proofpoint®

E-BOOK

Smarter, Faster Email Protection

5 reasons Proofpoint is a leading choice for augmenting Microsoft 365 email security via API

Introduction

Email has long been the No. 1 threat vector. And advanced attacks such as business email compromise (BEC), supply chain risk, ransomware and account compromise are on the rise.

This has led experts such as Gartner and Forrester to recommend augmenting Microsoft 365 with additional security.[1, 2]

To deliver complete email, cloud and data protection, API-based integrated cloud email security (ICES) solutions have sprung up to fill this need. These solutions rapidly deploy to address these advanced attacks head-on.

When Microsoft customers are looking to quickly augment their security, they overwhelmingly turn to Proofpoint. 85% of the Fortune 100—and more than 1.8 million customers worldwide—have chosen us as a security partner. We lead the industry in email and cloud protection.

Proofpoint Core Email Protection API sets a new standard for ICES. Not only does it deliver the next level in threat detection with 99.99% efficacy, but it also provides teams with seamless management tools. It's a future-proof platform that's powered by breakthrough AI technologies in Proofpoint Nexus and our unrivaled global threat intelligence. With Proofpoint, you'll be able to:

- Stop the widest variety of threats with the world's leading AI-based solution
- Realize your most efficient security operations center (SOC)
- Future-proof your security architecture for tomorrow's threat landscape

But those are only a few of the reasons. Here's a full list of why you should choose Proofpoint Core Email Protection API to augment Microsoft 365.

1. Mark Harris, Peter Firstbrook, et al. (Gartner). "Market Guide for Email Security." October 2021.
2. Jess Burn, Joseph Blankenship, et al. (Forrester). "Best Practices: Phishing Prevention." November 2021.

©Proofpoint, Inc. 2025

Reason 1

Stop the widest variety of threats

Threat intel is a key part of detecting and stopping threats. When the algorithms have more data to work with, they're better able to find anomalies.

Proofpoint boasts a unique combination of threat intel. Our multilayered detection stack, NexusAI, is trained by trillions of global data points that have been gathered over 20+ years from thousands of customers. We combine this intel with insights from our threat research team to maximize threat protection for our customers.

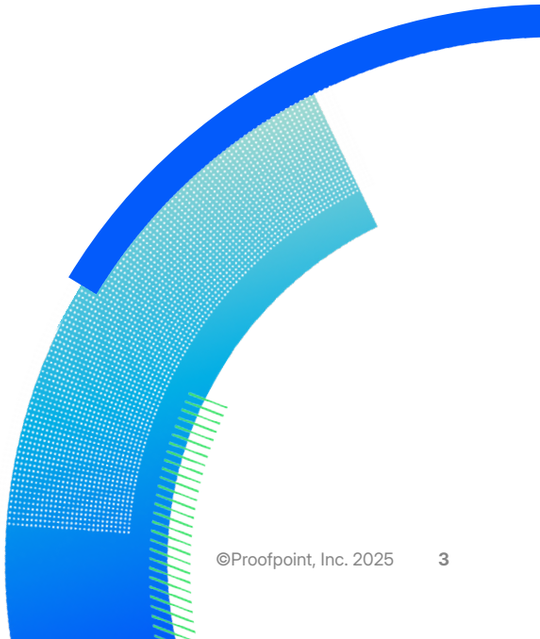
Be more precise

Most API-based solutions only rely on one detection technique, like anomaly detection. This means they often miss actual threats, or they stop legitimate messages from getting through. In contrast, Proofpoint combines AI and ML (AI/ML) techniques with threat intelligence and sandboxing so that our detection engines are more accurate. Because our data sets are comprehensive, we're not only able to see more threats, but we also generate fewer false positives.

Protect your organization from every angle

Proofpoint NexusAI integrates six powerful cores to counter a wide variety of AI-driven threats.

- **Nexus Language Model (LM)** recognizes subtle linguistic patterns and behavioral cues to identify BEC attacks before they can cause harm.
- **Nexus Generative AI** analyzes data across email, cloud and endpoints to identify nuanced patterns in phishing and exfiltration attempts.
- **Nexus Threat Intelligence (TI)** enriches threat detection models by providing real-time updates on attacker tactics, techniques and vulnerabilities.
- **Nexus Relationship Graph (RG)** monitors user behavior across systems, looking for anomalies that signal insider threats or account compromise.
- **Nexus Machine Learning (ML)** powers our predictive threat detection.
- **Nexus Computer Vision (CV)** identifies and neutralizes threats that are hidden in visual elements, such as phishing sites, QR codes, malicious attachments and spoofed emails.



©Proofpoint, Inc. 2025

Reason 2

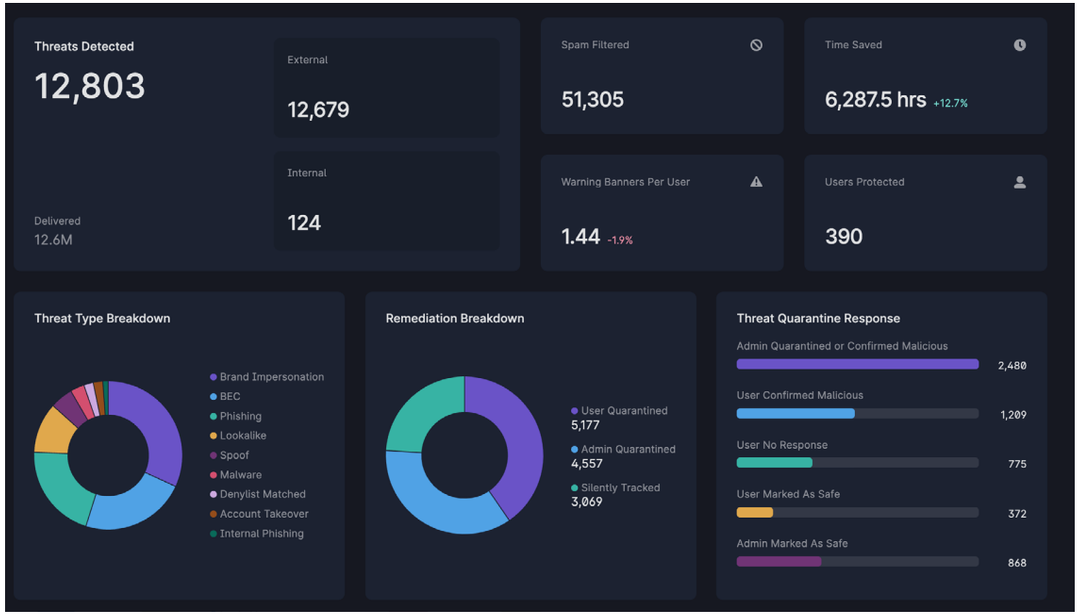
Realize your most efficient SOC

The longer a threat lingers in your Microsoft 365 environment, the more damage it can do. That's why fast, efficient incident response is critical to keeping Microsoft 365 secure.

Proofpoint Core Email Protection API automates email protection and provides high-efficiency workflows for SOC teams. This ensures they can focus on their most important tasks.

Here's how Proofpoint streamlines the SOC:

- **Automates email threat detection, remediation and response.** This reduces the volume of email threats that teams need to investigate.
- **Provides contextual warning banners and real-time coaching.** Warning messages and coaching help users make informed security decisions. This means that admins have fewer potential events to investigate and remediate.
- **Delivers brief threat summaries.** Teams get an intuitive rundown of the most important points for each threat, which is created by generative AI.
- **Speeds up threat hunting and remediation.** Integrated search and alert-based workflows help teams to jump on the right threats quickly and remediate them before they can cause any harm.
- **Deploys rapidly.** Our solution is integrated with the Microsoft Graph API and has an automated learning period of less than 48 hours.



When you choose Proofpoint

99.99% of email threats are stopped before they become compromises

30% fewer email threats need to be handled by the SOC

©Proofpoint, Inc. 2025

Reason 3

Protect against today's most evasive threats

Email threats are constantly evolving and hard to defend against. That's why protecting your people is daunting, even for the most sophisticated organizations. But Proofpoint can help.

With Core Protection API, you can find and stop known and unknown threats across your entire enterprise. This means advanced threats are stopped at the front door, not after they are delivered. These threats include:

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 defense against these malicious payloads.

BEC attacks

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

TOAD threats

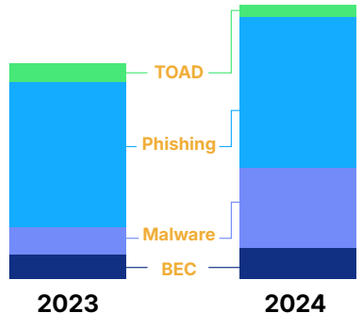
Telephone-oriented attack delivery (TOAD) is also known as callback phishing. In these attacks, cybercriminals send emails that try to trick recipients into calling them at a bogus call center. Threats can be challenging to detect because they rarely include malicious payloads.

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.

+45.8%

increase in threats* delivered to users YoY

*Malicious messages, detected by Proofpoint



124M

Number of BEC attacks that Proofpoint blocks every month

45%

Annual increase in email threats delivered to end users

9M

Number of TOAD attacks that Proofpoint blocks every month

©Proofpoint, Inc. 2025

Reason 4

Get the best user experience

When it comes to securing email, the best experience you can provide for users is one that's invisible. Our 99.99% detection rate gets you close. Proofpoint minimizes distractions for users across threats, spam and graymail.

With Core Email Protection API, you can provide users with:

- A native Outlook user experience for spam and graymail
- Fewer disruptions with industry-leading detection efficacy and rapid remediation
- Contextual user warnings to coach users in real time

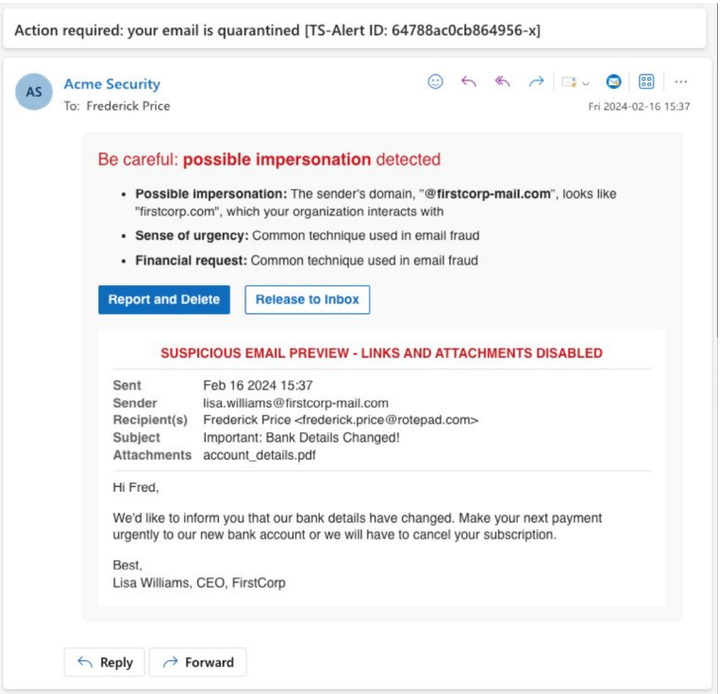
Deliver native Outlook user experiences

Today's users are overwhelmed with the volume of emails they receive daily. Proofpoint turns down the noise by automatically moving spam and graymail from the inbox to the default Microsoft junk folder.

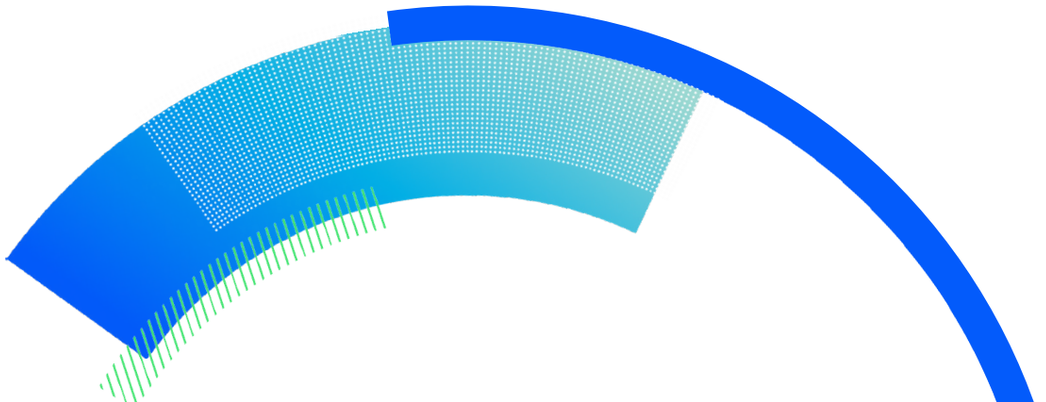
Users can drag and drop the messages that they want back to their inbox. This prevents emails from those senders from being marked as spam or graymail in the future.

Keep users and security teams productive

Core Email Protection API helps employees stay productive by delivering low-medium risk emails safely. These messages include real-time coaching to help users make informed security decisions and learn from their mistakes. As a result, admins have fewer potential events to investigate and remediate.



Real-time user coaching for suspicious emails.



©Proofpoint, Inc. 2025

Reason 5

Future-proof your security architecture

Proofpoint helps you reduce risk everywhere that your people interact—today and in the future. We protect your organization from attackers that impersonate your employees, partners and vendors, and we prevent both accidental and intentional data loss. Plus, we integrate with a wide range of tools to help you automate and consolidate across your security stack.

Our platform integrates with best-in-class security vendors, such as Palo Alto Networks, Okta, CrowdStrike and many more.

Consolidate vendors to improve your ROI

When you choose Proofpoint to augment Microsoft 365, you also get access to our comprehensive solutions that go beyond protecting your organization from email attacks. This means you can give your team leading-edge tools to streamline their workflows.

With Proofpoint, you get security that extends across your people, your data and your whole organization.

Stop human-targeted threats

- Protect email against malware, phishing and BEC
- Prevent impersonation and supplier compromise attacks
- Protect collaboration tools against credential and malware attacks

Safeguard your data and digital communications

- Prevent your users from putting data at risk by mistake
- Detect malicious insider activity and get real-time alerts
- Govern all your digital communications

Guide your people to better security choices

- Provide risk-based, tailored training
- Simulate attacks to assess how resilient your users are
- Encourage the right behavior with real-time nudges across email and web

Contain SaaS and identity sprawl

- Detect and respond to account takeover threats
- Proactively follow and understand attack paths through Active Directory
- Detect software-as-a-service (SaaS) accounts and reverse posture drift

©Proofpoint, Inc. 2025

Work with an industry leader

With Proofpoint, you don't have to choose between best-in-breed technology and a fully integrated solution. We're a proven industry leader across cybersecurity, data loss protection (DLP) and compliance.

Industry Analyst Recognition for Core Email Protection

Gartner

- **A Leader**
  2024 Magic Quadrant for Email Security Platforms
- **#1 in 4 of 5 Use Cases**
  In the 2024 Magic Quadrant for Email Security Platforms:
  - Core Email Protection
  - Outbound Security
  - Security Platforms
  - Power Users

FORRESTER®

- **The Forrester Wave™:**
  Enterprise Email Security, Q2 2023 | Leader

FROST & SULLIVAN

- **2023 Frost Radar™:**
  Email Security, 2023: Email security Market and Growth Index leader on the Frost Radar™ for the 9th year in a row
- **2024 Frost & Sullivan**
  Company of the Year Award Global Email Security Industry & Excellence in Best Practices
- **2025 Frost & Sullivan**
  Company of the Year Award | Australian Email Security Industry Excellence in Best Practices

GIGAOM

- **2023 GigaOm Radar for Anti-Phishing:**
  Positioned as a Leader and Fast Mover
- **2024 GigaOm Radar for Identity Threat Detection and Response:**
  Positioned as a Leader and Fast Mover
- **2024 GigaOm Radar for Deception Technology:**
  Positioned as a Leader and Fast Mover

kuppingercole ANALYSTS

- **2023 Leadership Compass for Email Security:**
  Leadership in all four categories: Overall, Product, Innovation and Market

OMDIA

- **2024 Omdia Universe Email Security:**
  Leader

- **2024 Radicati Market Quadrant for Email Security:**
  Top Player

proofpoint

© 2025 Proofpoint, Inc

Take the next steps

The best cyber defense is one that stops threats where they start. That's why more than 1.8 million customers worldwide have chosen us as their security partner.

Proofpoint Core Email Protection API 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.

Core Email Protection API 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.

Learn more about how Proofpoint can help you augment your Microsoft 365 email and cloud security.

proofpoint.com/us/products/threat-defense

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

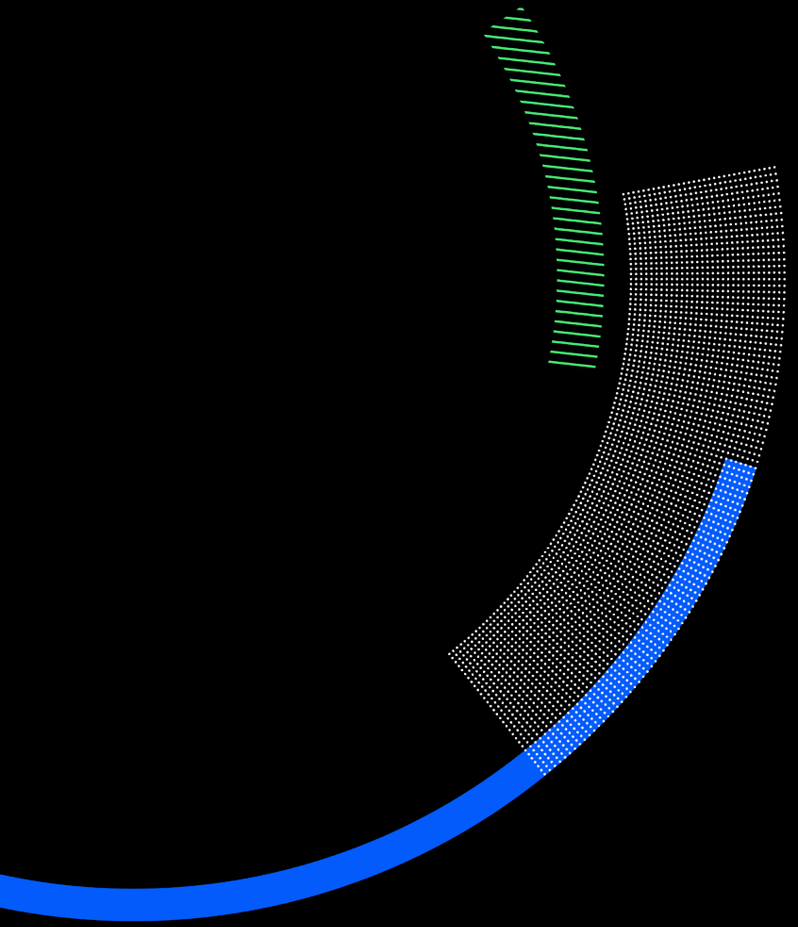
150+
Global ISP and mobile operators

85%
F100 protected by Proofpoint

50%
F100 using Proofpoint DLP

>60%
F1000 protected by Proofpoint

©Proofpoint, Inc. 2025



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 cyberattacks. Leading organizations of all sizes, including 85% 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

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

DISCOVER THE PROOFPOINT PLATFORM →

©Proofpoint, Inc. 2025