Proofpoint Targeted Attack Protection

Protection contre les menaces avancées et visibilité

PRINCIPAUX AVANTAGES

- Détectez, analysez et neutralisez les menaces avancées avant qu'elles n'atteignent votre boîte de réception.
- Bénéficiez d'informations pertinentes uniques permettant d'identifier vos VAP (Very Attacked People™, ou personnes très attaquées) et les risques de sécurité.
- Tirez parti de la threat intelligence de Proofpoint pour vous protéger des menaces et recevoir des données d'investigation numérique détaillées sur les attaques.
- Mettez en place des contrôles de sécurité adaptatifs au moyen de fonctionnalités d'isolation des URL et des formations de sensibilisation à la sécurité informatique.
- Offrez la possibilité à vos VAP de naviguer en toute confiance sur des sites Web inconnus en passant par la messagerie d'entreprise tout en les protégeant contre les attaques Web et basées sur des URL. Cette fonctionnalité fait partie de nos bundles de solutions.

Plus de 90 % des cyberattaques débutent par la réception d'un email[1], et ces menaces ne cessent d'évoluer. Proofpoint Targeted Attack Protection (TAP) propose une approche innovante afin de détecter, d'analyser et de bloquer les menaces avancées qui ciblent vos collaborateurs. Il offre également une visibilité unique sur ces menaces, vous permettant ainsi d'optimiser votre réponse.

Proofpoint TAP bloque non seulement les attaques par email connues, mais également les attaques émergentes. Il détecte et neutralise les malwares polymorphes, les documents piégés, le phishing d'identifiants de connexion et d'autres menaces avancées. Il surveille l'activité des applications cloud pour identifier les connexions suspectes, le partage de fichiers à grande échelle, les applications tierces à risque, etc. Il vous fournit en outre les informations dont vous avez besoin pour identifier et protéger vos collaborateurs les plus ciblés.

Protection contre les menaces BEC, hébergées dans le cloud et véhiculées par les pièces jointes et les URL

Proofpoint TAP s'appuie sur des techniques statiques et dynamiques pour détecter les nouveaux modes opératoires des attaques et s'y adapter en permanence. Nous analysons les menaces potentielles en mettant en œuvre différentes approches qui examinent leur comportement, leur code et le protocole qu'elles utilisent. Nous sommes ainsi en mesure d'identifier les menaces dès les premières étapes de la chaîne d'attaque, parfois même avant qu'elles ne causent des dommages.

Proofpoint TAP protège votre entreprise contre les tentatives de piratage de la messagerie en entreprise (BEC, Business Email Compromise) et de compromission de comptes fournisseurs. La plupart du temps, ces types d'attaques sont dépourvues de charge virale malveillante. Leur identification requiert donc des techniques de détection sophistiquées qui vont au-delà de l'analyse en environnement sandbox. Proofpoint TAP est optimisé par le graphique des menaces Nexus. Ce dernier collecte, analyse et met en corrélation mille milliards de points de données au niveau de la messagerie, du cloud, du réseau, des endpoints et des réseaux sociaux. Le moteur Advanced BEC Defense est conçu et entraîné grâce à des données complètes sur les menaces. Il s'adapte en temps réel et peut réagir rapidement aux évolutions du paysage des menaces.

Nous utilisons les technologies de sandboxing pour étudier un large éventail d'attaques. Il peut par exemple s'agir d'attaques qui recourent à des URL et des pièces jointes malveillantes pour installer des malwares sur les équipements ou inciter les utilisateurs à communiquer des informations sensibles. Une analyse statique et dynamique à l'exécution permet également d'optimiser la détection et l'extraction d'informations pertinentes.

1 Verizon, « Data Breach Investigations Report » (Rapport d'enquête sur les compromissions de données), juillet 2019.

Proofpoint TAP détecte également les menaces et les risques associés aux applications cloud, et les relie au vol d'identifiants de connexion et autres attaques par email afin de vous permettre de mieux comprendre les attaques dans le cloud. Notre technologie ne se contente pas de détecter les menaces : elle recourt également à l'apprentissage automatique pour observer les tendances, les comportements et les techniques déployées dans le cadre de chaque attaque. Fort de ces précieux renseignements, Proofpoint TAP apprend et s'adapte de façon à pouvoir intercepter plus rapidement les prochaines attaques.

Advanced BEC Defense

Advanced BEC Defense protège votre entreprise contre les tentatives d'attaque BEC et de compromission de comptes fournisseurs. Il procède à une analyse complète de chaque information contenue dans un message, parmi lesquelles :

- Données d'en-tête
- Adresse IP de l'expéditeur
- Relation entre l'expéditeur et le destinataire
- Analyse de la réputation
- Analyse approfondie du contenu

Advanced BEC Defense offre également une visibilité granulaire sur les techniques employées par les cybercriminels, des observations sur les menaces et des échantillons de messages. Il vous aide à comprendre comment vos utilisateurs sont ciblés.

URL Defense

TAP URL Defense offre une protection contre les menaces basées sur des URL propagées par email, notamment les malwares et le phishing d'identifiants de connexion. Il propose des fonctionnalités uniques d'analyse prédictive qui s'appuient sur des modèles de trafic de messages pour identifier et isoler les URL de manière préventive. Toutes les URL qui atteignent les boîtes de réception sont réécrites de façon transparente afin de protéger les utilisateurs sur n'importe quel terminal ou réseau. Une analyse en temps réel en environnement sandbox est également effectuée à chaque clic sur une URL.

Attachment Defense

TAP Attachment Defense offre une protection contre les menaces connues et inconnues distribuées via les pièces jointes. Ce module vous protège contre les menaces dissimulées dans un large éventail de types de fichiers, les documents protégés par mot de passe, les pièces jointes contenant des URL intégrées et les fichiers .zip.

SaaS Defense

Compatible avec Microsoft 365 et Google Workspace (anciennement G Suite), TAP SaaS Defense identifie les activités de connexion suspectes, notamment les connexions depuis des emplacements inhabituels ou les tentatives ou échecs de connexion excessifs. Il signale également les connexions excessives depuis des adresses IP malveillantes connues. Il offre en outre une visibilité sur les événements de partage de fichiers internes et externes comportant un risque d'exposition élevé. Vous pouvez ainsi déterminer plus facilement quand des données sensibles ont pu être divulguées au cours des 30 jours précédents. Enfin, TAP SaaS Defense détecte les applications tierces critiques et à haut risque utilisées par votre entreprise.

URL Isolation for VAP*

TAP URL Isolation for VAP est conçu pour protéger les VAP (Very Attacked People™, ou personnes très attaquées) de votre entreprise contre les attaques Web et basées sur des URL. Il identifie les tentatives de phishing en temps réel et permet de protéger les utilisateurs et les clics autorisés contre les URL inconnues et à risque. Grâce à notre solution d'isolation du navigateur, les VAP peuvent accéder en toute confiance aux sites Web à partir de leur messagerie d'entreprise, sachant que l'entreprise est protégée.

Informations détaillées et visibilité sur les menaces et leurs cibles

Proofpoint dispose d'une visibilité étendue sur de nombreux vecteurs de menaces, notamment la messagerie, le cloud, le réseau et les réseaux sociaux, grâce aux informations fournies par nos 115 000 clients et plus à travers le monde. Les données que nous recueillons sont transmises au graphique des menaces Nexus de Proofpoint. Elles sont corrélées afin d'améliorer la visibilité sur le paysage des menaces. Vous pouvez les consulter et obtenir d'autres informations importantes à l'aide du tableau de bord TAP Threat Insight, qui fournit des renseignements détaillés sur les menaces et les campagnes en temps réel. Vous pouvez ainsi mieux appréhender les attaques ciblées et de grande envergure. Le tableau de bord TAP Threat Insight vous donne accès à des détails sur les menaces, notamment les utilisateurs concernés, des captures d'écran de l'attaque et des données d'investigation numérique approfondies.

* Uniquement disponible pour les clients disposant d'un bundle P.

VAP

Proofpoint Attack Index vous aide à identifier vos VAP afin que vos équipes de sécurité puissent déterminer qui sont les principales cibles de votre entreprise. Cet indice consiste en un score composite pondéré de toutes les menaces envoyées à une personne déterminée au sein de votre entreprise. Il attribue à ces menaces une note sur une échelle de 0 à 1 000, sur la base de la sophistication de la menace, de l'envergure et de la cible de l'attaque, du type d'attaque et du volume global de l'attaque. Armé de ces connaissances, vous pouvez identifier la solution la plus efficace à appliquer en priorité pour neutraliser les menaces.

Attack Index à l'échelle de l'entreprise

L'outil Attack Index peut également être appliqué au niveau de l'entreprise et à d'autres secteurs à des fins de comparaison globale des risques auxquels votre entreprise est confrontée. Le rapport ainsi généré aidera votre RSSI et votre équipe de sécurité à comprendre si votre entreprise subit plus ou moins d'attaques que ses homologues au sein des différents secteurs. Le rapport contient notamment des informations sur la fréquence des attaques et les types de menaces. Fort de ces connaissances, vous pouvez hiérarchiser les contrôles de sécurité en fonction du paysage des menaces spécifique à votre entreprise.

Renseignements sur les cybercriminels

Alors que les collaborateurs continuent à être pris pour cible, il est plus important que jamais que les clients bénéficient d'une visibilité complète sur les cybercriminels qui lancent ces attaques. Nos chercheurs spécialisés en menaces collectent des données sur les cyberpirates depuis de nombreuses années. Ce sont ces données qui alimentent le tableau de bord TAP. Les clients peuvent identifier les cybercriminels qui les prennent pour cible, les personnes visées, les tactiques et techniques employées, ainsi que toute tendance émergeant au fil du temps. Les entreprises peuvent ainsi mettre en place des contrôles de sécurité et des mesures de correction supplémentaires afin de renforcer la protection de leurs collaborateurs.

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 et de la conformité 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.

0103-002-01-06 7/21