PRÉSENTATION DE SOLUTION

proofpoint.

# PROOFPOINT CLOUD APP SECURITY

## PROTECTION DES UTILISATEURS DU CLOUD ET DES DONNÉES

### PROBLÈMES

- Compromission des identifiants
- Malwares
- Fuite de données et risques de conformité

### PRINCIPAUX AVANTAGES

- Protection des utilisateurs et des données contre toute compromission de compte et les menaces avancées dans le cloud
- Intégration de la détection des menaces et de contrôles d'accès dans l'environnement de messagerie et le cloud
- Contrôle de l'accès au cloud grâce à l'analyse du comportement des utilisateurs et à l'authentification à plusieurs facteurs
- Intégration de renseignements sur les menaces pour empêcher les fuites de données
- Contrôle des modules complémentaires tiers
- Déploiement rapide dans le cloud

### PRODUITS

- Targeted Attack Protection (TAP)
- Cloud App Security Broker (PCASB)
- Email Data Loss Prevention and Encryption

Assurer la protection de vos collaborateurs et des données qu'ils génèrent n'a jamais été aussi difficile et critique qu'aujourd'hui.

En effet, les utilisateurs, les applications et les données ont franchi le périmètre de votre réseau. Les services de messagerie et applications cloud tels que Microsoft Office 365, Google G Suite et Box permettent aux utilisateurs de travailler depuis des endroits aussi divers que leur domicile, un café ou un train. Ces applications, qui hébergent des données sensibles, se connectent à un large éventail de modules complémentaires tiers.

De nos jours, les cyberattaques ciblent les individus, pas uniquement l'infrastructure. Nombre d'entre elles s'en prennent à des personnes ou à des entreprises spécifiques. Elles sont conçues pour émuler vos méthodes de travail. Elles incitent les utilisateurs à ouvrir des fichiers dangereux, à cliquer sur des liens malveillants et à installer des modules complémentaires à risque. Les conséquences ne se font pas attendre : compromission d'identifiants, propagation de malwares, fuite de données ou encore problèmes de conformité.

Le renforcement de la sécurité passe par une approche intégrée articulée autour des personnes. Pour une migration vers le cloud en toute sécurité, vous devez être en mesure de détecter les menaces, de mettre en place des contrôles d'accès et de protéger vos données. Ces fonctions essentielles doivent en outre couvrir l'ensemble de vos outils de productivité et de messagerie cloud.

Proofpoint Cloud App Security vous protège contre les compromissions de compte, les fichiers malveillants, la fuite de données et les risques de conformité dans le cloud. Notre solution complète, axée sur l'individu, sécurise les applications de messagerie, de stockage et de collaboration, et bien plus encore. Pour ce faire, elle combine plusieurs fonctionnalités essentielles :

- Protection contre les menaces avancées transmises par des fichiers malveillants
- Détection et neutralisation des comptes compromis
- Contrôles d'accès pour les utilisateurs et les applications tierces
- Prévention des fuites de données (DLP)
- Analyses et authentification à plusieurs facteurs

Grâce à ces puissantes fonctionnalités, vous pouvez vous protéger contre les attaques ciblées, sécuriser vos informations et préserver votre conformité dans le cloud.

## PROTECTION DES UTILISATEURS DU CLOUD CONTRE LES MENACES AVANCÉES

Les cyberattaques ont imité le comportement des utilisateurs et migré vers le cloud. Ransomwares, chevaux de Troie bancaires, vols d'identifiants de connexion, tentatives de phishing et autres — on ne compte plus les menaces avancées qui ciblent les utilisateurs au travers des services de messagerie et autres applications cloud.

Ainsi, un document malveillant chargé sur un service de stockage cloud peut se propager instantanément au sein de votre environnement par le biais des systèmes de synchronisation et de partage des fichiers d'entreprise (EFSS). D'où l'importance d'une détection précoce. Cependant, les outils d'ancienne génération ne sont pas armés pour détecter les malwares polymorphes et les liens malveillants (et leurs multiples variantes).

Cloud App Security détecte, analyse et bloque les URL et les fichiers malveillants. La solution combine analyse en environnement sandbox, informations de cyberveille et mise en corrélation des menaces sur plusieurs canaux pour identifier les menaces dissimulées et les contrer.

### Analyse en environnement sandbox

Les fonctions de sandboxing et d'analyse prédictive bloquent les menaces de façon rapide et précise — avant qu'elles ne provoquent le moindre dégât.

Des techniques d'analyse statique et dynamique inspectent l'intégralité de la chaîne d'attaque. Elles observent les comportements, le code et le protocole à la recherche de fichiers malveillants.

Notre technologie ne se contente pas de détecter les attaques, elle en tire également des enseignements. Elle observe les modes opératoires, les comportements et les stratagèmes déployés lors de chaque attaque de façon à pouvoir intercepter la suivante plus facilement. Elle vous aide à contenir les menaces en temps réel grâce une mise en quarantaine automatique et à d'autres fonctions de neutralisation.

### Cyberveille

Cloud App Security établit des corrélations entre les campagnes d'attaques en fonction des différents secteurs d'activité et zones géographiques touchés. Nous nous appuyons également sur les renseignements issus de Proofpoint Emerging Threats (ET) Intelligence, la source la plus précise et opportune de cyberveille sur les menaces disponible sur le marché. Notre tableau de bord des menaces vous offre une visibilité sur différents aspects des attaques :

- Personnes ciblées au sein de votre entreprise
- Auteur de l'attaque et mode opératoire
- Objectif de l'attaque

Vous pouvez ainsi facilement distinguer les attaques à large spectre de celles ciblant des cadres dirigeants et d'autres collaborateurs présentant un intérêt pour les cybercriminels.

### Corrélation multicanal

Cloud App Security met en corrélation les activités liées aux menaces dans l'environnement de messagerie et le cloud, vous permettant ainsi d'identifier les utilisateurs à risque et les compromissions de sécurité. Notre tableau de bord vous permet par ailleurs d'établir facilement les liens entre les attaques par phishing d'identifiants de connexion et les connexions suspectes. De cette façon, vous pouvez vous concentrer en priorité sur les utilisateurs les plus à risque. Vous pouvez surveiller de plus près ces comptes cloud ou leur appliquer des règles de contrôle d'accès plus strictes afin d'empêcher toute compromission.

Top User at Risk
Last 30 days

| User | Suspicious Logins | Failed Logins Attemps | Email Threats | Phishing Threats | Permitted Clicks | Last User Activity |
|---|---|---|---|---|---|---|
| **Joe Greene** Jgreene@acme.com | 14 | 0 | 0 | 0 | 0 | Jul 10 12:47 PM |
| **Abby Boyle** aboyle@acme.com | 12 | 0 | 0 | 0 | 0 | Jul 04 12:33 PM |

Cloud App Security met en corrélation les activités des utilisateurs et les risques en contexte

## SURVEILLANCE ET CONTRÔLE DE L'ACCÈS AU CLOUD

Les effectifs modernes exigent un accès au cloud continu, en tout lieu et sur n'importe quel appareil. Dans un tel environnement, il est plus important que jamais de surveiller le comportement des utilisateurs dans les applications cloud. Cela commence par l'établissement de comportements de base sûrs. Tout comportement anormal d'un utilisateur peut être le signe que les cybercriminels ont :

- compromis des comptes d'utilisateurs
- dérobé des informations
- détruit des données

Des indicateurs de risque vous permettent d'intervenir sans délai. Créez des règles pour contrôler l'accès aux services cloud. Mettez en place un système de validation des utilisateurs basé sur l'authentification à plusieurs facteurs. Notre analyse comportementale puissante, associée à une authentification robuste, vous aide à vérifier l'identité des utilisateurs. De cette façon, vous pouvez octroyer les niveaux d'accès appropriés aux utilisateurs et aux modules complémentaires tiers.

### Analyse comportementale

Cloud App Security combine données contextuelles et analyse du comportement des utilisateurs. Le contexte fournit notamment des informations sur l'emplacement de l'utilisateur, l'appareil, le réseau et l'application cloud à laquelle il tente d'accéder. Sont considérées comme des comportements anormaux les tentatives d'accès inhabituelles ou excessives, etc.

| SEVERITY | DATE | LOCATION | USER | CONTROL | TYPE | NOTIFIED | CLOUD SERVICE |
|---|---|---|---|---|---|---|---|
| – | Thu 19 Apr, 2018 16:38:53 | Hong Kong | Michael W. | Suspicious Login | Suspicious Login | | Office |

| | |
|---|---|
| ALERT GUID | 734df7ed69b4ccf86056398f848cd167 |
| GUID | f7533888f93fa93066a1a077da9cb6b7 |
| DATE | Thu 19 Apr, 2018 12:23:41 |
| URL | |
| LOCATION | Hong Kong |
| IP | 113.28.1.221 |
| FULL NAME | Michael Wallace |
| USERNAME | michael_wallace@omega-pfpt.com |
| AGENT | CBAInPROD |
| DEVICE | Other |
| OS | Other |
| BROWSER | Other |

| | |
|---|---|
| CLOUD SERVICE | Cross Applications |
| THREAT | N/A |
| DECISION | Other |
| CHALLENGE | N/A |
| CONTROL | Suspicious Source |
| RESOURCE | Login Service |
| ACTION | Login |
| DETAILED DESCRIPTION | Suspicious login attempt detected for michael_wallace@omega-pfpt.com, from Scanner, Brute_Forcer 113.28.1.221 (Milomex Limited) (ET Intelligence) |
| ALERT DESCRIPTION | Suspicious Login Has Been Detected |

Pour identifier les anomalies, nous recourons aux empreintes capturées précédemment, à des seuils d'alerte et à des fonctionnalités avancées d'apprentissage automatique. Diverses possibilités s'offrent à vous :

- Spécifier que seuls les appareils d'entreprise respectant vos normes de sécurité en matière de terminaux peuvent accéder à une application cloud déterminée
- Limiter les autorisations au moyen d'accès en lecture seule
- Restreindre les données que l'utilisateur peut télécharger

Cloud App Security met en corrélation des informations de cyberveille sur plusieurs canaux et des indicateurs de risque spécifiques à l'utilisateur. Cette approche vous permet de détecter rapidement toute activité suspecte, de prioriser les alertes et d'éviter une baisse de la vigilance due à un volume élevé d'alertes. Vous pouvez en outre enquêter sur des activités et des alertes antérieures à l'aide de nos tableaux de bord intuitifs et du filtrage. Grâce à nos modèles de règles robustes, vous recevez des alertes en temps réel. Vous pouvez dès lors mettre en place un système d'authentification basé sur le risque et, au besoin, réduire les privilèges. Vous évitez ainsi toute utilisation abusive de vos applications, ainsi que toute exposition ou suppression de vos données.

### Authentification à plusieurs facteurs

Notre proxy SAML vous permet d'intégrer des solutions existantes de gestion des identités. Notre solution d'authentification à plusieurs facteurs vérifie en outre l'identité des utilisateurs avant toute connexion ou activité à risque. Enfin, notre architecture multimodale vous permet de mettre en place un système de protection par le biais d'une API ou d'un proxy inverse et de transfert.

## PROTÉGEZ LES SERVICES SUIVANTS AVEC CLOUD APP SECURITY :

**SERVICES DE MESSAGERIE CLOUD**

- Office 365 Exchange Online
- Gmail

**SERVICES CLOUD**

- Office 365 Exchange Online (données au repos)
- Office 365 SharePoint Online
- Office 365 OneDrive
- Google Drive
- Google Cloud
- Box
- Dropbox
- Salesforce
- Amazon Web Services S3

## PRÉVENTION DES FUITES DE DONNÉES DANS LE CLOUD

La migration à grande échelle des données d'entreprise dans le cloud signifie que de plus en plus d'informations sensibles y sont stockées. Dans 50 % des cas, les compromissions de données signalées sont le fait d'identifiants de connexion faibles ou qui ont été dérobés. Pour s'emparer des identifiants, les cybercriminels recourent généralement à des techniques de compromission de données, au phishing, à des voleurs d'identifiants de connexion et à des attaques par force brute. Pour détecter et prévenir les compromissions de données, vous devez impérativement vous doter de fonctions de protection des données prenant en compte les risques et mettre en place une authentification robuste.

Cloud App Security combine détection des menaces sur plusieurs canaux, visualisation des données sensibles et contrôles DLP. La visibilité axée sur les utilisateurs et la surveillance des comportements permettent d'identifier rapidement les personnes ciblées, ainsi que toute activité sur des comptes orphelins et compromis. Pour déterminer qui accède aux données sensibles, Proofpoint DLP analyse divers éléments :

- E-mails en mouvement
- E-mails au repos
- Espace de stockage dans le cloud
- Données hébergées par d'autres applications cloud

Fort de ces connaissances, vous pourrez identifier rapidement les utilisateurs à protéger en priorité, et ainsi réduire les fuites de données sensibles et limiter les dégâts. Vous pouvez notamment définir des règles automatiques de sécurité des données pour chiffrer les e-mails, restreindre les autorisations d'accès aux fichiers et exiger une authentification à plusieurs facteurs pour les utilisateurs à risque.

### Prévention des fuites de données

Proofpoint DLP compte plus de 80 règles de sécurité des données prédéfinies. Vous pouvez notamment détecter et classer automatiquement les données sensibles. Ou encore, corriger les compromissions de données au niveau des services de messagerie et des applications cloud de façon à accélérer l'identification et la protection des données sensibles. Notre solution offre notamment les fonctionnalités suivantes :

- Des classificateurs de données unifiés suivent les données en mouvement et au repos.
- Des classificateurs intégrés couvrent la norme PCI, le code PII, la loi HIPAA et le RGPD.
- Des dictionnaires et des fonctions de mise en correspondance basée sur la proximité améliorent la détection des données sensibles et automatisent la conformité réglementaire.
- Les correspondances exactes de données permettent de charger facilement des dictionnaires ou identifiants personnalisés afin de détecter les informations propres à votre entreprise, notamment les numéros de compte et d'autres données structurées issues de bases de données.
- L'analyse de l'empreinte numérique des documents permet de détecter les données sensibles dans du contenu non structuré (formules, code source, formulaires, contrats, propriété intellectuelle, etc.).
- La solution est à même d'analyser 300 types de fichiers différents dès sa mise en service. Notre outil de profilage des types de fichiers prend en charge des types de fichiers nouveaux, personnalisés et propriétaires.

Des règles personnalisées flexibles vous permettent de créer vos propres règles DLP afin de contrôler l'envoi, le partage et le téléchargement de vos données. Vous pouvez notamment contrôler les accès dangereux ou non autorisés aux e-mails et aux fichiers afin de réduire le partage public grâce à des fonctions de chiffrement prenant en compte le contexte, de mise en quarantaine et d'autorisation de partage de fichiers. De plus, vous avez la possibilité de surveiller de près la conformité en vous abonnant à des alertes, ainsi que de filtrer les événements et les alertes pour la génération de rapports.

## AUTOMATISATION DES CONTRÔLES DES APPLICATIONS TIERCES

Le marché des applications cloud compte des centaines de modules complémentaires destinés à renforcer les capacités des plates-formes Microsoft Office 365, Google G Suite, Box et autres. Face à cette diversité, l'accès à vos données par des tiers est devenu un risque de conformité majeur.

Certains modules complémentaires d'édition d'e-mails et de fichiers exigent un accès total au contenu de vos e-mails, contacts et fichiers. Ils peuvent en outre stocker ces données en différents endroits, créant ainsi un risque d'infraction au RGPD et aux réglementations en matière d'informations d'identification personnelle.

Notre évaluation approfondie et indépendante vous protège contre les modules complémentaires et les scripts tiers. Ce niveau adéquat de visibilité et de contrôle vous permet de préserver la productivité de vos collaborateurs et de limiter le risque qu'ils présentent. Des alertes vous informent en cas d'installation d'applications et de scripts à risque. Des contrôles vous permettent de définir ou d'automatiser les mesures de correction en fonction des résultats de l'analyse et du score de risque de l'application. Enfin, des règles vous aident à définir les autorisations octroyées à un jeton d'accès. Elles peuvent également rejeter toute demande d'accès OAuth émanant d'une application ou d'un script dépassant les seuils spécifiés.

## DÉPLOIEMENT RAPIDE DANS LE CLOUD

Les plates-formes cloud nécessitent une protection hébergée dans le cloud. Notre architecture cloud permet un déploiement rapide et offre une rentabilité immédiate. Vous n'aurez pas à attendre des semaines, voire des mois, puisque quelques jours suffisent pour protéger des centaines de milliers d'utilisateurs. De plus, nous utilisons le cloud pour mettre quotidiennement à jour notre logiciel afin de vous aider à garder une longueur d'avance sur les cybercriminels. Notre déploiement dans le cloud vous offre également la flexibilité nécessaire pour protéger les utilisateurs sur n'importe quel réseau ou appareil.

## PRODUITS

**Proofpoint Targeted Attack Protection (TAP)** détecte, analyse et bloque les menaces avancées véhiculées par la messagerie électronique (TAP for Email) et les applications cloud (TAP SaaS Defense). La solution identifie les attaques connues et émergentes qui recourent à des fichiers malveillants et à des URL dangereuses. L'efficacité de TAP est sans égal lorsqu'il s'agit d'arrêter net les attaques ciblées qui font appel à des malwares polymorphes, des documents « piégés » et des techniques de phishing d'identifiants de connexion pour faire main basse sur les informations sensibles. Pour en savoir plus, consultez la page proofpoint.com/fr/product-family/advanced-threat-protection.

**Proofpoint Cloud App Security Broker (PCASB)** protège les utilisateurs d'applications cloud contre les menaces avancées, les accès non autorisés, les fuites de données et les risques de conformité. La solution offre une vue granulaire axée sur les personnes de l'accès aux applications et de la gestion des données. Elle combine protection contre les menaces avancées, contrôle de l'accès, prévention des fuites de données (DLP), gouvernance des applications tierces et authentification à plusieurs facteurs 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. Découvrez-en plus sur la solution et inscrivez-vous pour une évaluation gratuite des risques sur la page proofpoint.com/us/products/cloud-app-security-broker.

**Proofpoint Email Data Loss Prevention and Encryption** prévient les fuites de données sensibles via la messagerie et sécurise les e-mails et pièces jointes sensibles au moyen de fonctions de classification automatique et de chiffrement fondé sur des règles, sans les coûts et la complexité associés aux solutions d'ancienne génération. Pour en savoir plus, consultez la page proofpoint.com/fr/product-family/information-protection.