CLOUDFLARE

SOLUTION BRIEF

Cloudflare + Microsoft 365 Phishing Protection

Delivering autonomous, multi-channel protection for secure workspace communication

Ditch the legacy gateway and upgrade your phishing protection

In the early 2000s, secure email gateways (SEGs) were introduced to deal with a growing need around the routing and filtering of email. While SEGs were successful at their mission for many years, their fundamental design has made it impossible for them to keep pace as phishing threats rapidly grow in scope and sophistication.

Continuously updating manual rulesets and policies that were originally built for on-prem servers only inflates the amount of time and effort involved in maintaining a SEG. This has resulted in an increase in cost and complexity while still falling short of catching the most dangerous threats, such as business email compromise (BEC) attacks. The increase in overhead and decrease in effectiveness can be attributed to:

- **Emerging phishing tactics and zero-day threats** - modern phishing attacks employ increasingly deceptive tactics designed to evade static filters and traditional controls. This makes it difficult for SEGs to block new threats that lack known indicators of compromise.
- **Complex deployments** - SEGs require extensive configuration and constant tuning to adapt to emerging threats while also requiring multiple add-on modules to fully utilize their capabilities.
- **Time-consuming incident response** - when suspicious or malicious activity bypasses deployed SEG controls, the investigation and response process can be lengthy and cumbersome, involving a patchwork of interfaces and workflows.

Deploy high-efficacy, low-touch protection

As organizations continue to adopt Microsoft 365 to enhance communication and collaboration for their hybrid workforce, it's crucial to take advantage of Microsoft's native security features while integrating complementary, machine learning-based solutions to automatically block and isolate the most dangerous threats. This strategy not only significantly reduces phishing risk, but also simplifies workflows; minimizing the time and effort needed for ongoing security management.

91%

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

#1

attack vector to commit fraud and gain access[2]

$50B

in losses from BEC attacks over the last decade[3]

$4.88M

represents the average cost of a data breach in 2024[4]

1. 2020 Deloitte research
2. Microsoft SIR Report
3. 2023 FBI IC3 PSA
4. 2024 IBM Cost of a Data Breach

Microsoft's email security capabilities

Removing SEG overlap to reduce risk and cost

Analysts agree that consolidating capabilities to minimize overlapping functionality is helping organizations reduce cost and complexity. However, they also advise organization's to carefully assess native features to ensure they satisfy all use cases.

As Microsoft continues to build out its essential email security features, the growing overlap with SEGs has given organizations an opportunity to streamline security operations by leveraging capabilities already included in their E3 or E5 license. This shift enables organizations to eliminate complex and costly SEG deployments, redirecting a fraction of that budget to integrate lightweight solutions that effectively address the most dangerous phishing threats.

Cloudflare Email Security provides an integrated, low-touch solution that augments Microsoft 365 using machine learning threat analysis to automate the detection of BEC and multi-channel attacks.

Areas of overlapping SEG functionality include:

- **Email Hygiene**
  Rule-based policies for spam and bulk messages, with signature-based detection for known malware.
- **URL & Attachment Protection**
  Basic rewriting for all email links and sandboxing capabilities for attachments.
- **Investigation & Threat Hunting**
  Email search, incident investigation and correlation, hunting, and remediation.
- **Information Protection**
  Encryption, archiving, and DLP policies for email, files, and endpoints.
- **Awareness & Training**
  Phishing attack simulations and training for end users.

Exchange Online Protection

Included in every plan and provides essential email hygiene to filter bulk, spam, and malware.

- Anti-spam
- Signature-based malware protection

Microsoft Purview (DLP)

Configurable data loss prevention rules and enforcement. Integrated with Microsoft Information Protection.

- DLP for email & files
- DLP for Teams
- DLP for endpoints

Defender for O365 Plan 1

Additional security controls for basic protection against malicious links and attachments.

- Safe Links (URL rewriting)
- Safe Attachments (sandboxing)
- Internal email protection

Defender for O365 Plan 2

Includes everything in Plan 1 plus additional capabilities for threat hunting, investigation, training, and response.

- Threat hunting
- Cross-domain incident correlation
- Cyber-attack simulation training

E3 License

E3 License + Compliance

E3 License + Compliance + Security

E5 License

● Complete ● Limited ○ None

		SEG	M365	Cloudflare
Threat Prevention	Allow/Block Lists	●	●	●
	Known Bad Sender	●	●	●
	Known Bad URL/Attachment	●	●	●
	Spam/Bulk Filtering	●	●	●
	Machine Learning (Content Analysis)	●	○	●
	Zero-Day Malware/Ransomware	●	●	●
	Malicious Links	●	●	●
	URL Rewriting (Click-Time Analysis)	●	●	●
	Adaptive Link Isolation	○	○	●
	Business Email Compromise (BEC)	●	●	●
	Employee Impersonation	●	●	●
	Vendor Impersonation	●	●	●
	Employee Compromise (ATO)	●	●	●
	Vendor Compromise	●	●	●
	DMARC Management	●	●	●
	Malicious App Detection (OAuth Phish)	●	●	●
	Web Content Security	●	●	●
	Security Awareness & Training	●	●	●
Threat Response	Single, Intuitive Interface	○	●	●
	Automated Threat Triage	○	●	●
	Rapid Search & Investigation	●	●	●
	Auto-Retraction	●	●	●
	On-Demand Reporting	●	●	●
	Managed Detection & Response Service	●	○	●
Data Protection	Encryption	●	●	○
	Archiving	●	●	○
	Email DLP	●	●	●
	Cloud DLP (Collaboration Apps)	●	●	●
	Network DLP	●	●	●

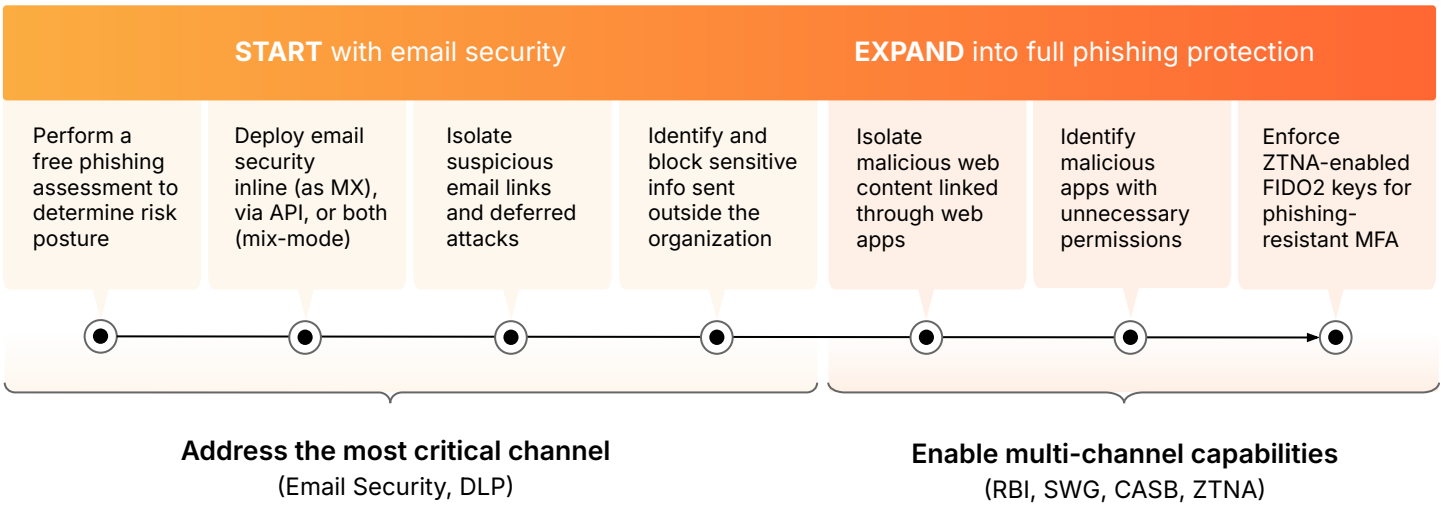
BENEFITS

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.

With Cloudflare's unified security platform, organizations can first deploy industry-leading email security to quickly address the most critical phishing channel; then easily enable 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.



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

© 2024 Cloudflare, Inc. All rights reserved.