GCX

DATA MADE SECURE

EMAIL SECURITY

THE GCX APPROACH

Today, email remains the life-blood of many organisations and because of its importance it's a massive vector for threats against businesses and individuals.

On-premise email servers are now much less widely used, replaced largely by cloud-based email solutions. However, email still represents the threat vector of choice by malicious individuals or groups looking to breach information security defences. It is cited that around 90% of all major breaches are down to just one thing: Phishing.

Thus, we can conclude that although 1 in 7 Fortune 1000 companies use two or more email security solutions, it is clear that most fall short at blocking malicious threats and other advanced attacks.

GCXs Email Security Service powered by Cloudflare Area 1 is a cloud-native email security service that identifies and blocks attacks before they hit user inboxes, enabling more effective protection against spear phishing, Business Email Compromise (BEC), and other advanced threats that evade existing defences. It enhances built-in security from cloud email providers with deep integrations into Microsoft and Google environments and workflows.

EFFECTIVE SECURITY

STOP TARGETED PHISHING THREATS	GCX Email Security service 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. Through a combination of massive-scale web crawling, small pattern analytics and enhanced detections, our service can stop phishing attacks days before they hit user inboxes.
BUSINESS EMAIL COMPROMISE (BEC) AND SOCIALLY ENGINEERED THREATS	In BEC, attackers impersonate or compromise trusted entities to steal money and data. GCX Email Security service analyses 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. GCX Email Security service analyses mail threads, message sentiment, and social graphs to stop these sophisticated attacks
EXTORTION AND RANSOMWARE EMAILS	Prevent ransomware attacks, which are often delivered via phishing. Post-incident, email-focused security orchestration and response (M-SOAR) from Area 1 also helps stop the spread of ransomware within the network.

BUSINESS SECURITY

GCX approach to Advance Email Protection is to elevate the service beyond traditional secure email gateways (SEG's) and instead enhance built-in security from cloud email providers with deep integrations into Microsoft and Google. This approach unlike other solutions, the GCX Email Security Service continuously and proactively crawls the web to discover new phishing campaigns and attacker infrastructure in the wild. On average, the service pre-emptively detects malicious sites and payloads a full 24 days before attacks launch.

The GCX Email Security Service also uses a variety of more advanced detection techniques, including NLU, NLP, social graph analysis (patterns of email communication), and image recognition, to detect and stop the most sophisticated attacks — including brand new, highly targeted threats that threaten users 1:1 vs. one to many.

THE GCX ADVANCED EMAIL PROTECTION SERVICE, POWERED BY CLOUDFLARE AREA 1 IS:

PRE-EMPTIVE

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

COMPREHENSIVE

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

CONTEXTUAL

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

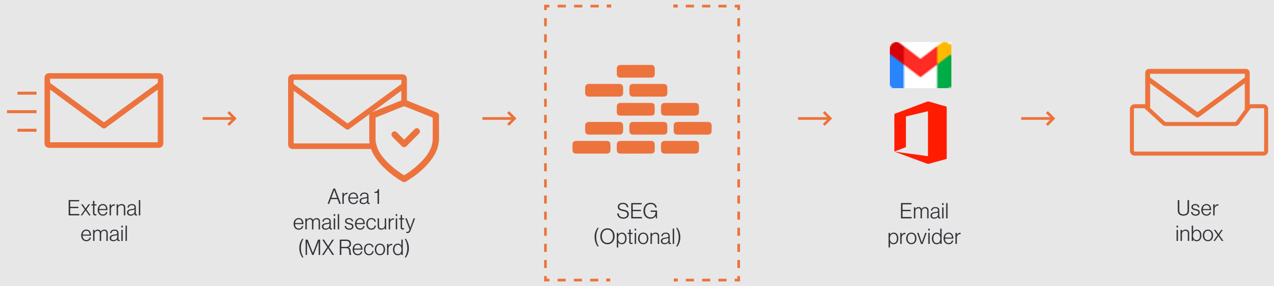
CONTINUOUS

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

CLOUD ARCHITECTURE

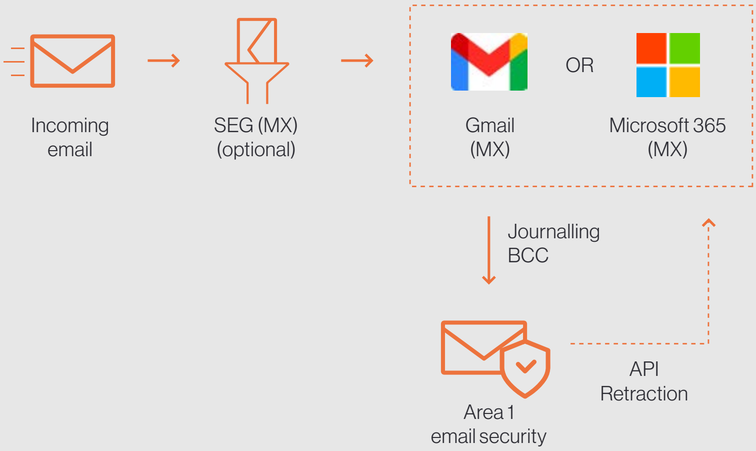
When you deploy GCX Advanced Email Protection Service to protect your organisation, you can choose between two main setup architectures: Inline and API.

Inline deployment: The service evaluates email messages before they reach a user's inbox. More technically, we become a hop in the SMTP processing chain and physically interacts with incoming email messages. Based on your policies, various messages are blocked before reaching the inbox.



CLOUD ARCHITECTURE

API deployment: In this scenario, email messages only reach our service after they have already reached a user's inbox. Then, through integrations with your current email provider, GCX Advanced email protection service can retract messages based on your organisation's policies.



BROWSER ISOLATION FOR EMAIL LINKS

While commodity phishing attacks are blocked by existing security controls, modern attacks and payloads don't have a set pattern that can reliably be matched with a block or quarantine rule. Additionally, with the growth of multi-channel phishing attacks, an effective email security solution needs the ability to detect blended campaigns spanning email and Web delivery, as well as deferred campaigns that are benign at delivery time, but weaponised at click time.

If we assume that human error is here to stay then it makes sense to automate certain responses to certain actions. For example with GCX Secure Web Gateway, users are protected with real time URL analysis and with blocks for known malicious sites and link isolation for any suspicious links.

GCX Email Security Service can enact browser isolation for suspicious email links. Instead of blocking and risking false positives and maintaining endless "white/black lists", it is more effective to load a remote browser to a website on a server on the GCX network and serve draw commands to the user's clientless browser endpoint.

By executing the browser code and controlling user interactions on a remote server rather than a user device, any and all malware and phishing attempts are isolated, and won't infect devices and compromise user identities.

WHY CHOOSE GCX?

GCX provide a flexible range of global services that can be as simple as assisting you to deliver and support your own self-build network through to providing a fully managed outsource service. Our solutions are backed by a team of expert consultants who can assist on every step of your data journey, whether it is design concerns like resilience or security, OEM and carrier selection, deployment, and management we are there all the way with approaches that adhere to best practices and are standards led wherever possible.

Our global presence ensures that we can deliver and support whenever, wherever.