proofpoint.

PROOFPOINT PRODUCTS

Your greatest asset and greatest security risk are your people. Proofpoint delivers the most effective cybersecurity tools available for unmatched protection at every level. We protect your people against the threats that target them. We protect the information they create and access. And we protect the users themselves.

Our comprehensive suite of advanced solutions spans email, social media, web, network and cloud—including Microsoft Office 365. And our integrations with top security vendors make your defenses even stronger. Explore what we have to offer and see how Proofpoint can protect your people and your organization from today's advanced attacks.

EMAIL PROTECTION

Email Protection

Proofpoint Email Protection provides protection from unwanted and malicious email, with granular visibility and business continuity for organizations of all sizes. It provides IT and security teams with confidence in securing employees from email threats and maintaining email communications during outages.

Email Fraud Defense 360

Proofpoint Email Fraud Defense 360 (EFD360) protects your employees, customers and business partners from all forms of email fraud. This comprehensive, integrated solution provides the visibility and controls you need to stop all impostor email attacks before they reach the inbox. From a single portal, you can see all email fraud threats—regardless of the tactic used or the person being targeted. Leveraging email authentication, machine learning and policy, and lookalike domain monitoring, EFD360 helps you block all the various fraud tactics that criminals use to launch these advanced attacks.

Internal Mail Defense

Proofpoint Internal Mail Defense provides a multi-layered defense that protects organizations' internal email and helps detect compromised accounts. It scans all internal mail for spam, malicious attachments and malicious URLs. If internally sent email is flagged, it can be automatically removed and quarantined. Security teams also gain visibility into the accounts that sent the malicious email so they can quickly track down and act upon potentially compromised accounts.

Essentials for Small Business

Proofpoint Essentials for Small Business harnesses the capabilities of Email Protection to fit the needs of small businesses. Essentials includes spam filtering, phishing detection, multi-layer anti-virus, robust filtering rules, email continuity, policy-enforced encryption and email archive. And it's all managed with a simple, intuitive user interface.

ADVANCED THREAT PROTECTION

Targeted Attack Protection in Email

Proofpoint Targeted Attack Protection (TAP) in Email helps detect, mitigate and block advanced threats that target people through email. It detects known and unknown threats that use malicious attachments and URLs. TAP is unmatched in stopping targeted attacks that use polymorphic malware, weaponized documents and credential-stealing phishing techniques to access sensitive information.

TAP Isolation Personal Browsing Defense

Proofpoint TAP Isolation Personal Browsing Defense enables IT and security teams to allow users to access websites and personal webmail from corporate devices while preventing malware or malicious content from impacting users and their devices. This helps solve the security, productivity and privacy challenges associated with untrusted high-risk web use by employees. Personal Browsing Defense is a secure and anonymous web browsing service that is simple to deploy, manage and support.

TAP Isolation Personal Webmail Defense

Proofpoint TAP Isolation Personal Webmail Defense protects people from advanced threats in personal email. It isolates web browsing activity when they access personal email and leverages TAP threat intelligence to detect and block clicks on malicious URLs. This technology can help minimize risk to corporate assets, maintain employee privacy and simplify regulatory compliance.

TAP SaaS Defense

Proofpoint TAP SaaS Defense detects suspicious logins and malicious files to safeguard organizations against hidden threats in cloud apps, such as Office 365 and G Suite. Suspicious logins could indicate account compromise. This includes unusual login locations, excessive login attempts and too many connections from unknown or unusual IP addresses. This type of activity may mean that attackers are attempting

to access and possibly exfiltrate your valuable data. With TAP SaaS Defense, security teams can take a "trust but verify" approach to how employees are using SaaS-hosted files.

Threat Response

Proofpoint Threat Response is designed for security operations teams working towards security maturity. This solution automates the threat data enrichment, forensic verification and response processes after security teams receive an alert. Unlike traditional incident response tools, Threat Response 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 Auto-Pull

Proofpoint Threat Response Auto-Pull (TRAP) provides security teams with orchestration and automation capabilities to retract malicious emails delivered to user inboxes. TRAP is an entry-level version of Threat Response, which removes internal copies of malicious emails based on alerts from TAP and implements additional business logic to find and remove internal copies of that messages that were forwarded to others.

Emerging Threats Intelligence

Proofpoint Emerging Threats (ET) Intelligence is the gold standard for threat researchers, with 100%-verified threat intelligence from one of the world's largest malware exchanges. Unlike other intelligence sources that report only domains or IP addresses, ET Intelligence includes a five-year history, proof of conviction, 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 for detecting and blocking threats using your existing network security appliances—including next-generation firewalls and network IDS/IPS. Updated daily in SNORT and Suricata formats, ET Pro covers over 37,000 rules in more than 40 different categories of network behaviors, malware command and control, DoS attacks, botnets, exploits, vulnerabilities, SCADA network protocols, exploit kit activity and more.

Premium Threat Information Service

Proofpoint Premium Threat Information Service (PTIS) provides security teams with deeper situational understanding of the changing threat landscape, helping them prioritize security decisions faster. The three parts of PTIS include direct access to our industry-leading threat researchers, monthly custom threat reports and advanced warning for emerging threats by accessing analyst logbooks.

CLOUD APP SECURITY

Cloud Account Defense

Proofpoint Cloud Account Defense (CAD) provides automated protection against the causes and consequences of account compromise in Office 365. These threats typically start with phishing, credential-stealing malware or brute-force credential stuffing. Attackers leverage compromised accounts to launch lateral attacks—everything from email fraud to internal phishing attacks—inside and outside the organization. CAD can help organizations quickly detect and investigate these incidents to prevent financial loss and data exfiltration.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) protects organizations from advanced threats, accidental sharing of sensitive data and compliance risks in the cloud. It provides a granular, people-centered view of app access and data handling. PCASB combines advanced threat protection, access control such as multi-factor authentication (MFA), data loss prevention (DLP), third-party application control and analytics to help you secure Microsoft Office 365, Google G Suite, Box and other cloud and SaaS services. Our powerful analytics help security teams grant users the right levels of access to third-party applications based on the risk factors that matter most to the organization.

INFORMATION PROTECTION

Data Discover

Proofpoint Data Discover provides complete visibility and response for unstructured data. It automates content analysis, enabling security teams to track information across the on-premises network. This includes file shares, SAN, NAS and SharePoint sites. Data Discover automatically identifies at-risk sensitive data—including PII, PHI and PII—and enables real-time remediation through quarantine, copy or delete.

Email DLP

Proofpoint Email DLP helps curtail employee negligence with more accurate and transparent control for outgoing communications. Instead of forcing users to make policy decisions about the type of content they send and how it's protected, security teams can allow them to work as usual while the solution transparently enforces email communication policies centrally and automatically.

Email Encryption

Proofpoint Email Encryption secures email simply and seamlessly with automated, policy-based encryption of messages and attachments. Now security teams can protect sensitive emails while ensuring that affiliates, business partners and users still have access to secured messages on computers or mobile devices.

USER PROTECTION

Phishing Simulation and Security Awareness Training from Wombat Security

Proofpoint combines simulation, assessments, education, reinforcement and metrics to provide the ideal foundation for security awareness and training programs. These solutions include more than 500 different phishing templates across 30 languages and in 13 categories simulate attacks. These evaluate users on their ability to identify various threats, including malicious attachments, embedded links and requests for personal data. If users fall for simulated attacks, they get immediate feedback with "just-in-time teaching." Administrators receive real-time reporting to focus awareness efforts and track progress.

Products include:
- ThreatSim® Simulated Phishing Attacks
- PhishAlarm® Email Reporting Button
- PhishAlarm® Analyzer Threat Prioritization
- CyberStrength® Knowledge Assessments

DIGITAL RISK PROTECTION

Digital Risk Protection

Proofpoint Digital Risk Protection is a unified solution that protects people against security and brand risks across the web and social media. It helps protect corporate domains from brand fraud and secures and monitors social media accounts for phishing, account takeovers and spam. It also monitors both deep web and dark web activity for executive threats, credential leaks, locations for physical attacks and nearby high-impact events.

ARCHIVING AND COMPLIANCE

Enterprise Archive

Proofpoint Enterprise Archive leverages cloud intelligence to help preserve, discover and supervise your business-critical information. This next-generation archiving solution addresses key business data challenges—legal discovery, regulatory compliance, high costs and complexity—without the headache of managing archiving in house. It offers a scalable cloud architecture, guaranteed search performance, unmatched customer satisfaction and the industry's most sophisticated encryption for 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. It allows you to manage these like any other critical asset, ensuring you remain compliant with your regulatory obligations. It gives you advanced features to automate and streamline critical compliance tasks. This includes mapping to user-specific journaling destinations, conditionally capturing content for all or a subset of users, indicating record followers and custom email tags.

E-discovery and Analytics

Proofpoint E-discovery and Analytics provides a proven and intuitive e-discovery workflow for your legal department. It increases insight with real-time search results, integrated early case analytics and predictive coding. It also provides a defensible approach to your collection, discovery and review strategy, supporting new content types and ever-evolving court decisions. This gives you more control with less cost and risk.

Intelligent Supervision

Proofpoint Intelligent Supervision helps financial services firms streamline compliance for stringent and complex regulations like FINRA, SEC and IIROC. It is fully integrated with Enterprise Archive for easy capture, efficient review and effective reporting for regulatory response. That means financial organizations gain complete visibility across your email, instant messages, collaboration tools and social media.

Social Media Compliance

Proofpoint helps bridge the gap between social media compliance and marketing practices. From FINRA to FCC, current compliance and governance requirements include regulations for social media. Proofpoint Social Patrol seamlessly integrates with leading archiving solutions to intelligently collect and classify social media content for future search and e-discovery. It also archives contextual information, including remediation workflow and content classification. This saves you time and money during an audit.