CLOUDFLARE
AREA 1 SECURITY

SOLUTION BRIEF

Enhance Microsoft 365 Email Defenses with Cloudflare Area 1

Extend Zero Trust to your #1 communications tool — cloud email

Keep Microsoft inboxes threat-free with preemptive, cloud-native email security

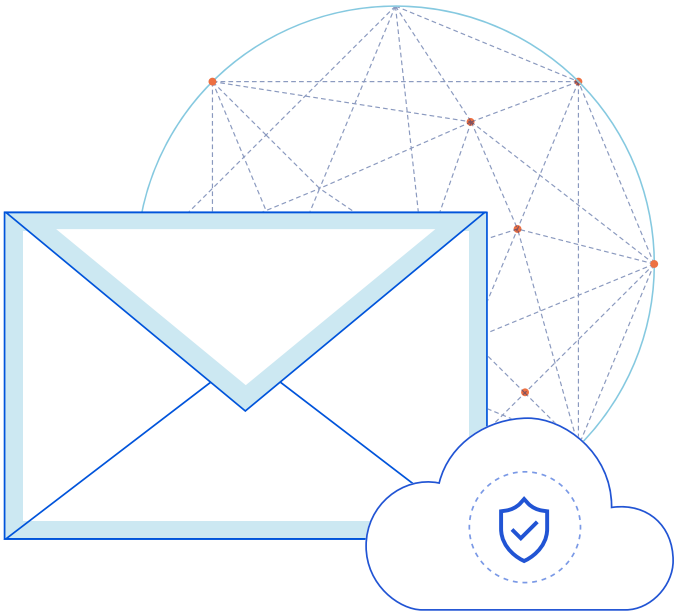
Microsoft 365 delivers excellent protection against high-volume threats, such as spam and viruses, and provides additional protection for Microsoft Advanced Threat Protection (ATP) customers.

Yet, Gartner® notes that[1], "As built-in security … has improved, threat actors are also getting more sophisticated, often targeting them using fake login pages as a way of harvesting credentials. Sophisticated email threats include compromised websites and weaponized documents used to deploy malware. Many ransomware-as-a-service gangs use email as the initial entry point. Beyond malware, Business Email Compromise (BEC) and account takeover threats continue to rise, with significant financial losses as a result."

Low-volume, sophisticated threats such as those noted above are first built with attack infrastructure and techniques that Cloudflare Area 1 is uniquely capable of discovering "in the wild." By identifying and automatically blocking campaigns early in the attack lifecycle (on average 24 days pre-launch), Area 1 keeps inboxes threat-free.

As part of the Cloudflare Zero Trust platform, the Area 1 email security service also:

- **Exposes malware-less financial fraud**, often conducted over multiple email conversations with "trusted" vendors/suppliers
- **Blocks never-before-seen attacks in real-time**, without your needing to "tune" a SEG or wait for signature/policy updates
- **Discovers compromised accounts and domains**, as well as new, lookalike, and proximity domains that attackers use to bypass DMARC/SPF/DKIM
- **Isolates and blocks blended and deferred** attacks with integration into Cloudflare Browser Isolation (beta)



Solution overview

In a cloud-first world, traditional secure email gateways (SEGs) are inflexible and ineffective against constantly evolving threats, such as Business Email Compromise, spoofing, and ransomware.

Cloudflare Area 1 provides preemptive, cloud-native email security to comprehensively stop these and other targeted phishing attacks.

Organizations layering Microsoft 365 with Cloudflare Area 1 receive:

- **Comprehensive phishing protection** across internal and external email, web, and network traffic
- **Reduced IT complexity** and phishing incident response time
- **Simple deployment in minutes** with an API-first approach
- **Expedited SOC investigations** with post-delivery message retractions and SIEM/SOAR integrations

How can you block more threats with Area 1's cloud email security approach?

Microsoft 365 delivers great security for high-volume email threats; however, low-volume, highly targeted phishing attacks that cause upwards of 90% of cyber breaches can still slip through.

How should organizations using Microsoft 365 and still dealing with missed phish handle modern threats?

Enter **integrated cloud email security** (ICES) solutions. According to Gartner®, "Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease evaluation and deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform."[2]

"By 2023, at least 40% of all organizations will use built-in protection capabilities from cloud email providers rather than a secure email gateway (SEG), up from 27% in 2020.

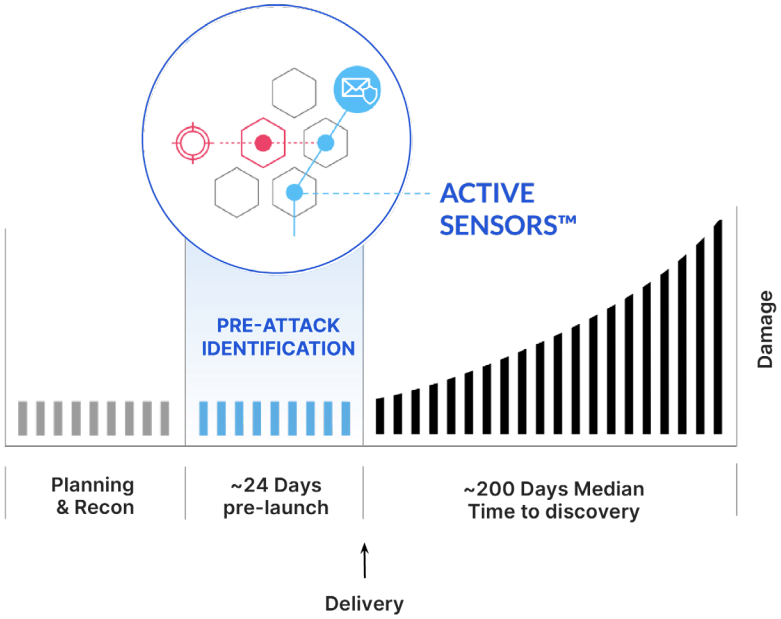
"By 2025, 20% of anti-phishing solutions will be delivered via API integration with the email platform, up from less than 5% today."

— 2021 Gartner® Market Guide for Email Security

Area 1 Horizon (now Cloudflare Area 1 email security) is a Representative Vendor in the Integrated Cloud Email Security (ICES) category in the Gartner Market Guide report.

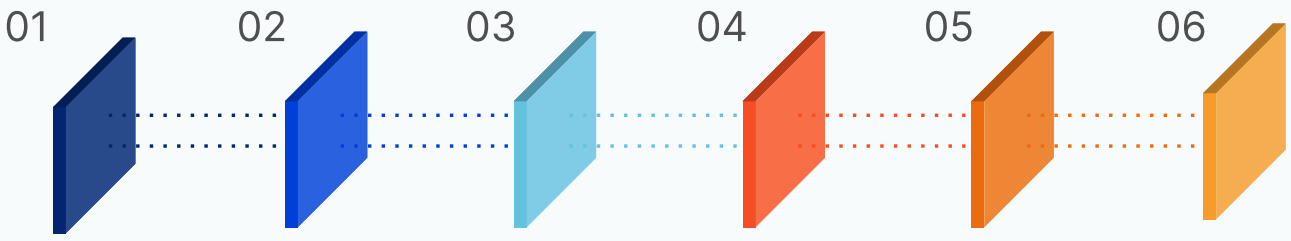
Unlike other solutions, the Area 1 solution **continuously and proactively crawls the web** to discover new phishing campaigns and attacker infrastructure in the wild. On average, Area 1 preemptively detects malicious sites and payloads a full 24 days before attacks launch.

Figure 1: Preemptively stop phishing attacks — before they reach your inbox — with Cloudflare Area 1



Area 1 also uses a variety of more **advanced detection techniques**, including NLU, NLP, social graph analysis (patterns of email communication), and image recognition, to detect and stop the most sophisticated attacks — including brand new, highly targeted threats that threaten users 1:1 vs. one to many.

Figure 2: Analyze the content, context, and social graphs of email communications to stop modern threats like BEC



Structural Analysis
Headers
Body, Images, Computer Vision
Links, Payloads

NLU Modeling
(Natural Language Understanding)
Writing Patterns
Categories
Expressions

Sentiment Analysis
Intent, Tone, Relationship, Hierarchy

Thread Analysis
Conversations
Variations
Length

Industry Modeling
Verticals
Lingua Franca
Business Processes

Trust Graphs
Partner Social Graphs, Sending History, ATO Discovery
Partner Impersonations

Simple deployment in minutes

With an API-first approach that integrates seamlessly into Microsoft 365, Area 1 takes just minutes to deploy. Detect and block phish more accurately and effectively — without the IT complexity needed to constantly "tune" an ineffective traditional SEG.

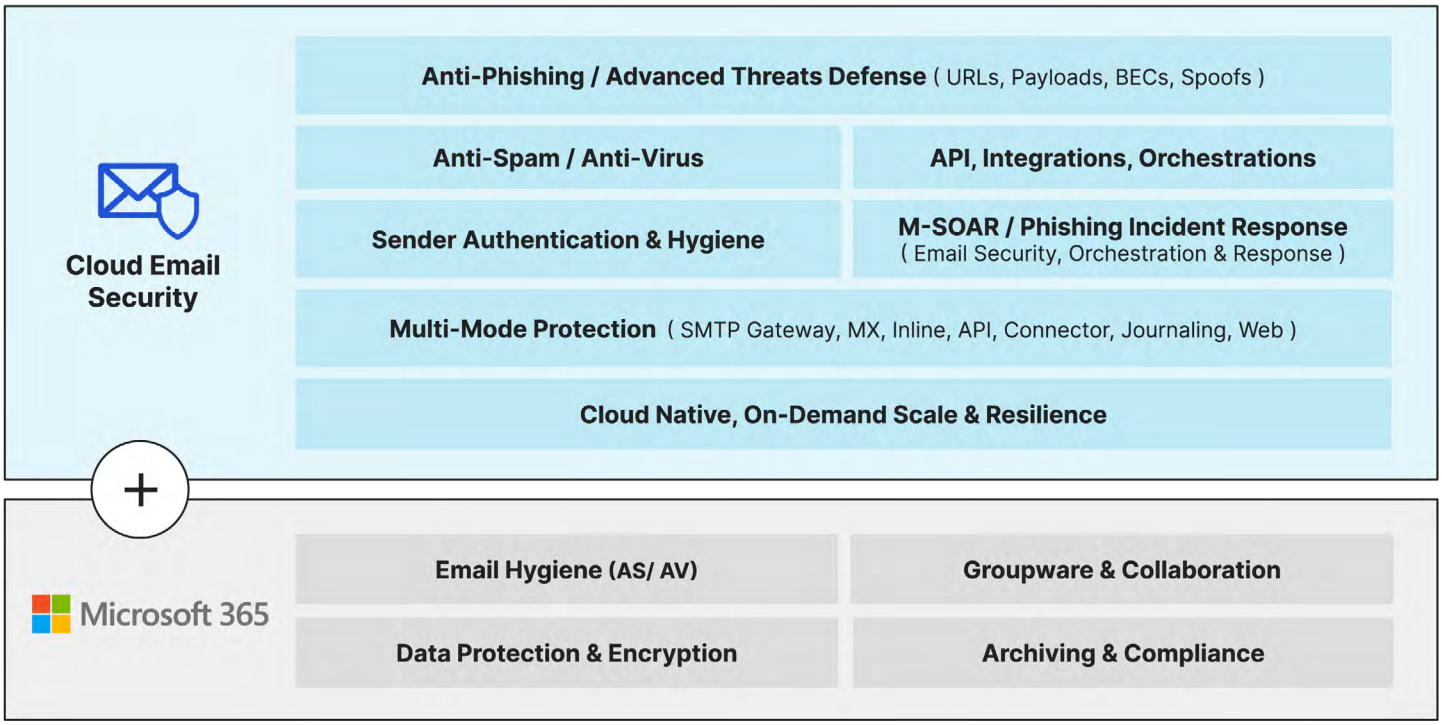
Figure 3: Example Area 1 email security deployment option

Area 1:

- Can be deployed in less than five minutes, with nothing to install and no impact to your existing infrastructure;
- Provides more flexible deployment options (including MX/inline, connector and API) compared to other solutions;
- Integrates seamlessly with Microsoft 365's other email security features like anti-spam, DLP, encryption, and archiving;
- Can effortlessly remove all malicious messages directly from Microsoft 365 mailboxes with built-in remediation and message retraction; and
- Is completely transparent to your end users, while providing comprehensive, end-to-end phishing detection and remediation.

Benefits of protecting your Microsoft 365 email environments with Cloudflare Area 1 include:		
Best-in-Class Cloud Email Security	**Seamless Workflows**	**Increased Operational Efficiency**
• Augments native Microsoft defenses for comprehensive protection against modern threats including BEC, email supply chain attacks, compromised vendor accounts, insider threats, and more. • Broader threat visibility and forensics improve investigations and response times.	• Deep integration with Microsoft environments, APIs, and workflows. • Integrate with ADFS, send alerts to Teams, and forward logs to Azure Sentinel. • End users stay in native Microsoft dashboards for continued productivity and no distractions.	• Built on cloud-native, dynamically scalable infrastructure to handle cloud traffic spikes. • Replaces traditional SEGs for better security and operational efficiency. • Advanced detection, triage, and response in a single platform for defense-in-depth.

Keep your inboxes free of threats with comprehensive, integrated cloud email security:



Microsoft + Cloudflare: enabling a more secure and private cloud

Cloudflare has built deep integrations with Microsoft to help organizations take the next step in their Zero Trust journey. These integrations empower organizations to make customer implementations operationally efficient while delivering a seamless user experience and scaling operations.

In addition to Area 1, Cloudflare's Zero Trust services integrations include:

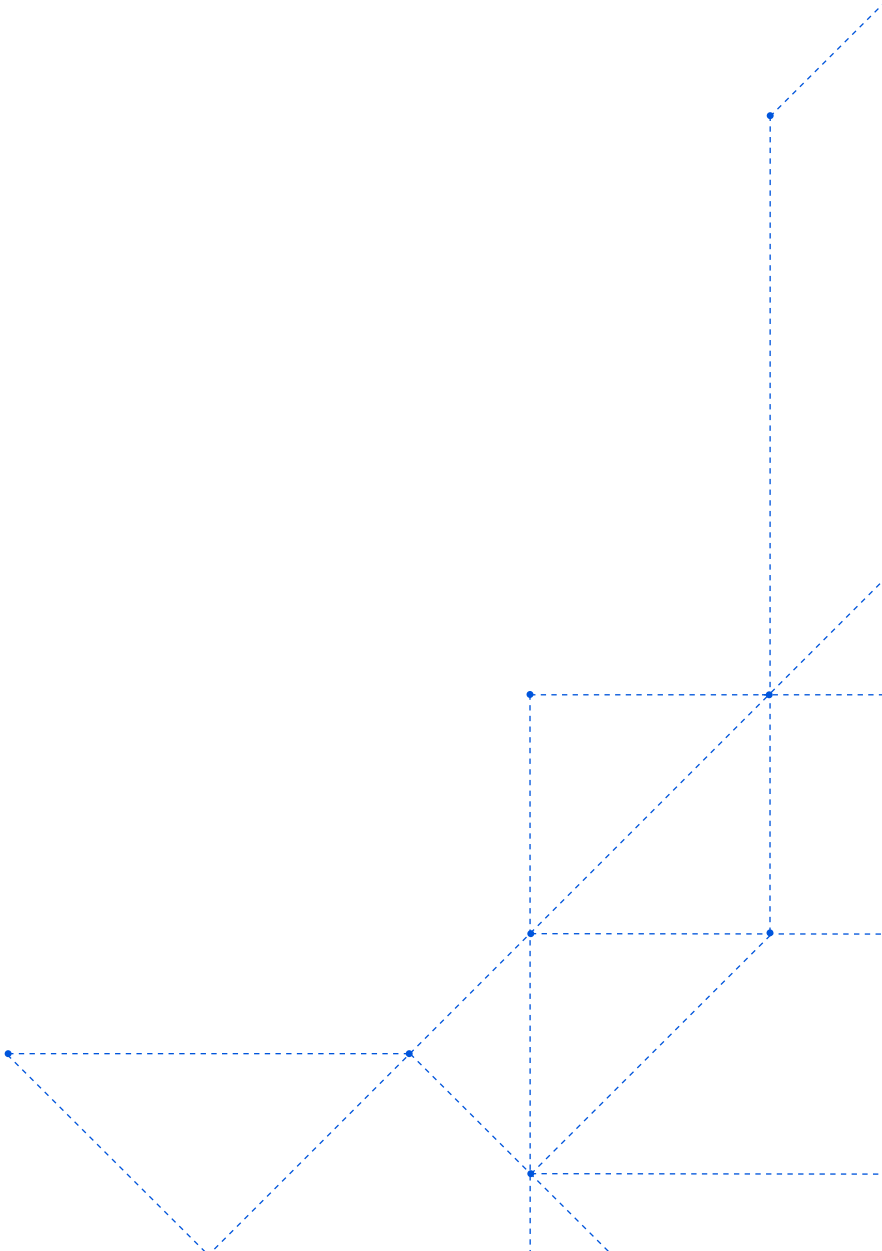
- **Azure Active Directory (AD)** — Leverage powerful authentication tools, including multi-factor authentication (MFA), conditional access policies, and risk-based controls.
- **Microsoft Cloud App Security (MCAS)** — Launch the M365 integration to scan for and present new security issues to customers related to M365 users, data, and in-app services.
- **Zero Trust for Azure Apps** — Enable secure access to on-premise applications or Azure-hosted applications — no VPN required.
- **Microsoft Endpoint Manager** — Evaluate client posture at the time of sign-in via Microsoft Intune, allowing Cloudflare to allow or deny access based on security or device posture signals.
- **Microsoft 365** — Deliver a faster and more secure user experience by optimizing user connectivity to Microsoft 365 via Cloudflare and Microsoft's Networking Partner Program.

To learn more about Cloudflare's partner integrations with Microsoft, contact us.

To see how Cloudflare Area 1 can enhance your Microsoft 365 phishing defenses, request a custom risk assessment here.

References

1 & 2 Gartner, “Market Guide for Email Security,” 7 October 2021, Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer



AREA 1 SECURITY

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3778/2022SEPT07