Cloud Email Security (CES)

Cloudflare, an analyst-recognized email security leader, preemptively detects and stops phishing threats

Protect against targeted phishing attacks

Effortlessly block or isolate threats that other solutions miss

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. As organizations continue to increasingly adopt cloud email services through Microsoft 365 and Google Workspace to better support hybrid workers, threat actors have pivoted to more targeted, low-volume attacks that are able to evade traditional Secure Email Gateways (SEGs) like Proofpoint and Mimecast.

That's why Cloudflare's cloud-native email security solution (called Area 1) was uniquely designed to leverage preemptive campaign intelligence, ML-based content analysis, and a unified Zero Trust platform to stop phishing threats before they reach your workforce.

91%

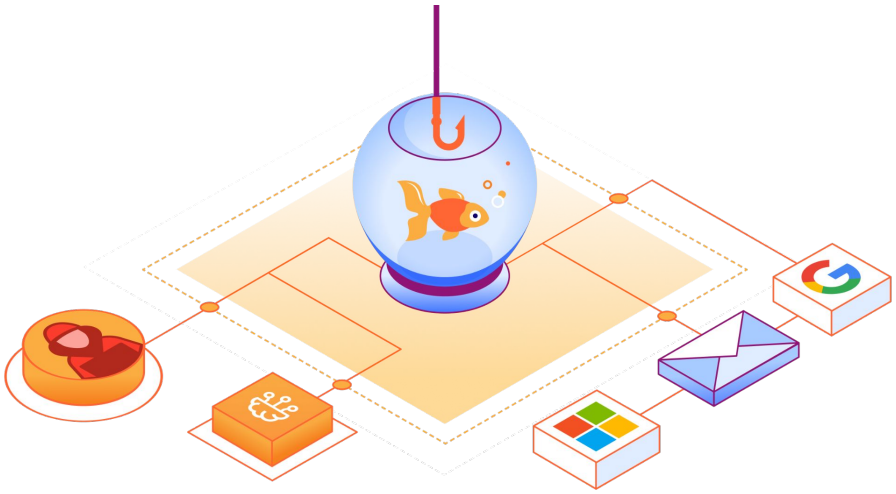
of all cyber attacks begin with a phishing email[1]

50B

in losses from BEC attacks over the last decade[2]

81%

of orgs experienced a multi-channel attack in the past 12 months[3]



Stop business email compromise (BEC)

Detect impersonated and compromised accounts with layered, ML-powered contextual analysis.

Isolate deferred and multi-channel attacks

Insulate users from malicious web content that's delivered via unknown or deceptive links.

Block ransomware and malicious attachments

Prevent extortion attempts and malicious code from compromising your organization.

Greater protection & simplicity

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

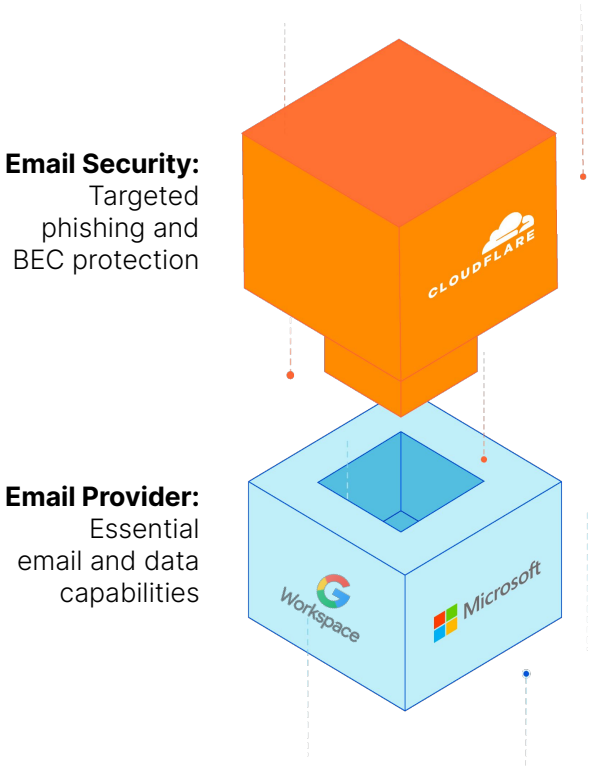
As phishing attacks continue to proliferate, Microsoft and Google have continued to build out native functionality that enables essential email and data protection capabilities, such as authentication, archiving, data loss prevention (DLP), and client-side encryption. However, threat actors have evolved 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 inbound 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 solution management.

> "Since we implemented Cloudflare [on top of M365], we have seen a 50% reduction in the number of malicious or suspicious emails our users receive every day. That frees up multiple hours we can reinvest into other goals."
>
> **Werner Enterprises**
> (Fortune 1000)



Reinvest hours saved from increased automation

Cloudflare's automated, lightweight solution offers seamless integration with Microsoft and Google workflows while providing a single, intuitive UI for analyst activities.

Achieve 99.997% detection efficacy

Combining email provider's native capabilities with Cloudflare's phishing and BEC protection ensures businesses have comprehensive coverage for minimal risk.

Realize greater value at a lower cost

Replacing outdated, expensive, and complex deployments with Cloudflare's low-touch solution can reduce operational overhead, redundant features, and excessive tuning.

Stop sophisticated BEC attacks

$50 billion in reported losses and growing

With BEC attacks responsible for a staggering amount of losses over the last decade, it's surprising that some organizations have still not prioritized addressing such an effective form of financial fraud. While BEC attacks represent a much smaller percentage of phishing threats, they often go undetected by SEGs and cloud email providers, resulting in greater financial loss. These targeted attacks are difficult to catch because they take advantage of impersonated or compromised accounts and conversational context to masquerade as an employee or trusted vendor.

Extending Zero Trust principles to email

When leveraging a compromised employee or vendor email account, attackers can evade traditional security controls that only attempt to confirm the legitimacy of the sender account. Cloudflare goes one step further by analyzing a wide-array of behavioral attributes, writing patterns, sentiment indicators, and conversation history to determine the authenticity of the sender. Cloudflare's ML-powered threat models and extensive network intelligence provides the most effective weapon against compromised accounts that are used to extract fraudulent payments.

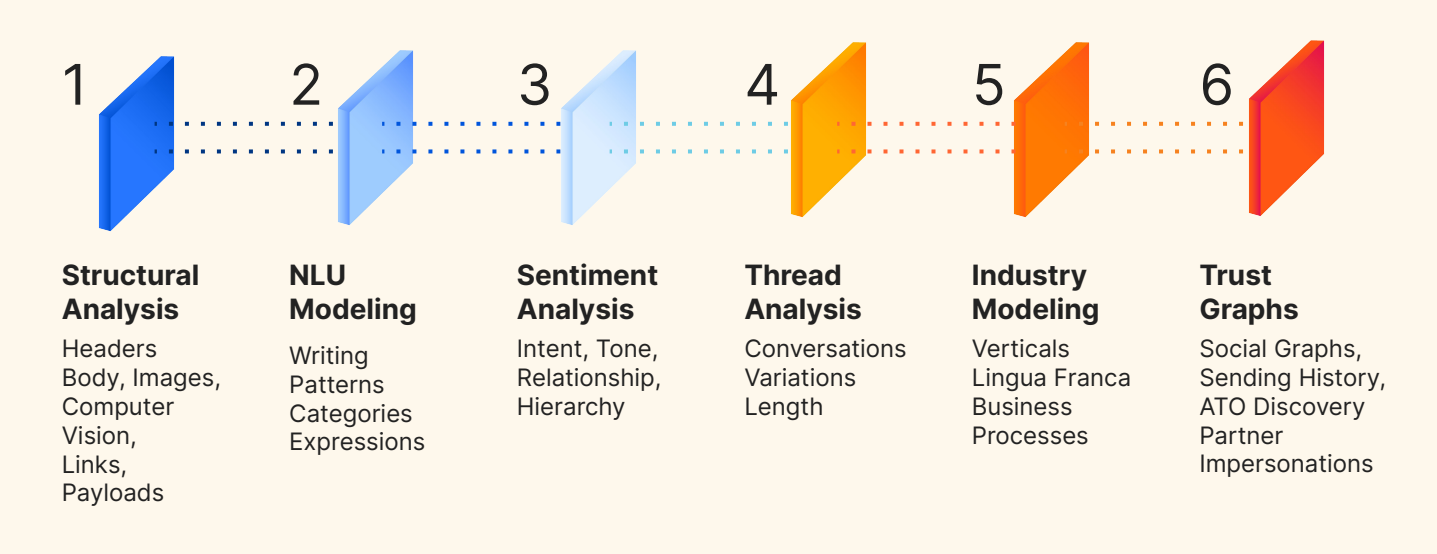


Figure 1: Message analysis

Detecting BEC with ML-based contextual analysis

Accurate identification of BEC attacks requires more than just structural analysis of a message. Successful detection also involves a granular understanding of the variations within conversational style and intent. Cloudflare's expansive network telemetry (1T+ DNS requests daily) and evolving ML models power the small-pattern analytics engine that deconstructs every aspect of an email message to evaluate writing patterns, sentiment, historical context, and a wide range of other variables that help uncover the authenticity of the sender.

Isolate dangerous & deceptive URLs

Protect users from untrusted email links

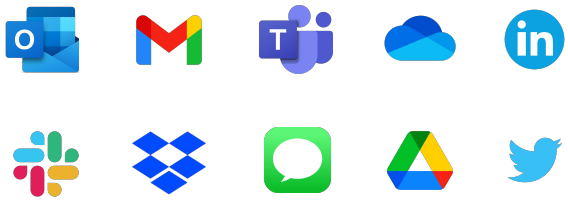
As modern phishing attacks become more deceptive, even the best trained security solutions struggle to accurately identify malicious links 100% of the time. Link shorteners increase this problem by enabling deferred attacks, where malicious links are activated post-delivery. This leads to an increase in:

- **Risk** from clicking unknown links.
- **Disruption** from potentially blocking safe links.
- **Cost** from investigating untrusted links.

With adaptive isolation, Cloudflare enables users to safely access untrusted links by neutralizing malware and other malicious web content; removing the burden of time-consuming investigations and policy updates.

Prevent multi-channel phishing attacks

While email is still the primary delivery mechanism for malicious links, attackers have expanded their tactics beyond just email, engaging users across various applications used for daily collaboration. By extending protection beyond email with Cloudflare's Zero Trust platform, organizations can proactively insulate users from malicious web content that comes through:



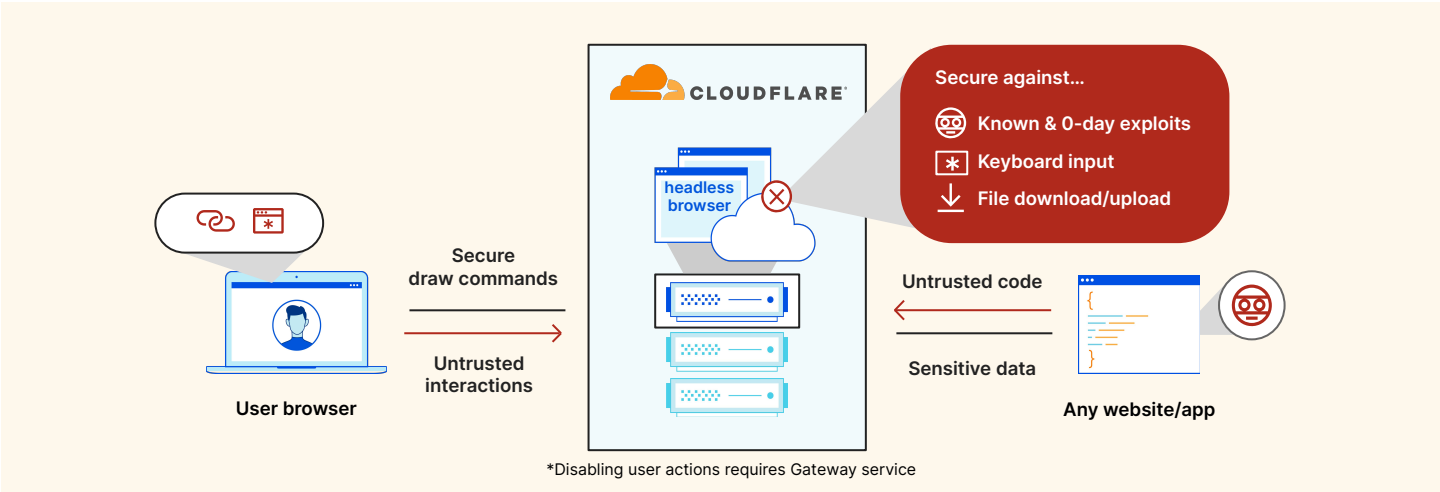


Figure 2: Isolated session

Reinventing remote browser isolation security

Cloudflare Browser Isolation uses proprietary Network Vector Rendering (NVR) technology that delivers a seamless, secure, and scalable solution for isolating untrusted links and web content. NVR streams safe, lightweight draw commands to the device, with isolated browser sessions able to run on any server, within any data center located across the 300+ cities covered by Cloudflare's network. This helps eliminate the risk of untrusted code running on the end-user device while providing a transparent, low-latency experience that's invisible to users.

Rapid investigation & response

Intuitive, low-touch solution management

With greater automation and minimal configuration needed for optimal results, Cloudflare significantly reduces the time and effort required for ongoing email security management. Security teams can immediately gain a complete view of all top-line metrics and trends within the dashboard, with the ability to click into more granular detail around flagged messages. Drilling into trends enables quick discovery of frequent attack types, which executives are being targeted, deferred attacks mitigated, and other critical data points.

All analytics, telemetry, threat observables, and indicators of compromise (IOCs) are available through an extensive API for easy integration into existing analyst workflows and orchestration tools.

> "I often tell coworkers how Cloudflare is both simple and easy to use as a cloud-based SaaS solution and discuss how satisfied I am with its high level of accuracy."
>
> **Japan Airlines**

Managed phishing detection and response

Cloudflare's managed email security service, PhishGuard, supplements your existing SOC team to free up security investigation cycles and provide valuable threat intelligence. PhishGuard can help neutralize phishing campaigns by assisting with investigations, insider threat assessments, active fraud takedowns, and complex remediation needs. PhishGuard extends security resources and expertise to actively notify on potential fraud and insider threats, while also performing email-based threat hunting.

PhishGuard features and benefits:

- Managed phish submissions and incident response for faster resolution.
- Proactive BEC and fraud notifications so organizations can quickly respond early in the attack lifecycle.
- Dedicated resources for real-time monitoring, periodic account reviews, and ongoing threat assessments.
- Custom blocking signatures based on a threat analysis of the managed environment.

1100+

Hours saved annually from automating manual triage efforts

Cloudflare's automated solution removes manual, time-consuming tasks to improve response times and unlock additional cycles.

50%

Reduction in malicious or suspicious emails delivered (on top of M365)

Layering Cloudflare on top of Microsoft 365 enables organizations catch targeted attacks and reduce the overall number of malicious emails.

40

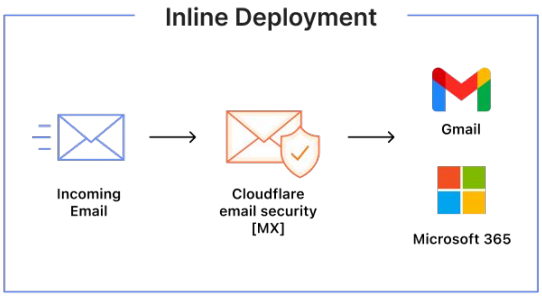
Total hours spent over seven years on email security configuration

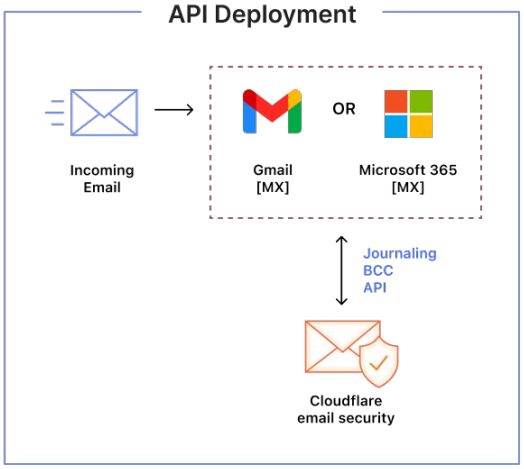
Cloudflare's low-touch email security requires little upfront configuration and ongoing tuning, providing high detection efficacy out of the box.

Flexible, easy-to-deploy protection

Inline, API, and multi-mode options for fast, simple deployment without the added risk

Organization's can choose the approach that's best for their environment and deploy in minutes without any hardware, agents, or appliances. Unlike SEG or API-only vendors, Cloudflare provides flexible options that enable both pre- and post-delivery protection for continuous threat remediation while offering seamless integration with existing SOC workflows and SIEM/SOAR platforms.





FORRESTER Leader in the Forrester Wave™ for **Enterprise Email Security**, Q2 2023

Evaluate and compare

Start a phishing risk assessment (PRA) and see what attacks are being missed

Quickly assess your email environment and determine which phishing threats are slipping through your current defenses. Evaluate against other providers with zero out-of-the-box tuning to see which email security solution offers the fastest and easiest protection.

Experience market-leading phishing protection today

Request a PRA

1. 2020 Deloitte research: Source
2. 2023 FBI IC3 PSA: Source
3. 2023 Forrester Opportunity Snapshot: Source