Proofpoint Products and Solutions

Proofpoint gives you protection and visibility for your greatest asset and security risk—your people. We deliver the most effective tools available to protect against the threats that target people, to protect the information they create and access, and to protect the users themselves.

Our cybersecurity and compliance solutions span email, social media, the web, networks, and cloud platforms, including Microsoft Office 365. We also have strategic technology integrations with the industry's best security providers. This helps you better protect your people, data and brand.

This document describes the solutions that Proofpoint offers in its product and service lines. The document groups the solutions by platform, service type and solution bundles.

Contents

Proofpoint Aegis

Proofpoint Aegis is the only AI/ML-powered threat protection platform that disarms today's advanced attacks, including BEC, phishing, ransomware, supply chain threats and more.

Aegis Threat Protection Solutions

PRODUCT	DESCRIPTION
Proofpoint Digital Risk Protection	Proofpoint Digital Risk Protection secures both your organization and your brand against digital security risks across web domains, social media and the deep web. It protects corporate domains from brand fraud; secures and monitors social media accounts for phishing, account takeovers and spam; and monitors deep and dark web activity for executive threats, credential leaks, locations for physical attacks and nearby high-impact events. Digital Risk Protection uses machine learning (ML) to help users get in front of threats—whether the threats are planned, imminent or occurring in real time.
Proofpoint Email Fraud Defense	Proofpoint Email Fraud Defense provides visibility into all emails that use your domain—including messages from third-party senders—to help protect you from identity deception tactics. It identifies suppliers who may be impersonated or compromised. Email Fraud Defense helps you protect your company's reputation in email fraud attacks. It also simplifies your DMARC journey with consultants. And it allows you to achieve DMARC compliance effectively with hosted authentication service.
Proofpoint Email Isolation	Proofpoint Email Isolation lets users freely access personal webmail and corporate email from corporate devices without security concerns. It uses cloud-based remote browser isolation technology to allow this, without exposing your organization to malware and data loss. Email Isolation helps solve the security and productivity challenges that come with targeted phishing attacks and high-risk personal webmail use. When your people click on URLs in corporate email or webmail, Email Isolation renders the page in a secure container off your network. This keeps harmful content out of your environment. Users can view and interact with their web page as normal. But malware and other harmful content are removed from the page. Uploads and downloads may also be controlled to prevent data theft and loss.
Proofpoint Email Protection	Proofpoint Email Protection uses machine learning (ML) and multilayered detection techniques to identify and block malicious email. It protects users against unwanted and malicious email—both malware and non-malware threats—such as impostor email or business email compromise (BEC). Email Protection catches both known and unknown threats that others miss. With this solution, your security teams can control all aspects of inbound and outbound email and set up granular policies to better protect users from myriad email threats.

PRODUCT	DESCRIPTION
Proofpoint Emerging Threats Intelligence	Proofpoint Emerging Threats Intelligence is the most timely and accurate source of threat security intelligence. It helps you with threat discovery, security enforcement, threat hunting, engaging in incident response or enriching other solutions. It combines actionable information, including up-to-the-minute IP and domain reputation feeds, with a database of globally observed threats and malware analysis. Emerging Threats Intelligence gives your security teams the intelligence they need to stop malicious attacks and the context to investigate them. It helps your teams understand the deeper, historical context about the origin and author of a threat and integrates seamlessly with their security tools. Unlike other intelligence sources that report only domains or IP addresses, Proofpoint intelligence includes a 10-year history of proof of conviction, with more than 40 threat categories and related IPs, domains and samples.
Proofpoint Emerging Threats Pro Ruleset	Proofpoint Emerging Threats Pro Ruleset is a timely and accurate rule set that detects and blocks threats using your existing network security appliances. Examples of these may include next-generation firewalls, network intrusion detection systems (IDS) and intrusion prevention systems (IPS). It is updated daily and is available in SNORT and Suricata formats. It covers more than 40 different categories of network behaviors, malware command and control, DoS attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols, exploit kit activity and more.
Proofpoint Internal Mail Defense	Proofpoint Internal Mail Defense protects your organization's internal email and helps detect compromised accounts. It also gives your security team visibility into the email senders so it can quickly track down and act on potentially compromised accounts. Internal Mail Defense provides a robust, multilayered approach to cybersecurity that protects your people from advanced threats in internal email.
Proofpoint Secure Email Relay	Proofpoint Secure Email Relay consolidates and secures transactional email from applications. It enables third parties sending on your behalf to send DMARC-compliant email, accelerating full DMARC implementation. Options include message archiving, payload encryption and data loss prevention (DLP) to protect sensitive data in your application email. Secure Email Relay prevents compromised third-party senders from sending malicious email using your domains and enables DKIM signing to help you meet DMARC compliance and achieve your cloud migration initiatives.
Proofpoint Security Awareness Enterprise	Proofpoint Security Awareness Enterprise is a training package designed for enterprise and multinational organizations that educates users to be more resilient against cybersecurity threats. It includes everything in the Proofpoint Security Awareness Standard package. And it provides all content available, with a wide variety of styles and formats to fit your culture. It also includes content translations and localization in more than 40 languages. With Proofpoint Targeted Attack Protection (TAP), you can use the TAP Guided Training integration to run more focused programs based on real user risk from their email environment. This package includes an option to automate the removal of user-reported malicious emails with Proofpoint Closed-Loop Email Analysis and Response (CLEAR). And it helps you better understand user risk by integrating user vulnerability data into Nexus People Risk Explorer. Security Awareness Enterprise helps you tackle one of the most pressing concerns of every organization: reducing the security risk that people pose.

PRODUCT	DESCRIPTION
Proofpoint Security Awareness Standard	Proofpoint Security Awareness Standard is a training package that engages users and drives behavior change to ensure they have the right response to security or privacy threats. It lets you choose from a variety of microlearning modules, customizable training, phishing templates and educational materials. It includes Proofpoint's PhishAlarm email reporting add-in, as well as Proofpoint's threat detection stack, which automatically analyzes user-reported messages and delivers dispositions of those messages to administrators to save time and accelerate threat response. The CISO Dashboard makes it easy for administrators to demonstrate program performance to stakeholders, benchmark against peers and optimize future effort. Proofpoint Security Awareness Standard enables organizations to deploy engaging awareness programs and reduce IT overhead.
Proofpoint Targeted Attack Protection	Proofpoint Targeted Attack Protection (TAP) detects, analyzes and blocks advanced threats and gives you the insight you need to identify and protect your most targeted people. It provides in-depth analysis and protection against emails that contain malicious URLs, attachments or business email compromise (BEC) threats. It offers detailed forensics as well as in-depth visibility into your Very Attacked People™ (VAPs), VIPs, company-level attack risk and threat objectives. It also surfaces details of cloud account compromise and file-sharing activity in Microsoft 365 and Google Workspace. And it identifies risky third-party applications. Proofpoint TAP offers unique visibility into advanced threats that target your people so you can optimize your response to them.
Proofpoint Threat Response	Proofpoint Threat Response is a security, automation and response (SOAR) solution that helps your security teams respond faster and more efficiently to the dynamic threat landscape. It automatically confirms malware infections, checks for evidence of past infections and enriches security alerts by automatically adding internal and external context and intelligence. Threat Response is designed for security operations teams working toward security maturity. It takes the manual labor and guesswork out of incident response, which helps your teams resolve threats faster and more efficiently.
Proofpoint Threat Response Auto-Pull	Proofpoint Threat Response Auto-Pull (TRAP) recalls malicious emails already delivered to a user's inbox. It also generates reports showing quarantine attempts, successes and failures, and a list of users who are targeted the most. Proofpoint TRAP reduces the workload of your security team. It takes the manual labor and guesswork out of incident response, helping your team resolve threats faster and more efficiently.

Proofpoint Sigma

Proofpoint Sigma is the only information protection platform that merges content classification, threat telemetry and user behavior across channels in a unified, cloud-native interface.

Sigma Information Protection Solutions

PRODUCT	DESCRIPTION
Proofpoint Browser Isolation	Proofpoint Browser Isolation is a remote browser isolation technology that secures the web browsing and email activities of your users. It allows your people to access websites and their personal and corporate email freely, without exposing your organization to malware and data loss. Browser Isolation helps solve the security, productivity and privacy challenges that come with browsing malicious websites, targeted phishing attacks and high-risk personal webmail use. When your people browse to a risky website or click on a URL in corporate email or webmail, Browser Isolation renders the page in a secure container off your network and off your users' device. This keeps harmful content out of your environment. Users can view and interact with an isolated web page as normal, but malware and other harmful content are removed from the page.
Proofpoint Cloud App Security Broker	Proofpoint Cloud App Security Broker (CASB) provides cloud apps with people-centric threat protection, data security (including data loss prevention) and cloud app governance. It supports both application programming interface (API) and proxy-based deployment models. Proofpoint CASB protects users from cloud account takeovers and malicious cloud files. This helps you stay privacy and data security compliant by safeguarding sensitive data and governing cloud and OAuth apps.
Proofpoint Email Encryption	Proofpoint Email Encryption uses policy-based encryption to make secure communication via messages and attachments seamless and automated for users. Proofpoint Email Encryption allows you to protect sensitive email messages while ensuring that your affiliates, business partners and users have seamless access to secured messages on computers or mobile devices. While traditional encrypted email services can be challenging for users, with Email Encryption, they do not need to manually encrypt their email to send and receive messages, as this occurs in the background.
Proofpoint Endpoint Data Loss Prevention	Proofpoint Endpoint Data Loss Prevention (DLP) mitigates the risk of sensitive data loss through email and ensures compliance by enforcing policy-based prevention and encryption. Our solution is easy to deploy with. With built-in reporting and analytics, it helps you detect and prevent data movement that could lead to data loss and theft. It also helps you triage, respond to and manage risky actions quickly. Proofpoint Endpoint DLP protects against data loss and brand damage involving insiders who act maliciously, carelessly or unknowingly.

PRODUCT	DESCRIPTION
Proofpoint Enterprise Data Loss Prevention	Proofpoint Enterprise Data Loss Prevention (DLP) is a solution bundle that modernizes your DLP solution with our people-centric approach. It brings together rich context across content, behavior and threats to provide people-centric insights into data loss and prevent it from happening. The bundle includes: • Email DLP • Cloud App Security Broker • Endpoint DLP • Insider Threat Management (for 3% of users) Enterprise DLP equips your security and compliance teams with telemetry across email, cloud and endpoint to address the complete range of people-centric data loss scenarios in a single solution. **NOTE:** Enterprise DLP is also cross-listed under the Solution Bundles and Nexus People Risk Explorer section.
Proofpoint Insider Threat Management	Proofpoint Insider Threat Management helps you protect sensitive data from insider threats and data loss at the endpoint. It combines context across content, behavior and threats to provide you with deep visibility into user activities. And it protects against data loss and brand damage involving insiders acting maliciously, carelessly or unknowingly. Insider Threat Management addresses some of the most common problems that security teams have when dealing with insider threats. It helps streamline their responses to incidents and provides them with a wealth of information so they can prevent more of them from happening in the first place.
Proofpoint Intelligent Classification and Protection	Proofpoint Intelligent Classification and Protection is our artificial intelligence (AI) powered data discovery and classification solution. It takes inventory of your content in today's most common workplace productivity platforms. Its AI engine analyzes and classifies that content and can then recommend how best to prioritize its protection. Intelligent Classification and Protection mitigates your data security risk by giving you complete visibility into and control of your business-critical data. It augments your existing data loss prevention (DLP) programs. And together with Proofpoint Information Protection solutions, it can be a solid part of your people-centric strategy to protect against data loss caused by careless, compromised and malicious users.
Proofpoint Web Security	Proofpoint Web Security protects your users against advanced threats when they browse the web. It inspects all internet traffic, including encrypted traffic, to seamlessly deliver access control to users. Web Security supports your distributed workforce by ensuring secure internet access for all of your workers, whether they're inside or outside of your perimeter. It enforces your organizations' acceptable use policy and controls access to cloud applications to help with the issue of shadow IT. It integrates with our threat intelligence, making it easier for you to block the most sophisticated, web-borne threats. It also enforces inline and real-time DLP, preventing data loss from the web channel.

Proofpoint Identity Threat Defense

Solutions in the Proofpoint Identity Threat Defense platform detect and prevent identity risk to stop lateral movement and privilege escalation.

Identity Threat Defense

PRODUCT	DESCRIPTION
Proofpoint Shadow	Proofpoint Shadow detects attackers trying to move laterally within your organization. It accelerates this detection by deterministically identifying threats based on attacker interaction with deceptions. It transforms every endpoint into a web of deceptions. And it uses the attackers' interactions with these deceptions to track their movement. Shadow consistently identifies attacks that often bypass signature and behavioral approaches to detection.
Proofpoint Spotlight	Proofpoint Spotlight automatically discovers and remediates identity vulnerabilities before attackers can exploit them for unauthorized lateral movement and privilege escalation. Spotlight prevents attacks by taking away what attackers need to complete their crime: privileged account access.

Proofpoint Intelligent Compliance

Proofpoint Intelligent Compliance is a platform of solutions for compliance and archiving. These solutions help you make more informed compliance decisions, manage information risk and improve investigation readiness.

Intelligent Compliance

PRODUCT	DESCRIPTION
Proofpoint Archive	Proofpoint Archive is an intelligent cloud archiving solution that quickly surfaces insights and proactively reveals risks in the most complex enterprise data infrastructures. It immutably retains, discovers, supervises and safeguards modern digital communications for comprehensive enterprise and regulatory compliance.
	Archive helps you address all your basic e-discovery requirements by ensuring your data is secure with SSAE-18 SOC 2 Type II certification for its fully managed service and the Proofpoint facilities that host the service. The data is protected both in transit from your data source and while under management within our cloud infrastructure.
Proofpoint Automate	Proofpoint Automate is an add-on to Proofpoint Archive with Supervision that uses machine learning (ML) models to eliminate supervision of low-value content.
	Automate reduces the time and cost your people spend on manually reviewing electronic communications to ensure regulatory compliance. It helps to lessen reviewer fatigue and reduce the number of human errors that can result from that fatigue. This mitigates compliance risk and improves ROI when it comes to supervising users.
Proofpoint Capture	Proofpoint Capture captures content from a variety of sources and delivers it to your data store or downstream services for record-keeping and compliance. It unites and normalizes feeds across public social media, enterprise collaboration apps, instant messenger chats, text messaging and more. It also keeps track of updates to source platforms and ensures that connections are up to date.
	Capture helps you meet regulatory or corporate governance requirements by allowing you to capture and retain content efficiently from all the tools your employees use to communicate.
Proofpoint Discover	Proofpoint Discover is an add-on to Proofpoint Archive that offers advanced features to help modernize the orchestration of your response to e-discovery requests. It addresses all your basic e-discovery needs by providing robust, built-in features for search, litigation hold and export.
	Discover empowers your legal teams with self-service control over e-discovery to reduce time, cost and risk. It automates the mundane task of searching for and reviewing data, allowing you to respond confidently and promptly to e-discovery requests and internal investigations.
Proofpoint Patrol	Proofpoint Patrol provides full visibility into the social activity of your employees and customers and allows you to act quickly when problems arise. It lets you monitor, remediate and report on social media compliance at scale. It also features intelligent classifiers, automated workflows and intuitive reporting.
	Patrol helps your social compliance teams to be more efficient by simplifying compliance for social media communications. You can free up valuable resources by streamlining review and approval workflows for social profiles. And your employees can freely engage with clients by continuing to use the same tools they do now as well as monitor customer communications and posts.

PRODUCT	DESCRIPTION
Proofpoint Supervision	Proofpoint Supervision is an add-on to Proofpoint Archive that allows you to supervise, monitor and report on all digital correspondence, including email. It helps you to identify, review, address and maintain audit trails as well as build, maintain, refine and execute an audit-ready supervision plan. Supervision streamlines business and helps you comply with regulatory supervision requirements. It allows you to sift through and reduce the low-value "noise content" that your review teams would normally monitor and review. This means you can pinpoint compliance violations faster and more accurately. And it prepares you to respond to regulatory audit requests at a moment's notice, with analytics, real-time dashboards and collaboration features.
Proofpoint Track	Proofpoint Track is a centralized hub that audits and monitors all of your communications and ensures they are saved in your downstream archives. It gives you control of and complete visibility into your capture stream. It features end-to-end data reconciliation protection. And it ensures that what you have in your data stores includes every record that was sent to them. Track is ideal for firms that must meet even the strictest regulatory compliance and litigation requirements. It simplifies the audit process. It features a built-in feedback loop as well as audit-level reporting. And its reconciliation reports allow you to defensibly prove that all of your messages are delivered to and received by your archives.

Proofpoint Managed Services

Proofpoint Managed Services provides highly skilled Proofpoint experts to help you with many of your cybersecurity needs.

Managed Services

PRODUCT	DESCRIPTION
Managed Email Threat Protection Services	Proofpoint Managed Email Threat Protection Services helps you get the most out of your investment in Proofpoint email security and threat protection products. It includes: • Email Protection • Targeted Attack Protection • Threat Response Auto-Pull Let our skilled experts continually tune your systems, rules and policies to stay ahead of advanced attacks in email. We also provide regular reports to show your executives and board how your security posture is improving over time.
Managed Information Protection Services	Proofpoint Managed Information Protection Services provides you with highly skilled experts to comanage your Proofpoint information protection products. It includes: • Cloud App Security Broker • Email Data Loss Prevention • Endpoint Data Loss Prevention • Insider Threat Management • Enterprise Data Loss Prevention You can reduce operational burdens from system management to policy governance to incident triage. It also provides executive summaries and reports to show stakeholders how your investment is producing healthy returns.
Managed Security Awareness Services	Proofpoint Managed Security Awareness Services provides you with a dedicated resource who will take care of designing, adapting and maintaining a security awareness program tailored to your business goals and needs. Let Proofpoint bring our expertise in cybersecurity to help you run phishing simulations, perform knowledge assessments and assign training modules to your users based on real-world threats and risk. Periodic reporting will be delivered to show how your activities impact cultural and behavioral change among your employees.

Proofpoint Premium Services

Proofpoint Premium Services can act as a force multiplier for your team. Leverage best practices and industry knowledge, optimize your systems and response to threats and deliver on the promise of a people-centric security strategy.

Premium Services

PRODUCT	DESCRIPTION
Proofpoint Recurring Consultative Service	Proofpoint Recurring Consultative Services provides Proofpoint professional services on retainer, to be available on a regularly scheduled basis (we have options for 8, 16 or 32 hours per month) when a much deeper level of expertise is needed. The Recurring Consultative Services is best for organizations that need supplemental guidance or dedicated help to address a variety of challenges in today's changing and complex security landscape. This may include activities such as ongoing tuning of data loss prevention (DLP) rules, implementing advanced email routing or monitoring supervision policies over time.
Proofpoint Technical Account Manager	The Proofpoint Technical Account Manager premium service can help you make the most of your technology investments with Proofpoint. Our technical account managers provide weekly, ongoing assistance to optimize, integrate and maintain your Proofpoint deployment. You gain deep technical expertise, real-world insight from our vast customer base and the best threat intelligence in the industry, focused on your unique environment and business needs.
Proofpoint Threat Intelligence Services	Proofpoint Threat Intelligence Services provides deep situational understanding of the threat landscape and your organization's place in it. These services enable you to make better, faster security decisions to avoid business disruption from advanced threats. Proofpoint offers multiple tiers of our Threat Intelligence Services based on your organization's needs and desired consumption. At its core, the services give you access to a world-class threat analyst that provides insights into your organization's threat landscape, actionable recommendations for mitigating risk, responses to custom threat intelligence inquiries and bespoke reporting.

Proofpoint Solution Bundles and Nexus People Risk Explorer

Proofpoint provides holistic solution bundles that address the modern threat landscape, extend your resources and progress with you as you elevate your security strategy. We also offer the Proofpoint Nexus People Risk Explorer, which gives security executives visibility into the risk people pose to the rest of the organization.

Solution Bundles and Nexus People Risk Explorer

PRODUCT	DESCRIPTION
Proofpoint PX	Proofpoint PX is an integrated cloud email security solution bundle that delivers advanced AI-powered protection to complement native Microsoft defenses. It uses machine learning (ML), behavioral analytics and threat intelligence to block phishing, business email compromise (BEC), supply chain and malware/ransomware attacks with 99.999% efficacy. Proofpoint PX is ideal for IT and security teams that want to augment native M365 capabilities with AI-powered, API-based protection that's easy to deploy and manage.
Proofpoint P0	Proofpoint P0 is a solution bundle that protects your organization from the leading vectors in today's threat landscape: email and cloud apps. It resolves 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, which addresses threats such as phishing, business email compromise (BEC), ransomware and other malware. P0 includes: • Email Protection • Targeted Attack Protection (TAP) • Threat Response Auto-Pull (TRAP) • Closed-Loop Email Analysis and Response (CLEAR) • Basic email encryption (TLS) • Basic email DLP (RegEx) • Nexus People Risk Explorer • TAP URL Isolation for VAPs Proofpoint P0 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.
Proofpoint P1	Proofpoint P1 is a solution bundle that enhances the Proofpoint P0 solution bundle by training end users to be more resilient against threats they receive. It augments threat protection with a robust security awareness training program that integrates with your email security controls and includes phishing simulation and comprehensive training. P1 includes everything in P0 and: • Proofpoint Security Awareness Enterprise Proofpoint P1 does everything Proofpoint P0 does and more. It allows you to tailor the training curriculum delivered to your users based on the actual threats they receive. Utilize the full catalog of interactive training and tools that are designed to change end user behavior. The suite of capabilities includes threat simulations that test user response to phishing attacks using thousands of templates, more than 35 languages and 13 categories. These can help establish a security baseline, train employees to avoid security risks and report progress over time. The progress of your program can be visualized in a specially designed CISO dashboard that emphasizes the metrics that senior security leaders care about the most.

PRODUCT	DESCRIPTION
Proofpoint P1+	Proofpoint P1+ is a solution bundle that increases protection from email and domain fraud, including BEC, to stop inbound and outbound email spoofing attacks sent on your organization's behalf. It offers 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. P1+ includes everything in P1 and: • Proofpoint Email Fraud Defense • Proofpoint Supplier Risk Explorer • Proofpoint TAP URL Isolation for all users • Proofpoint Internal Mail Defense for organizations with fewer than 5,000 users Proofpoint P1+ does everything Proofpoint P1 does and more. It lets you 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.
Proofpoint Nexus People Risk Explorer	Proofpoint Nexus People Risk Explorer is a dashboard that provides a unified view of integrated data from Proofpoint products and third-party systems in your environment. The dashboard helps you understand who is putting your organization at risk, how they are doing it and the security controls that can mitigate the risk. Nexus People Risk Explorer improves your cyber risk posture by helping you move your organization from a reactive approach to a proactive one. It helps you manage and mitigate your security risk in a people-centric way. And it makes it easy for you to assess risk through the behavioral vulnerability, attack surface and data access privileges of your people.

PRODUCT	DESCRIPTION
Proofpoint Enterprise Data Loss Prevention	Proofpoint Enterprise Data Loss Prevention (DLP) is a solution bundle that modernizes your DLP solution with our people-centric approach. It brings together rich context across content, behavior and threats to provide people-centric insights into data loss and prevent it from happening. The bundle includes: • Email DLP • Cloud App Security Broker • Endpoint DLP • Insider Threat Management (for 3% of users) Enterprise DLP equips your security and compliance teams with telemetry across email, cloud and endpoint to address the complete range of people-centric data loss scenarios in a single solution. **NOTE:** Enterprise DLP is also cross-listed under the Proofpoint Sigma section.

LEARN MORE

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

---

proofpoint.