CLOUDFLARE

SOLUTION BRIEF

Safeguard your workforce from multi-channel phishing

Layered protection that extends beyond the inbox

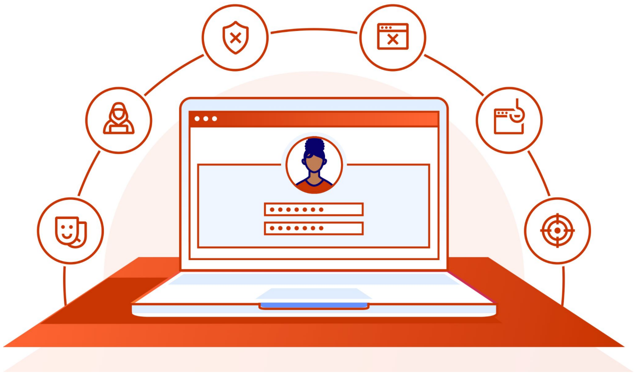
OVERVIEW

Phishing attacks are no longer limited to just email

While email continues to be the most prevalent and effective delivery mechanism for phishing campaigns, attackers are increasingly using clever tactics that target and exploit users across multiple channels (i.e. applications) used for daily communication and collaboration. These attacks often employ cleverly obfuscated links to deceive users and pivot their target to malicious content and insecure environments.

More channels = more ways to exploit employees

Targeting employees with deceptive links within email and other collaboration apps allows attackers to circumvent traditional detection methods while engaging users in a way that increases the perception of authenticity. This raises the risk of an employee clicking on malicious web content, divulging credentials, or leaking sensitive information. Email security can only help when an attack originates via inboxes, but a broader security solution is required to block these attacks when they spread to other apps.



CHALLENGES

Multi-channel threats can bypass traditional email filtering

Multi-channel attacks leverage complex link obfuscation and various collaboration apps to bait users into clicking malicious content or leaking sensitive information. This type of attack can be difficult to address due to:

- **Link obfuscation** (URL redirects/shorteners)
- **Image-based URLs** (QR codes)
- **Deferred attacks** (activated post-delivery)
- **Distributed engagement** across work apps

89%

of security decision-makers are concerned about multi-channel threats[1]

#1

Malicious links are the top phishing threat based on detection volume [2]

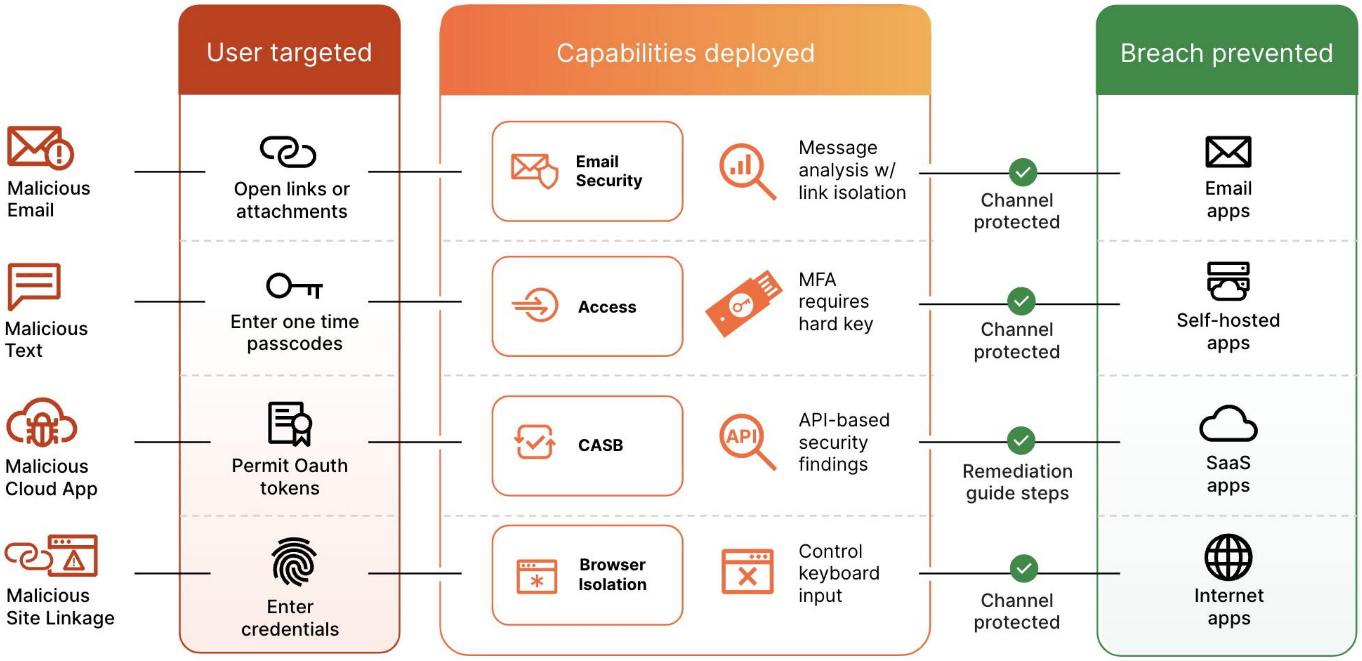
81%

of organizations have experienced a multi-channel attack in the past 12 months[1]

SOLUTION

Unified security at every point of phishing exposure

Stopping multi-channel attacks requires a platform that can address the full scope of vulnerabilities that exist in employee workflows and in-app interactions. That's why Cloudflare offers the most complete phishing solution focused on delivering seamless protection across employees and applications. Leveraging the Cloudflare One platform, organizations can take advantage of natively-integrated email security (ES) + Zero Trust services to deploy layered protection for email, self-hosted apps, SaaS apps, and Internet apps — providing defense-in-depth to stop fraudulent payments and data breaches.



	User targeted	Capabilities deployed			Breach prevented
Malicious Email	Open links or attachments	Email Security	Message analysis w/ link isolation	✓ Channel protected	Email apps
Malicious Text	Enter one time passcodes	Access	MFA requires hard key	✓ Channel protected	Self-hosted apps
Malicious Cloud App	Permit Oauth tokens	CASB	API-based security findings	✓ Remediation guide steps	SaaS apps
Malicious Site Linkage	Enter credentials	Browser Isolation	Control keyboard input	✓ Channel protected	Internet apps

Preemptively stop email-borne threats

Detect business email compromise (BEC), malware, and other email-originating threats with AI/ML-powered content analysis for automated protection.

Prevent breaches that result from credential theft

Stop breaches with conditional access + hard key requirements that act as a last-line-of-defense in case credentials are stolen or compromised.

Block and isolate evasive link-based attacks

Insulate users from targeted attacks that bait employees through commonly used messaging apps via cleverly obfuscated links that are difficult to catch.

Stop email-borne threats (ES)

With email representing the most used and most exploited business application, it's more critical than ever to shield users from phishing attacks that seek to manipulate their trust through email. By augmenting or replacing current email defenses with Cloudflare, organizations can automatically mitigate sophisticated phishing attacks that leverage embedded email links, attachments, and impersonated or compromised accounts to steal sensitive information and commit financial fraud.

Cloudflare's lightweight, cloud-native solution can be deployed in minutes to complement the built-in email capabilities provided by Microsoft and Google. With greater automation and minimal tuning needed for optimal results, Cloudflare significantly reduces the time and effort required for ongoing management.

Business Email Compromise (BEC)
AI/ML-powered content analysis deconstructs every message to evaluate conversation history, writing patterns, sentiment, and other variables to determine the authenticity of the sender.

Ransomware & malicious attachments
ML detection models on payloads, signatureless detection, computer vision, remote extraction, and other forms of analysis are used to identify encrypted and unencrypted malicious payloads.

Malicious email links
Advanced techniques for deconstructing and drilling-down into complex URLs are combined with adaptive link isolation to ensure a safe, frictionless web experience for employees.

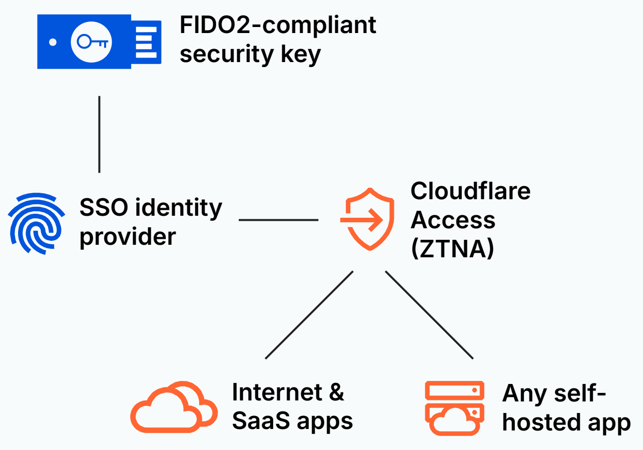
Mitigate OAuth phishing attacks (CASB)

OAuth phishing takes advantage of legitimate identity providers and authorization workflows to bait users into granting permissions to malicious apps. The Cloudflare One platform delivers the ability to detect such apps while providing remediation guidance to quickly mitigate these threats.

Prevent breaches from compromised credentials (ZTNA)

While many organizations implement extensive preventative measures to avoid employee credentials from landing in the wrong hands, the painful truth is that preventative measures are never 100% foolproof. In the unfortunate case that credentials are stolen or unknowingly leaked, there must be a last-line-of-defense to prevent an all out breach.

With Cloudflare Access acting as an aggregation layer around every resource, including self-hosted or non-web resources, organizations can consistently enforce FIDO2-compliant authentication for phishing-resistant MFA. So even in the event that employee credentials are compromised, organizations are still able to ensure that their data is protected.



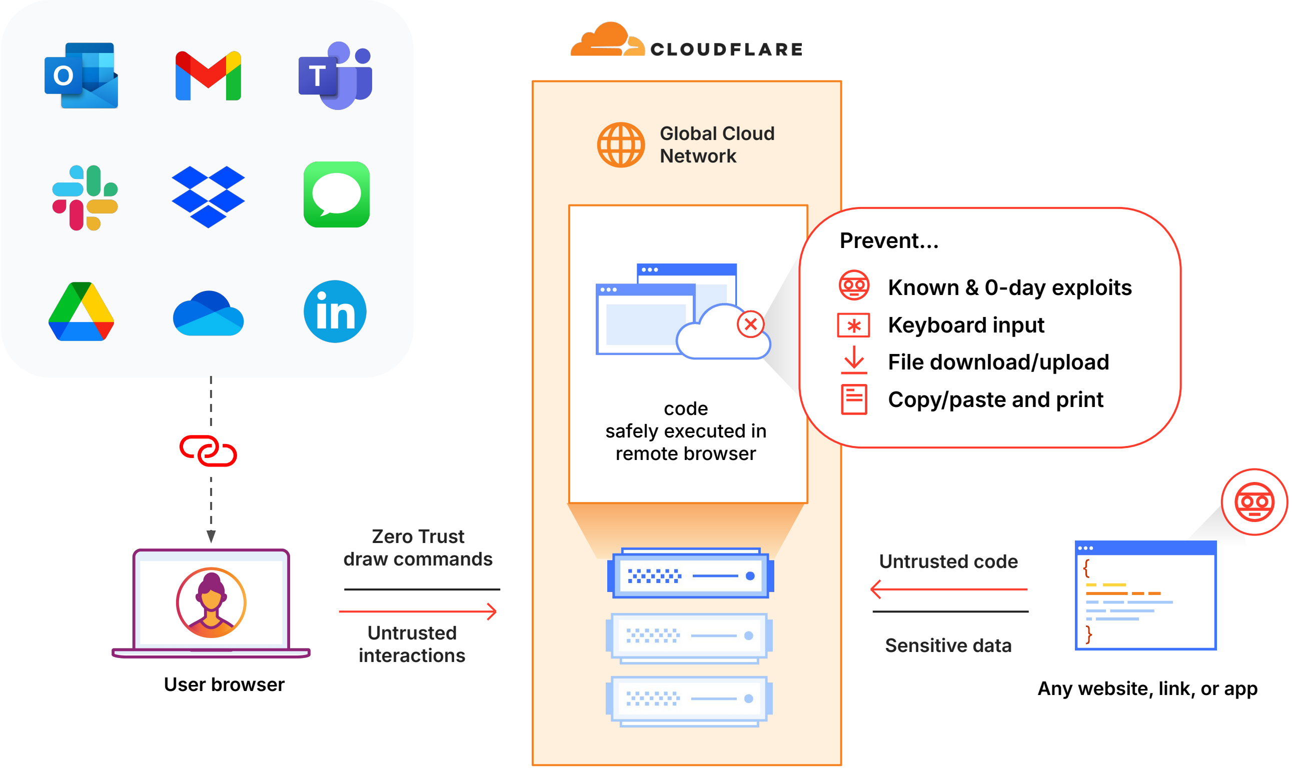
Isolate link-based attacks (ES + RBI + SWG)

Link-based attacks have become the go-to method for stealing credentials, loading malware/ransomware, and extracting sensitive information. Using a combination of email, chat, SMS, social, and cloud drives to deliver these links further complicates the process of ensuring that both employees and data are protected from targeted phishing attacks.

Cloudflare Browser Isolation solves for link-based phishing attacks by rendering all web code remotely on our global cloud network instead of on the user's local device. This mitigates malware and browser zero days, while also providing granular control over user actions (e.g. disable keyboard input) to prevent credential harvesting and data leaks.

Eliminate phishing risk without slowing down your workforce

By integrating next-generation browser isolation capabilities built on our unique Network Vector Rendering (NVR) technology, Cloudflare is able to deliver a seamless, secure, and scalable solution for isolating potentially malicious links. Unlike bandwidth-heavy techniques, NVR streams safe draw commands to the device. This helps eliminate the risk of malicious web content without impacting the end-user experience. Thanks to NVR and Cloudflare's low-latency network, organizations can isolate multi-channel threats while ensuring disruption-free productivity for their employees.



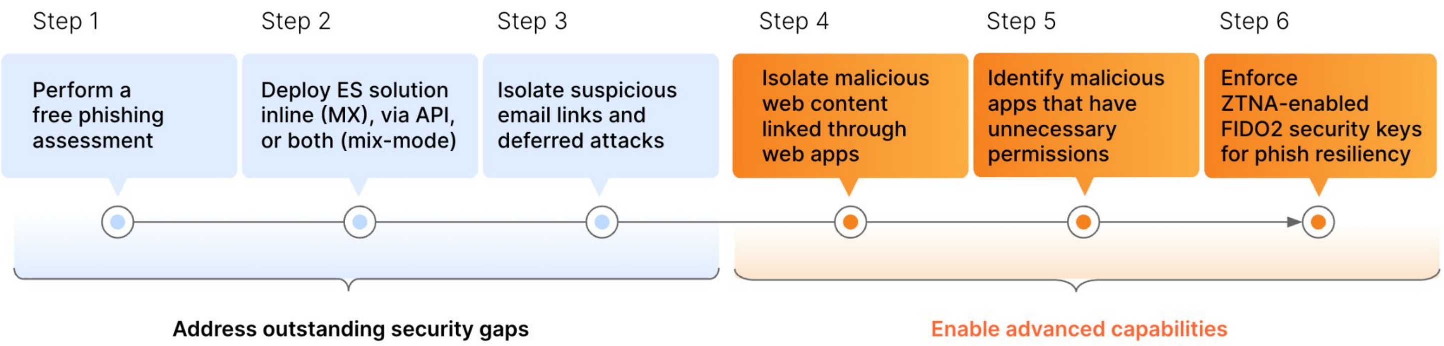
BENEFITS

Complete multi-channel protection

As phishing campaigns rapidly expand beyond email, it's now more urgent than ever for organizations to implement a phishing solution that provides a quick and simple path to full multi-channel protection.

Using the Cloudflare One platform, organizations can first deploy industry-leading email security to quickly address the most critical phishing channel; then easily enable additional Zero Trust services to extend protection to all channels — effectively stopping known and emerging phishing threats.

- **Low-touch, high efficacy protection:** Minimize phishing risk with industry-leading detection efficacy that requires minimal tuning.
- **Greater consolidation, lower cost:** Reduce spend with a single, fully-integrated platform that solves for all phishing use cases.
- **Fast to deploy, easy to manage:** Ensure immediate protection while reducing the time and effort needed for ongoing management.



Step 1
Perform a free phishing assessment

Step 2
Deploy ES solution inline (MX), via API, or both (mix-mode)

Step 3
Isolate suspicious email links and deferred attacks

Step 4
Isolate malicious web content linked through web apps

Step 5
Identify malicious apps that have unnecessary permissions

Step 6
Enforce ZTNA-enabled FIDO2 security keys for phish resiliency

Address outstanding security gaps

Enable advanced capabilities

Evaluate and compare

Assess your current email defenses and see which threats are being missed

Run a free retro scan (O365 inboxes) in minutes to see which phishing threats were delivered in the past 14 days or request a phishing risk assessment (PRA) to monitor any inboxes for phish as they're delivered. Evaluate against other providers with zero out-of-the-box tuning to see which email security solution offers the fastest and easiest protection.

See which phishing threats are getting through your defenses

Run a retro scan | Request a PRA

CLOUDFLARE

1. 2023 Forrester Opportunity Snapshot: Source
2. 2023 Phishing Threats Report Source