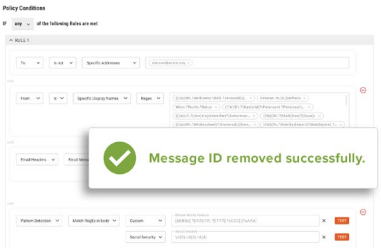
GreatHorn Google Workspace™

Email Security in Google Workspace: What Works – and What Doesn't

Has your organization transitioned its electronic communications to the Google Workspace cloud email platform? If so, then your attackers have shifted their assault tactics to include zero-day attacks and complex social engineering.

Google Workspace handles certain email security threats well. But to address ongoing vulnerabilities and emerging attacks, you need the sophisticated, multilayered approach of the GreatHorn Cloud Email Security Platform. With GreatHorn, you have the capabilities you need to reliably and effectively respond to risk across every phase of your end-to-end email lifecycle.



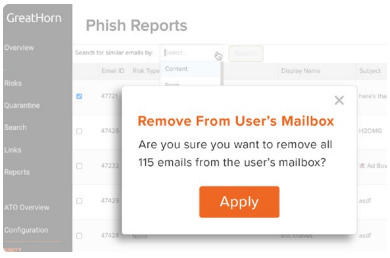
Configuration

Google Workspace is essentially a "black box," with minimal configuration options. That limitation prevents you from tailoring controls based on individual users, roles or risk types.

What's more, the platform doesn't let you customize email controls based on header information, sender and receiver relationships, or domain reputation. And what if one of your business partners, such as a supply chain vendor, is compromised? Google Workspace has no means of detecting the problem.

GreatHorn empowers you to configure and customize your email protection based on your unique needs – aligned with your business requirements and tuned to the level of risk that's right for your organization.

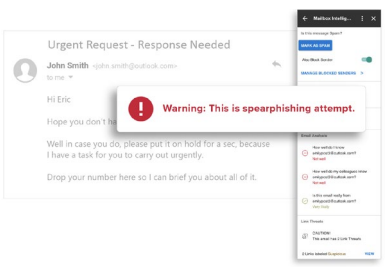
In addition, GreatHorn delivers advanced anomaly detection to reduce the risk of email-borne attacks. The solution adapts to your organization with out-of-the-box spoofing detection and an anomaly-detection model that evaluates relationships, communication patterns and technology fingerprints unique to each sender and recipient organization.



Malicious Threats

Google Workspace is effective at identifying known malicious attachments and links. Administrators can configure the platform to quarantine suspicious email, move it to a spam folder or label it with a warning. But that still leaves you vulnerable to zero-day attacks. And it does little to engage users in the moment of risk.

GreatHorn combines patented algorithms with context-based relationship analysis and content review to dynamically identify potential threats. Customizable banner alerts and stoplight visuals inform users, tune behavior and ultimately help mitigate phishing risk.

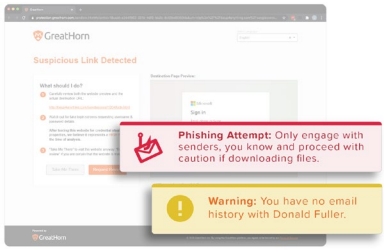


Suspicious Links

Google Workspace can identify links behind short URLs, scan linked images for malicious content and display a warning when users click on links to untrusted domains. Trouble is, a link to a website that was safe when the message was delivered can become malicious in an instant.

GreatHorn provides time-of-click analysis, with security based on the URL's status at the moment the user clicks. It can then present the user with a dynamic warning – including a screen capture of the destination page that highlights relevant risks – to drive safe user behavior. As a result, your organization can avoid the financial and legal risks of credential theft – a top threat of phishing attacks.

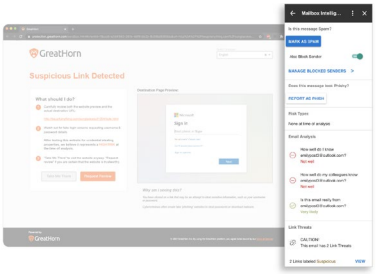
GreatHorn



Bannering

Google Workspace provides warning banners only in the web browser and on the Gmail™ mobile app web platform. It doesn't deliver a consistent bannering experience across all email clients, such as Apple® Mail, iPhone® mobile email and the Microsoft® Outlook® client.

But a consistent experience across email clients is crucial for driving users to take the right actions as they interact with email on multiple devices. GreatHorn provides consistent and customizable banners to warn employees of critical email threats. Our banners alert users to the exact risks associated with each email as they engage with it. They likewise provide specific and context-relevant instructions to immediately inform users of the potential threat.



User Education

Google Workspace provides no security training to users. This leaves out a key element effective email security: your people.

When protecting against business email compromise (BEC), impersonations, brand lookalikes and advanced spoofing attacks, your employees can be your last, best line of defense. GreatHorn provides your users with the facts and in-the-moment training that empower them to take the right actions at the right time – so they can protect your organization when it needs it most.

GreatHorn Cloud Email Security Platform

The GreatHorn Cloud Email Security Platform layers sophisticated detection of polymorphic phishing threats with user engagement and an integrated incident response. You can address advanced threats the moment they target your environment. Ultimately, you can transform the way you manage email security – and business risk.

Empower Users With In-the-Moment Risk Mitigation

User engagement provides the context and nuance that are crucial to risk mitigation. Stoplight visuals and customized, policy-based banners empower your users to recognize and respond to threats.

Reduce Exposure With Incident Response and Reporting

From automated removal to two-click threat remediation, GreatHorn's integrated incident response accelerates action, reduces exposure and simplifies workflows for analysts.

Improve Your Risk Profile With Fact-based Analytics

Reduce mean time to detect (MTTD) and mean time to respond (MTTR) for threats that bypass the perimeter. Measure risk across the entire email environment, including relationship analytics, to automate granular policy-based actions.

Get the Facts Sooner with a Free Demo. Learn more at www.greathorn.com.