Produits Proofpoint

Proofpoint vous offre visibilité et protection pour les ressources les plus importantes et les plus à risque de votre entreprise : vos collaborateurs. Nous fournissons les outils les plus efficaces du marché pour protéger les collaborateurs contre les menaces dont ils sont la cible et sécuriser les données qu'ils créent et consultent.

Nos solutions de cybersécurité et de conformité couvrent la messagerie électronique, les réseaux sociaux, Internet, les réseaux et le cloud, notamment Microsoft Office 365. Nous proposons également des intégrations de technologies stratégiques avec les plus grands éditeurs de solutions de sécurité du secteur. Vous pouvez ainsi protéger plus efficacement vos collaborateurs, vos données et votre marque.

PROTECTION DE LA MESSAGERIE

Protégez-vous contre les menaces email, assurez la continuité de la messagerie et implémentez des règles pour les messages entrants et sortants.

Email Protection

Proofpoint Email Protection protège les utilisateurs contre les emails indésirables et malveillants, qu'ils contiennent ou non des malwares, par exemple les emails d'imposteurs et les attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise). Cette solution garantit une visibilité extrêmement précise et la continuité des activités des entreprises de toute taille. En contrôlant toutes les facettes des emails entrants et sortants et en définissant des règles, nous aidons votre équipe informatique et de sécurité à protéger les utilisateurs finaux et à assurer la continuité de la messagerie électronique en cas d'incident.

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) protège vos collaborateurs, vos clients et vos partenaires commerciaux contre la fraude par email sous toutes ses formes en bloquant les attaques email d'imposteurs avant qu'elles n'atteignent la boîte de réception. Vous pouvez autoriser les messages légitimes, bloquer les messages frauduleux et visualiser toutes les menaces, quelle que soit la tactique utilisée ou la personne ciblée, depuis un portail unique. Grâce à l'authentification des emails combinée à l'apprentissage automatique, à des règles et à la mise en œuvre de l'authentification DMARC, Proofpoint Email Fraud Defense vous aide à contrer toutes les tactiques de fraude utilisées par les cybercriminels pour lancer des attaques sophistiquées.

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) tire parti de fonctions d'orchestration et d'automatisation pour rappeler les emails malveillants déjà remis dans les boîtes de réception des utilisateurs. Cette version de base de la solution Proofpoint Threat Response identifie et supprime les emails malveillants en fonction des alertes générées par Proofpoint Targeted Attack Protection (TAP). Elle applique ensuite une logique métier pour suivre les copies délivrées à d'autres destinataires afin de les éliminer. TRAP génère également des rapports indiquant les tentatives de mise en quarantaine et l'échec ou le succès de ces tentatives, en plus de proposer une liste des utilisateurs les plus ciblés — ce qui réduit la charge de travail de votre équipe de sécurité.

Internal Mail Defense

Proofpoint Internal Mail Defense s'appuie sur une approche multicouche robuste de la sécurité pour protéger la messagerie interne des entreprises et faciliter l'identification des comptes compromis. La solution analyse l'intégralité des emails internes à la recherche de spam, de pièces jointes dangereuses et d'URL malveillantes. Les emails internes marqués sont ainsi automatiquement éliminés et mis en quarantaine. Votre équipe de sécurité bénéficie également d'une visibilité sur les comptes à l'origine de l'envoi des URL malveillantes et peut ainsi en remonter rapidement la trace et agir sur ces comptes potentiellement compromis.

Essentials pour PME

Proofpoint Essentials pour PME adapte les fonctionnalités de Proofpoint Email Protection aux besoins des petites entreprises. La solution propose de multiples fonctions : filtrage antispam, détection du phishing, antivirus multicouche, analyse dynamique des URL en environnement sandbox, puissant moteur de règles de filtrage, continuité de la messagerie électronique, chiffrement fondé sur des règles, archivage des emails et protection des comptes de réseaux sociaux. Une interface utilisateur simple et intuitive facilite sa gestion, un atout précieux pour les PME à la tête d'une équipe informatique limitée.

PROTECTION CONTRE LES MENACES AVANCÉES

Détectez, analysez et neutralisez les menaces de façon plus rapide, précise et fiable.

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) permet de détecter, neutraliser et bloquer les menaces avancées contenant des pièces jointes et des URL malveillantes qui ciblent les utilisateurs au travers des services de messagerie et autres applications cloud, notamment Microsoft Office 365 et Google G Suite. Cette solution vous offre une visibilité complète sur les VAP (Very Attacked People, ou personnes très attaquées) de votre entreprise. Elle permet également de réécrire toutes les URL intégrées afin de protéger les utilisateurs sur n'importe quel appareil ou réseau, et de repérer les clics sur des liens malveillants.

Email Isolation

Proofpoint Email Isolation permet aux équipes informatiques et de sécurité d'autoriser les utilisateurs à accéder à leur messagerie Web personnelle depuis des appareils d'entreprise, en toute sécurité. La solution peut être intégrée à Targeted Attack Protection (TAP) pour renforcer la sécurité des VAP tout en protégeant tous les utilisateurs contre les sites Web inconnus ou dangereux. Pour ce faire, elle empêche les malwares et le contenu malveillant d'affecter les utilisateurs et les appareils. Notre service cloud isole le contenu Web des données et des réseaux d'entreprise. Il simplifie la gouvernance des risques et le contrôle des frais d'exploitation tout en renforçant votre niveau de sécurité.

Browser Isolation

Proofpoint Browser Isolation étend les fonctionnalités de Proofpoint Email Isolation à la navigation Web afin de protéger tous vos utilisateurs, y compris les VAP. Il propose un service de navigation Web sécurisé et anonyme facile à déployer, à gérer et à prendre en charge. La vie privée de vos utilisateurs est ainsi protégée lorsqu'ils accèdent à certains sites comme la messagerie Web, sans que cela constitue un risque supplémentaire pour votre entreprise.

Threat Response

Proofpoint Threat Response est conçu pour améliorer l'efficacité des équipes de sécurité. Il offre une vue exploitable sur les menaces réseau, et permet d'enrichir les alertes et d'automatiser la collecte et la comparaison de données d'investigation numérique. La solution permet d'éliminer les tâches manuelles et les estimations empiriques associées à la gestion des incidents. Votre équipe de sécurité peut ainsi neutraliser les menaces plus rapidement et avec une efficacité accrue. De plus, à la différence des outils traditionnels liés aux processus de réponse aux incidents, Proofpoint Threat Response confirme les infections par des malwares, recherche les preuves d'infections antérieures et ajoute aux alertes de sécurité les informations de cyberveille et le contexte pertinents collectés auprès de sources internes et externes — le tout automatiquement.

Emerging Threats Intelligence

Proofpoint Emerging Threats (ET) Intelligence constitue LA référence pour les chercheurs spécialisés en menaces. Cette solution fournit des informations entièrement validées sur ces dernières provenant de l'une des principales plates-formes d'échange de malwares au monde. Elle aide également à mieux comprendre le contexte historique d'une menace, de son origine et de son auteur tout en s'intégrant en toute transparence avec vos outils de sécurité. Notre cyberveille se distingue des autres sources similaires, qui signalent uniquement les domaines ou les adresses IP à l'origine d'activités malveillantes. En plus de classer les menaces dans plus de 40 catégories, elle inclut leur historique sur dix ans, des preuves de leur détection dans le cadre d'attaques, ainsi que leurs domaines, adresses IP et échantillons associés.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro Ruleset est un jeu de règles qui permet d'identifier et de bloquer de façon précise et instantanée les menaces avancées qui se jouent de vos appliances de protection du réseau, notamment les pare-feux de nouvelle génération et les systèmes de détection et de prévention des intrusions (IDS/IPS). Mis à jour quotidiennement dans les formats SNORT et Suricata, ET Pro Ruleset couvre plus de 40 catégories différentes : comportements réseau, infrastructures de commande et contrôle des malwares, attaques par déni de service, réseaux de robots (botnets), exploits, vulnérabilités, protocoles de réseau SCADA, activité des kits d'exploitation et bien d'autres encore. Grâce aux mises à jour quotidiennes et à l'utilisation d'un environnement sandbox automatisé, votre équipe de sécurité a l'assurance que toutes les menaces sont soigneusement évaluées.

Premium Threat Information Service (PTIS)

Proofpoint Premium Threat Information Service (PTIS) permet de hiérarchiser les décisions de sécurité en fournissant des informations contextuelles plus approfondies sur le paysage des menaces actuel. Il s'appuie sur trois composantes : un accès direct à nos chercheurs de premier plan spécialisés en menaces, des rapports mensuels personnalisés sur les menaces et des alertes avancées à propos des menaces émergentes grâce à un accès aux journaux de bord de nos analystes. Ce service facilite la tâche de vos analystes en sécurité en cela qu'il réduit les processus manuels et leur permet de se concentrer sur des problèmes plus graves.

FORMATIONS DE SENSIBILISATION À LA SÉCURITÉ

Transformez vos utilisateurs finaux en véritables piliers de votre défense contre le phishing et autres cyberattaques grâce à des formations qui leur permettront d'identifier et de signaler les menaces.

Anti-Phishing Suite

Proofpoint Anti-Phishing Suite vous aide à identifier et à réduire jusqu'à 90 % la vulnérabilité de vos collaborateurs aux attaques de phishing et aux infections de malwares. Si un utilisateur se

laisse piéger par une simulation d'attaque de phishing ThreatSim, il en est automatiquement informé par un « message éducatif » et des conseils pour mieux se protéger à l'avenir. Cet utilisateur peut par ailleurs être automatiquement inscrit à l'un de nos huit modules de formation à la lutte contre le phishing. Ces modules peuvent également être attribués de façon sélective. Enfin, ce pack offre aux administrateurs un accès au bouton de signalement d'emails de phishing PhishAlarm® et aux outils d'analyse des messages PhishAlarm Analyzer. Ces outils constituent la première étape du cycle d'analyse et de réponse lancé par Closed Loop Email Analysis and Response (CLEAR), une solution qui rationalise la procédure de signalement et automatise la réponse aux attaques de phishing actives.

Security Awareness Training Enterprise

Le pack Proofpoint Security Awareness Training (PSAT) Enterprise inclut tous les modules de Proofpoint Anti-Phishing Suite ainsi que les simulations d'attaque par clé USB ThreatSim, les évaluations des connaissances CyberStrength®, toute notre bibliothèque de formations et l'ensemble de nos supports de sensibilisation, y compris les vidéos. Ce pack est la solution idéale pour les clients qui souhaitent mettre en place un programme de formation et de sensibilisation à la sécurité complet et performant. Cet éventail d'outils destinés à identifier les risques, modifier les comportements et réduire l'exposition aux menaces vous permet de mettre en œuvre une stratégie plus efficace de réduction des risques axée sur les personnes.

SÉCURITÉ DES APPLICATIONS CLOUD

Protégez vos employés et vos données contre les menaces, les fuites de données et les risques de conformité associés aux applications cloud.

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) offre une protection automatisée contre les compromissions de comptes et les fichiers malveillants dans Office 365 et G Suite. Ces compromissions sont généralement le fait d'une attaque de phishing, d'un malware voleur d'identifiants de connexion ou d'une attaque par force brute, telle que le recyclage d'identifiants de connexion (« credential stuffing »). Les comptes compromis sont généralement utilisés pour lancer d'autres attaques internes ou externes, comme le piratage de la messagerie en entreprise (BEC) ou le phishing. Proofpoint CAD vous permet de détecter les comptes compromis, de mener des investigations et de vous défendre contre les cybercriminels qui accèdent à vos données sensibles et à vos comptes approuvés. La solution propose de multiples fonctions, dont la détection des menaces centrée sur les personnes, la corrélation des activités malveillantes, des investigations numériques granulaires fondées sur une cyberveille très complète et des règles flexibles pour la réponse automatisée.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) protège les entreprises contre la compromission des comptes cloud, le partage excessif de données sensibles et les risques de conformité dans le cloud. La solution offre une vue granulaire axée sur les personnes de l'accès aux applications et de la gestion des données. Elle combine des fonctions de détection des comptes compromis, de contrôle de l'accès, de prévention des fuites de données (DLP), de contrôle des applications tierces et d'analyse pour vous aider à sécuriser les plates-formes Microsoft Office 365, Google G Suite, Box et bien d'autres. Nos analyses puissantes vous aident à octroyer les niveaux d'accès appropriés aux utilisateurs et aux applications tierces en fonction des facteurs de risque les plus importants à vos yeux.

PROTECTION DES INFORMATIONS

Offrez-vous une solution capable de localiser, surveiller et protéger les données des emails, des applications cloud, des partages de fichiers sur site et des sites SharePoint.

Email Data Loss Prevention (DLP)

Proofpoint Email Data Loss Prevention (DLP) vous aide à éviter les incidents dus à la négligence de certains collaborateurs dans leurs emails sortants grâce à une solution de prévention des fuites de données confidentielles et sensibles. N'obligez plus vos utilisateurs à prendre des décisions concernant les types de contenus qu'ils envoient et la protection qu'ils nécessitent (ce qui leur complique la tâche et leur fait perdre du temps) : confiez à notre solution le soin d'appliquer les règles adaptées en matière de communication par email, de façon centralisée et automatisée. Grâce à plus de 80 règles élaborées avec soin pour détecter, classer et bloquer automatiquement les messages sensibles, la solution réduit la probabilité d'une compromission des données.

Email Encryption

Proofpoint Email Encryption offre aux utilisateurs une solution capable de sécuriser les communications par email de manière simple, transparente et automatisée grâce au chiffrement des messages et des pièces jointes basé des règles. Les services de messagerie chiffrés traditionnels posent parfois des difficultés aux utilisateurs. Avec Proofpoint Email Encryption, ils ne doivent plus chiffrer manuellement les messages qu'ils envoient et reçoivent : la solution se charge de tout, à l'arrière-plan. Grâce à Proofpoint, vous pouvez protéger efficacement vos emails sensibles tout en permettant à vos collaborateurs, partenaires commerciaux et utilisateurs de continuer à y accéder sans la moindre difficulté sur leurs ordinateurs et appareils mobiles.

Data Discover

Proofpoint Data Discover localise, surveille et protège les données sensibles hébergées sur les partages de fichiers, sur les sites SharePoint et dans les banques de données. La solution analyse le contenu de façon automatisée afin d'assurer le suivi des informations sur l'ensemble du réseau sur site de votre entreprise. Elle procède ensuite à l'identification automatique des données sensibles (informations d'identification personnelle et données médicales personnelles) susceptibles d'être divulguées sans autorisation. Enfin, elle permet de prendre les mesures correctives voulues en temps réel : mise en quarantaine, blocage ou suppression.

Meta

Proofpoint Meta est une solution de nouvelle génération offrant un accès sécurisé aux applications d'entreprise. Son approche centrée sur les personnes assure aux collaborateurs, aux sous-traitants et aux partenaires un accès Zero Trust et basé sur l'identité aux ressources de l'entreprise, que celle-ci se trouvent dans un centre de données ou sur le cloud.

ObserveIT Insider Threat Management

Proofpoint a fait l'acquisition d'ObserveIT en novembre 2019. Insider Threat Management propose une solution légère de protection des terminaux qui permet aux entreprises d'identifier et de réduire les risques liés aux menaces internes. Dotée de fonctionnalités de détection et de prévention, cette solution protège les données contre les comportements malveillants ou négligents dont peuvent faire preuve les collaborateurs, les utilisateurs à privilèges ou encore les tiers. Grâce à Insider Threat Management, qui surveille le comportement des utilisateurs, fournit des informations en temps réel et utilise des techniques de dissuasion, les entreprises peuvent considérablement réduire le risque d'incidents de sécurité. ObserveIT réduit la durée d'investigation de plusieurs jours à quelques minutes et permet de reconstituer les incidents de sécurité afin d'optimiser les délais de réponse et de simplifier la conformité.

PROTECTION CONTRE LES RISQUES NUMÉRIQUES

Protégez votre marque et vos clients contre les menaces associées aux réseaux sociaux, aux domaines et au Web clandestin.

Digital Risk Protection

Proofpoint Digital Risk Protection protège votre marque et vos clients contre les risques pour la sécurité numérique sur les domaines Web, les réseaux sociaux et le Deep Web, ou « Toile invisible ». Elle protège les domaines d'entreprise contre la fraude aux marques et elle sécurise et surveille les comptes de réseaux sociaux pour bloquer les tentatives de phishing, la prise de contrôle de comptes et le spam. Elle surveille également le Deep Web et le Web clandestin afin d'identifier les menaces ciblant les dirigeants de l'entreprise, les fuites d'identifiants de connexion, les emplacements des attaques physiques et les incidents proches à fort impact. La solution s'appuie sur l'apprentissage automatique pour vous permettre d'anticiper les menaces, qu'elles soient planifiées, imminentes ou en temps réel.

ARCHIVAGE ET CONFORMITÉ

Garantissez la conformité de votre entreprise grâce à des solutions alliant des fonctions de rétention, de recherche et de supervision des données sur toutes les plates-formes de communication.

Enterprise Archive

Proofpoint Enterprise Archive tire parti d'une cyberveille basée dans le cloud et de l'apprentissage automatique pour détecter et protéger les informations stratégiques. Cette solution résout trois problématiques fondamentales, à savoir la recherche de preuves à des fins juridiques, la conformité réglementaire et la réduction des coûts et de la complexité. Qui plus est, elle élimine les difficultés liées à la gestion de l'archivage en interne. Elle se distingue par un taux de satisfaction des clients exceptionnel, une architecture cloud évolutive, la garantie de performances élevées lors des recherches et un chiffrement d'un niveau de sophistication hors pair. Résultat : elle offre une totale maîtrise des questions juridiques et de conformité.

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive applique des contrôles basés sur des règles pour capturer des contenus à caractère social provenant de plates-formes telles que Salesforce Chatter, Jive, Skype Entreprise, LinkedIn, Twitter et d'autres. Ces contenus sont ensuite gérés et analysés comme n'importe quelle autre information stratégique dans votre plate-forme d'archivage ou de supervision. Vous êtes ainsi assuré d'être en conformité avec les obligations réglementaires. Par ailleurs, ses fonctions avancées automatisent et rationalisent des tâches essentielles de mise en conformité.

Intelligent Supervision

Proofpoint Intelligent Supervision aide les sociétés de services financiers à rationaliser la conformité aux réglementations strictes et complexes auxquelles elles sont soumises, notamment celles de la FINRA, de la SEC et de l'OCRCVM. La solution s'intègre parfaitement à Proofpoint Enterprise Archive et tire parti de l'apprentissage automatique pour faciliter la capture et optimiser l'examen et les rapports à des fins réglementaires. Vous bénéficiez ainsi d'une visibilité complète sur vos emails, messages instantanés, outils de collaboration, SMS, messages vocaux et réseaux sociaux.

E-Discovery Analytics

Proofpoint E-Discovery Analytics fournit aux équipes juridiques un workflow d'investigation électronique (e-discovery) intuitif. La solution utilise l'apprentissage automatique allié à des résultats de recherche en temps réel et à des analyses de cas rapides intégrées pour vous offrir des informations plus détaillées et complètes. Elle vous permet de vous préparer de manière proactive aux litiges, ce qui se traduit par un contrôle accru et un risque réduit.

Social Media Compliance

Proofpoint contribue à mettre en adéquation la conformité des réseaux sociaux et les pratiques marketing pour aider les utilisateurs à respecter les réglementations en vigueur en matière de réseaux sociaux. Proofpoint Digital Risk Protection s'intègre aux principales solutions d'archivage pour collecter et classer de façon intelligente le contenu des réseaux sociaux à des fins de recherches et d'investigations électroniques ultérieures. Vous gagnez ainsi un temps précieux et économisez de l'argent en cas d'audit.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.