# Proofpoint Solution Bundles

## Protect people. Defend Data.

Proofpoint provides a unique people-centric approach to cybersecurity. This starts with understanding your Very Attacked People™ (VAPs) and assessing the risk they pose to your organization. Our threat protection and information protection solution bundles provide holistic solutions that address the modern threat landscape, extend your resources and progress with you as you elevate your security strategy. This document provides an overview of these solution bundles and explains how they can help you protect your people and defend you data.

## AI/ML Innovation Powered by Nexus Threat Graph

Proofpoint uses artificial intelligence (AI) and machine learning (ML) to protect people and defend data. AI and ML are weaved throughout our product suite to give customers complete and constantly evolving protection against a wide range of external threats. We harness nearly two decades of AI, ML and data science experience in the AI platform that powers Proofpoint products. This allows the products to effectively address a broad spectrum of cybersecurity and compliance risks.

Our Threat Intelligence and Detection stack breaks through the market with ML models trained by the trillion-plus node Proofpoint Nexus Threat Graph. Nexus Threat Graph has access to massive cybersecurity data sets across email, cloud, networks, domains and more. Our integrated data science team includes doctorates and master's degree holders in computer science from cybersecurity, government and academia. We've partnered with leading universities to be at the cutting edge of data science. This team works across our threat protection, information protection and archiving and compliance products in collaboration with threat researchers. The collaboration maximizes the effectiveness of our machine learning.

# Proofpoint Threat Protection Bundles—Protect Your People

Protect your people from the threats that target them. By integrating multiple controls across email, cloud, users and suppliers, the Proofpoint Threat Protection platform provides a comprehensive way to defend against phishing, BEC email fraud, malware and ransomware. An integrated, AI-powered platform, it provides unparalleled visibility into your attack surface, more effective protection against modern threats and positive operational outcomes. All bundles are available in easy-to-deploy inline+API or MX-based offerings. And all offer the same powerful protection.

## Proofpoint Threat Protection Overview

| CAPABILITIES | | PX | P0 | P1 | P1+ |
|---|---|---|---|---|---|
| Deployment and Management | • On-premises hybrid or cloud<br>• Inline+API or MX-based | • M365 cloud only<br>• Inline+API only | ✓ | ✓ | ✓ |
| Business Email Compromise | AI/ML, behavioral and reputation | ✓ | ✓ | ✓ | Supplier Risk Dashboard |
| Phishing, Ransomware and Malware | AI/ML, behavioral and reputation | ✓ | ✓ | ✓ | ✓ |
| | URL rewriting and click-time sandboxing | | ✓ | ✓ | ✓ |
| | Attachment sandboxing | | ✓ | ✓ | ✓ |
| Account Takeover | Account takeover visibility | ✓ | ✓ | ✓ | ✓ |
| | Post-access investigation in timeline view | + | + | + | + |
| | Remediate email and cloud environments | + | + | + | + |
| Email Reporting and Remediation | Automated mSOAR | ✓ | ✓ | ✓ | ✓ |
| | Automated abuse mailbox | ✓ | ✓ | ✓ | ✓ |
| | User email reporting | ✓ | Email Warning Tags | | |
| Threat and User Dashboards | Threat insights including VAPs | ✓ | ✓ | ✓ | ✓ |
| | User risk dashboard | | ✓ | ✓ | ✓ |
| Inbound Hygiene and Configuration | Antispam, antivirus and graymail | ✓ | ✓ | ✓ | ✓ |
| | Executive/VIP features | | ✓ | ✓ | ✓ |
| | Customized policies | | ✓ | ✓ | ✓ |
| User Defense-in-Depth | Isolate rewritten email clicks | + | VAPs | | All |
| | Security awareness training | + | + | ✓ | ✓ |
| Email Authentication and Internal Protection | DMARC implementation, insights | + | + | + | ✓ |
| | Internal email threat protection | + | + | + | <5,000 users |

| LEGEND |  |
|---|---|
| ✓ | Included with bundle |
| + | Available with added cost |

## Threat Protection Bundle Descriptions

| BUNDLE | OVERVIEW | DESCRIPTION | INCLUDES |
|---|---|---|---|
| PX | Fast and easy AI-powered email protection for Microsoft 365.<br><br>Best for smaller organizations looking to augment native M365 security while simplifying email security administration with preconfigured settings. Deployed in minutes with inline+API. | Proofpoint PX is only available for cloud Microsoft 365 instances. It is the fastest, easiest way to get industry's best email and cloud security. Using ML, behavioral analytics and threat intelligence, PX accurately detects, blocks and remediates spear phishing, business email compromise (BEC), supply chain and ransomware attacks that bypass Microsoft security. | AI-powered detection and automated remediation to complement native Microsoft defenses |
| P0 | Advanced email and cloud security.<br><br>Best for organizations with more targeted threats and those that need additional customization and configuration | Resolve your email threats across the entire attack chain, from detection to response. This includes the ability to automate abuse mailbox management by removing malicious user-reported phishing emails. This addresses threats such as phishing, business email compromise (BEC), supplier fraud, ransomware and other malware. This solution helps you gain visibility into who is being attacked, how they are being attacked, whether they click on or report phishing and whether they are compromised | Everything in PX and:<br><br>• More flexible deployment options (hybrid or on-premises)<br>• Mail flow management with customization using full admin console<br>• Advanced click-time protection for attachment and URL attacks, including URL isolation for VAPs<br>• HTML warning tags with report suspicious capabilities<br>• User email hygiene including antispam, antivirus, graymail and user mail controls<br>• Integrated user risk dashboard with recommended controls (Nexus People Risk Explorer) |
| P1 | Advanced threat protection.<br><br>Best for organizations needing educated users with additional integrated, defense-in-depth capabilities. | Train end users to be more resilient against threats they receive. Augment threat protection with a robust security awareness training program that integrates with your email security controls and includes phishing simulations, cultural and knowledge assessments, comprehensive training and awareness materials.<br>Tailor the training curriculum delivered to your users based on the actual threats they receive. Use the full catalog of interactive training and tools designed to change end user behavior. Capabilities include threat simulations that test user response to phishing attacks using thousands of templates, more than 40 languages and 13 categories. These can help establish a security baseline, train employees to avoid security risks and report progress. The progress of your program can be visualized in a special CISO dashboard. This emphasizes the metrics that senior security leaders care about the most. | Everything in P0 and Security Awareness Training Enterprise |

| BUNDLE | OVERVIEW | DESCRIPTION | INCLUDES |
|---|---|---|---|
| **P1+** | Complete email and cloud threat protection.<br><br>Best for enterprises that need advanced email and cloud protection via defense-in-depth capabilities and insights | Increase protection from email and domain fraud, including BEC, to stop inbound and outbound email spoofing attacks sent on your organization's behalf. BEC attacks can use several identity deception tactics. You need a multilayered security approach that works to protect your employees, customers and business partners. Proofpoint's integrated BEC solution addresses all threat tactics, provides visibility across your email ecosystem and gives you controls to stop these attacks before they reach the inbox.<br>Go beyond DMARC to expose fraud risks posed by your suppliers. Proofpoint provides this unique visibility into supplier vendor risk to help you overcome the challenge with complex supply chain attacks. Automatically identify your suppliers and assess the risk level of the domains they use to send email to your users. By integrating data across the threat protection platform, we reveal the message volume, the threats detected from supplier domains, as well as the messages blocked from malicious lookalikes of your suppliers' domains.<br>Additionally, organizations with fewer than 5,000 users can also benefit by gaining real-time visibility and automatically responding to internal email threats sent from compromised accounts. You can quickly identify which accounts are compromised and who is being impacted. | Everything in P1 and:<br><br>• Email Fraud Defense (EFD)<br>• Supplier Risk Explorer<br>• TAP URL Isolation for all users<br>• Internal Mail Defense for organizations with fewer than 5,000 users |

## Proofpoint Information Protection Bundle—Defend Your Data

Modernize your data loss prevention (DLP) solution with our Proofpoint Enterprise DLP bundle. This bundle takes a people-centric approach. It brings together rich context on content, behavior and threats for actionable insights into and prevention of data loss. Equip your security and compliance teams with telemetry across email, cloud and endpoint. This allows them to address the complete range of people-centric data loss scenarios—all in a single solution.

Enterprise DLP includes:

- **Email DLP.** Provides data loss protection with built-in policies, file fingerprinting and smart-send remediation.
- **Cloud App Security Broker (CASB).** Provides cloud threat protection and cloud DLP, including oversharing of sensitive data, third-party app control and support for handling shadow IT.
- **Endpoint DLP and Insider Threat Management (ITM).** For 3% of users. Mitigate insider risk with this lightweight endpoint agent. Prevent malicious and negligent user behavior from employees, privileged users and third parties.

### LEARN MORE
For more information, visit **proofpoint.com**.

**proofpoint.**