

Cloudflare Email Security

G-Cloud 15



GCloud 15 Service Definition for Cloudflare Email Security

Cloudflare Email Security

Solution Overview

Greater protection & simplicity

Implement layered security that delivers greater protection at a fraction of the cost

As phishing attacks continue to proliferate, Microsoft and Google have continued to build out native functionality that enables essential email and data protection capabilities, such as authentication, archiving, and client-side encryption. However, threat actors have evolved their tactics to execute more targeted and evasive attacks that often bypass native security controls and yield a higher success rate.

By layering on Cloudflare, organizations can automatically block or isolate targeted phishing attacks that leverage malicious links, attachments, and compromised accounts to steal sensitive information and commit financial fraud.

Augment your existing email security controls

Cloudflare's cloud-native email security solution can be deployed in minutes to enhance existing SEG deployments or complement the built-in email capabilities provided by Microsoft and Google. With little to no tuning required, organization's can achieve greater phishing protection with less time and effort dedicated to ongoing security management.

Solution strategy

Complementary

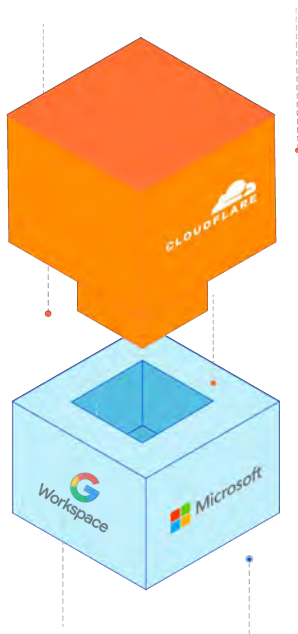
Augments email provider's native capabilities and other existing email security controls

Consolidated

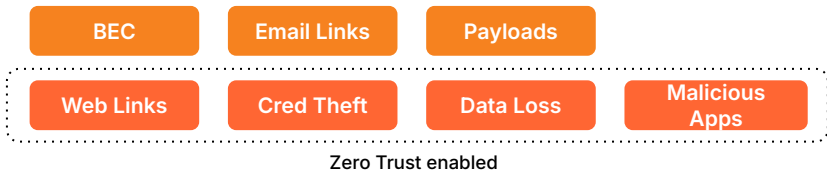
Integrated w/ Zero Trust platform to provide defense-in-depth for multi-channel phishing protection

Continuous

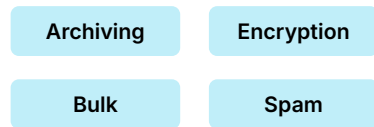
Pre/post-delivery protection that safeguards employees at every stage of a phishing attack



Email Security + Zero Trust



Email Provider



Cloudflare Impact

1

Low-touch, high-efficacy phishing protection

2

Greater consolidation, lower overall cost

3

Fast to deploy, easy to manage

Cloudflare Email Security Solution Overview

Solution strategy

Complementary

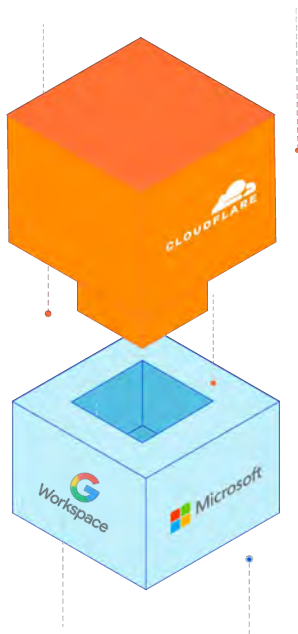
Augments email provider's native capabilities and other existing email security controls

Consolidated

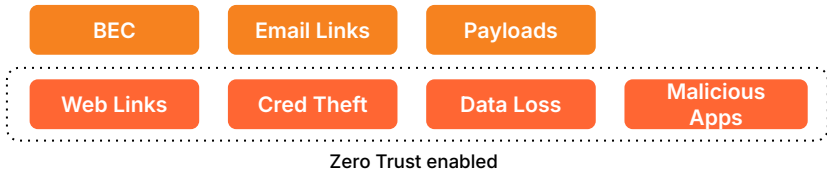
Integrated w/ Zero Trust platform to provide defense-in-depth for multi-channel phishing protection

Continuous

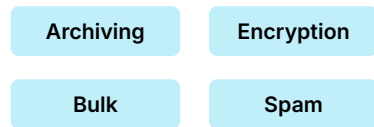
Pre/post-delivery protection that safeguards employees at every stage of a phishing attack



Email Security + Zero Trust



Email Provider



Cloudflare Impact

1

Low-touch, high-efficacy phishing protection

2

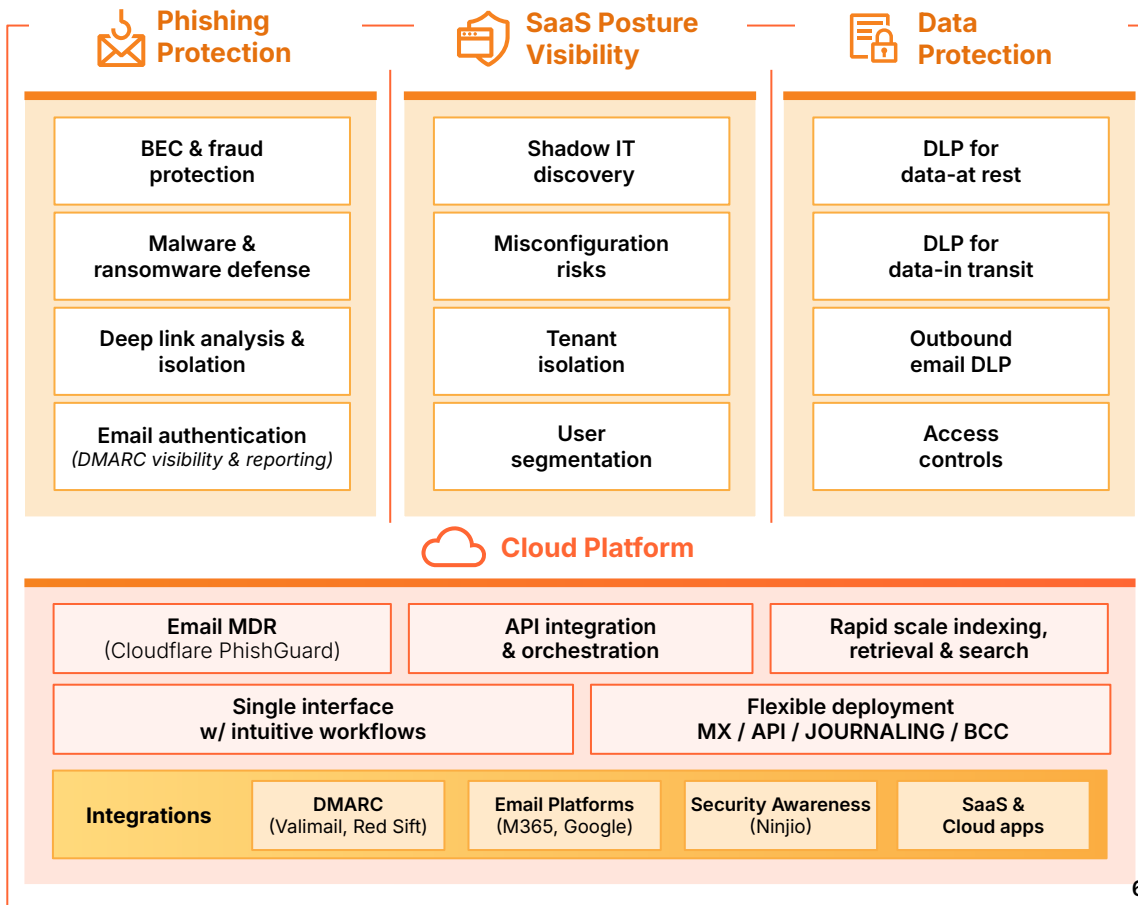
Greater consolidation, lower overall cost

3

Fast to deploy, easy to manage

Email at the center of workspace security

- Stop threats from targeting your people (multi-channel threat defense)
- Prevent data loss (DLP)
- Remediate data & SaaS exposures (CASB)
- Continuous guidance (SAT)

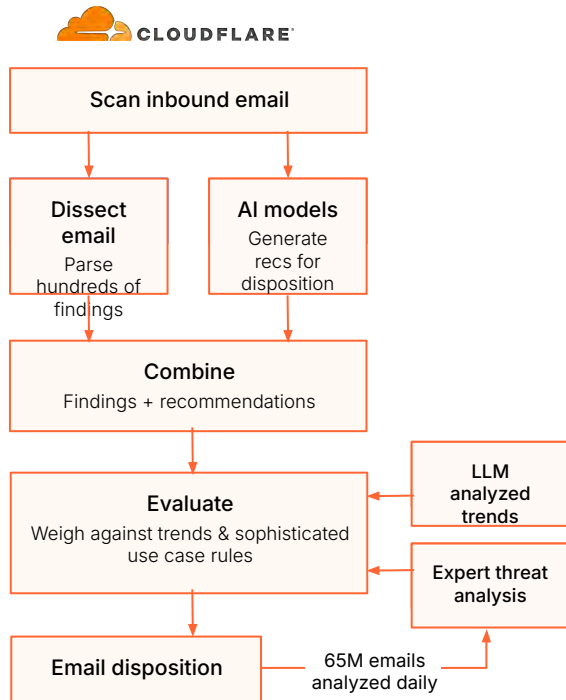
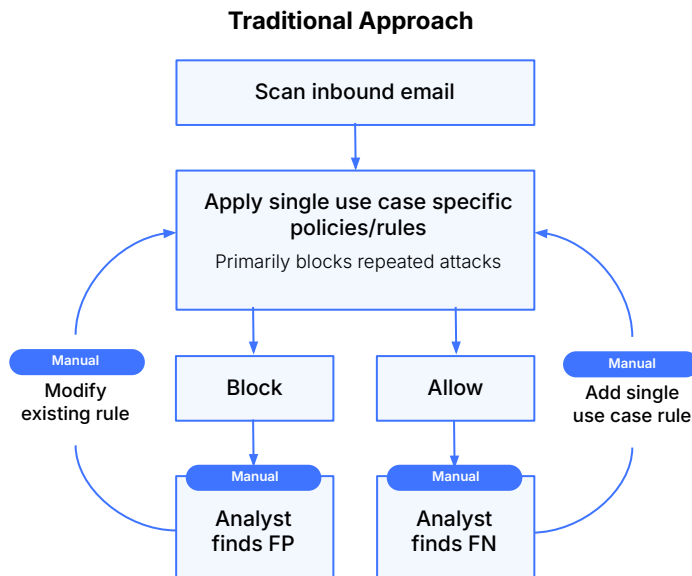


Adaptive, AI-enabled Processing

for greater efficacy & automation

Benefits

1. Improves detection efficacy and outcomes
2. Places burden of detections on Cloudflare, not analysts
3. Significantly reduces time spent tuning & investigating
4. Minimizes disruption & delays to email delivery



Email Security Capabilities Enabled

Capabilities Enabled	Status
Flexible Deployment (BCC Journaling)	✓
Pre-emptive Phishing Detection	✓
Malicious Attachment Detection	✓
Malicious Link Detection	✓
Impersonation & Fraud Defense (BEC Protection)	✓
Analytics & Investigation	✓
Tenant Specific Adaptive Machine-Learning	✓

Unified interface

Cloudflare Dash

Email Security enabled

BEC

Email Links

Payloads

Insider Threats

Web App Links

Data Loss

Credential Theft

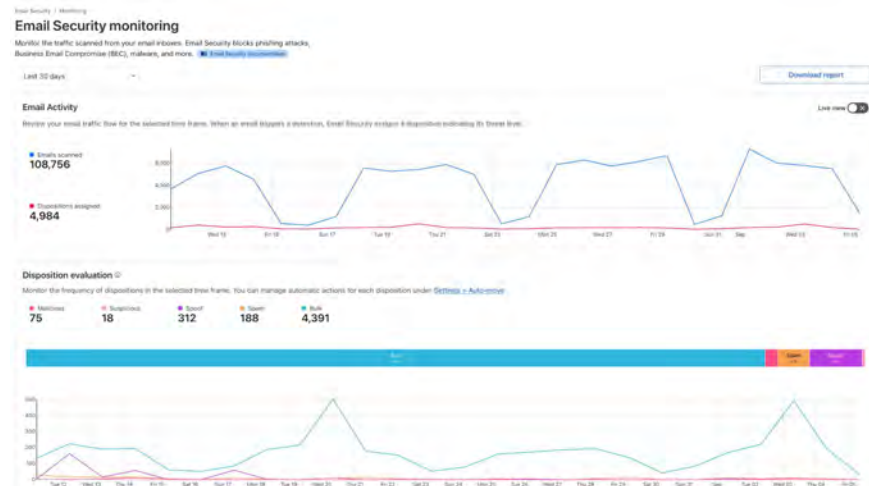
Malicious Apps

Zero Trust enabled

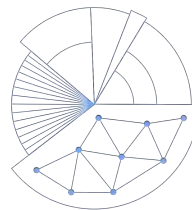
**Fully-Integrated
Protection**

Email Security + Zero Trust

Delivering an integrated, defense-in-depth solution to stop multi-channel phishing



AI-powered message analysis



SPARSE™
(Small Pattern Analytics Engine)™

01



Structural Analysis

Headers
Body, Images,
Computer Vision
Links, Payloads

02



NLU Modeling (Natural Language Understanding)

Writing Patterns
Categories
Expressions

03



Sentiment Analysis

Intent, Tone,
Relationship,
Hierarchy

04



Thread Analysis

Conversations
Variations
Length

05



Industry Modeling

Verticals
Lingua Franca
Business Processes

06



Trust Graphs

Partner Social Graphs,
Sending History,
ATO Discovery
Partner Impersonations

Cloudflare Email Security Unique Value Proposition

Expanded Link Analysis

Open Links in RBI

Customers can open up links found within messages within an RBI session from the UI directly.

On Demand Crawling for Customers

Customers can run our crawler on demand. The outcome of our results will be displayed as a report that can be shared internally with the SOC team or with leadership.

Links identified *Showing 3 of 3 links*

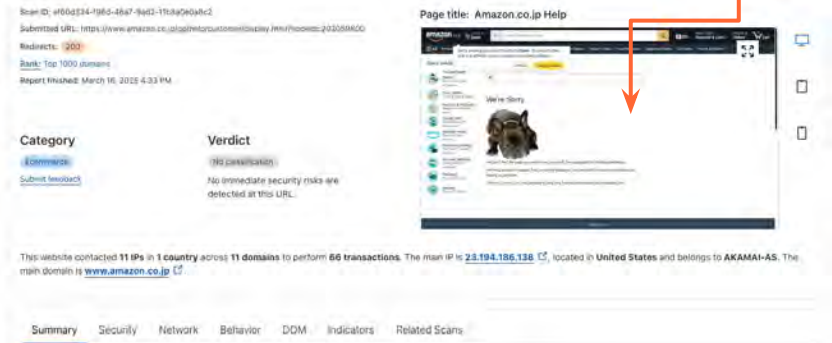
hxxps://www[.]amazon[.]co[.]jp

hxxps://scalloper[.]cn/amalogin

hxxps://www[.]amazon[.]co[.]jp/gp/help/customer/display[.]html?nodeId=202059800



Scan report for 'https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=202059800'



Scan report for 'https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=202059800'

Scan ID: e100d334-19d5-46a7-9a12-11c8a9d9a1c2
Submitted URL: https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=202059800
Redirects: 200
Rank: Top 1000 domains
Report finished: March 16, 2023 4:33 PM

Category
Information

Verdict
No immediate security risks are detected at this URL.

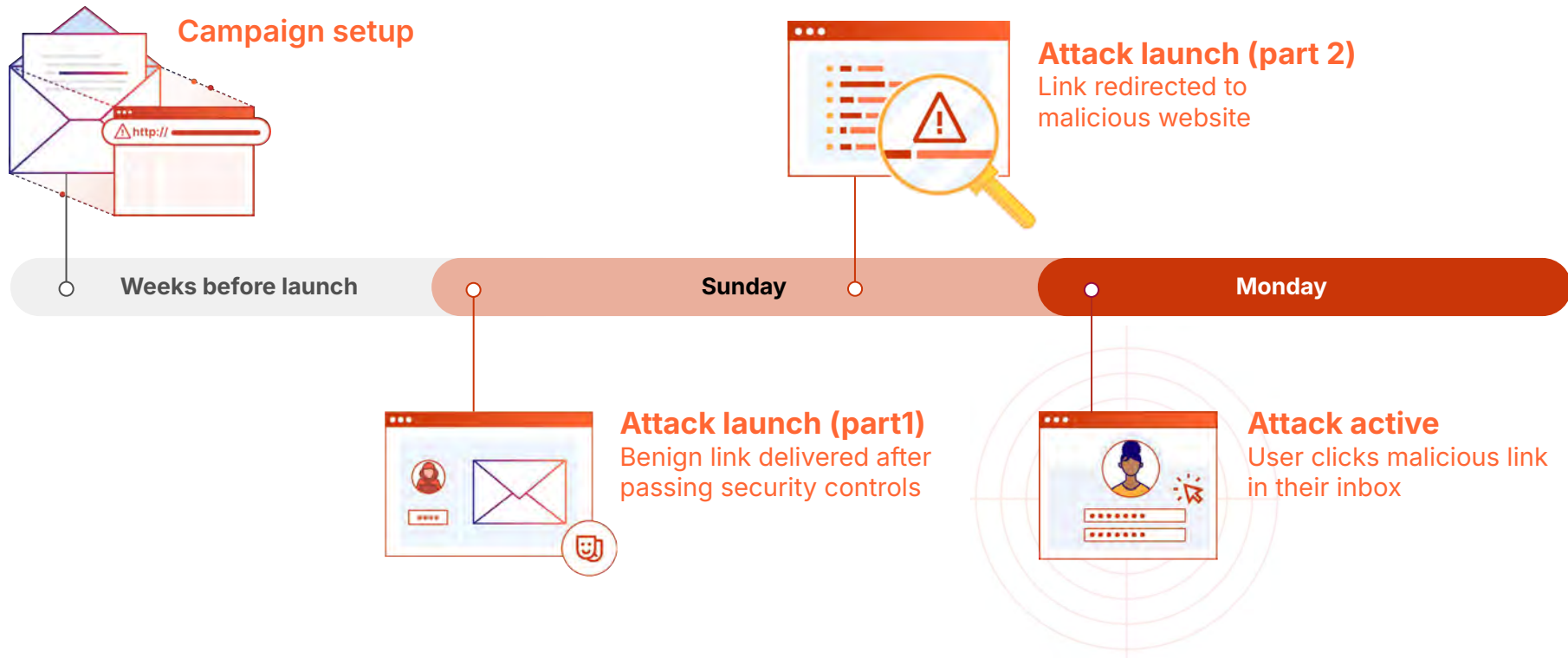
This website contacted 11 IPs in 1 country across 11 domains to perform 66 transactions. The main IP is 23.194.186.138, located in United States and belongs to AKAMAI-AS. The main domain is www.amazon.co.jp.

Summary Security Network Behavior DOM Indicators Related Scans

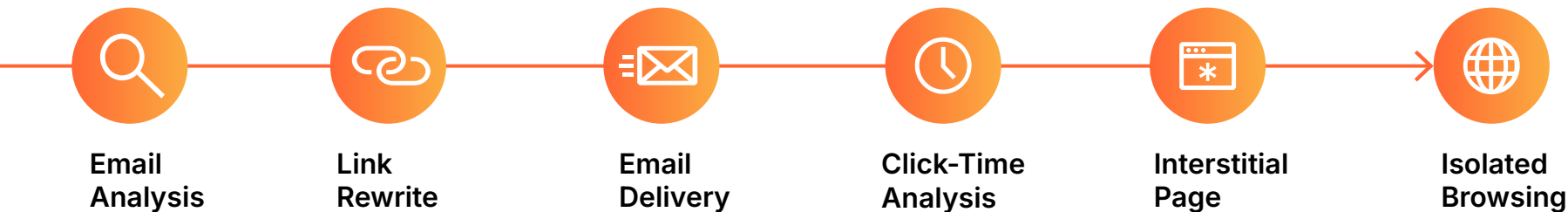
Web page components and interactions
Components that make up and interact with the web page served by (URL).

HTML 5	Stylesheets 4	Scripts 12	Images 24
Links 16	Cookies 25	JavaScript variables 167	Console log messages 69

Deferred attacks (post-delivery)



Only isolating suspicious links



Reduced risk from clicking unknown links.



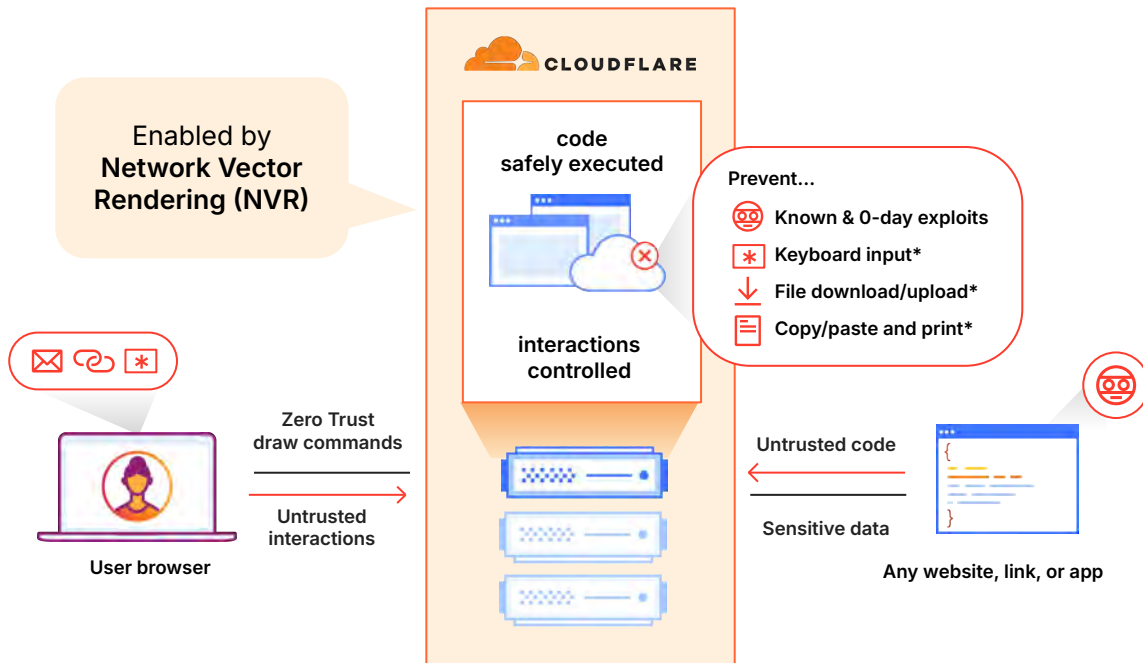
No disruption to users from blocking safe links



Lower cost, fewer investigations into sites

How link isolation works

- **Adaptive link isolation** that insulates users from untrusted web content
- **Secure and scalable** remote browsing via Network Vector Rendering (NVR) technology
- **Low-latency, high resolution** user experience that feels like local browsing
- **Universal browser compatibility** for greater ease-of-use



*Disabling user actions requires SWG + RBI services

Detect & protect sensitive data in O365

(DLP Assist)

Identify sensitive data

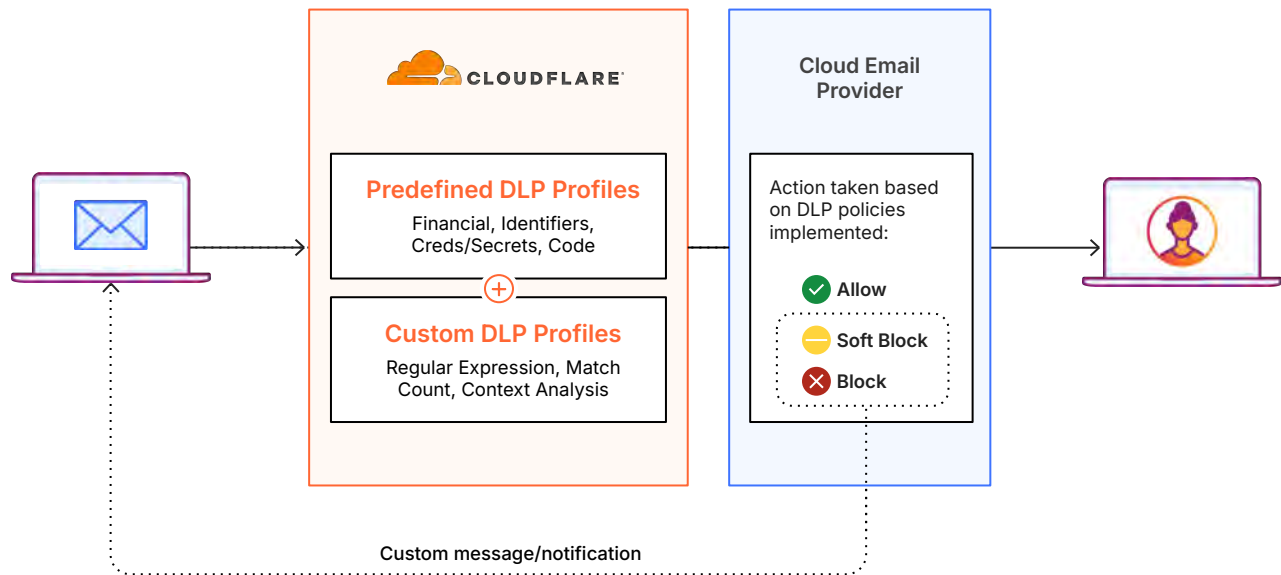
Use predefined and custom profiles to detect sensitive data in outgoing emails

Reduce risk of data loss

Block emails containing sensitive information from being sent externally

Simplify data compliance

Easily comply with regulatory requirements for sensitive information

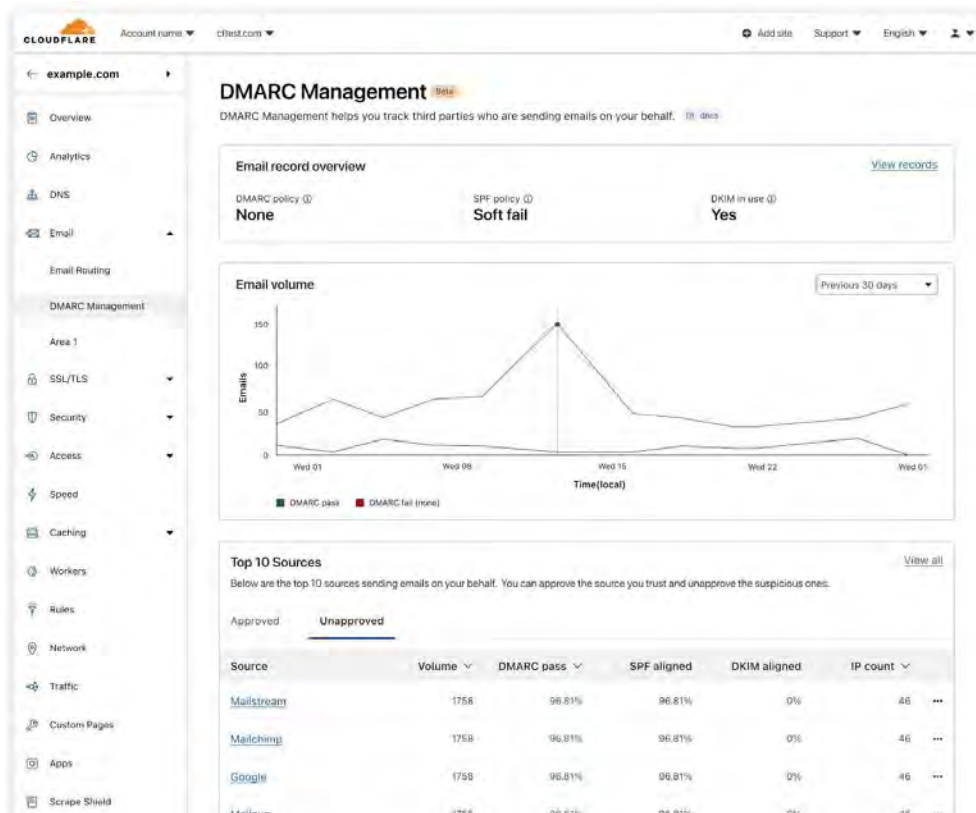


DMARC Management

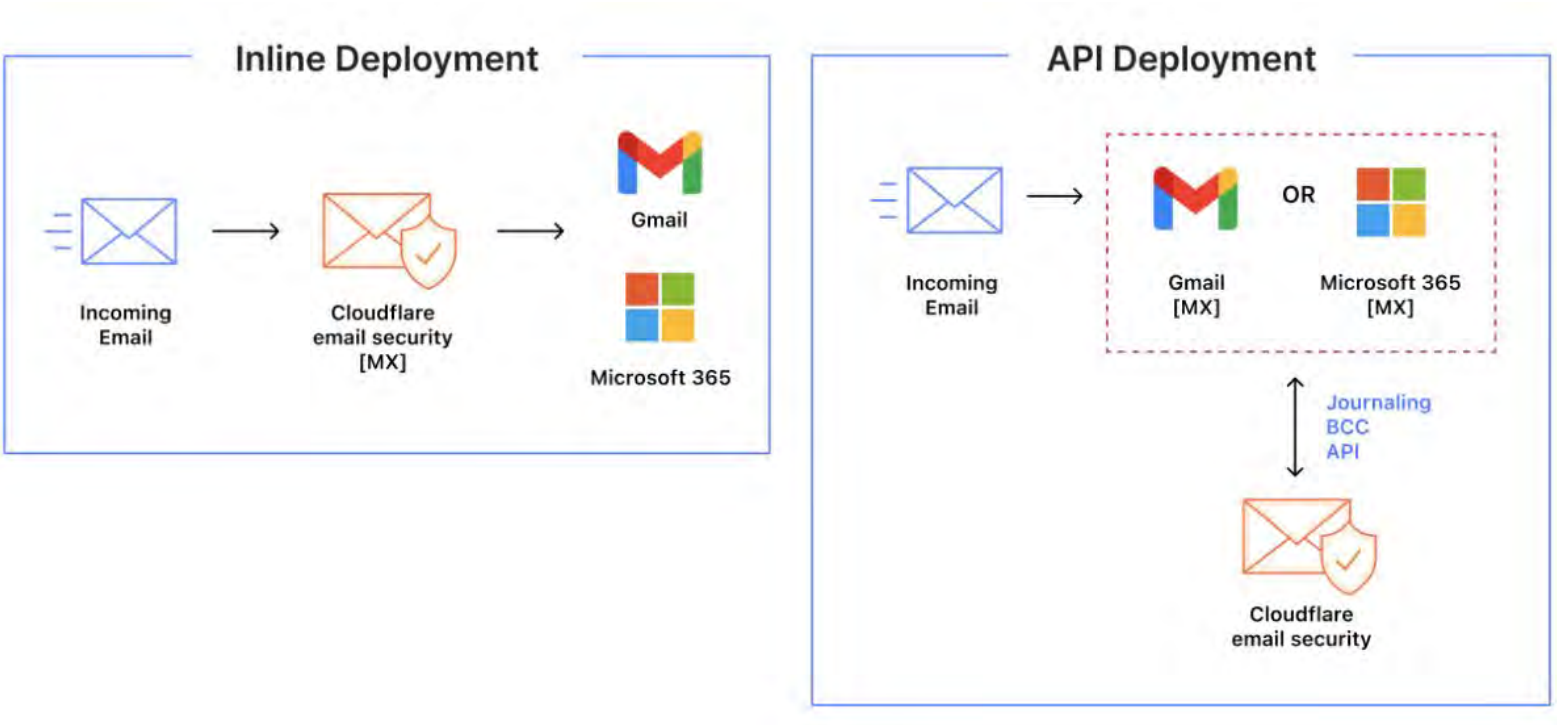
Cloudflare DMARC Management

DMARC Management (beta) is available to all Cloudflare customers with Cloudflare DNS.

<https://blog.cloudflare.com/dmarc-management/>



Deployment Options



Inline vs. API Comparison

Inline		API	
Benefits	Disadvantages	Benefits	Disadvantages
• Messages are processed and physically blocked before delivery to the users mailbox • Simplest deployment method, any complex processing occurs downstream and does not require any modifications in process • Can modify the message, adding subject or body mark-ups • Provides High Availability and Adaptive Message pooling • Dispositioned messages that are not quarantined receive an X header that may be used for advanced handling downstream	• If MX, requires DNS change. If many domains, many DNS zones to update • Can increase complexity in the SMTP architecture if not deployed as MX • May require policy duplication on multiple solutions and the MTA	• Easy way to add protection in complex email architectures with no changes to mailflow operations • Agentless deployment for M365 and Gmail • M365 Defender/ATP and Google security operates on the message first	• Dependent on MSFT or GOOG API infrastructure. Outages will increase message dwell time in the inbox • Microsoft may throttle all API requests to the M365 organization • Requires read/write access into mailboxes. Some security/email teams may not want this • Only M365 and Gmail have API support. On-prem architectures typically do not have APIs for retractions. Exchange requires PowerShell.

Ensuring your success



[Community](#)



[Docs](#)



[Resource Hub](#)



[Help Center](#)



[Discord](#)



[Blog](#)



[theNET](#)



[Cloudflare Radar](#)



[CloudflareTV](#)



[YouTube](#)

Thank you

Matt Johnson
Head of Public Sector

CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH
Email: bidteam@cds.co.uk

Telephone: 07939 866831

Website: www.cds.co.uk