Cloudflare Area 1 Email Security

Preemptively protect your users against phishing, Business Email Compromise (BEC), and email supply chain attacks.

Phishing is one of the most frequent and expensive cyber threats that organizations face.

Cloudflare Area 1 is a cloud-native email security platform that identifies and blocks attacks before they hit user inboxes, enabling more effective protection against spear phishing, BEC, and other advanced threats that evade existing defenses.

Area 1 enhances built-in security from cloud email providers with deep integrations into Microsoft and Google environments and workflows.

Area 1 is part of our Zero Trust services.

Stop targeted phishing threats

Area 1 protects against a broad spectrum of phishing attacks, from large-scale campaigns to highly targeted email supply chain compromise attempts that are months in the making.

Phishing

The Verizon 2021 DBIR cites phishing as the most common breach tactic. Through a combination of massive-scale web crawling, small pattern analytics and enhanced detections, Area 1 can stop phishing attacks days before they hit user inboxes.

BEC and socially engineered threats

In BEC, attackers impersonate or compromise trusted entities to steal money and data. Area 1 analyzes the content and context of email communications to stop these “needle in the haystack” threats.

Email supply chain attacks

Attackers compromise a vendor’s email, observe mail patterns, and intercept existing threads to carry out invoice fraud. Area 1 analyzes mail threads, message sentiment, and social graphs to stop these sophisticated attacks.

Extortion and ransomware emails

Gartner estimates that 40% of ransomware attacks start over email. Area 1 helps proactively defend against ransomware emails before they reach end users and also removes malicious messages before they spread.

A cut above traditional email gateways

Preemptive

Identify attacker infrastructure and delivery mechanisms ahead of time to stop phishing at the earliest stages of the attack cycle.

Contextual

Leverage advanced detection techniques (language analysis, computer vision, social graphing, etc.) to catch BEC, vendor email fraud, and other payloadless threats.

Comprehensive

Covers the full range of email attack types (URLs, payloads, BEC), vectors (email, web, network), and attack channels (external, internal, trusted partners).

Continuous

Assume defense-in-depth with threat protection layers before, during, and after an email hits the inbox.

Benefits

Enhance native email security

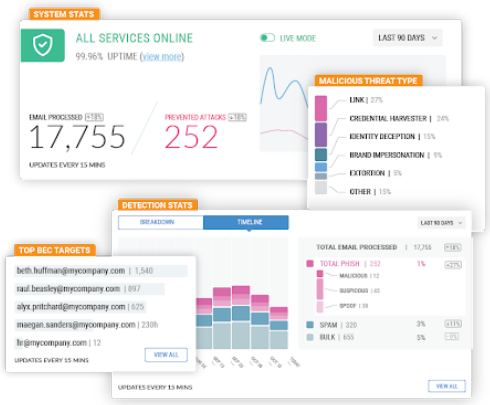
Stop advanced phishing and BEC attacks evading your built-in security layers. Leverage deep integrations into cloud email environments with little to no impact on email productivity.

Adopt a cloud-first architecture

Avoid the heavy lift and inflexibility of a traditional email gateway in favor of a modern, scalable architecture. Reduce spend on security layers that duplicate native email security capabilities.

Save time for your SOC team

Deploy in minutes without any hardware, agents, or appliances. Free up time otherwise spent creating and tuning policies. Speed up SOC investigations with SIEM and SOAR integrations.



Request phishing risk assessment

Request to run Area 1 on your live email production traffic and see - in real-time - what email attacks get through your existing security controls.

The assessment requires no hardware or software installation and will not impact mail flow.

Request your assessment here.