Microsoft and Proofpoint: More Secure Together

Protecting your people from today's modern threats

Key Benefits

- Stop the widest variety of damaging threats accurately
- Stop email threats before they reach your people's inbox
- Focus on your riskiest people
- Stay one step ahead of threat actors with rich threat intelligence
- Change unsafe behaviors with a threat-driven program

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Microsoft is the de facto standard for email and collaboration. Bad actors recognize this, and they increasingly target its defenses. Microsoft does provide native email security, but this offers only limited protection from today's modern threats. As such, organizations need a complementary email security solution to supplement the native Microsoft 365 security. Proofpoint is that solution.

Business Is Good and Bad Actors Know It

Microsoft boasts a worldwide market share of 88.1% for productivity software.[1] Unfortunately, bad actors know this, and they actively try to exploit its success. According to the 2024 Proofpoint *State of the Phish* report, these actors sent more than 68 million malicious emails that abused the Microsoft brand and its products.[2] Their goal? To trick unsuspecting users into revealing their credentials. These attacks are costly. And their numbers are only increasing. The average cost of a data breach reached a record high of $4.45 million in 2023, for example.[3] This is an increase of 15% over the past three years.

Microsoft 365 Email Security Isn't Enough

The basic security from Microsoft can detect and block commoditized malware and ransomware attacks. Built natively into the Microsoft 365 platform, Microsoft Exchange Online Protection (EOP) provides spam detection, IP blocking, antivirus scanning and basic protection against content-based phishing. For more security features, you can buy Microsoft Defender for Office 365. Defender supports device and server security, endpoint detection and response. But even with all of these email security capabilities, modern email threats such as malicious URLs, advanced malware and phishing, business email compromise (BEC) attacks are still getting through to user's inboxes.

[1] Gartner. "2023 Vendor Rating Report." 2023
[2] Proofpoint. "State of the Phish Report." 2024
[3] IBM. "Cost of a Data Breach Report." 2023

API-Based Security Solutions Are Insufficient

As Microsoft 365 becomes more widely adopted, new ways to enhance email security have emerged. These include what Gartner calls integrated cloud email security (ICES) and Forrester calls cloud-native API-enabled email security (CAPES), which use Microsoft-specific APIs to receive email notifications.

No pre-delivery detection and blocking

API-based solutions may be straightforward, but they do not provide complete email protection. Their downside? They analyze emails only after the messages have been delivered to a user's mailbox. Think of it this way: When protecting your home against burglars, do you want to stop them from getting into your house? Or would you want to wait until after they have broken in and have had time to look and around? This post-delivery-only approach can still expose your organization to message payload detonation, data breaches and increased risk.

No multilayered detection stack

Most API-based solutions rely solely on anomaly detection to spot email-based threats. But this method can lead to a lot of false alerts, which can disrupt business. False alerts often block legitimate emails and create more work for security teams. For better accuracy at detecting and preventing modern email threats, you need a multilayered detection stack that correlates multiple signals, such as behavioral anomalies, threat intelligence and more.

No threat intelligence

Your users are your greatest asset, but they are also your greatest risk. Unfortunately, API-based solutions do not include threat intelligence and research. This means they can't proactively identify threat actors, trends or Very Attacked People™ (VAPs). With this kind of blind spot, your security and IT teams cannot know who poses the most risk to your organization. They can't see who has clicked on real malicious messages. And they can't identify specific attacks that target your users. Typical API-based solutions narrowly focus on anomaly detection for only BEC attacks.

This means your organization can still be exposed to many other sophisticated email threats. Given all these limitations, it is easy to see why API-based solutions are not enough to address today's modern threats.

> *"We were told it would be a set it and forget it with Abnormal, but found it couldn't be further from the truth."*
>
> IT director at a Fortune 500 financial services organization

> *“Proofpoint was selected as the favored solution for enhancing Microsoft 365 due to its capability to effectively thwart threats at both pre- and post-delivery stages.”*
>
> Vice president of IT at a global online retailer

Microsoft and Proofpoint, Best of Both Worlds

The threat landscape is constantly evolving. So, you must take a multilayered approach to strengthening your email defenses. The approach should complement native Microsoft 365 security to protect your people and business. This is where Proofpoint can help.

Detect and stop email threats faster with pre-delivery detection

Proofpoint allows you to implement a defense-in-depth approach to better protect your users. Proofpoint Threat Protection detects and blocks advanced email threats before they reach user inboxes, complementing Microsoft 365 security. This pre-delivery approach helps you identify known and unknown attacks across the entire enterprise. It stops sophisticated threats such as socially engineered attacks, BEC and advanced credential phishing at the “front door,” not after they were delivered. Combined with automated post-delivery threat detection and remediation, you can protect your people all the time from today’s modern email threats.

Stop more threats more accurately with AI-driven, multilayered detection

Proofpoint uses a multilayered detection stack that compromises threat intelligence, machine learning, behavioral AI, sandbox detection, content analysis and semantic analysis (LLMs). This stack works together to detect many types of modern threats. We augment Microsoft 365 security to achieve a detection rate of 99.99%. This means fewer false negatives and false positives. In other words, we stop malicious messages more accurately. And we don’t block good messages or don’t impede your business.

Defense-In-Depth Protection		Microsoft 365 Commoditized malware and ransomware protection	+	Proofpoint Modern threat protection (social engineering, BEC, etc.)	=	Defense-In-Depth More Secure Together
Inbound / Outbound Hygiene	Spam Graymail	●		●		●
Malware Protection	Attachment, URLs, SocGholish, Ransomware, Fileless Malware, Rootkits, Keyloggers	◑		●		●
Phishing Protection	Internal/External Phishing, Spear-Phishing, EvilProxy, eSignature Phishing, Quishing	◑		●		●
Social Engineering Protection	BEC, CEO Fraud, Invoice Fraud, Payroll Diversion, Vishing, Whaling, Smishing	◔		●		●
Account Compromise Protection	Internal Account, Vendor Account, Attorney Impersonation, Bogus Invoice Scam	◔		●		●
Advanced Email Threat Protection	Advanced Phishing, TOAD, Malicious URLs	◔		●		●
Modern AI-powered Detection	Multi-layered detection stack, threat intel, ML, Behavioral AI, Sandboxing, Semantic analysis	◔		●		●
Visibility & Explainability	Very attacked people insights, threats targeting very attacked people visibility, executive and condemnation summary and explainability	◔		●		●
Simple, Flexible Deployment	On-premises, hybrid, or cloud, Inline+API, Secure email gateway	◑		●		●
High Fidelity Efficacy	99.99% pre-delivery detection and blocking efficacy out-of-the-box	◔		●		●

Figure 1: Proofpoint complements native Microsoft 365 email security to provide you with defense-in-depth protection.

84%

of Fortune 100 companies trust Proofpoint to augment their Microsoft 365 security.

Comprehensive people risk and threat visibility

Proofpoint allows your organization to gain unique insights into who your VAPs are and what threats are targeting them. In doing so, you can implement targeted adaptive controls, like browser isolation, security awareness training and step-up authentication. Along with people risk visibility, you better understand your people risks on how attacked they are, how vulnerable they are, and what privileges they have. Combined with Proofpoint's threat intelligence and research, we analyze more than 3 trillion email messages a year across our ecosystem of more than 230,000 customers, partners and provider. Our threat visibility gives you early warning telemetry into new, previously unknown threats.

Why Microsoft 365 and Proofpoint?

The growth in Microsoft 365 adoption and the increase in attacks that target the Microsoft platform makes augmenting any native email security capabilities a high priority. Security needs to cover both inbound and outbound email. It must also provide a modern defense against advanced email threats. The only way to keep your users completely safe is to detect and block malicious messages before they are delivered to the user's inbox. That is why you need to adopt a defense-in-depth approach, which can better protect your users from even the most sophisticated email threats.

By complementing Microsoft 365 native security with the Proofpoint Threat Protection solution, your organization can better protect users and fortify your email defenses against the rising tide of cyberthreats.

To learn more about how to secure your Microsoft 365 infrastructure, then go to **www.proofpoint.com/us/solutions/secure-microsoft-365** or take the free email **rapid risk assessment** today!

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.