Barracuda
Your business, secured.

Top 5 reasons to add a layer of protection to Google Workspace's native email security

Google Workspace provides a solid baseline for email security and effectively blocks large volumes of spam, phishing and known malware. But today's attacks are far more subtle — quieter, highly targeted and engineered to exploit human trust rather than technical vulnerabilities. Security coverage can also vary by configuration and license tier, creating blind spots that are difficult for teams to monitor and that attackers are quick to take advantage of.

Here are five critical gaps in Google Workspace's native email security — and how Barracuda Email Protection closes them with layered, purpose-built defenses designed for today's most sophisticated attacks.

37% OF ACCOUNT TAKEOVERS START WITH PHISHING OR STOLEN CREDENTIALS

84% YEAR-OVER-YEAR INCREASE IN EMAIL DELIVERED INFO STEALING MALWARE

Source: IBM X-Force 2025 Threat Intelligence Index

01 | Impersonation detection focuses on authentication, not intent

Google limitation

Google Workspace relies heavily on sender authentication checks to identify spoofing and impersonation attempts. While this approach can surface obvious attacks, it doesn't fully account for message context, behavioral patterns or malicious intent. Many advanced impersonation attacks leverage properly authenticated domains, compromised vendor accounts or subtle lookalike identities that easily pass technical validation checks.

How Barracuda can help

Barracuda goes beyond authentication to analyze intent. Barracuda Email Protection evaluates sender identity, historical communication patterns, writing style, relationship context, and behavioral anomalies to determine whether an email makes sense for that recipient and moment in time. This deeper analysis enables Barracuda to detect CEO fraud, vendor impersonation and other social-engineering attacks when emails appear seemingly clean.

02 | Post-delivery threat response is manual and time-consuming

Google limitation

When a phishing email bypasses initial defenses, Google Workspace provides investigation and remediation tools, but response is largely manual. Administrators often rely on log searches, scripts or user-reported messages to identify threats and remove them from mailboxes. These processes require time, experience and coordination, especially in larger environments. During this response window, malicious emails can remain active in inboxes, increasing the likelihood that users click links, reply with sensitive information or forward the message internally.

How Barracuda can help

Barracuda delivers post-delivery protection that identifies threats after messages reach user inboxes. Using AI analysis, community threat intelligence and user-reported emails, Barracuda automatically removes malicious messages from affected mailboxes. This automated remediation reduces dwell time, limits user exposure and helps security teams respond faster without relying on manual cleanup.

03 | Limited visibility after account compromise

Google limitation

Google Workspace is effective at preventing unauthorized sign-ins, but once an attacker logs in using valid credentials, activity often appears legitimate. Post-login behaviors, such as mailbox rule creation, message forwarding and data access aren't continuously evaluated for signs of malicious activity. Without behavioral monitoring after authentication, compromised accounts can be abused to impersonate trusted users, spread attacks laterally and quietly exfiltrate data.

How Barracuda can help

Barracuda monitors mailbox behavior after login to identify signs of account takeover. By analyzing abnormal sending patterns, suspicious forwarding rules and risky configuration changes, Barracuda surfaces compromised accounts earlier. This early visibility helps security teams intervene before attackers can abuse trust, escalate privileges or cause widespread damage.

04 | Malware-free phishing exploits psychology, not identity

Google limitation

Many modern phishing attacks don't rely on impersonating a specific trusted individual. Instead, they exploit psychology by using short, plausible messages that appear routine and harmless. These emails often don't contain malicious links or attachments and may come from unrelated but legitimate-looking domains or free webmail accounts.

Google Workspaces native filters may not flag these messages because they pass authentication and lack obvious technical indicators of compromise. They are designed to blend seamlessly into everyday email traffic that ask quick questions, include informal follow-ups or make simple requests. As a result, users are more likely to respond, even when the sender isn't explicitly trusted.

How Barracuda can help

Barracuda uses AI-driven behavioral analysis to evaluate how a message behaves rather than who it claims to be from. By analyzing tone, timing, conversational flow, domain similarity, and message intent, Barracuda identifies suspicious behavior patterns that indicate social-engineering attempts.

This approach allows Barracuda to stop emails that rely on manipulation rather than identity abuse.

05 | Security capabilities vary by Google Workspace edition

Google limitation

Advanced security features in Google Workspace vary significantly by license tier and configuration. Capabilities such as advanced investigation, automated remediation and enhanced threat analysis may be unavailable depending on the edition in use or could require manual enablement. This variability can create inconsistent protection across users and departments, leaving some mailboxes more vulnerable than others. Attackers exploit these uneven security levels by targeting the least-protected users as an entry point into the business.

How Barracuda can help

Barracuda adds an additional layer of email protection that businesses can easily apply consistently across users, independent of Google Workspace edition. By extending advanced detection, behavioral analysis, automated response, and visibility beyond Google Workspace's native controls, Barracuda helps reduce licensing-driven gaps and limit opportunities attackers commonly exploit.

Closing the gaps with layered email protection

While Google Workspace provides a foundation for email security, it's not built to stop every type of modern, human-targeted attack on its own. Barracuda strengthens Google Workspace's native protections by focusing on the threats most likely to slip through — impersonation, socially engineered phishing, account takeover, and post-delivery attacks that unfold inside compromised inboxes.

Together, Google Workspace and Barracuda create a true layered defense. Google Workspace blocks known and commodity threats at scale, while Barracuda adds the intelligence, behavioral context and automated response needed to detect and stop sophisticated, trust-based attacks. The result is broader coverage, faster response and stronger protection — without disrupting users or replacing Google Workspace.

Barracuda
Your business, secured.