Pythian's Email Security Deep Dive for Google Workspace

Protect your domain reputation

Email fraud is expensive — and it's a growing problem. With AI making it easier and faster for bad actors, the prevalence of phishing schemes, where legitimate-looking emails, text messages, and phone calls trick individuals into revealing personal or financial details, is becoming both more widespread and harder to detect. In fact, a 2024 study of phishing email click-through rates found that large language model (LLM)-generated phishing messages had a significantly higher click-through rate (54%) compared to likely human-written phishing messages (12%).

Phishing attacks have increased by 4,151% since ChatGPT's public debut in late 2022, according to "The State of Phishing 2024" report. And 68% of all phishing emails are text-based BEC. "The diversity and sophistication of BEC types have received a significant boost from the public availability of generative AI chatbots," according to the report.

As the primary channel for business communications, every organization should be concerned about email security, which is a major target for threat actors looking to solicit funds and personal information from unsuspecting employees. However, many of these threats and losses are preventable—which is why email shouldn't be an afterthought in an organization's cybersecurity strategy.

Cloud misconfigurations pose a major security risk. Improper setup or maintenance can lead to unauthorized access and data breaches, with **75% of security failures** resulting from inadequate management of identities, access, and privilege, according to a report by the Cloud Security Alliance.

Highlights

- Audit, secure, and configure your Google Workspace email settings to guard against phishing, spoofing, and domain impersonation with this 8-10 week engagement.
- Identify legitimate sources, block unauthorized senders, and safeguard your brand reputation with expert DMARC policy setup.
- Equip your admins with the knowledge to manage spam filtering, email authentication, and proactive threat defenses.

Make the most of Google Workspace security features

Google Workspace has a suite of built-in security protections that can help keep your organization's data safe, including phishing protections, email encryption and proactive alerts. With certain Enterprise editions, you'll also have access to Security Sandbox, which can scan attachments that may be missed by traditional antivirus programs in a virtual environment.

But **these features are only as good as their configurations**. If they're not set up properly, you could be leaving the door open for spam, spoofing and phishing.

Does your team have advanced knowledge of Google's spam filtering service and email security settings? Are you using all available features in Google Workspace to secure your email services and protect your data? Are you sure that all settings are configured properly, so there aren't any holes in your security defenses? And is your domain protected against spoofing with an aggressive DMARCian policy? If you're not sure about the answers to these questions, Pythian can help.

Pythian's Email Security Deep Dive

If you're not sure about the answers to these questions, Pythian's Email Security Deep Dive service can help. As part of this fixed-fee service, we'll make sure you're taking advantage of Google Workspace's robust security features and confirm that all settings have been configured properly. We'll also help to authenticate sources and protect against spoofing of your domain, while providing training to your team to maintain your security going forward.

How it works

1

Phase 1: Auditing and reporting

We'll review your email service and group settings in Google Workspace and provide a comprehensive report with our recommendations and best practices. In a workshop setting, we'll collaborate with your team to ensure our recommended features and configurations meet your needs.

2

Phase 2: DMARCian trial

From there, we'll run a DMARCian trial to make recommendations for a Domain-based Message, Authentication, Reporting and Conformance (DMARC) policy. DMARCian allows you to identify and authenticate legitimate sources and implement a DMARC policy that blocks any non-authenticated sources.

DMARCian also allows you to manage responses to the results of SPF (Sender Policy Framework) and DKIM (Domain Key Identified Mail) email authentication methods to help protect the reputation of your domain from senders attempting to impersonate your domain.

3

Phase 3: Training

In addition to providing a configuration record report, we'll also review email security best practices and provide advanced email security training for administrators on managing Google's spam filtering service, spam settings, and email authentication.

4

Phase 4: Implementation

We'll work with you to implement prioritized and actionable recommendations to mitigate spoofing and protect your domain reputation.

Why Pythian?

Pythian goes beyond technical security reviews of Google Workspace, focusing on the human element and change management to ensure your data is protected through a people-first approach. We help your teams understand what was done and why it was done, empowering them for future success.

Our expertise in DMARC, SPF, and DKIM applies to any email platform your organization is running, including Microsoft 365 and Gmail. So, whichever email platform you're using, we can provide consultation and professional services to help boost your organization's email security, mitigate email risk, and protect your domain.

Our proven delivery method has been used to support some of the world's largest, most complex companies—and we can do the same for you.

Get started with Pythian

Getting the most out of Google Workspace often requires a partner by your side. Contact us to find out how we can help you secure your Workspace environment and get the most out of your productivity tools.

About Pythian

Founded in 1997, Pythian is a data and analytics 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.

Contact us

+1-866-798-4426 | info@pythian.com | Linkedin | X

Offices

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

love your data