# Cloudflare Area 1 E-Mail-Sicherheit

Schützen Sie Ihre Benutzer präventiv vor Phishing, Kompromittierung von Geschäfts-E-Mails (BEC) und Angriffen auf die E-Mail-Supply-Chain.

Phishing ist eine der häufigsten und teuersten Cyber-Bedrohungen, denen Unternehmen ausgesetzt sind.

Cloudflare Area 1 ist eine cloudnative E-Mail-Sicherheitsplattform, die Angriffe identifiziert und blockiert, bevor sie den Posteingang des Nutzers erreichen. Sie ermöglicht einen effektiveren Schutz vor Spear-Phishing, BEC und anderen komplexen Bedrohungen, die bestehende Abwehrmechanismen umgehen.

Area 1 verbessert die integrierte Sicherheit von Cloud-E-Mail-Anbietern durch tiefe Integrationen in Microsoft- und Google-Umgebungen und -Workflows.

Area 1 ist Teil unserer Zero Trust-Dienste.

## Stoppen Sie gezielte Phishing-Bedrohungen

Area 1 schützt vor einem breiten Spektrum von Phishing-Angriffen, angefangen bei groß angelegten Kampagnen bis hin zu sehr gezielten Versuchen, die E-Mail-Supply-Chain zu kompromittieren, die sich über Monate hinziehen.

### Phishing

Der Verizon 2021 DBIR nennt Phishing als die häufigste Angriffstaktik. Durch eine Kombination aus massivem Web-Crawling, Small-Pattern-Analytics und verbesserten Erkennungsfunktionen kann Area 1 Phishing-Angriffe stoppen, bevor sie den Posteingang des Nutzers erreichen.

### E-Mail-Supply-Chain-Angriffe

Angreifer kompromittieren die E-Mail eines Anbieters, beobachten Mailmuster und fangen bestehende Threads ab, um Rechnungsbetrug zu begehen. Area 1 analysiert Mail-Threads, Nachrichtenstimmungen und soziale Graphen, um diese raffinierten Angriffe zu stoppen.

### BEC und Social-Engineering-Bedrohungen

Bei BEC geben sich Angreifer als vertrauenswürdige Personen aus oder kompromittieren sie, um Geld und Daten zu stehlen. Area 1 analysiert den Inhalt und den Kontext der E-Mail-Kommunikation, um diese „Nadel im Heuhaufen"-Bedrohungen zu stoppen.

### Erpressung und Ransomware-E-Mails

Gartner schätzt, dass 40 % der Ransomware-Angriffe per E-Mail beginnen. Area 1 hilft bei der proaktiven Abwehr von Ransomware-E-Mails, bevor sie Endnutzer erreichen, und entfernt böswillige Nachrichten, bevor sie sich verbreiten.

## Besser als herkömmliche E-Mail-Gateways

### Präventiv

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

### Kontextabhängig

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

### Umfassend

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

### Kontinuierlich

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

## Vorteile

### Verbessern Sie die native E-Mail-Sicherheit

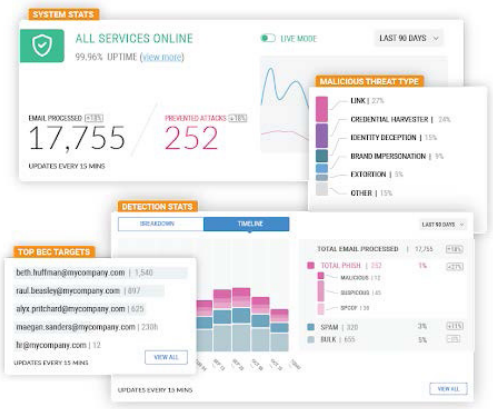
Stoppen Sie fortgeschrittene Phishing- und BEC-Angriffe, die Ihre integrierten Sicherheitsebenen umgehen. Nutzen Sie tiefe Integrationen in Cloud-E-Mail-Umgebungen mit geringen oder gar keinen Auswirkungen auf die E-Mail-Produktivität.

### Führen Sie eine Cloud-first-Architektur ein

Vermeiden Sie die schwerfälligen und unflexiblen Strukturen eines herkömmlichen E-Mail-Gateways und setzen Sie stattdessen auf eine moderne, skalierbare Architektur. Reduzieren Sie die Ausgaben für Sicherheitsebenen, die die nativen E-Mail-Sicherheitsfunktionen duplizieren.

### Sparen Sie Ihrem SOC-Team Zeit

Stellen Sie die Lösung in wenigen Minuten bereit – ohne Hardware, Agenten oder Appliances. Sparen Sie Zeit, die Sie sonst für die Erstellung und Anpassung von Richtlinien aufwenden müssten. Beschleunigen Sie SOC-Untersuchungen mit SIEM- und SOAR-Integrationen.




## Analyse des Phishing-Risikos anfordern

Fordern Sie Area 1 für Ihren Live-E-Mail-Produktions-Traffic an und sehen Sie in Echtzeit, welche E-Mail-Angriffe Ihre bestehenden Sicherheitskontrollen überwinden.

Für die Analyse müssen weder Hardware noch Software installiert werden; der E-Mail-Traffic wird nicht beeinflusst.

Fordern Sie Ihre Analyse hier an.