get full visibility of all 3rd-party apps installed with assigned risk levels. This security feature provides an administrator with a set of tools to monitor and detect risky applications and prevent corporate data from leaks caused by suspicious or dangerous software.


WEB DIRECT
WEB DIRECT SRL
Backup & Recovery
Dashboard
Users
Activity
Settings
Cybersecurity
Apps Audit
Data Audit
Domain Audit
Security Alerts
Terms of Service - Privacy policy
©2016 Spinbackup, Inc.
Search by User/Email/App
Domain audit
All risk levels
All types
Jan 22, 2016 - Nov 29, 2016
51 - 100 of 1206
50
Time
Risk
User
Type
Application
Ip
Country
City
Nov 29, 2016 09:18PM
INFO
Victor Smith
vs@webdirect.md
Login
G Suite
2602:306:ccd9:9d00:94a4:d413:ff31:c406
United States
Pasadena
Nov 29, 2016 09:17PM
INFO
John Lewis
info@webdirect.md
Logout
G Suite
52.91.82.137
United States
Ashburn
Nov 29, 2016 12:46AM
HIGH
Ravi Jagtiani
ravi@webdirect.md
Install
178.63.169.69
Germany
Nov 29, 2016 12:45AM
INFO
Edward Wong
test@webdirect.md
Transfer
Spinbackup for Work
178.63.169.69
Germany
Nov 28, 2016 11:12AM
MEDIUM
Victor Smith
vs@webdirect.md
Download
Google Drive
209.126.103.56
United States
St Louis
Nov 28, 2016 11:12AM
INFO
Victor Smith
vs@webdirect.md
Remove
2602:306:ccd9:9d00:94a4:d413:ff31:c406
United States
Pasadena
Nov 28, 2016 11:11AM
INFO
Victor Smith
vs@webdirect.md
Remove
2602:306:ccd9:9d00:94a4:d413:ff31:c406
United States
Pasadena
Nov 28, 2016 11:10AM
MEDIUM
John Lewis
info@webdirect.md
Data sharing
G Suite
52.91.82.137
United States
Ashburn
Nov 25, 2016 01:22AM
MEDIUM
Victor Smith
vs@webdirect.md
Data sharing
G Suite
178.63.169.69
Germany
Nov 25, 2016 01:22AM
LOW
Victor Smith
vs@webdirect.md
Login
G Suite
2602:306:ccd9:9d00:94a4:d413:ff31:c406
United States
Pasadena

4.

Watch Out for Abnormal Usage

As an admin, you need to monitor your systems for abnormal usage. For a G Suite admin, monitoring is especially important, as G Suite is used to manage massive amounts of personal financial information. Monitoring may help you prevent an incident before it occurs. Abnormal user behavior is one of the first signs of upcoming dangers.

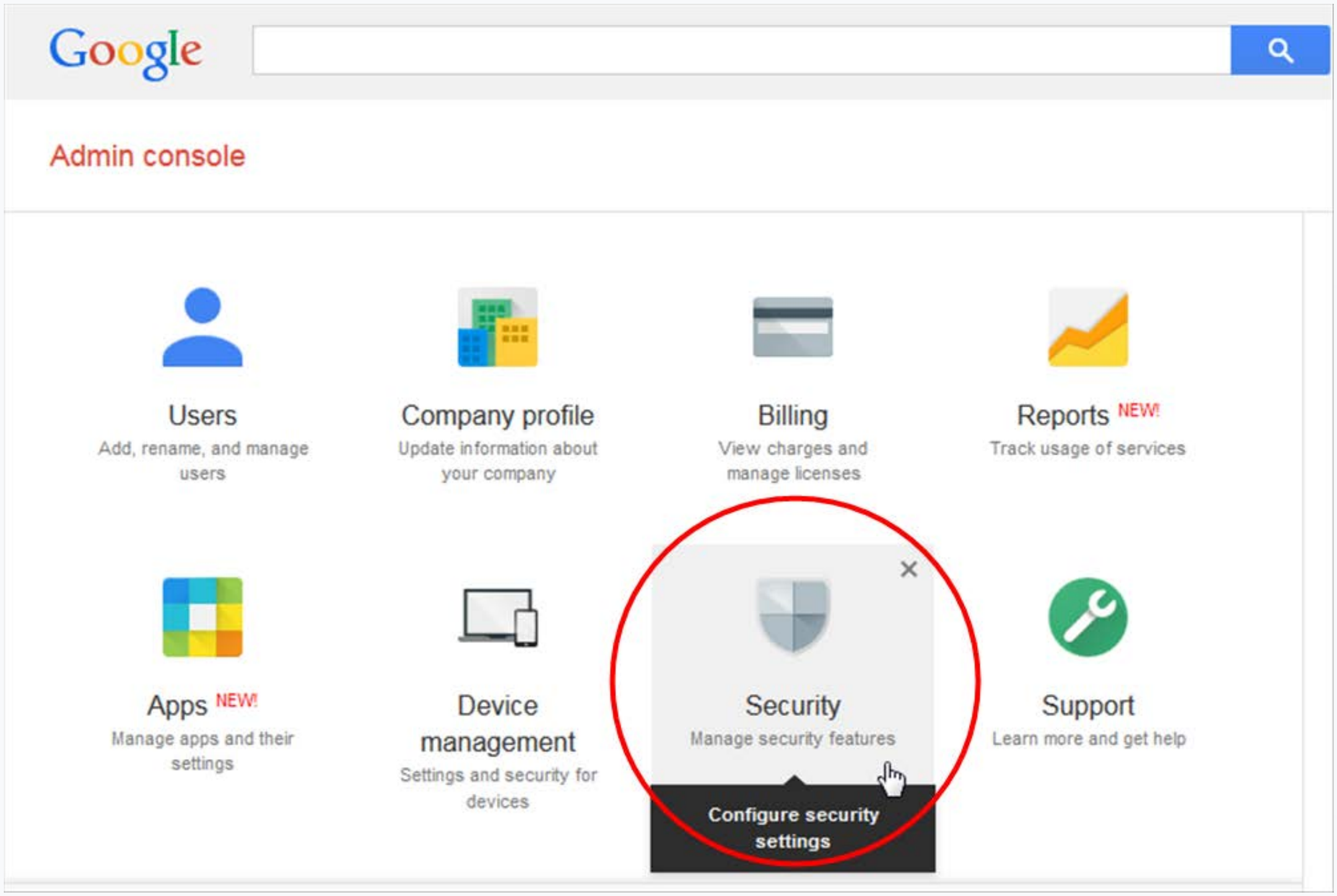
Abnormal behavior may include too frequent user's logging in and out and unusually high user activity. Monitoring abnormal usage will also help you detect suspicious activities in Google apps. Any data spike in Google Drive storage may mean the malicious actions of a third-party app.

With the understanding of abnormal actions, a perfect G Suite admin can decide whether these usages are safe or not.

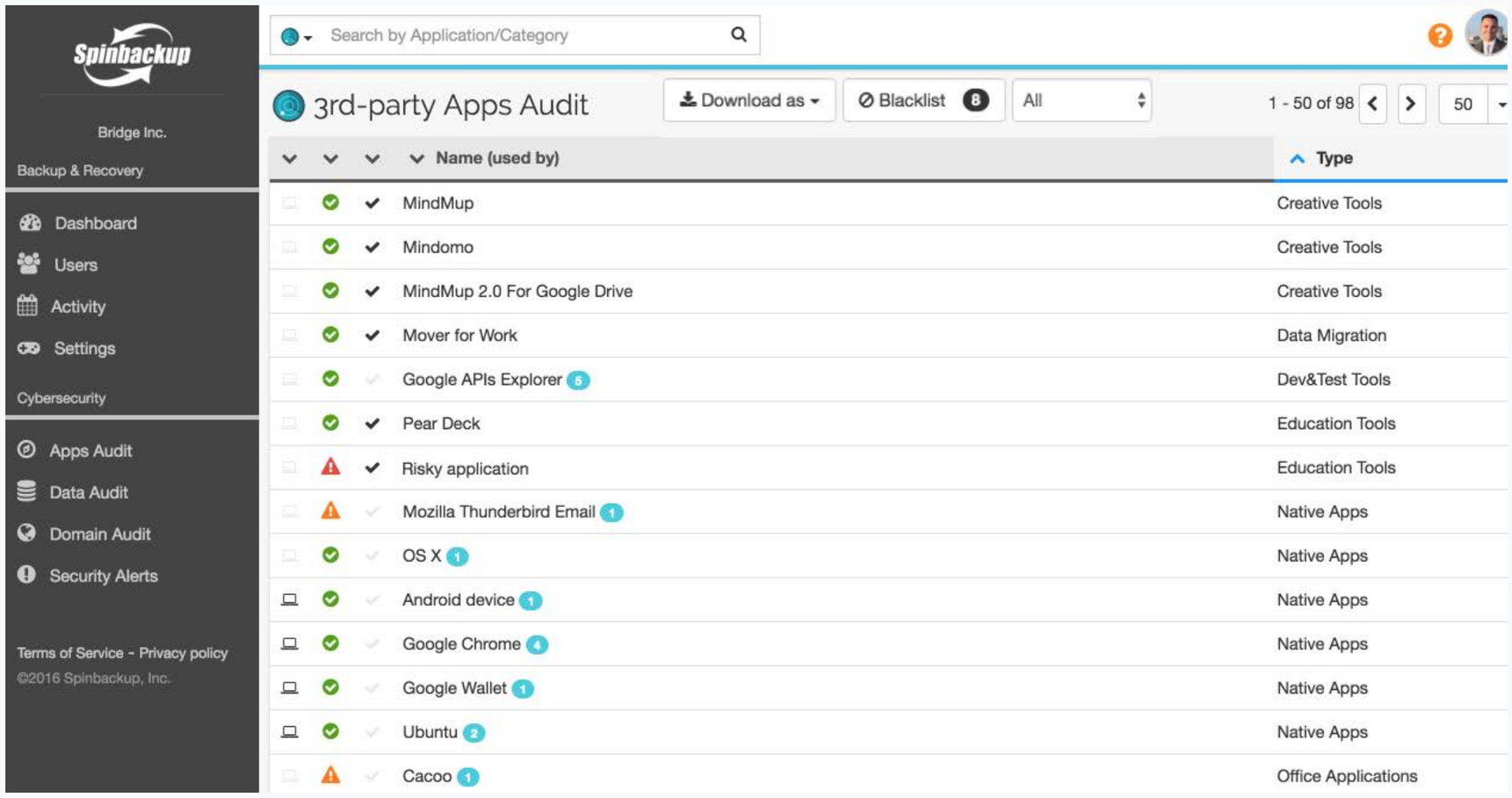
Abnormal activities may mean that your data is under a threat of data leakage. Spotting abnormal usage is not an easy task. First of all, the amount of data you need to monitor is significant. There are many metrics to look at for detecting abnormal usage including Storage, User's Status, and Security. Manual monitoring is extremely time-consuming.

Abnormal usage is not always easy to detect from the admin console. Google domain admin must audit every application. But there is always a chance that you miss some suspicious behavior. In other words, the results of manual monitoring may not be sufficient.

That's why many administrators turn to automated tools. For example, this automated security service is designed to detect suspicious activities. It sends automated alerts within and outside G Suite about an oncoming attack, abnormal user activities, and risky applications installed.



You can research abnormal usage through the Google Apps and Reports links in the admin panel. It is highly recommended to use Google Apps Reports in pair with the SpinOne Domain Audit to reach synergy in monitoring security issues.



5.

Create an Incident Response Plan

SaaS Data Protection Guide

Make sure you implement ransomware preventive measures

There are many potential G Suite security incidents. Data leakages, phishing attacks, ransomware infections, to name a few. In fact, they can happen anytime. Usually, the damage becomes more serious with time.

That’s why it is a good practice to create an Incident Response Plan. This plan will allow you to act quickly in time of a security incident to minimize the damage and prevent the whole system from collapse.

A response plan consists of three major elements: detection, prevention, and control.
Prevention is a set of actions, aimed at making the chance of a cyber attack as low as possible. Perhaps, the most important prevention action is ensuring a 2-Step Verification is used consistently.

Detection is the foremost defense. You must be able to distinguish unwanted incidents such as viruses, hacks, and other malicious attacks. Your G Suite admin’s response plan should include the ability to detect almost all suspicious activities before they take place.

The major suspicious activity is access to unauthorized data, instigated by third-party apps, malicious codes, and even hackers – including employees.

You need to use control measures when access to unauthorized data occurs. For a compromised account, you can use the following measures of the response plan:

- Changing the access password immediately
- Neutralizing the attack or mitigating cyber risks
- Updating the system.

The main goal of these actions is to fix the consequences of an incident. Sometimes, the control operations include a whole set of actions to restore the system to initial capacity. The control measures can help even if an admin account itself was targeted.

6.

Instill Proper Process for Employees Joining/Leaving the Company

SaaS Data Protection Guide

Major security threats can originate from insiders – especially employees joining or leaving the company. The more new employees gain access to the corporate network, the more potentially vulnerable endpoints appear. An admin has to prevent and avoid a security breach both from within and from outgoing entities.

The solution you need is the implementation of insider security policy. The policy will ensure that system activities of your employees can be monitored at all times. Moreover, it will raise the cybersecurity awareness of the staff. More security awareness = less potential threats.

A G Suite admin should also make sure that employees follow the company's Bring Your Own Device (BYOD) policy put in place. Many security attacks arise from breaches, which take place on employees' external devices such as USBs, hard drives, or even smartphones and laptops. In fact, fresh employees are often unaware that a USB flash drive they bring in may be infected with malware.

If employees do leave the company, they should be denied further permission to access the company's data and information, and the admin should provide a secure employee's exit.

7.

Remember to Backup

In the case of a cyberattack, the loss and/or modification of data is inevitable. The consequences might be severe, from a denial of service or compromised transactions.
Why is data backup so important? The answer is quite simple. It is one of the best ways to restore your lost or modified data.
To ensure data loss prevention of G Suite data you need to do automated daily backups so you could restore your data at any time. Over 50% of data loss issues are due to end-user mistakes.

For example, removable storage devices that a new employee uses might be infected with malware. If you want 100% data loss protection, you can use the SpinOne G Suite Backup solution with a free trial available.

To sum up, becoming a perfect G Suite admin can be challenging. Understanding G Suite administrator fundamentals takes some time, but implementing these practices will help you.
Mastering the above G Suite data protection practices will ensure the success of your organization and its data. Plus, you will have the power to prevent data breaches.

Try SpinOne Free →

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)