Proofpoint Products

Proofpoint provides protection for and visibility of your greatest asset and security risk—your people. We deliver the most effective tools available to protect against 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.

EMAIL PROTECTION

Defend against email threats, ensure continuity of email communications, and implement inbound and outbound email policies.

Email Protection

Proofpoint Email Protection protects users against unwanted and malicious emails, including both malware and non-malware threats such as impostor email or business email compromises (BEC). We do this by providing granular visibility and business continuity for organisations of all sizes. By controlling all aspects of inbound/outbound email traffic and establishing policies, we help your IT and security team protect your end users from email threats and maintain email communications in the event of an outage.

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) protects your employees, customers and business partners from all forms of email fraud by stopping impostor email attacks before they even reach the inbox. From a single portal, you can authorise legitimate email, block fraudulent messages, and see all threats—regardless of the tactic used or the person being targeted. By leveraging email authentication, machine learning and policies and enforcing DMARC authentication, EFD helps you block all fraud tactics used by criminals to launch advanced attacks.

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) uses orchestration and automation capabilities to recall malicious emails that have been delivered to a user's inbox. This entry-level version of Threat Response identifies and removes malicious emails based on alerts from TAP. It then uses business logic to follow the email's path to the larger group of recipients and find and recall the messages. TRAP also generates reports showing quarantine attempts, successes/failures, and a list of which users are most targeted—reducing your security team's workload.

Internal Mail Defense

Proofpoint Internal Mail Defense uses a robust, multilayered approach to protect your organisation's internal email and help detect compromised accounts. It scans all internal mail for spam, malicious attachments and URLs. If an internal email is flagged, it is removed and quarantined automatically. Your security team also has visibility of the accounts that sent these malicious URLs, so they can quickly track down and act upon potentially compromised accounts.

Essentials for Small Business

Proofpoint Essentials tailors the capabilities of Email Protection to the needs of small businesses. It provides spam filtering, phishing detection, multilayer anti-virus protection, dynamic sandboxing of URLs, a robust filter engine, email continuity, policy-enforced encryption, email archiving and social media account protection. Best of all, it is managed via a simple and intuitive user interface, making it easy to manage for SMBs who might have smaller security teams.

ADVANCED THREAT PROTECTION

Detect, research and respond to threats more quickly, accurately and confidently.

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) helps detect, mitigate and block advanced threats containing malicious attachments and URLs that target people through emails and cloud apps such as Microsoft Office 365 and Google G Suite. TAP provides you with visibility of the Very Attacked People (VAPs) within your organisation. It also allows you to rewrite all embedded URLs to protect your users on any device and track clicks on malicious links.

Email Isolation

Proofpoint Email Isolation enables your IT and security teams to allow users to access personal webmail from corporate devices without security concerns. It can be integrated with TAP for an additional layer of security for your VAPs, while protecting all users from unknown or dangerous websites. This is achieved by preventing any malware or malicious content from impacting the user or device. Our cloud service isolates web content from corporate data and networks and simplifies how you manage risk and operational costs, while increasing your security.

Browser Isolation

Proofpoint Browser Isolation extends the capabilities of Proofpoint Email Isolation to protect all web browsing activities for all end users, including your VAPs. It provides a secure and anonymous web browsing service that is simple for your IT team to deploy, manage and support. This provides your users with privacy when they access sites such as webmail and poses no additional risks to your organisation.

Threat Response

Proofpoint Threat Response is designed for security operation teams working towards security maturity. It allows you to get an actionable view of your network threats, enhance alerts, and automate forensic collection and comparison. It also takes the manual labour and guesswork out of incident response. This helps your security team resolve threats more quickly and efficiently and unlike traditional incident response process related tools, it automatically confirms malware infections, checks for evidence of past infections, and enhances security alerts by automatically adding internal and external context and intelligence.

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence (ET) is the gold standard for threat researchers. It offers 100% verified threat intelligence from one of the world's largest malware exchanges and helps you understand the deeper, historical context of a threat's origin and author, integrating seamlessly with your security tools. Unlike other intelligence sources that only report domains or IP addresses, our intel includes a 10-year history and proof of conviction, with more than 40 threat categories and related IPs, domains and samples.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro is a timely and accurate rule set that detects and blocks threats using your existing network security appliances, such as next-generation firewalls and network IDS/IPS. Updated daily in Suricata and SNORT formats, ET Pro covers more than 40 different categories of network behaviours, malware command and control, DoS attacks, botnets, exploits, vulnerabilities, SCADA network protocols, exploit kit activity and more. By running daily updates and using an automated sandbox environment, your security team can rest assured that all threats will successfully be evaluated.

Premium Threat Information Service (PTIS)

Proofpoint Premium Threat Information Service (PTIS) enables you to prioritise security decisions by providing you with a deeper situational understanding of the ongoing threat landscape. It includes three components: direct access to our industry-leading threat researchers, monthly custom threat reports, and advanced warning for emerging threats through access to our analyst logbooks. This service can aid and retain hard-to-find security analyst staff by reducing manual processes and allowing them to focus on the most critical issues.

SECURITY AWARENESS TRAINING

Turn your end users into a strong last line of defense against phishing and other cyber attacks by enabling them to identify and report threats.

Anti-Phishing Suite

Proofpoint Anti-Phishing Suite helps you identify and reduce your employees' susceptibility to phishing attacks and malware infections by up to 90%. If a user falls for a ThreatSim simulated phishing attack, they are provided with a teachable moment with tips on how to stay safe in the future. Users who fail a simulated attack can be automatically enrolled into one of our 8 anti-phishing training modules, or they can be assigned separately. In addition, with this package, administrators have access to our PhishAlarm® email reporting button and PhishAlarm Analyzer email analysis tools. These tools are the beginning of our Closed Loop Email Analysis and Response (CLEAR) solution, which makes for streamlined reporting and automated responses to active phishing attacks.

Enterprise Security Awareness Training

The Proofpoint Security Awareness Training Enterprise package includes everything from the Anti-Phishing Suite and ThreatSim USB to CyberStrength® Knowledge Assessments, our entire library of Training Modules, and all of our Awareness Materials, including videos. This package is ideal for customers looking to administer the most effective and comprehensive security awareness training programme. With access to more tools to identify risk, change behaviour, and reduce exposure, you can implement a more impactful people-centric risk reduction strategy.

CLOUD APP SECURITY

Protect your people and data from threats, data loss and compliance risks in cloud applications.

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) offers automated protection against account compromises and malicious files in Office 365 and G Suite. Account compromises typically start with phishing, credential-stealing malware, or brute-force attacks such as credential stuffing. Compromised accounts are most often used to launch further attacks, such as BEC or phishing, both inside and outside organisations. CAD helps you quickly detect, investigate and defend against cyber criminals accessing your sensitive data and trusted accounts. It provides you with people-centric threat detection, correlation of threat activity, granular forensics with rich threat intel, and flexible policies for automated response.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) protects organisations from cloud account compromise, oversharing of sensitive data, and compliance risks in the cloud. PCASB provides a granular people-centric view of app access and data handling. Our solution combines compromised account detection, access control, data loss prevention (DLP), third-party app control, and analytics to help you secure Office 365, G Suite, Box and more. Our powerful analytics help you grant the right levels of access to users and third-party apps based on the risk factors that matter to you.

INFORMATION PROTECTION

Find, track and safeguard data in emails, cloud applications, on-premises file shares and SharePoint.

Email Data Loss Prevention (DLP)

Proofpoint Email DLP prevents employee negligence in outgoing communication by preventing the loss of sensitive, private information. Instead of forcing end users to make policy decisions about the nature and protection of content they send (which can increase burden and time resources), you can allow them to operate normally while our solution enforces email communication policies centrally and automatically. With more than 80 fine-tuned policies that automatically find, classify, and block sensitive messages, you can rest assured that the likelihood of a data breach will be reduced.

Email Encryption

Proofpoint Email Encryption uses policy-based encryption to make secure communication via messages and attachments seamless and automated for your end users. 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, since this happens in the background. With us, you can protect sensitive email messages while ensuring your affiliates, business partners, and end users have seamless access to secured messages on computers or mobile devices.

Data Discover

Proofpoint Data Discover finds, monitors and protects sensitive data on file shares, data stores and SharePoint sites. It does so by automating content analysis to track information across your organisation's on-premises network. It then automatically identifies sensitive data—including PII and PHI—at risk to unauthorised exposure. And it enables real-time remediation through quarantine, copying or deletion.

Meta

Proofpoint Meta is the next generation in secure enterprise application access. A people-centric solution, Meta ensures employees, contractors and partners have zero-trust, identity-based access to enterprise resources in the datacenter and any cloud.

ObserveIT Insider Threat Management

Proofpoint acquired ObserveIT in November 2019. Insider Threat Management offers a lightweight endpoint solution that helps organisations identify and mitigate insider risk. The solution provides detection and prevention to defend data against both malicious and negligent user behaviour from employees, privileged users, and third parties. With Insider Threat Management, organisations can significantly reduce the risk of security incidents by monitoring user behaviour and offering real-time education and deterrence. ObserveIT cuts investigation time from days to minutes and offers full playback of security incidents to improve response times and simplify compliance.

DIGITAL RISK PROTECTION

Protect your brand and customers from social media, web domain and dark web threats.

Digital Risk Protection

Proofpoint Digital Risk Protection secures both the customer and their brand against digital security risks across web domains, social media, and the deep web. This includes the ability to protect corporate domains from brand fraud; secure and monitor social media accounts for phishing, account takeovers and spam; and monitor deep and dark web activity for executive threats, credential leaks, locations for physical attacks, and nearby high-impact events. Through the use of machine learning, our solution helps you get in front of threats, whether they are planned, imminent or occurring real-time.

ARCHIVING AND COMPLIANCE

Retain, discover and supervise data across all communication platforms to ensure compliance.

Enterprise Archive

Proofpoint Enterprise Archive uses cloud intelligence and machine learning to preserve and discover business-critical information in a manner that is easy to find. It addresses three fundamental challenges—legal discovery, regulatory compliance, and cost and complexity reduction. And it does this without the headaches of an IT team managing archiving in-house.

Our scalable cloud architecture, guaranteed search performance, unmatched customer satisfaction, and the industry's most sophisticated encryption all provide you with complete legal and compliance control.

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive applies policy-based controls to capture social content from Salesforce Chatter, Jive, Skype for Business, LinkedIn, Twitter and other platforms to be managed or reviewed as any other critical data asset in your compliance archive or supervision platform. This ensures you remain compliant with your regulatory obligations. It also provides you with advanced features that automate and streamline critical compliance tasks.

Intelligent Supervision

Proofpoint Intelligent Supervision helps streamline compliance for financial services firms, who are subject to some of the world's most stringent and complex regulations, such as FINRA, SEC and IIROC. It is fully integrated with Enterprise Archive and leverages machine learning to facilitate easy capturing, efficient reviewing, and effective reporting for regulatory response. This gives you a complete overview across your email, instant messages, collaboration tools, voice, SMS, and social media.

E-Discovery Analytics

Proofpoint E-Discovery Analytics provides an intuitive e-discovery workflow for legal teams. It increases insight by using machine learning with real-time search results and integrated early case analytics. We help you achieve proactive litigation readiness, which means more control and less risk.

Social Media Compliance

Proofpoint helps bridge the gap between social media compliance and marketing practices to help users comply with the current social media regulations. Digital Risk Protection integrates with leading archiving solutions to collect and classify social media content for future search and e-discovery. Not only do we do this, but we also collect and classify social media content for future search. All of this saves you time and money during an audit.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' 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 cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, 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.**