

Symantec Technology Partner: ZeroFOX



Partner Product: ZeroFOX Platform

Symantec Product: Symantec Email Security

Business challenges

Attackers exploit any channels available to gain unauthorized access to an organization and its data. The most effective channels are always the ones with real people at the other end. This fundamental security truth is why so many attackers continue to use email as a their preferred delivery mechanism and why social media has exploded in recent years as an ideal channel to find, target, and engage a potential victim.

Email

The security challenges with email are as old as email itself. Attackers spoof everyone from members of someone's own organizations to Nigerian princes with suspiciously deep bank accounts. The possible payloads are as diverse as the tactics: scams, spam, malware exploits, spear phishing, and more. Email is so well established as one of the top attack vectors that email security has long been a staple of every modern security perimeter. As the adversary continues to develop, businesses demand smarter and more efficient email security solutions to prevent this pervasive threat.

Social Media

Social media and digital channels—Facebook, LinkedIn, Twitter, Slack, forums, domains, mobile app

stores, recruitment sites, and more—have become core communication platforms for every modern business. Cyber criminals and scammers are adopting them as well, and attackers take advantage of the scale, trusted nature, lack of security visibility, and anonymity of social platforms to launch a new breed of highly effective attacks, all of which occurs outside the firewall. With a fundamental lack of visibility and control, modern organizations struggle to identify and remediate risks and cannot protect themselves across social and digital channels.

These risks can have massive financial impacts. ZeroFOX estimates the global annual cost of phishing attacks on social media is \$1.2 billion; the average email spear phishing attack sits in the range of 1.6 million; and financial scams found on Instagram alone cost businesses roughly \$420 million each year. Ninety percent of respondents in a recent Symantec survey report that the average cost of a social media incident is an amazing \$3,588,611.

Security teams miss critical intelligence around threats by failing to ingest data from email and social media. More important, even if an organization is ingesting data from one of those sources, it misses the combined, contextualized understanding of attacks that often only comes from identifying a campaign from multiple angles, thus exposing the full scope of the threat.

Social media data is often the most up-to-date, real-time intelligence available anywhere and, if ingested correctly, it can tip the scales from the social media adversary to the defender, especially when combined with already robust email-based intelligence. On social media, adversaries boast of their exploits, plan attacks, collude with other cyber criminals, target customers, and distribute phishing links, scams, and malware



exploits—all in the broad daylight of the internet’s most popular social platforms. This intelligence is an ideal complement to existing email perimeter data as it provides additional early warnings, situational awareness, and investigative context before, during, and after an attack, respectively.

Combined benefits

The combined ZeroFOX and Symantec offering ensures you can:

- Identify threats on social media and digital channels
- Correlate those threats with critical intelligence already in Symantec Email Security
- Protect your business from scams, phishing, and malware
- Add investigative context to threats and campaigns with information around fraudulent accounts
- Gain full visibility into your business’ social and digital presence
- Get early warnings when an attacker is discussing your business online

Integrated solution

The ZeroFOX Platform with Symantec Email Security provides coverage across the two most vulnerable attack vectors.

The Symantec Email Security solution secures your email in the cloud and on premises, blocking new and sophisticated email threats with the highest effectiveness and accuracy. Multilayered technologies, including link protection and a complete defense against impersonation threats, prevent dangerous attacks such

as spear phishing, ransomware, and business email compromise (BEC).

Email threat isolation—available only from Symantec—renders suspicious links in a remote execution environment and suspicious websites in read-only mode, further strengthening protection; attacks meant to be delivered via malicious links simply cannot be delivered. This is coupled with security awareness and education that prepares users to recognize and evade email attacks, and advanced analytics that help organizations respond to threats through deep visibility into targeted attacks. All these capabilities are included in the Symantec Email Security solution, which is an integral part of the Symantec Integrated Cyber Defense Platform that protects users, information, messaging, and the web.

The ZeroFOX Platform identifies security risks and business threats targeting employees, customers, and organizations across social media and digital channels. Using diverse data sources and artificial intelligence-driven analysis engines, the ZeroFOX Platform automatically identifies and remediates fraudulent accounts, phishing attacks, customer scams, exposed personally identifiable information (PII), account takeovers, and more. This intelligence is wholly unique in the security team’s infrastructure; it is not data otherwise ingested through the traditional product stack.

By combining Symantec Email Data and ZeroFOX data in visualization, analytics, threat intelligence platform (TIP), security orchestration, automation, and response (SOAR) and security information and event management (SIEM) systems, security teams understand the full context of the intelligence both within and outside of their perimeter. Attack data is correlated across

About ZeroFOX

ZeroFOX, the market leader in [social media and digital protection](#), safeguards modern organizations from [dynamic security, brand and physical risks](#) across social, mobile, web and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, ZeroFOX protects modern organizations from targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. [The patented ZeroFOX SaaS platform](#) processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, HipChat, Instagram, Pastebin, YouTube, mobile app stores, the deep and dark web, domains and more.

Led by a team of information security and high-growth company veterans, ZeroFOX has raised nearly \$100M in funding from NEA, Highland Capital, Silver Lake Waterman, Redline Capital and others, and has collected top industry awards such as Red Herring North America Top 100, the SINET16 Champion, Dark Reading's Top Security Startups to Watch, Tech Council of Maryland's Technology Company of the Year and the Security Tech Trailblazer of the Year.

attack vectors—both email and social media—creating a more robust defensive posture for identifying and investigating attacks.

How it works

Symantec Email Security can be hosted in the cloud or on premises. As a cloud service, Symantec Email Security functions as a cloud-based mail transfer agent (MTA) that sits between the email system and the public internet. When on premises, Symantec Email Security sits in gateway as a physical or virtual appliance.

The ZeroFOX Platform is a cloud-based solution requiring no on-premises or in-network installation. Configuration requires just a few simple steps, ensuring customers are identifying threats in the wild as quickly as possible.

Built entirely on REST APIs, the ZeroFOX Platform is readily extensible, extending social and digital protection seamlessly into the existing security operations center (SOC) and providing a perfect complement to Symantec Email data and intelligence. Combine Symantec Email Security data and ZeroFOX data in a multitude of visualization, analytics, TIP, SOAR, or SIEM systems to achieve full visibility across attackers' two favorite attack vectors.

- 1. Define What's Important** – Tune ZeroFOX to collect data by defining what matters to you: profiles, pages, keywords, images, domains, and more.
- 2. Create Custom Security Policies** – Configure policies to tackle countless external threats via AI-based classifiers, emerging FoxThreat rules, and custom FoxScript analysis.
- 3. Monitor Social and Digital Channels** – Continuously collect and analyze millions of pieces of content as posts and profiles change.
- 4. Integrate with Symantec Data** – Using visualization or analytics software, pull together ZeroFOX data with existing Symantec data to create robust coverage complete with social media intelligence.

About Symantec technology partners:

To learn more about Symantec technology partners, visit www.symantec.com/partners.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our [blogs](#), or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com