PRODUCT LINE CARD

Proofpoint Solutions for Government Agencies and the Defense Industrial Base

Contents

Proofpoint provides federal government agencies and defense industrial base (DIB) partners protection and visibility for their greatest asset and security risk—their people. Our cybersecurity and compliance solutions protect against the threats that target people as well as the information they create and access.

Proofpoint products and services feature protection that spans email, social media, the web, networks and cloud platforms—including Microsoft Office 365. We have flexible deployment options, including CMMC and Zero Trust frameworks. We have strategic technology integrations with the industry's best security providers. This allows our solutions to bolster a robust, defense-in-depth approach to support your mission and break the attack chain.

This product line card includes the top deployed products at federal customers across the country. They can be deployed in FedRAMP cloud, commercial US cloud and customer environments on premise. For information about our new Government Threat Protection Packages, please see this blog.

Data Security

Find, track and safeguard data in email, cloud apps, on-premises file shares and SharePoint through either cloud or on-premises deployments.

Data Security solutions

PRODUCT	DESCRIPTION
Proofpoint Email Data Loss Prevention	Proofpoint Email Data Loss Prevention (DLP) reduces risk of employee negligence in outgoing communication by preventing the loss of sensitive, private information. It can be activated directly within the gateway. In doing so, it can be a FedRamp moderate solution. Proofpoint Email DLP enforces policies centrally and automatically from within the email gateway, allowing users to operate normally, rather than forcing them to make policy decisions about the nature and protection of content they send. Proofpoint Email DLP features more than 80 fine-tuned policies that find, classify and block sensitive messages to greatly reduce the likelihood that you will have a data breach including identifying CUI and MIP labels too.
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. It provides detection and prevention to defend data against both malicious and negligent user behavior from employees, privileged users and third parties. With Insider Threat Management, you can greatly reduce the risk of security incidents by monitoring user behavior and offering real-time education and deterrence. It cuts investigation time from days to minutes. And it offers full playback of security incidents to improve response times and simplify compliance. Proofpoint Insider Threat Management ensures your compliance with Executive Order 13587. It is FIPS 140-2 compliant and is deployed on-premises.
Proofpoint Data Security Posture Management	Proofpoint Data Security Posture Management (DSPM) discovers, classifies, and protects sensitive data across cloud and hybrid environments. With advanced AI-powered, agentless scanning, it identifies valuable and sensitive data in place to maintain compliance and operational efficiency. DSPM prioritizes human-centric risks to data. It assigns monetary value to data, visualizes attack paths, and highlights access risks, enabling security teams to allocate resources effectively. Its guided remediation simplifies issue resolution, reducing attack surfaces like over-permissioned access or forgotten data. Additionally, DSPM ensures AI tools like LLMs use the right data, supporting safe adoption and enhancing business agility.

Threat Protection

Proofpoint Threat Protection solutions provide a multilayered approach to cybersecurity, addressing threats from email, web, cloud and third-party sources. You can detect, research and respond to threats more quickly, accurately and confidently.

Threat Protection solutions

PRODUCT	DESCRIPTION
Proofpoint Email Fraud Defense *(part of the Government P1+ package)*	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. And it protects your employees, customers and business partners from all forms of email fraud by stopping impostor email attacks before they reach the inbox. You can use a single portal to authorize legitimate email, block fraudulent messages and see all threats regardless of the tactic or person being targeted. Email Fraud Defense uses email authentication, machine learning (ML) and policy, and enforces DMARC authentication to help you block all fraud tactics that threat actors use to launch advanced attacks.
Proofpoint Email Protection	Proofpoint Email Protection is a FedRAMP Moderate-authorized solution that uses ML and multilayered detection 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 can also be deployed on-premises with appliances or virtually. Proofpoint Email Protection provides visibility and business continuity for organizations of all sizes. It catches both known and unknown threats that others miss. With it, you can control all aspects of inbound and outbound email and set up granular policies to better protect users from email threats.
Proofpoint Targeted Attack Protection	Proofpoint Targeted Attack Protection (TAP) is a FedRAMP Moderate-authorized solution that 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 and in-depth visibility into your Very Attacked People™ (VAPs), VIPs, company-level attack risk and threat objectives. It also equips you to rewrite all embedded URLs to protect your users on any device and track clicks on malicious links.

PRODUCT	DESCRIPTION
Proofpoint Threat Response Auto-Pull *(Part of the Government P0 package)*	Proofpoint Threat Response Auto-Pull (TRAP) recalls malicious emails already delivered to user inboxes. It follows the path of malicious emails so it can find and retract messages sent to larger groups of recipients. It also generates reports of quarantine attempts, successes and failures and lists of users who are targeted the most. Proofpoint TRAP can be deployed virtually, on-premises or as a cloud solution. It takes the manual labor and guesswork out of incident response. This reduces the workload of your security teams by helping them resolve threats faster and more efficiently.
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 and incident response as well as enriches other solutions. It combines actionable information, such as up-to-the-minute IP and domain reputation feeds, with a database of globally observed threats and malware analysis. Emerging Threats Intelligence is the gold standard for threat researchers. It offers 100% verified threat intelligence from one of the world's largest malware exchanges. It integrates seamlessly with your security tools. And it helps you understand the deeper, historical context of the origins and authors of threats. Unlike other intelligence sources that report only domains or IP addresses, our intel includes a 10-year history and proof of conviction. It covers 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 appliances may include next-generation firewalls, network intrusion detection systems (IDS) and intrusion prevention systems (IPS). Emerging Threats Pro Ruleset is updated daily. And it is available in SNORT and Suricata formats. It covers more than 40 different categories of network behaviors, malware command and control, denial of service (DoS) attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols, exploit kit activity and more.

Identity Threat Defense

Stop attackers from leveraging identity vulnerabilities, privilege escalation and lateral movement to gain access to critical data.

Identity Threat Defense solution

PRODUCT	DESCRIPTION
Proofpoint Identity Threat Defense	The Identity Threat Defense platform discovers and remediates privileged identity risk policy violations that are exploited in all ransomware and other cyberattacks. It includes component products such as Proofpoint Shadow and Proofpoint Spotlight. It features Attack Path Management, Identity Threat Assessment and agentless deception-based detections. These allow you to discover, prioritize and remediate vulnerable identities. They also help you detect active threats. This solution is used by federal civilian agencies, the Department of Defense and federal systems integrators among others Despite significant investment to protect identities, including deployment of privileged access management (PAM) and multifactor authentication (MFA) solutions, every government organization has exploitable identities. Identity Threat Defense makes it easy to find these previously unknown vulnerable identities sprawled across your endpoints and servers, then eliminate them and deploy proven deception techniques to stop attackers. Identity Threat Defense is deployed virtually on-premises and aligns to Cybersecurity Maturity Model Certification (CMMC) Level 3.

Security Awareness Training

Turn your users into a strong last line of defense by enabling them to identify and report threats.

Security Awareness Training solution

PRODUCT	DESCRIPTION
Proofpoint ZenGuide *(part of the Government P1 package)*	Proofpoint ZenGuide arms your users against real-world cyberattacks using personalized training based on our industry-leading threat intelligence. ZenGuide houses a library of more than 450 custom training modules, knowledge assessments and awareness materials. By leveraging a seamless integration with Proofpoint TAP, administrators are armed with real- time information on the most risky, vulnerable and targeted people across your organization from threats they see in the wild. This allows you to effectively train them on what matters most to reduce risk. The product supports CMMC Level 2 and 3 certifications in the Awareness and Training (AT) domain.

Premium Services

Proofpoint Premium Services blend people, process and technology to help customers optimize and evolve their threat protection programs.

Advisory Services

PRODUCT	DESCRIPTION
Proofpoint Threat Intelligence Services	Proofpoint Threat Intelligence Services provide deep situational understanding of the threat landscape and your organization's place in it. This can help you better prioritize your security decisions. Threat Intelligence Services offer: • Direct access to our industry-leading US threat researchers for RFIs • Monthly custom threat reports • Advanced warning for emerging threats through access to our analyst logbooks The services can aid and help you retain hard-to-find security analyst staff by reducing the number of manual processes and allowing them to focus on the most critical issues. Our researchers have more than a combined 100 years of experience within federal agencies like the NSA, the US Cyber Command and service branches.
Proofpoint Takedown *(part of the Government P1+ package)*	With Proofpoint Takedown, you get a dedicated team of analysts to help manage takedowns of malicious sites that target your company or customers. The service involves threat investigation and a double-action mitigation process that comprises both blocklist and a takedown actions. Customers submit sites to the Takedown team for investigation and review. The team's analysts then investigate that site and pull pieces of evidence to make a case for a mitigation action on your behalf. Once malicious activity is confirmed and evidence requirements are met, the Takedown team immediately blocklists the site throughout all Proofpoint traffic and automates the blocklist reporting to our partner providers. These blocklist partners block malicious sites on different levels, including web, DNS and email. This action typically takes effect within 24 to 48 hours. This provides rapid protection while the Takedown team assists further with the takedown action. In the takedown action, the team's analysts contact providers attached to the domain, provide the evidence and request mitigation steps to protect your company and internet users. These providers typically include the registrar, hosting provider, top-level domain (TLD) provider and more. A successful takedown can include suspension of the domain and the responsible user, removal of the domain registration or removal of various content or services attached to the domain.

PRODUCT	DESCRIPTION
Proofpoint's ZenGuide™ Premium Services	With Proofpoint's ZenGuide™ Premium Services, you get access to a partner who will help you elevate user education. Security awareness programs are critical to defense-in-depth strategies for people protection. Our team can help you design, implement, document and measure a program that will prioritize behavior change and align to your culture and objectives Our team supports enterprises of all sizes, across many industries and global regions. We do not believe in a one- size-fits-all approach. And our multitier offering reflects this. We offer three service levels: • Silver—This service provides a baseline, single-stream program for up to 2,500 users. You get monthly access to a Proofpoint program administrator who guides and manages quarterly phishing and training efforts. • Gold—This service enables a more strategic, single- stream program for any number of users. You get weekly access to a Proofpoint program administrator who guides and manages monthly phishing simulations as well as quarterly global and targeted training efforts. • Platinum—This top-tier service supports a highly strategic, multistream approach for any number of users. It is ideal for multitenant organizations and those with more complex program objectives. You get weekly access to Proofpoint work stream administrators as well as ongoing access to a program coordinator. It includes all of the benefits of Gold, additional support for threat-driven and role-based risk management initiatives and other key enhancements