proofpoint

E-BOOK

More Secure Together: Proofpoint and Microsoft

Augment Microsoft 365 with advanced threat detection and filtering for spam and graymail

Enhancing Microsoft 365 protection

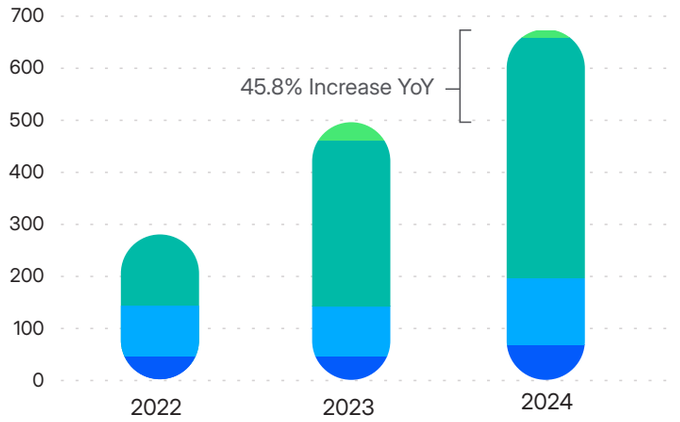
It doesn't matter if you have basic Microsoft email security or you have upgraded to Microsoft Defender for Office 365. As Microsoft 365 becomes the default platform across the enterprise, attacks will only increase. With email as the starting point for a large percentage of today's cyberattacks, strengthening your Microsoft email security should be your top priority.

One of the reasons these trends are so alarming is that email-borne attacks continue to pose a challenge for many organisations, even those using Microsoft's built-in defences. Proofpoint email security assessments reveal that advanced threats can still evade detection. As a result, organisations are still at risk for threats like:

- Advanced phishing
- Malware
- Business email compromise (BEC)
- QR codes
- Malicious URLs
- Telephone-oriented attack delivery (TOAD)

Rising Threats, Relentless Protection

Advanced Threats Detected by Proofpoint in Threat Assessment



3.88% of TOAD threats

63.19% of phishing threats

23.88% of malware threats

9.05% of BEC threats

Advanced protection for evasive cyberattacks

Phishing, URLs and malware

Attackers continue to send a barrage of malicious links and attachments via email, which can only be stopped with advanced email protection.

Proofpoint uses predictive sandboxing, URL extraction, evasion detection, browser isolation and a range of other advanced techniques to achieve the highest efficacy defence against these malicious payloads.

BEC protection

Zero payload impersonation attacks like BEC are among the most challenging to detect because these emails often look like they are legitimate.

Proofpoint NexusAI engines analyse people's relationships and their language while also looking at other potential threat indicators. Header attribute mismatches, DMARC feedback loops and sender behaviour all provide valuable insights that we use to stop BEC threats in their tracks.

TOAD protection

Telephone-oriented attack delivery (TOAD) is also known as callback phishing. In these attacks, cybercriminals send emails that try to trick recipients into calling them at a bogus call centre.

Threats can be challenging to detect because they rarely include malicious payloads. Proofpoint NexusAI engines use machine learning and computer vision to look for known threat indicators to block these threats. These include malicious phone numbers, QR codes and image-based impersonations.

Microsoft customers who want to strengthen their email security overwhelmingly choose Proofpoint; 85% of the Fortune 100—and more than 1.88 million customers worldwide—have chosen us as a trusted security partner.

Proofpoint leads in analyst reports like the Gartner Magic Quadrant. In Gartner's latest *Critical Capabilities for Email Security Platforms Report*, Proofpoint ranked No. 1 in 4 out of 5 use cases.[1]

Proofpoint Core Email Protection stops 99.99% of email threats, spam and graymail. Our multilayered detection stack Proofpoint Nexus combines relationship graphs, machine learning, computer vision and semantic analysis. It's powered by threat data from the more than 3 trillion emails that we scan every year. As a result, it can prevent today's most advanced threats, including:

- BEC
- Account takeovers
- QR code threats
- Impersonation
- Lateral phishing

Core Email Protection does more than stop threats. It also helps security teams, which get streamlined, alert-based workflows and integrated search. What's more, user-reported emails are automatically remediated. And users get coaching in the moment whenever they report a suspicious email.

'The [Proofpoint] platform excels in core email protection due to its robust AI-powered threat detection, multilayered content analysis and advanced sandboxing capabilities.'[2]

GARTNER

1. Gartner. *Critical Capabilities for Email Security Platforms Report*. January 2025.
2. Ibid.

SEG or API? Proofpoint offers choice

Criteria 1: Time to value

When to choose an API

Proofpoint API deployments happen in days. You get automated protection within 48 hours after the system learns from a year's worth of your user data. Our API solution is best for teams that want powerful but low-touch email cybersecurity.

When to choose an SEG

Proofpoint Secure Email Gateway (SEG) deployments can take up to a few weeks. This time investment helps reduce the most risk by enabling pre-delivery, post-delivery and click-time protection. Our SEG solution provides more options for configuring and customising your deployment. It's best for teams that want to maximise protection for their architecture.

Criteria 2: Microsoft orientation

When to choose an API

If you're inclined toward augmenting Microsoft's SEG with post-delivery protection from Proofpoint, then you should leverage our integration with Microsoft's Graph API. The Proofpoint API solution provides a native Outlook user experience for email threats, spam and graymail.

When to choose an SEG

If you're inclined toward replacing Microsoft's SEG, then you should use Proofpoint. Our SEG solution provides pre-delivery, post-delivery and click-time protection through Proofpoint browser isolation.

Criteria 3: Sophistication of email infrastructure

When to choose an API

If you want to use your organisation's Microsoft SEG for mail routing, then you should choose the Proofpoint API solution. The typical API customer has standard, straightforward requirements for their email infrastructure.

When to choose an SEG

If your organisation has a sophisticated email infrastructure, then you should choose an SEG. The typical SEG customer wants to apply policies that control the flow of mail, which are based on conditions like sender domain, authentication and more.

Why Proofpoint?

About Proofpoint

People Protection

3.4T
Emails scanned per year

>1.4T
SMS/MMS scanned per year

124M
BEC attacks stopped per month

>183M
Phishing simulations per year

0.8T
Attachments scanned per year

21T
URLs scanned per year

177M
TOAD attacks stopped per year

Market Adoption

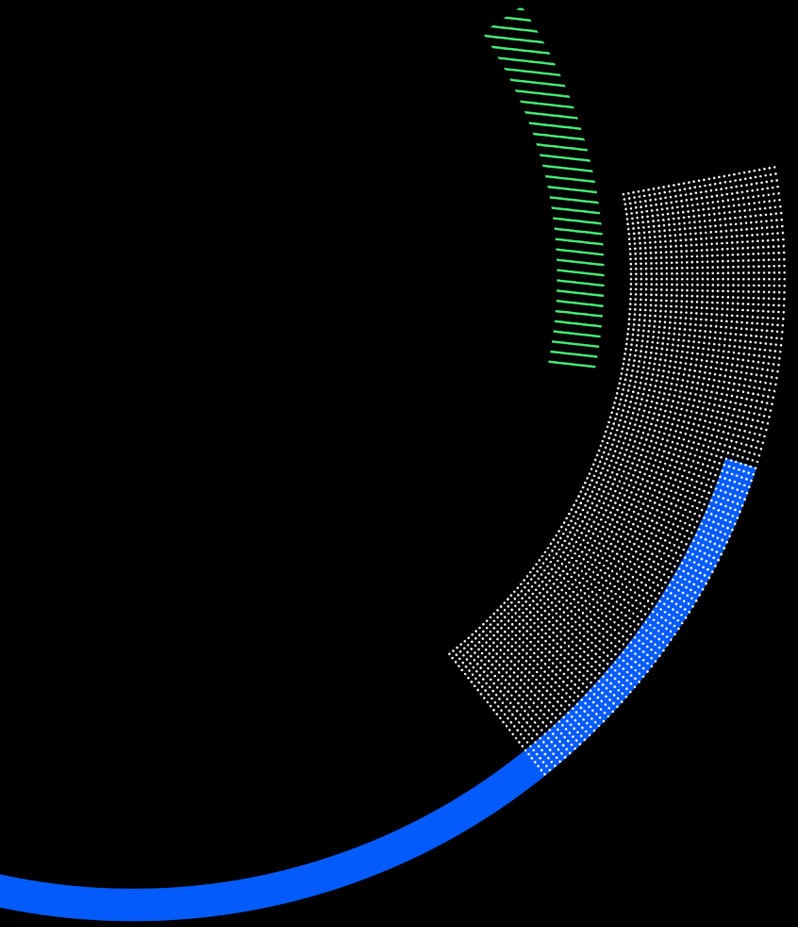
1.88M+
Customers

150+
Global ISP and mobile operators

85%
F100 protected by Proofpoint

50%
F100 using Proofpoint DLP

>60%
F1000 Protected by Proofpoint



proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 cyberattacks. Leading organisations of all sizes, including 85 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.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →