



AREA 1.



PROBLEM

Missed Phish over Gmail

G Suite is simplifying business communication and collaboration across the globe, but unfortunately, business communication continues to be the target of relentless global cyberattacks, overwhelmingly delivered by phishing emails. Phish sneak past email defenses to land in user inboxes, bringing countless threats. Customers who believe that traditional email filters and rules protect them from phish learn the hard way that this isn't true. Unlike email threats such as spam and viruses, phish are engineered to present a low-volume attack profile that doesn't appear on even the best email filter's "radar."

Email threat defense lack insight into targeted phishing campaigns. Threat data is collected from active, high-volume attack campaigns, but the low-volume, targeted outbreaks of phish successfully bypass defenses. So phish posing as valid communications breach email defenses. These criminals lure users into clicking a malicious link, opening a piece of malware, or forwarding confidential data and even funds to them.

SOLUTION

Area 1 Horizon

Stop Phishing Over Inbound Gmail. Close the Phishing Security Gap.

- Detects and blocks 99.997% of phishing attacks
- Deploys and integrates in minutes with Gmail
- Protects across all attack vectors - email, web and network traffic
- Offers the industry's only fully accountable solution. With the Pay-Per-Phish program, we catch phish—or you pay nothing.

Area 1 Security closes the phishing gap with a preemptive, comprehensive, and accountable defense against the socially engineered phish that sneak past Gmail defenses. Area 1 Security integrates quickly and smoothly to work with G Suite's email security features like anti-spam, DLP, encryption, and archiving. Fortified with Area 1 Security's anti-phish capabilities, Gmail can now detect and block phishing attacks to provide complete, real-time, and effective protection.

Area 1 Security's innovative technology continuously and proactively crawls the web, discovering phishing campaigns and infrastructure before attacks launch. On average, the solution detects malicious sites and payloads a full 24 days before industry benchmarks. The resulting early insight and threat information powers the Area 1 Horizon anti-phishing service to detect and block phishing threats providing an added layer of protection for Gmail.

