

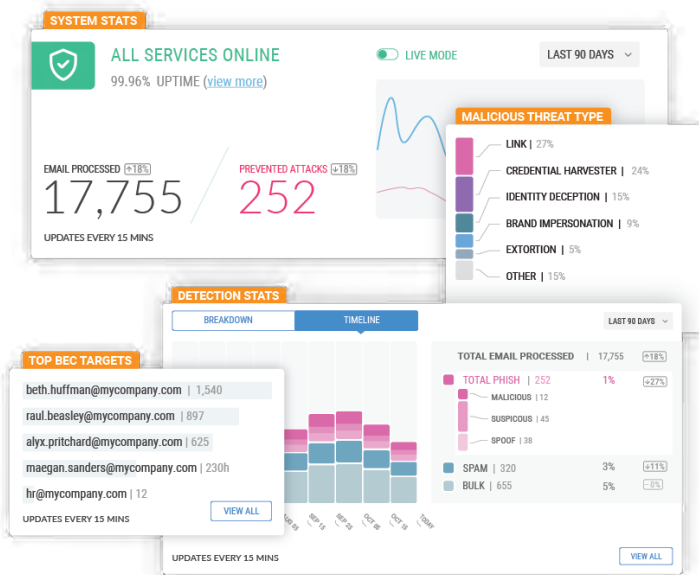
# Complimentary Phishing Risk Assessment

Cloudflare Area 1 identifies and blocks the threats bypassing your current email defenses

Cloudflare Area 1 is designed to protect organizations from the cause of over 90% of data breaches: phishing attacks. In Q2 2022 alone, the Anti-Phishing Working Group observed over 1 million total phishing attacks, representing “the worst quarter for phishing that APWG has ever observed.”

As part of the Cloudflare Zero Trust platform, Area 1 email security inherently assumes that no email can be trusted. We preemptively identify phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of an attack cycle.

**Discover and stop the threats that are currently evading your email defenses with a complimentary phishing risk assessment.**



Area 1 frequently catches 30% more phish than legacy secure email gateways (SEGs) and cloud email suites.

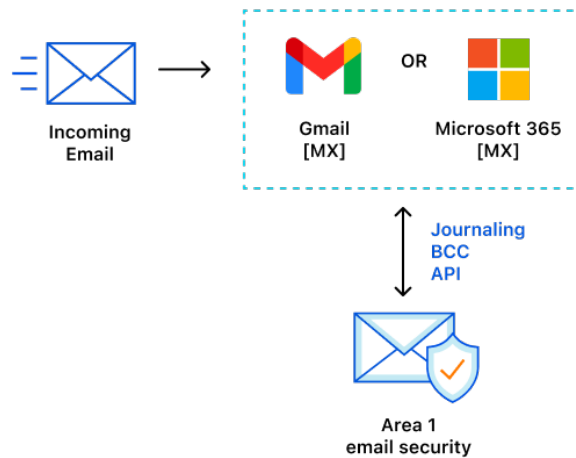
**With an Area 1 phishing risk assessment, you'll access customized, real-time data on:**

- **Who** within your organization is most targeted by phishing
- **What** specific threats are evading your other defenses (e.g., SEGs, cloud email suite, email authentication protocols)
- **Which** attack groups and Indicators of Compromise you are facing
- **Where** the malicious attacks are originating
- **How** to close any current email security gaps

## How it Works

The best way to assess the effectiveness of security products is by using real-world data. Area 1's fully elastic, cloud-native service lets you get up and running in minutes, without needing to deploy any hardware or software.

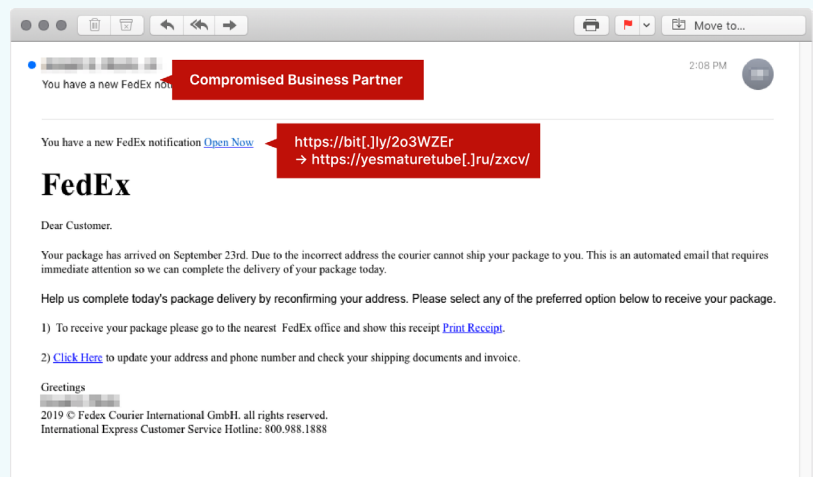
- [Set up](#) in minutes without affecting mail flow or impacting your end users.
- Choose the deployment option best for your organization — inline, API or multi-mode.
- Integrate Area 1 into your SIEM and other security integration points to get full detection metrics and forensic details.
- Our assessment typically runs for 15 to 30 days, after which we will deliver an in-depth custom analysis. You can access your dashboard at any time during the assessment.
- Your Area 1 account team will also alert you in real-time to critical phishing incidents during the assessment.



Area 1 will process forwarded messages from your SEG or email provider via BCC or journaling rules, to identify and block any missed threats.

## Sample phish missed by existing controls

This is an example of a supply chain email attack, where the business partner's email account was likely compromised first. The compromised account was then used to phish another organization. This phishing email was missed by Proofpoint, but detected by Area 1.



## Example assessments

Cloudflare Area 1 hunts for phishing infrastructure, sources and delivery mechanisms, blocks campaigns across different attack vectors, and provides end-to-end phishing triage and response. We stop the most sophisticated and malicious phishing attacks that we often observe traditional SEGs missing.

Below are examples of one-month observations from organizations using other email security providers. It takes just one missed threat to cause a security disaster.

---

Missed threats in a one-month period sitting behind other email security providers.

Organization industry	Email security system used	Missed threats	Total email volume
Insurance	Microsoft 365	517,968	103,099,539
Pharmaceutical	Proofpoint	448,440	432,611,141
Food & Beverage	Cisco Email Security (IronPort)	105,603	420,088,334
Education	Custom	90,763	142,672,221
Financial Services	Mimecast	1,727	17,223,584

### See for yourself how Cloudflare Area 1:

- ✓ Prevents BEC and email-based fraud
- ✓ Protects against low-volume and highly targeted attacks
- ✓ Accelerates phishing triage and response

[Get started with a risk-free phishing risk assessment today.](#)