

Bundles Proofpoint

Neutralisez les menaces de cybersécurité les plus urgentes

Pour neutraliser les attaques avancées actuelles, vous devez impérativement placer la protection des personnes au centre de vos priorités. Proofpoint propose une approche unique de la cybersécurité axée sur les personnes, qui commence par l'identification de vos VAP (Very Attacked People ou personnes très attaquées) et l'évaluation du risque posé par chacun d'eux pour votre entreprise. Nos bundles vous fournissent des solutions globales qui répondent au paysage actuel des menaces, renforcent vos ressources et évoluent au rythme de votre stratégie de sécurité.

Bundle P1 : Sécurité avancée de la messagerie

Commencez par protéger votre entreprise contre le principal vecteur de menaces : la messagerie électronique. Neutralisez les menaces véhiculées par la messagerie électronique à toutes les étapes de la chaîne d'attaque, de la détection à l'intervention. Bénéficiez d'une visibilité sur les cibles des attaques et les techniques d'attaque employées. Déterminez si les utilisateurs ciblés cliquent sur les emails de phishing ou les signalent, et s'ils ont été compromis. Bloquez net les attaques par email (qu'elles impliquent ou non des malwares), renforcez la résilience de vos utilisateurs face aux menaces qu'ils reçoivent grâce à des formations et automatisez les mesures de correction. Optimisez votre protection contre les menaces grâce à un solide programme de formation et de sensibilisation à la sécurité informatique comprenant des simulations d'attaques de phishing, une formation complète et la gestion automatisée des boîtes email de signalement d'abus.

CONTENU DU BUNDLE P1 :

- Email Protection
- Targeted Attack Protection (TAP)
- Threat Response Auto-Pull (TRAP)
- PSAT (Proofpoint Security Awareness Training) Enterprise
- Email Encryption – Fonctions de base (TLS)
- Email DLP – Fonctions de base (RegEx)

Bundle P1+ : Protection contre les attaques BEC

Renforcez votre protection afin de contrer les attaques email d'imposteurs, telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise), notamment les attaques entrantes qui ciblent vos utilisateurs et les attaques sortantes usurpant votre identité pour s'en prendre à vos clients et partenaires commerciaux. Ces attaques BEC peuvent recourir à différentes techniques d'usurpation d'identité. La mise en œuvre de l'authentification DMARC combinée à votre passerelle de messagerie vous offre une approche multicouche de la sécurité permettant de bloquer les attaques email d'imposteurs. Notre solution BEC intégrée prend en compte toutes les techniques utilisées par les cybercriminels, vous offre une visibilité complète sur votre écosystème de messagerie et vous procure les contrôles nécessaires pour bloquer ces attaques avant qu'elles n'atteignent la boîte de réception.

CONTENU DU BUNDLE P1+ : P1 ET ...

- Email Fraud Defense (EFD)

Bundle P2 : Protection contre les attaques BEC et EAC

Identifiez et gérez les signes de compromission de comptes de messagerie (EAC, Email Account Compromise), notamment les emails internes malveillants envoyés depuis des comptes compromis. Bénéficiez d'une visibilité en temps réel sur les comptes compromis, les cibles des attaques et les techniques utilisées pour cibler votre entreprise. Automatisez les mesures d'intervention, notamment l'élimination des emails malveillants, la réinitialisation des mots de passe, la suspension des comptes et bien plus. Neutralisez les attaques ciblant votre messagerie Web personnelle et les URL renvoyant vers des sites Web dangereux dans vos emails d'entreprise.

CONTENU DU BUNDLE P2 : P1+ ET ...

- Internal Mail Defense (IMD)
- Cloud Account Defense (CAD)
- Email Isolation
- Email Encryption
- Email DLP

Bundle P2+ : Protection des applications cloud

Protégez vos collaborateurs et vos données lors de l'utilisation de Microsoft Office 365, Google G Suite et autres applications cloud. L'ajout de notre solution CASB à votre stratégie de sécurité axée sur les personnes vous offre une vue centralisée de votre environnement cloud. Vous bénéficiez en outre d'une protection contre les menaces dans le cloud et les compromissions de comptes, d'une visibilité sur les applications cloud tierces dangereuses et d'une protection des données précieuses créées et consultées par vos collaborateurs.

CONTENU DU BUNDLE P2+ : P2 ET ...

- Cloud App Security Broker (CASB)

Bundle P3 : Sécurité complète axée sur les personnes

Développez un programme de sécurité stratégique qui englobe l'ensemble de votre surface d'attaque humaine, y compris l'écosystème plus large de votre entreprise. Ce programme doit couvrir la protection de vos domaines, comptes de réseaux sociaux, dirigeants et sites, ainsi que de toute autre infrastructure technologique dans votre environnement, de même que l'accès au Web. Protégez vos VAP grâce à des contrôles adaptatifs intégrés permettant d'isoler les menaces. Bénéficiez d'une recherche personnalisée sur les menaces spécifique à votre entreprise par un analyste en menaces dédié.

CONTENU DU BUNDLE P3 : P2+ ET ...

- Browser Isolation
- Threat Response
- Digital Risk Protection
- Premium Threat Information Service (PTIS)

Bundles

proofpoint.

P1 P1+ P2 P2+ P3

Protection contre les menaces	<ul style="list-style-type: none"> Protection contre les emails de phishing, l'usurpation de comptes de messagerie et les malwares <i>Email Protection, Targeted Attack Protection (TAP)</i> Approche centrée sur les personnes offrant une visibilité sur les VAP (Very Attacked People, ou personnes très attaquées) et les menaces auxquelles ils sont exposés <i>TAP, CASB</i> Suppression automatique des emails malveillants des boîtes de réception lorsque ceux-ci sont identifiés après la remise ou signalés par les utilisateurs <i>TRAP, CLEAR</i> Authentification des emails afin de bloquer les messages frauduleux envoyés à partir de domaines légitimes <i>Email Fraud Defense (EFD)</i> Protection contre les risques liés à l'utilisation de messageries Web personnelles sur des appareils d'entreprise <i>Email Isolation</i> Investigation et gestion des risques liés aux comptes cloud compromis, y compris les menaces internes provenant de ces comptes <i>TRAP, CAD, IMD</i> Possibilité pour les utilisateurs de naviguer sur Internet tout en empêchant le contenu malveillant d'affecter les appareils d'entreprise <i>Browser Isolation</i> Détection des tentatives de fraude émanant de domaines et de comptes de réseaux sociaux suspects <i>Digital Risk Protection</i> Analystes en menaces dédiés fournissant des conseils et des informations de cybersécurité à l'entreprise <i>PTIS</i> 	•	•	•	•	•
Protection des utilisateurs	<ul style="list-style-type: none"> Simulations d'attaques permettant de tester le comportement des utilisateurs face aux attaques de phishing Des milliers de modèles, dans plus de 35 langues et 13 catégories <i>ThreatSim</i> Formations interactives visant à modifier le comportement des utilisateurs finaux <i>Security Awareness Training</i> Mise en place d'une ligne de conduite en matière de sécurité, formation des collaborateurs pour qu'ils apprennent à reconnaître et éviter les risques de sécurité et suivi de leurs progrès dans le temps <i>CyberStrength</i> 	•	•	•	•	•
Protection des données	<ul style="list-style-type: none"> Utilisation d'expressions régulières pour prévenir les fuites de données par email ; chiffrement TLS des emails <i>Email Protection (RegEx)</i> Règles intégrées, analyse de l'empreinte numérique des fichiers et fonction d'autocorrection Smart Send. TLS de secours pour le chiffrement de type push/pull, portail Web compris. <i>Email DLP et Email Encryption</i> Protection contre les menaces dans le cloud Prévention des fuites de données, couvrant le partage excessif de données sensibles, le contrôle des applications tierces et les applications non approuvées (Shadow IT) <i>CASB</i> 	•	•	•	•	•

P1 Sécurité avancée de la messagerie

P1+ Protection contre le piratage de la messagerie en entreprise (BEC, Business Email Compromise)

P2 Protection contre les attaques BEC et les compromissions de comptes de messagerie (EAC, Email Account Compromise)

P2+ Protection des applications cloud

P3 Programme de sécurité complet axé sur les personnes

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, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.