As one of the popular enterprise email environments and cloud collaboration apps, Microsoft 365 (formerly known as Office 365) use has skyrocketed in recent years. At the same time, Microsoft 365 email has become a popular vector for perpetrating cyber attacks including Business Email Compromise (BEC), fraud and other targeted attacks. Although Microsoft is continuously improving its native email security and Advanced Threat Protection (ATP), a staggeringly large volume of phishing messages still get through.

In their most recent Market Guide for Email Security, Gartner mentioned that despite Microsoft's continued investment in security, organizations are dissatisfied with native capabilities, choosing to supplement with third party email security solutions like Area 1 Security.

Area 1 Security, a Certified Microsoft Partner, closes the security gap with the industry’s only preemptive and comprehensive cloud-native defenses against phishing campaigns targeting organizations using Microsoft 365 email.
Microsoft 365 delivers great baseline functionality for high-volume email threats such as spam and viruses, but it does not protect your users from the low-volume, dangerous phishing attacks that cause 95 percent of cyber breaches. Even Microsoft's Advanced Threat Protection (ATP), as well as leading Secure Email Gateways (SEGs), routinely miss phish — leading to significant damages to organizations large and small alike.

As detailed in our Office 365 missed threats report, over one six-month period, we uncovered nearly 1 million (more than 925,000) phish missed by Microsoft and leading SEGs from vendors including Proofpoint, Mimecast and Cisco.

These gaps in protection put your organization at substantial risk of a breach from threats like the ones caught by Area 1 below.
Examples of Microsoft 365 phishing attacks blocked by Area 1:

01 ・ Credential Phish
- Compromised user impersonating IT
- Redirect to malicious site

02 ・ Brand Impersonation
- Spoofed Sender
- Bank Impersonation
- Message is actually an image linking to credential harvester

03 ・ Type 4 BEC
- Compromised Sender
- Redirecting to attacker email
Area 1 Security’s innovative technology continuously and proactively crawls the web, discovering phishing campaigns and attacker infrastructure before attacks launch. On average, our solution detects malicious sites and payloads a full 24 days before industry benchmarks. The resulting early insight and visibility powers the Area 1 Horizon email security platform to detect and block phishing and advanced threats that Microsoft 365 and other defenses miss.

Through flexible deployment options including MX, inline, connector and API, Area 1 integrates quickly and works seamlessly with Microsoft 365’s other email security features like anti-spam, DLP, encryption and archiving. With built-in remediation and Message Retraction, Area 1 can also effortlessly remove all malicious messages directly from Microsoft 365 mailboxes, providing comprehensive, real-time protection from detection to response.

To learn more about Area 1 Security’s preemptive capabilities and how to protect your cloud email environment from advanced phishing attacks, watch our "Microsoft Office 365, Compromised" on-demand webinar here, or request a free trial, here.
About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit www.area1security.com, follow us on LinkedIn, or subscribe to the Phish of the Week newsletter.