CLOUDFLARE

PRODUCT OVERVIEW

Email Security

Strengthen your workspace resilience with AI-powered phishing protection and integrated SASE controls.

Protect against targeted phishing attacks

Effortlessly block and isolate threats that other solutions miss

With email being the most used and most exploited business application, it's more critical than ever to shield users from phishing threats that seek to manipulate their trust. As organizations shift to Microsoft O365 and Google Workspace to support hybrid work, attackers are pivoting to contextually-aware and targeted techniques. These deceptive attacks often bypass traditional Secure Email Gateways (SEGs) that are hampered by outdated, complex architectures.

That's why Cloudflare's cloud-native email security solution was uniquely designed to leverage preemptive campaign intelligence, AI-driven content analysis, and a unified SASE platform to stop phishing threats before they reach your workforce.

$50B

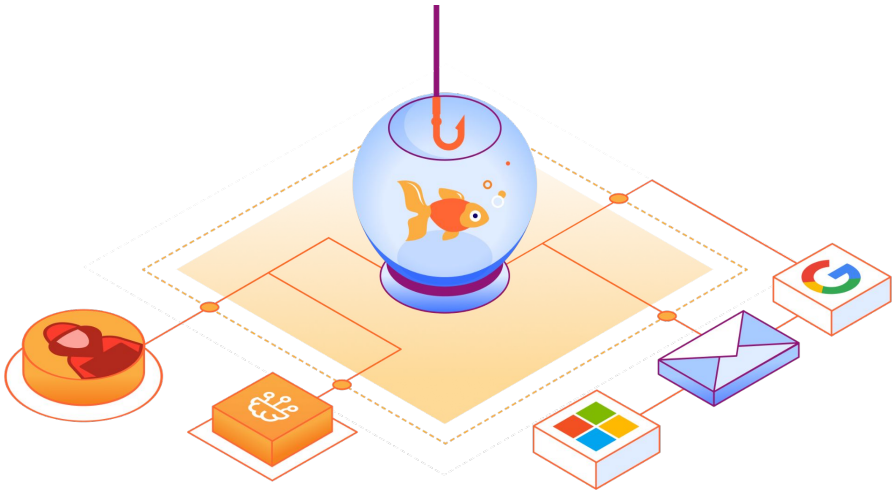
in losses from BEC attacks over the last decade[1]

62%

more malicious emails caught than Microsoft O365[2]

74%

more malicious emails caught than Google Workspace[2]



Stop business email compromise (BEC)

Detect impersonated and compromised accounts with layered, AI-enabled contextual analysis.

Isolate suspicious links and deferred attacks

Insulate users from malicious web content that's delivered through unknown and obfuscated 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, 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.

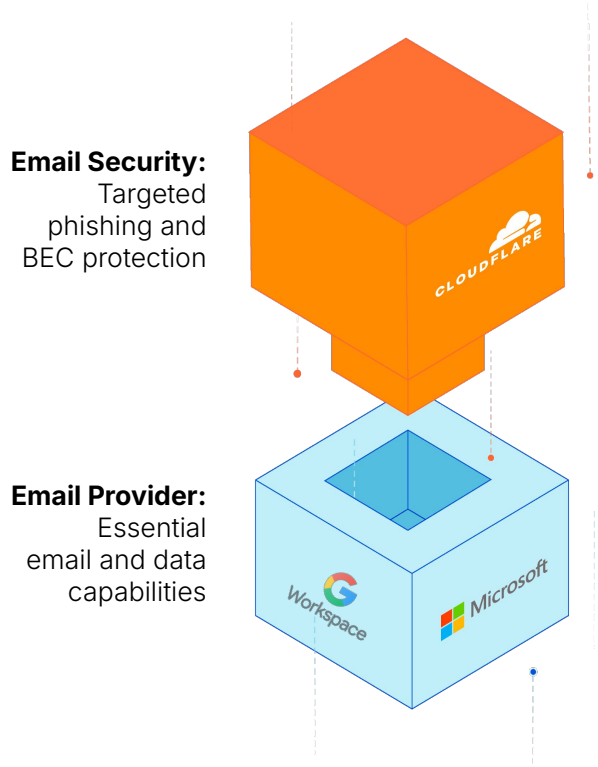
By layering on Cloudflare Email Security, organizations can automatically block or isolate targeted phishing attacks that leverage malicious links, malware, and compromised accounts in an attempt to steal sensitive information, gain access, or commit financial fraud.

Deploy inline, via API, or a combination of both

Cloudflare's cloud-native email security solution can be deployed in minutes to complement the built-in email capabilities provided by Microsoft and Google, or enhance existing SEG implementations. With little configuration and no tuning, organizations can achieve both pre- and post-delivery protection that requires less time and effort for solution management.

EQS GROUP
Regulatory technology

10 mins
to deploy, with several malicious emails caught in the first hour that other solutions missed



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.

Catch more malicious emails than Microsoft O365 & Gmail

Combining email provider's native capabilities with Cloudflare's phishing and BEC protection ensures businesses are fully protected against all forms of phishing.

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.

AI-powered detections

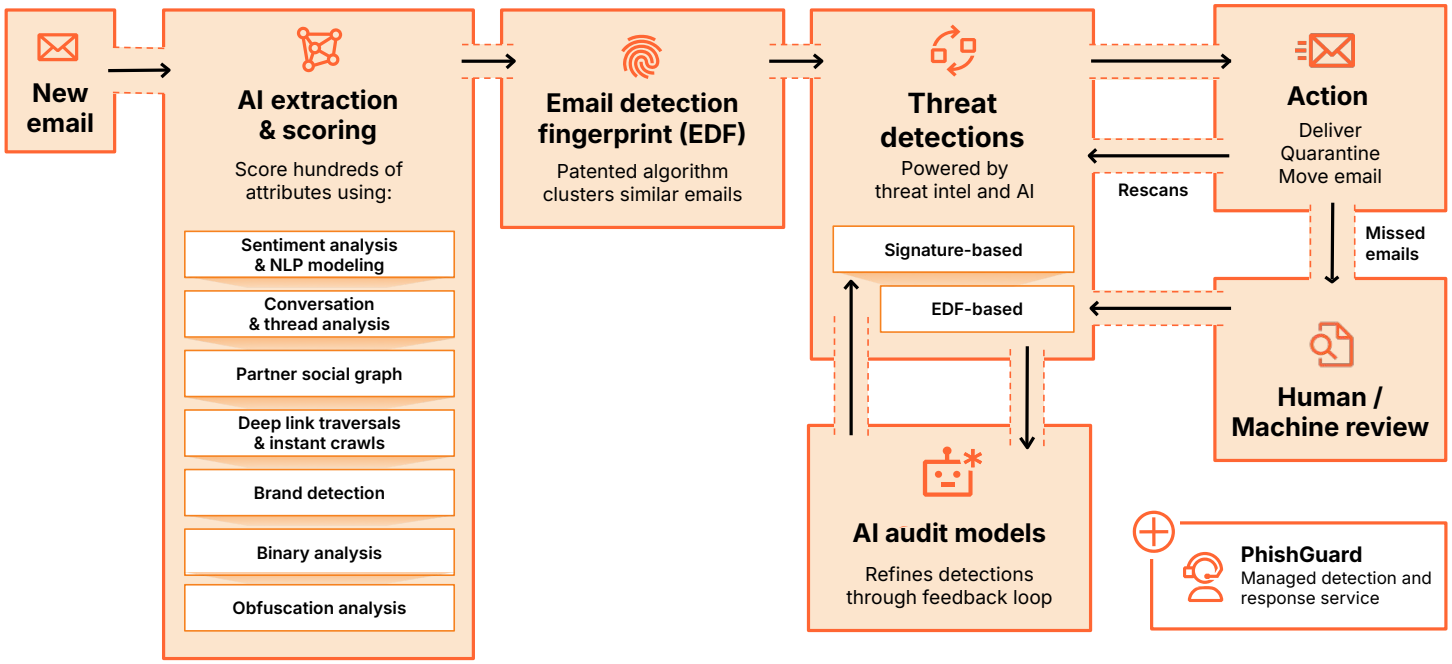
Improve detection efficacy and outcomes

Cloudflare uniquely secures the inbox by combining deep AI analysis with patented **Email Detection Fingerprints (EDF)**. While traditional tools struggle with context, Cloudflare's models score hundreds of attributes—from sender sentiment to conversation context—to identify stealthy attacks. Its unique EDF technology tracks broader campaigns by finding hidden similarities across disparate emails, while continuous rescanning catches post-delivery link redirects. This automated, multi-layered approach is reinforced by AI audit models and our internal team.

Refine detections through submissions

Our AI audit models and internal experts automatically transform customer submissions into global detection updates, ensuring your defenses evolve without the need for manual, time-consuming rule updates. This new model of refinement ensures:

- **Ever-improving detections:** Models are refined via submissions instead of constant rule tuning.
- **Lower overhead:** Significantly reduces time spent tuning and investigating detections.
- **Less disruption:** Minimizes security-driven delays to email delivery.



Identify and block BEC attacks with AI-enabled contextual analysis

Accurate identification of BEC campaigns 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 and refined AI 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.

Integrated SASE controls

As phishing evolves into a multi-channel threat—using obfuscated links and malicious apps to load malware or steal data—securing the inbox is no longer enough. To stay ahead, enterprises must deploy integrated controls that protect all vulnerable collaboration tools, not just email.

Integrated Browser Isolation for suspicious email links

Cloudflare solves for highly-deceptive links and deferred attacks by automatically rewriting any suspicious URLs so that they render 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 to prevent credential harvesting and data leaks.

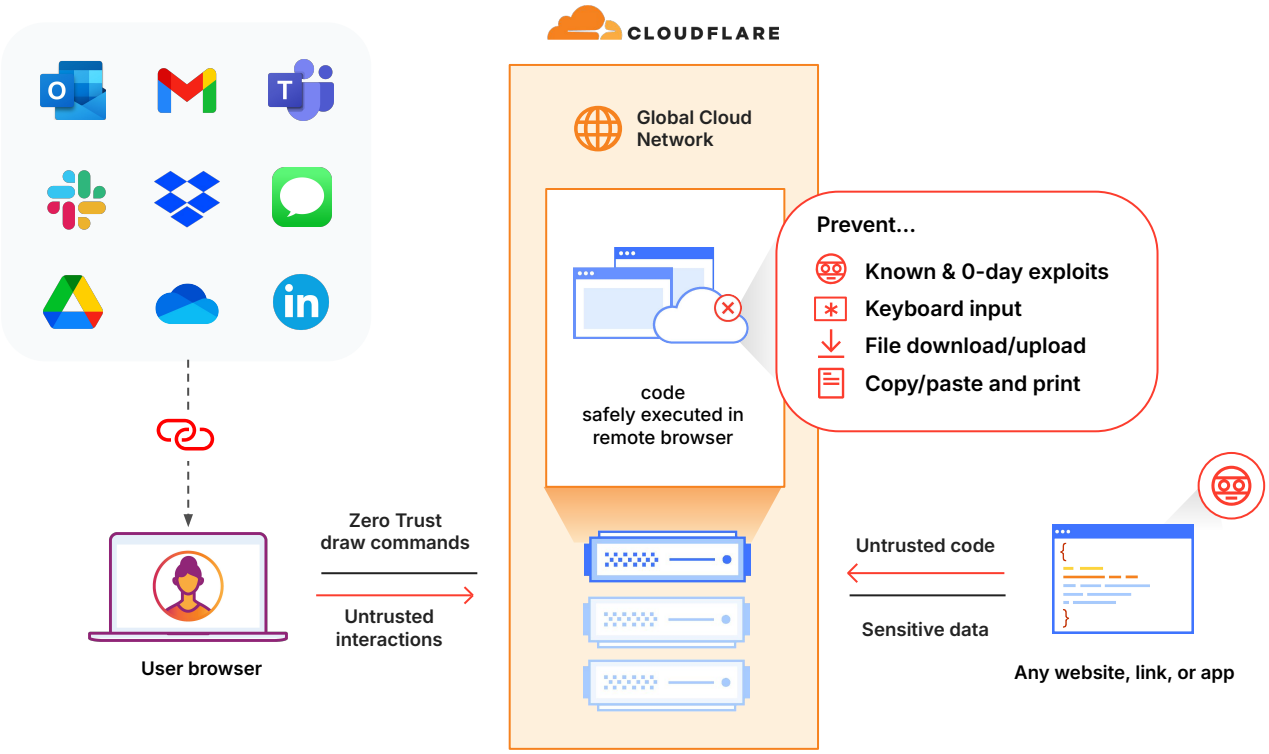


Figure 1: Isolating links in a remote browser

Integrated Data Loss Prevention (DLP)

Cloudflare simplifies data protection by providing integrated Email Security + DLP. This eliminates the need for third-party tools by providing a unified control plane to identify and block the exfiltration of sensitive information—like PII, PCI, or proprietary code—via email. This holistic approach provides security teams with consistent policy enforcement and granular visibility across the entire workspace.

Integrated Cloud Access Security Broker (CASB)

Cloudflare's integrated CASB enables faster configuration and extends security beyond the inbox, providing deep visibility into SaaS applications. By identifying misconfigurations, shadow IT, excessive permissions, and risky file sharing in platforms like Microsoft 365 and Google Workspace, it closes security gaps that email defenses alone can't reach—all through a single, unified interface.

Rapid investigation & resolution

Intuitive, low-touch security management

With greater automation and minimal configuration, Cloudflare Email Security significantly reduces the time and effort required for day-to-day 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 greater detail and email disposition summaries. LLM-powered insights are also surfaced to end users to provide context before they report an email, offering real-time guidance that prevents unnecessary submissions; significantly reducing the manual review burden on SOC teams.

Additional dashboard capabilities

- **Link and attachment isolation** to enable analysts to quickly and securely investigate an incident.
- **On-demand link crawling** for instant analysis of any embedded URLs within an email.
- **API integration** to seamlessly plug into existing analyst workflows and orchestration tools.
- **On-demand security report** to quickly surface critical data points and areas of risk.
- **AI-enabled assistance** for config optimization, detection summaries, and submission guidance.

International airline

"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."

Transportation & logistics

50%

reduction in malicious emails and cut email triage efforts by several hours per day

Managed detection & response (PhishGuard)

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

Technical specialists dedicated to:

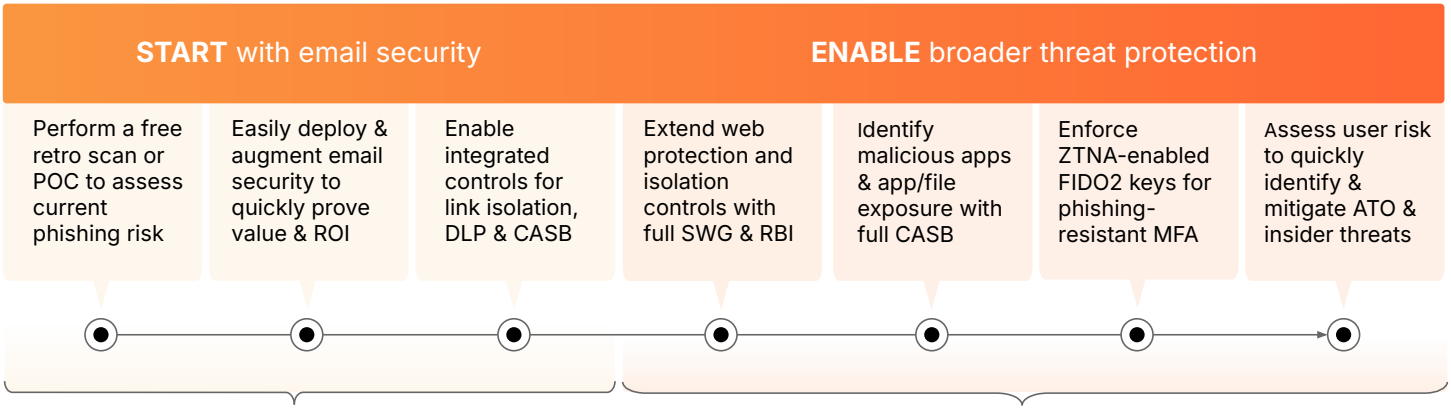
- Managing phish submissions
- Proactive BEC/fraud notification
- Real-time email monitoring
- Threat hunting & assessments
- Custom block signatures

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.

With Cloudflare's unified SASE platform, organizations can first deploy industry-leading email security to quickly address the most critical phishing channel; then easily enable integrated SASE controls 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 no rule 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.



Evaluate and compare

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

Run a free retro scan in minutes to see which phishing threats have slipped through over the past 14 days or request a phishing risk assessment (PRA) to monitor 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.

Run a retro scan | Request a PRA

1. 2023 FBI IC3 PSA: Source
2. Based on average detection rates across customers using O365 or Gmail

© 2024 Cloudflare, Inc. All rights reserved.