CLOUDFLARE
AREA 1 SECURITY

KURZDARSTELLUNG

Cloudflare Area 1 und Google Cloud:

Integrierte Cloud-E-Mail-Sicherheit und präventiver Anti-Phishing-Schutz

Herausforderungen der Branche:

Die ausgeklügelten Phishing-Angriffe von heute, wie z. B. Kompromittierung von Geschäfts-E-Mails (BEC, Business Email Compromise) ohne Malware, auf Kontoübernahme basierender Betrug und Insider-Bedrohungen, sind für herkömmliche sichere E-Mail-Gateways oder E-Mail-Authentifizierung nur schwer zu erkennen.

Die Lösung:

Der Cloudflare Area 1-E-Mail-Sicherheitsservice durchforstet proaktiv das Internet, um Phishing-Kampagnen zu entdecken, und nutzt diese frühen Erkenntnisse sowie kontextbezogene E-Mail-Analysetechniken, um Ihre Posteingänge vor Phishing-Angriffen zu schützen – bevor Schaden entstehen kann.

Area 1 wurde auf der Google Cloud Platform entwickelt und ist in wenigen Minuten einsatzbereit, um eine branchenführende Anti-Phishing-Sicherheitsebene zur Tiefenverteidigung zu bieten.

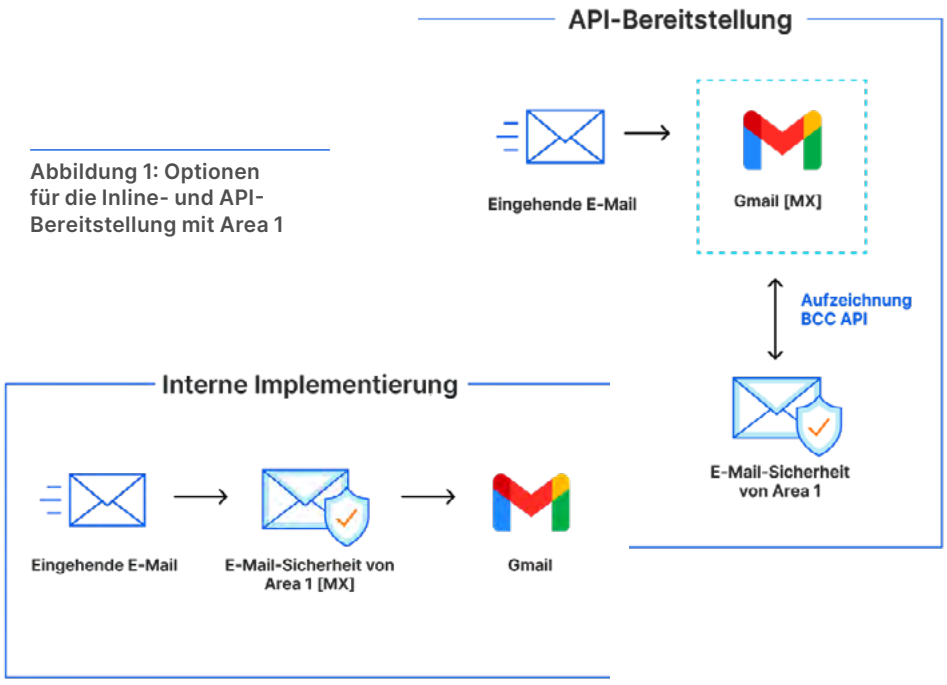

Abbildung 1: Optionen für die Inline- und API-Bereitstellung mit Area 1

Verteidigen Sie sich gegen moderne Angriffe, die auf Ihre Cloud-Anwendung Nr. 1 abzielen – E-Mail.

Stoppen Sie präventiv Phishing, BEC, E-Mail-Betrug und andere raffinierte Bedrohungen.

Isolieren und verhindern Sie Multi-Channel-Bedrohungen mit der Integration von Cloudflare Area 1 und Cloudflare Remote-Browserisolierung.

Entdecken Sie kompromittierte Konten und Domains sowie neue, täuschend ähnliche und imitierende Domains, die von Angreifern zur Umgehung von SPF/DKIM/DMARC verwendet werden.

Warum Cloudflare Area 1

Präventive Sicherheit

Identifizieren Sie die Infrastruktur und die Übermittlungsmechanismen der Angreifer im Voraus, um Phishing in den frühesten Stadien des Angriffszyklus zu stoppen.

Umfassender Schutz

Deckt das gesamte Spektrum der E-Mail-Angriffsarten (URLs, Nutzdaten, BEC), Vektoren (E-Mail, Web, Netzwerk, Multi-Channel) und Angriffskanäle (extern, intern, vertrauenswürdige Partner) ab.

Kontextbezogene Analyse

Nutzen Sie fortschrittliche Erkennungstechniken (Sprachanalyse, Computer Vision, Social Graphs uvm.), um BEC, E-Mail-Betrug durch Anbieter und andere fortschrittliche Bedrohungen zu erkennen.

Fortlaufender Schutz

Setzen Sie auf Defense-in-Depth mit Schutzebenen vor Bedrohungen, bevor, während und nachdem eine E-Mail den Posteingang erreicht.

Warum Cloudflare Area 1 plus Google Cloud:

- **Betriebliche Effizienz verbessern —** Komplexität reduzieren, indem herkömmliche sichere E-Mail-Gateways durch eine moderne, Cloud-first-Architektur ersetzt werden.
- **Nahtlose, flexible Bereitstellung —** Bereitstellen des vollständig elastischen Area 1-Service in weniger als 5 Minuten und nahtlose Integration mit den nativen Funktionen von Google Cloud, wie Anti-Spam, DLP, Verschlüsselung und Archivierung.
- **Vereinfachte SaaS-Sicherheit —** Zusätzlich zur integrierten Area 1 Cloud-E-Mail-Sicherheit bietet die Cloudflare Zero Trust-Plattform Cloud Access Security Broker (CASB)-Fähigkeiten für Google. Ganz einfach Datenlecks und Compliance-Verstöße verhindern und eine zentrale Anlaufstelle erhalten, um Datenverlust, Phishing, Ransomware, Schatten-IT und laterale Bewegungen in Ihrem Unternehmen zu stoppen.

Fallstudie: S&P-100-Unternehmen und führender Konsumgüterhersteller schützt Führungskräfte und Nutzer vor Cloud-E-Mail-Bedrohungen

Herausforderungen des Kunden	Ergebnisse mit Cloudflare Area 1
• Bedrohungen, die an Google Workspace und der bestehenden Sicherheitsinfrastruktur vorbeigehen • BEC-Angriffe auf leitende Angestellte und Vorstandsmitglieder • IT-Team verbringt Zeit und Ressourcen mit der ständigen Anpassung von E-Mail-Sicherheitsregeln und Blocklisten	• Mehr als 8 Millionen gezielte Angriffe innerhalb eines Jahres abgewehrt • Das IT-Team ist nun in der Lage, bessere E-Mail-Sicherheitsmetriken und Berichte für Vorstandssitzungen zu erstellen. • Produktivitätssteigerungen und deutlich reduzierte Risiken im Bereich der Cybersicherheit

Sie möchten erfahren, wie Cloudflare Area 1 Ihren Phishing-Schutz für Gmail verbessern kann? Dann fordern Sie hier eine individuelle Risikoanalyse an.