Email Security Deep Dive

Protect your domain reputation

Email fraud is real—and it's expensive. More than 90% of cyberattacks begin with phishing, which is estimated to cost organizations millions each year. That doesn't even touch on losses from business email compromise (BEC) and spoofing, or the reputational risk if a threat actor uses your corporate domain to victimize people.

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

Security features in Google Workspace

Google Workspace has a plethora of built-in security protections that can help to keep data safe— including phishing protections, email encryption and proactive alerts. Depending on which edition you're using, you may be entitled to additional security features. With certain Enterprise editions, you'll have access to Security Sandbox, which can scan attachments that may be missed by traditional antivirus programs in a virtual environment.

But remember, **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?

Highlights

- Configuration record report
- Implementation of DMARCian
- Advanced email security training

Pythian's Email Security Deep Dive

If you're not sure about the answers to these questions, Pythian's Email Security Deep Dive service offering 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 its settings have been configured properly. As part of the service, we'll help to authenticate sources and protect against spoofing of your domain, while providing training to your team to maintain your security going forward.

Key components of Pythian's approach to email security

- **Phase 1: Audit and reporting**
  We'll review your email service and group settings in Google Workspace, then provide a comprehensive report with our recommendations and best practices.

  We'll collaborate with you in a workshop setting to ensure the features and configurations we recommend meet your needs, whatever your team or corporate structure.

- **Phase 2: DMARCian trial**
  We'll implement a DMARCian trial to enable analysis and 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. These protocols are designed to help protect the reputation of your domain from senders attempting to impersonate your domain.

- **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.

- **Phase 4: Implementation**
  We'll work with you to implement the prioritized and actionable recommendations discussed in the process to mitigate spoofing and protect your domain reputation.

Why Pythian?

With Pythian, you can maximize your investment in Google Workspace by leveraging our long-established expertise. We offer a variety of strategic and technical services across major platforms and technologies to help you meet your business goals. Our expertise in DMARC, SPF and DKIM applies to any email platform your organization is running, including Microsoft 365 and Gmail. 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.

Get Started with Pythian

Getting the most out of your cloud computing environment often requires a partner by your side. Pythian provides end-to-end services and support for Google Workspace features and functionality, including advanced email security and permissions configurations.

To find out more, email us at 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.

Contact us

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

Offices

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

Pythian

love your data