

Cloudflare Area 1 and Google Cloud:

Integrated Cloud Email Security and Preemptive Anti-Phishing

Industry challenges:

Today's sophisticated phishing attacks such as malware-less business email compromise (BEC), account takeover-based fraud, and insider threats are difficult for traditional secure email gateways or email authentication to detect.

The solution:

The Cloudflare Area 1 email security service proactively crawls the web to discover phishing campaigns and uses that early insight, plus contextual email analysis techniques, to protect your inboxes from phishing attacks — before damage can occur.

Built on the Google Cloud Platform, Area 1 deploys in just minutes to deliver a best-of-breed, defense-in-depth anti-phishing security layer.

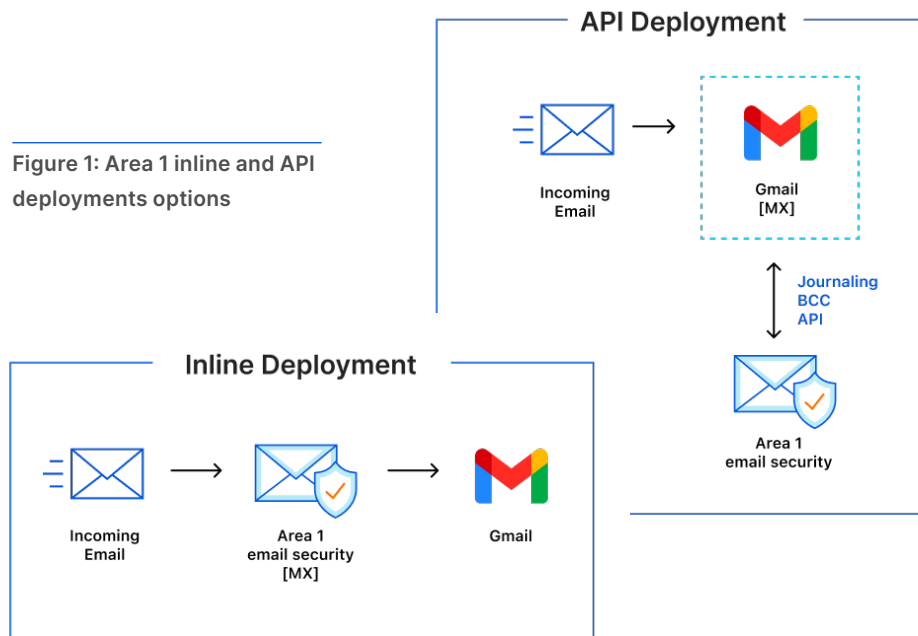


Figure 1: Area 1 inline and API deployments options

Defend against modern attacks that target your #1 cloud application — email.



Proactively stop phishing, BEC, email fraud, and other advanced threats.







Isolate and prevent multichannel threats with the Cloudflare Area 1 and Cloudflare Remote Browser Isolation [integration](#).



Discover compromised accounts and domains, as well as new, lookalike, and proximity domains used by attackers to bypass SPF/DKIM/DMARC.

Why Cloudflare Area 1:

 <p>Preemptive Security</p> <p>Identify attacker infrastructure and delivery mechanisms ahead of time to stop phishing at the earliest stages of the attack cycle.</p>	 <p>Comprehensive Protection</p> <p>Covers the full range of email attack types (URLs, payloads, BEC), vectors (email, web, network, multichannel), and attack channels (external, internal, trusted partners).</p>	 <p>Contextual Analysis</p> <p>Leverage advanced detection techniques (language analysis, computer vision, social graphs, and more) to catch BEC, vendor email fraud, and other advanced threats.</p>	 <p>Continuous Protection</p> <p>Assume defense-in-depth with threat protection layers before, during, and after an email hits the inbox.</p>
--	---	---	---

Why Cloudflare Area 1 plus Google Cloud:

- **Improve Operational Efficiency** — Reduce complexity by [replacing traditional secure email gateways](#) for a modern, cloud-first architecture.
- **Seamless, Flexible Deployment** — [Deploy](#) the fully elastic Area 1 service in under 5 minutes and integrate seamlessly with Google Cloud’s native features, such as anti-spam, DLP, encryption, and archiving.
- **Simplified SaaS Security** — In addition to integrated Area 1 cloud email security, the Cloudflare Zero Trust platform provides cloud access security broker (CASB) [capabilities](#) for Google. Easily prevent data leaks and compliance violations, and get a one-stop shop to stop data loss, phishing, ransomware, shadow IT, and lateral movement across your organization.

Case Study: S&P 100 consumer packaged goods leader protects executives and users against cloud email threats	
Customer challenges	Results with Cloudflare Area 1
<ul style="list-style-type: none"> • Threats slipping past Google Workspace and existing security infrastructure • BEC attacks targeting senior executives and board members • IT team spending time and resources constantly tuning email security rules and blocklists 	<ul style="list-style-type: none"> • 8 million+ targeted attacks blocked within one year • The IT team is now able to provide better email security metrics and reporting for Board meetings • Improvements in productivity and significantly reduced cybersecurity risk

To see how Cloudflare Area 1 can enhance your Gmail phishing defenses, request a custom risk assessment [here](#).