Proofpoint Cloud App Security Broker

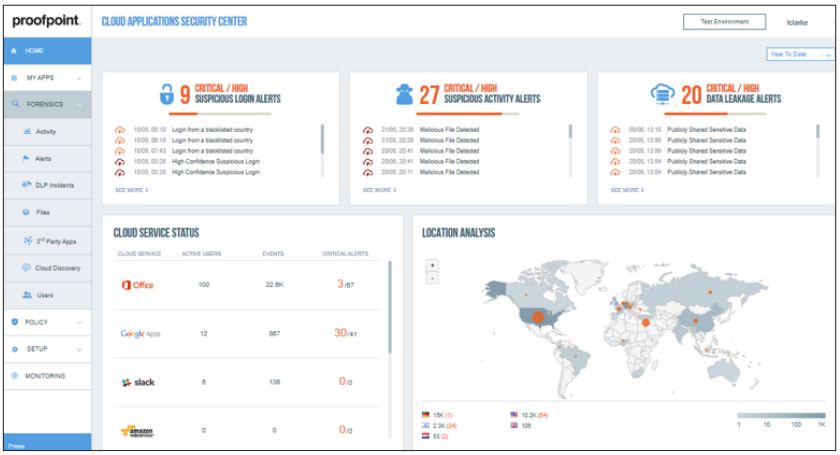
Améliorez la visibilité et le contrôle sur vos applications cloud

PRINCIPAUX AVANTAGES

- Protégez les utilisateurs du cloud grâce à une visibilité sur les menaces et à des contrôles d'accès adaptatifs pour les applications cloud, selon une approche centrée sur les personnes.
- Réduisez les délais nécessaires pour découvrir et protéger les données cloud réglementées au moyen de règles préconfigurées de prévention des fuites de données (DLP).
- Protégez les données sensibles et simplifiez les opérations au moyen de règles DLP précises et unifiées sur les deux principaux vecteurs de fuites de données : les applications cloud et les emails.
- Découvrez les applications cloud et contrôlez leurs usages (Shadow IT), notamment les applications OAuth tierces.
- Identifiez les comptes et les ressources IaaS, surveillez les comptes afin de détecter toute activité suspecte et gérez le niveau de sécurité du cloud.
- Installez la solution en quelques jours et obtenez des résultats exploitables en moins de quatre semaines.

De plus en plus d'entreprises, ainsi que leurs collaborateurs, adoptent des solutions cloud de tous types. Plus aucun périmètre réseau ne protège vos utilisateurs, vos applications et vos données. Vos collaborateurs partagent des données sensibles sans supervision, et ce depuis un grand nombre de terminaux personnels. La sécurité est un défi difficile à relever et les cyberattaques continuent à évoluer pour compromettre des comptes cloud, de même que subtiliser de l'argent et des données. Par son approche centrée sur les personnes, Proofpoint Cloud App Security Broker (Proofpoint CASB) protège vos utilisateurs contre les menaces dans le cloud, préserve vos données sensibles, découvre les applications non approuvées (Shadow IT) et assure la gouvernance des applications OAuth cloud et tierces.

La sécurité du cloud doit commencer par la sécurisation des applications approuvées par l'équipe informatique qui contiennent vos données les plus critiques : Microsoft 365 (anciennement Office 365), Google G Suite, Salesforce, Box, etc. Mais cela ne suffit pas. Vous avez besoin d'une approche intégrée et centrée sur les personnes permettant de mettre en corrélation les menaces et d'appliquer des règles DLP cohérentes tant à votre messagerie électronique qu'aux applications cloud. Proofpoint CASB vous protège contre les compromissions de compte, les partages excessifs de données, les erreurs de configuration des ressources IaaS et PaaS, ainsi que les risques de conformité. Notre solution sans agent vous assure une visibilité sur les menaces axée sur les utilisateurs, des contrôles d'accès adaptatifs, une réponse automatisée en cas d'incident et une sécurité complète des données par le biais de sa fonction de prévention des fuites de données, sans oublier une gouvernance des applications cloud et tierces, incluant la gestion du niveau de sécurité du cloud.



Console Proofpoint CASB

Extension de la visibilité centrée sur les personnes aux applications cloud

Proofpoint CASB procure une visibilité sur les menaces liées au cloud et à la messagerie électronique. Son approche centrée sur les personnes vous permet d'identifier vos VAP (Very Attacked People™, ou personnes très attaquées) et de protéger leurs données et comptes cloud. Proofpoint CASB permet également d'identifier les fichiers de vos applications cloud qui contreviennent aux règles DLP, à qui ils appartiennent, qui les télécharge, qui les partage et qui les modifie.

Ses outils d'analyse et contrôles adaptatifs performants vous aident à octroyer les niveaux d'accès appropriés aux utilisateurs et aux applications OAuth tierces en fonction des facteurs de risque les plus importants à vos yeux.

Protection des utilisateurs contre les menaces dans le cloud

Proofpoint CASB tire parti d'informations de threat intelligence très complètes collectées sur plusieurs canaux (cloud, messagerie et autres), qu'elle associe à des données contextuelles propres aux utilisateurs afin d'exécuter une analyse comportementale et de détecter des anomalies sur l'ensemble des applications et locataires cloud. Grâce à l'apprentissage automatique et à un système de threat intelligence étoffé, nous vous aidons à détecter les compromissions de comptes cloud. Lorsqu'un incident se produit, vous pouvez enquêter sur les activités et alertes antérieures à l'aide de notre tableau de bord intuitif, notamment les activités suspectes liées aux fichiers ou aux fonctions d'administration. Parallèlement, vous pouvez exporter des données d'investigation numérique manuellement ou à l'aide d'API REST vers une solution SIEM pour des analyses ultérieures.

Nos contrôles adaptatifs centrés sur les personnes permettent de contrer diverses menaces dans le cloud. Nous vous protégeons contre la compromission de comptes de messagerie (EAC, Email Account Compromise), l'exploitation des ressources IaaS et le vol de données, le tout sans nuire à la productivité des utilisateurs. Nos règles efficaces vous alertent en temps réel en cas d'incident, appliquent les mesures nécessaires aux comptes compromis, mettent en quarantaine les fichiers malveillants et appliquent une authentification tenant compte des risques, le cas échéant. Vous pouvez également intégrer des solutions de gestion des identités au moyen de l'authentification SAML (Security Assertion Markup Language).

Unification des règles DLP destinées aux applications cloud et à d'autres canaux

Proofpoint CASB partage les classificateurs DLP (dont des identifiants intelligents intégrés, des dictionnaires, des règles et des modèles) avec d'autres produits Proofpoint pour accélérer l'identification et la protection des données sensibles. Vous pouvez facilement déployer des règles DLP cohérentes qui s'appliquent à la fois aux applications SaaS, aux buckets IaaS et à la messagerie électronique. De même, vous pouvez unifier la gestion des incidents DLP en l'appliquant à plusieurs canaux grâce à la console Proofpoint CASB. Plus de 240 classificateurs intégrés couvrent la norme PCI, le RGPD et les réglementations sur les données personnelles et les données médicales personnelles. Des règles contextuelles personnalisées et des technologies de détection avancées, telles que la correspondance exacte de données, vous permettent de créer vos propres règles DLP afin de contrôler le partage ou le téléchargement des données. Vous pouvez restreindre l'accès aux données à partir de terminaux non gérés, mettre en quarantaine des fichiers et limiter les autorisations de partage pour les fichiers et les buckets afin d'assurer le maintien de votre conformité.

Nous vous aidons à protéger les données à risque en identifiant les autorisations étendues sur les fichiers et les partages de données non autorisés. Vous pouvez mettre en corrélation des connexions suspectes ou des buckets AWS S3 mal configurés avec des incidents DLP.

Gouvernance des applications cloud et tierces

Proofpoint CASB vous procure une visibilité sur les applications non approuvées (Shadow IT) dans toute l'entreprise. Nous vous aidons à auditer les journaux du trafic réseau et à découvrir les applications cloud. Notre catalogue comprend 46 000 applications et propose plus de 50 attributs pour chacune d'elles. Les applications cloud peuvent être catégorisées par type et par score de risque. Cette classification vous aide à déterminer les risques de sécurité, les vulnérabilités aux fuites de données et les points de non-conformité. Vous pouvez bloquer les applications à risque ou accorder aux utilisateurs des accès en lecture seule à celles-ci.

Nous détectons et évaluons également les autorisations OAuth pour les applications et scripts tiers qui accèdent aux services cloud de base approuvés par l'équipe informatique. Notre analyse approfondie vous permet d'identifier les applications à risque, y compris celles qui sont malveillantes, ainsi que de réduire votre surface d'attaque. Vous pouvez définir ou automatiser certaines actions en fonction du score de risque et du contexte.

Simplifiez la sécurité et la conformité IaaS multicloud et multirégion grâce à une gestion centralisée. Une console unique vous permet de gérer le niveau de sécurité de votre cloud IaaS. Nous vous aidons à identifier les ressources et les comptes IaaS approuvés et non approuvés, ainsi qu'à détecter les erreurs de configuration et les problèmes de conformité.

Déploiement rapide grâce à une architecture sans agent

Notre architecture sans agent offre une valeur ajoutée exceptionnelle. Des fonctionnalités intégrées efficaces fonctionnent en collaboration avec vos produits cloud existants pour prévenir, détecter et neutraliser les menaces dans le cloud, rapidement et automatiquement. L'authentification SAML tenant compte des risques et l'isolement du Web permettent d'assurer une prévention des menaces dans le cloud aussi précoce que possible. Vous pouvez également intégrer la solution avec des API cloud, des outils hybrides de gestion des identités et des produits d'orchestration de la sécurité (dont Proofpoint Threat Response) dans le but de détecter et de neutraliser toute menace qui franchirait les défenses.

POUR EN SAVOIR PLUS, PROFITEZ D'UNE ÉVALUATION GRATUITE

Consultez la page **proofpoint.com/fr/products/cloud-app-security-broker**.

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.

0105-002-01-02 7/20