proofpoint.

Proofpoint Threat Protection

## Protect your people from today's modern threats

Key Benefits

- Detect and block modern email threats faster
- Stop emerging threats more accurately with continuous AI
- Get insights on your human and threat risks
- Improve operational effectiveness
- Empower your people and drive behavior change

Email is the primary threat vector for cybersecurity threats. And these days, there are many malware, phishing and social engineering schemes that target your people. According to 2023 Verizon Data Breach Investigations Report, 74% of all data breaches include a human element. With Proofpoint Threat Protection, your organization can protect your people from today's modern threats.

Cybercrime is a growth business

Cybercrime is a growth business because the returns are great and the risks are low. According to Cybersecurity Ventures, the cost of cybercrime is projected to hit an annual $10.5 trillion by 2025. Cybercrime organizations run just like regular enterprises whose motivation is financial gain. Bad actors seek to steal valuable personal and corporate information, commit identity theft, and launch attacks aimed at committing financial fraud through email. And because email is a fundamental cornerstone of modern business, it is the No. 1 threat vector targeting your people. What's more, these threats are constantly evolving and hard to defend against. This is why protecting your people from these modern threats is daunting, even for the most sophisticated and complex organizations. But Proofpoint can help.

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.
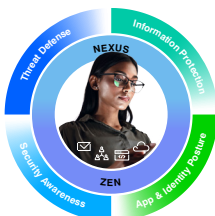
1   Verizon. *2023 Data Breach Investigations Report*. 2023.
2   Steve Morgan (*Cybercrime Magazine*). "Cybercrime To Cost The World 8 Trillion Annually In 2023." October 2022.

84%

of the Fortune 100 trust Proofpoint to protect their people from threats.

Source: Proofpoint, 2023

Detect and stop email threats faster with pre-delivery detection

With our pre-delivery detection, you can find and stop known and unknown threats across your entire enterprise. This means sophisticated threats are stopped at the front door, not after they are delivered. These threats include:

- Advanced credential phishing

- Malware

- Ransomware

- Business email compromise (BEC)

- Malicious URLs

- QR codes

- Attachments

- And more

When this is combined with our automated post-delivery detection and remediation, your organization can holistically protect your people with a single, comprehensive solution.

Identify threats with AI-driven, multilayered detection

We use a multilayered detection stack that comprises threat intelligence, machine learning, behavioral AI, sandbox detection, content and semantic analysis (LLMs). These work together to detect multiple types of modern threats. As a result, the stack delivers a high-fidelity detection rate of 99.99% with better threat explainability. And unlike single-layered detection email security solutions, it yields fewer false negatives and fewer false positives because it can more accurately stop malicious messages without blocking good messages and impeding your business.

Figure 1: Proofpoint AI-driven, multilayered, pre-delivery detection in action.

Get comprehensive people-risk and threat visibility

With Proofpoint, you get unique insights into your Very Attacked People™ (VAPs) and the threats targeting them. In doing so, you can implement targeted adaptive controls. These include browser isolation, security awareness training, step-up authentication and more. And combined with our people-risk visibility, you gain valuable knowledge about your people—how attacked they are, how vulnerable they are and what privileges they have. Also, Proofpoint analyzes over 3 trillion email messages per year across our 230,000+ customer, partner and provider ecosystem. Our threat intelligence and research provides you with early warning telemetry into new, previously unknown threats.

Improve operational efficiencies

With Proofpoint, you can automatically detect and remediate malicious emails post-delivery. This automation of the triage process and removal of messages containing deceptive payloads helps you to identify and resolve threats faster and more efficiently. Whether these unwanted emails are from internally compromised accounts or have been forwarded or received by other users, Proofpoint provides you

with automated alerts, comparison threat analysis and actionable views of threats. This reduces your remediation time. It also lightens your team's workload, making them more efficient. In addition, users can easily report suspicious messages with one click from an email warning tag or a phish alarm email button. If a user-reported message is found to be malicious, then it and all other copies are quarantined automatically. In turn, users receive an email notification that lets them know the message was malicious and automatically removed. This closed-loop notification helps to reinforce future behavior to report similar messages.

Empower your people and drive behavior change

Proofpoint helps you further mitigate your people risk by changing unsafe behavior and building sustainable security habits. We use our rich threat intelligence to inform your program in various ways. These include designing real-world phishing simulations, enabling threat-guided training that allows you to educate your top clickers and most attacked, and automating threat investigation of user-reported email. We help you keep users engaged by providing you with personalized learning experiences. Our adaptive approach helps your people retain what they learn and cultivate positive and lasting security habits. And we allow you to better communicate your people risk and program impact to your leadership team by tracking real-world behavior change and benchmarking it against your industry peers.

Figure 2: Proofpoint provides people-risk visibility into your Very Attacked People™ (VAPs).

Proofpoint managed service offerings

Proofpoint provides the following managed services for Proofpoint Threat Protection:

- **Managed Email Threat Protection—**Get proactive expertise, staffing continuity, and executive insights via hands-on management of your email security solution. We also provide you with day-to-day operational checks and proactive application of threat intelligence.

- **Managed Abuse Mailbox—**Reduce the burden of manual reviews of user-reported email messages. Our team performs analysis and assigns definitive dispositions to all unclassified reported messages.

- **Managed Security Awareness—**Elevate and evolve your approach to user security education. We guide your program strategy with a focus on behavior change and building a more resilient security culture.

For more information, visit: proofpoint.com/us/products/protect-people.

Learn more at proofpoint.com