Google Workspace

Help prevent cyber threats before they emerge with Google Workspace

From ransomware to intellectual property theft, cybercrime is an everyday reality, with phishing and social engineering scams being some of the most common entry points for data breaches. In fact, 89% of initial attempts to gain access to networks and systems in 2023 were phishing emails with 65% of successful intrusions beginning with an exploit, phishing, or stolen credentials. With that in mind, commercial and public sector organizations must be vigilant about their digital interactions to reduce the cyber threat surface and minimize the likelihood of a data breach.

As a cloud-native service with automated threat defenses powered by Google AI, Workspace is designed for the modern threat landscape and can help commercial, education, and government organizations to:

Defend against harmful content with Google AI

- Enable enhanced security checks and automatically block more than 99.9% of spam, phishing, and malware before they reach users
- Set up and manage email quarantines for admin review and enforce additional actions for certain file types and attachments
- Protect users by identifying dangerous links in emails and showing warnings if users unknowingly click on them

Prevent account takeovers

- Implement login protections and controls to guard against targeted attacks and help prevent account takeovers
- Transition to passwordless login with passkeys, a simpler and more secure method than passwords
- Provide added safeguards to accounts at high risk for targeted attacks, such as admins or business leaders, by enrolling them in Google's Advanced Protection Program

Identify, triage, and respond to threats

- Take action on alerts and view reports to discover potential security and configuration issues within your domain
- Identify, triage, and take action on security and privacy issues in your domain with the security investigation tool
- Get actionable suggestions on how to improve the security posture across your organization, all from a single location

Google Workspace

“ ***Snap chose Gmail and Workspace to gain a stronger security posture****. In fact, since adopting FIDO2 Security Keys and moving to shorter login sessions across our company, we've had zero account takeovers for more than two years.”*

Nick Reva, Head of Corporate Security Engineering, Snap Inc.

“Keeping our citizens' data safe is paramount to our mission, and ***we chose Gmail primarily because of its security****. After replacing a legacy email provider with Gmail, our users noticed a meaningful decrease in spam, phishing, and malware, helping us reduce our cyber security risks.”*

Abdullah H. Hammoud, Mayor, City of Dearborn

ARIZONA DEPARTMENT OF ADMINISTRATION TECHNOLOGY

Gmail is much better than our previous malware filter. *The first month after we migrated, we ran the 2 systems in parallel. Gmail removed 107,000 malicious emails that the old system didn't catch."*

Morgan Reed, State CIO, State of Arizona

Automated threat defenses and security controls in Workspace can help organizations lower their cybersecurity risks and insurance premiums:

1

50%

fewer email security incidents for organizations using Workspace vs Microsoft 365 [1]

2

62%

fewer email security incidents for organizations using Workspace vs Microsoft Exchange [1]

3

50%

could be saved on cyber security insurance premiums by using Workspace [1]

[1] Ranking Email Security Solutions: A Data Analysis of Cyber Insurance Claims, At-Bay, 2/2023

Ready to get started?

Get the conversation started or sign up for a free trial.