Pythian's Enterprise Guide to Google Workspace Security

Harden your Google Workspace security today.

Google Workspace

Pythian

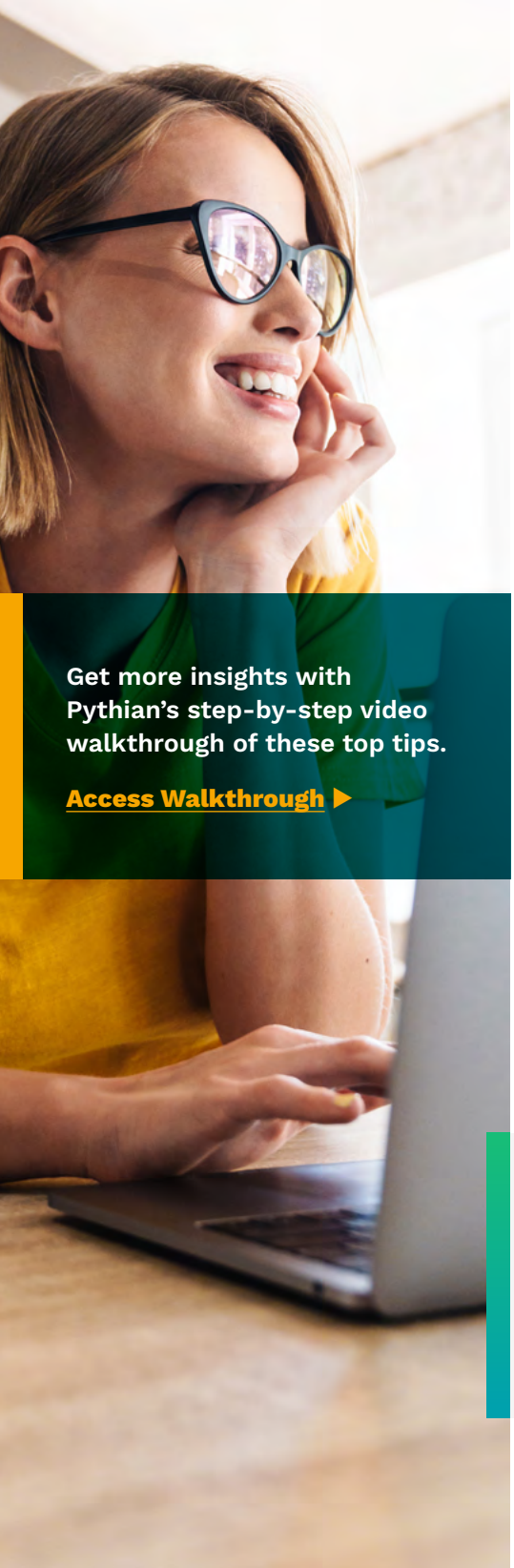
While Google Workspace offers native security controls, this suite of collaboration and productivity tools also runs on a shared responsibility model. That means, as an IT administrator, you're responsible for implementing policies and procedures such as access controls and permissions. And if you work in a highly regulated industry or with highly sensitive data, you may require more robust security controls.

Recent **research** on collaboration tools shows that 73% of employees can access data they didn't create; 69% can view data they didn't contribute to; and 59% can see data from other departments. And more than one-third believe file sharing has made them more complacent about data security.

So how do you harden your Google Workspace security posture? In this handbook, we'll take a look at common watchpoints, their potential risks and our recommendations for mitigating those risks. Every organization has different requirements, so once you understand your specific configurations and use cases, you can make an educated decision on how to proceed.

Here are four key watchpoints to help you harden your Google Workspace security posture:

1 Google Takeout



Get more insights with Pythian's step-by-step video walkthrough of these top tips.

Access Walkthrough ▶

What is it?

Google Takeout allows users to export data from their organizational accounts to a local machine, with support for more than 50 different types of data including Drive, Calendar and Gmail. Some use this option to free up space in Google accounts where cloud storage is limited, while others use it to copy data onto local storage or to another account.

What you need to know about this setting:

While Google Takeout is a great tool for on-demand exports and manual backups, the drawback is that leaving this option on for everyone means your organization is open to unwanted or unwarranted data exfiltration. This can leave the organization at risk of data loss if careful steps aren't taken to control who can use this option and what data is allowed to be exported.

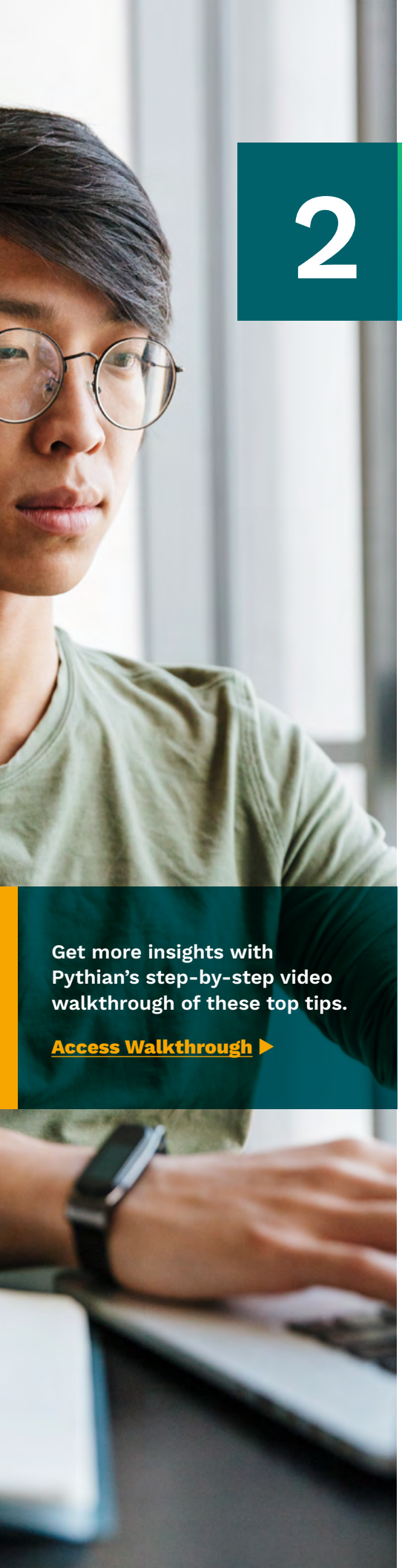
Recommendations:

- Turn this option off at the root organizational unit (OU) or global OU. Limit Takeouts to very specific use cases, and ensure these cases are approved by the appropriate parties.
- Even if you disable Takeouts on a global level, you can still allow access to export data using Takeouts, which can help alleviate these restrictions.
- A best practice is to set up a lone OU and only allow use of Takeouts to users within this OU.
- The same practice can be transferred to the use of a specific group instead of an OU, if current infrastructure is better suited to do so.

Google Workspace Security Health Check

Looking for more help with keeping your Google Workspace environment secure? Our Google Security Health Check can help your organization reduce risks, better protect users and company data through a review and assessment of your current configuration settings.

Learn more ▶



Get more insights with Pythian's step-by-step video walkthrough of these top tips.

Access Walkthrough ▶

2 Gmail: Advanced Security and Safety Settings

What is it?

Advanced security and safety settings that further assist with Gmail security include links and external image protections, spoofing and authentication, and attachment protections. You can provide the strongest level of protection for a domain or organizational unit by turning on all security options or you can customize security settings by checking only the options you want to turn on.

What you need to know about this setting:

Many organizations are using SPF, DKIM and DMARC to assist with spam and authentication, but fall short of enabling additional security features in Google Workspace—so they still fall victim to phishing attacks, malicious attachments and hidden links from untrusted senders. Additional settings include the ability to protect against content sent from untrustworthy parties; scan and identify links behind images and shortened URLs; and additional protections against spoofing of employee names, similar domain names or unauthenticated emails.

Recommendations:

- Regularly review Gmail settings and ensure your organization is up-to-date with any new features that have been released since your last audit.
- Enable as many (or all) of the safety settings for each section. Each setting has an option that allows you to choose what action to take when a potentially malicious email is flagged.
- If sending emails to a quarantine, ensure notifications are turned on when an email is sent to that quarantine.
- You may need to monitor and finetune these settings when you first enable them. Have a plan to manage these spam classifications and quarantines by delegating various tasks to your IT staff.

3

Google Drive: Sprawling Sharing Settings

What is it?

As an IT administrator, you control whether users share Google Drive files and folders with people outside your organization (who also have Google accounts). These **sharing settings** apply to items from Google Docs, Sheets, Slides, My Maps and folders—and anything else stored in Drive. Depending on your Google Workspace edition, you can turn external sharing on or off for your entire organization or for specific child organizational units or configuration groups.

What you need to know about this setting:

External sharing is a great way for internal and external users to collaborate on documents, presentations and spreadsheets. But these settings should be closely monitored and set to the most restrictive settings at the root (and then opened up to child OUs or configuration groups for more open-ended sharing settings). Misconfigured sharing settings can lead to unwanted sharing permissions and links being shared publicly.

Recommendations:

- If your organization allows for external sharing, review each setting in detail, both for My Drive and Shared Drives.
- You can choose to share only with domains in your designated allowlist, which will limit which organizations your users are able to share files with.
- Disable the option to make files and published web content visible to anyone with the link, since links can be shared easily and with anyone. Stick to explicit sharing permissions.
- With Shared Drives, it's best practice to limit shared drive creation to administrators. Decide if external users or non-members will be allowed access to files contained within the Shared Drive; if so, limit exposure by keeping "internal" and "external" versions.

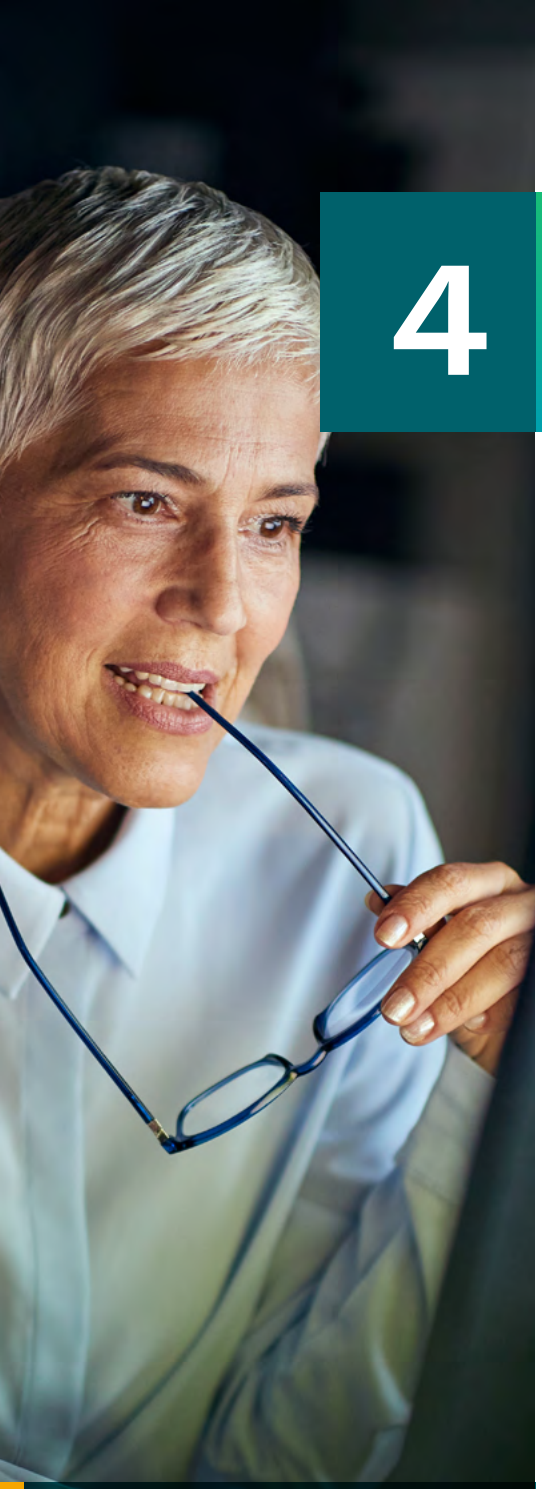
Get more insights with Pythian's step-by-step video walkthrough of these top tips.

Access Walkthrough ▶

Google Workspace Security Posture Analysis

Get the support you need with Pythian's Security Posture Analysis. Pythian's approach couples our Google Workspace Security Health Check with a deep dive into the actual data within your organization..

Learn more today ▶



4 General Gmail Settings: Forwarding, Delegation, POP/IMAP

What are they?

A number of traditional email settings have been around for years, such as email delegation, automatic forwarding and POP/IMAP. They make everyday tasks easier and more efficient, and when used in the correct manner they're somewhat inconsequential. However, if left unchecked, they can have sprawling and unintended consequences.

What you need to know about these settings:

EMAIL FORWARDING: This makes it easy to forward emails from one organizational account to another, or to a Google group or collaborative inbox. But there could be confidential information contained in those emails and various compliance policies to adhere to.

EMAIL DELEGATION: Executives often delegate access to their mailbox to their executive assistant. While this is common practice and fairly harmless, risks can include unauthorized access, data loss and abuse of rights.

POP/IMAP: For synchronizing Google Workspace account emails with other email clients such as Microsoft Outlook or Apple Mail, you need to turn on POP or IMAP in the Google Admin console. With POP, email messages and attachments are removed from the mail server after they're opened on a user's device (which could be a problem for email audits). With IMAP, they stay on the mail server even after they're opened. Ensure that when using either of these sync options, you're doing so with managed devices, including desktops, laptops and mobile devices.

Recommendations:

- At the root, disable email forward. If needed, set up a child organizational unit or configuration group that will allow for automatic forwarding.
- Regularly audit email delegations to ensure that every delegate has been approved and is currently active. Any terminated users or users who have changed positions and no longer require access should be removed.
- If allowing POP/IMAP, do so using a separate OU or group. Regularly audit who is using POP and IMAP and their last date of use. Set a policy to revoke this option after not being used after a certain time period.

Get more insights with Pythian's step-by-step video walkthrough of these top tips.

Access Walkthrough ▶

Google Cloud Partner
Managed Service Provider

Google Cloud
Partner of the Year
Data Management
2020

Staying on top of security

These are just a few items to look out for in your Google Workspace environment. Some of these options may not apply to your workflows, and not every recommendation is going to work across every organization. The key is to stay on top of your own security posture and remain vigilant. Knowing where you stand is half the battle.

For more information, visit the Pythian Google Workspace Hub, or talk to a **Pythian Google Workspace Expert**.

linkedin.com/company/pythian

twitter.com/Pythian

Contact us at +1-866-798-4426 or info@pythian.com

ABOUT PYTHIAN

Founded in 1997, Pythian is a global IT services company that helps organizations transform how they compete and win by helping them turn data into valuable insights, predictions and products. From cloud automation to machine learning, Pythian designs, implements and supports customized solutions to the toughest data challenges.

OFFICES

Ottawa, Canada | New York City, USA | Minneapolis, USA | London, England | Hyderabad, India