Solutions Proofpoint et Amazon Web Services

Comment Proofpoint offre aux clients AWS une sécurité et une conformité centrées sur les personnes

Produits

- Contrôles d'accès adaptatifs
- Proofpoint Cloud App Security Broker
- Gestion du niveau de sécurité cloud
- Proofpoint Email Fraud Defense
- Proofpoint Emerging Threats Intelligence
- Proofpoint Enterprise Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Threat Response Auto-Pull
- Proofpoint Zero Trust Network Access

Principaux avantages

- Simplification de la sécurité et de la conformité multirégion d'AWS grâce à une gestion centralisée
- Identification des données sensibles et classification dans des référentiels de stockage cloud
- Blocage des connexions suspectes et prévention de la prise de contrôle de comptes de ressources AWS
- Visibilité sur les activités des utilisateurs et les mouvements de données dans les instances AWS EC2 et Amazon WorkSpaces
- Sécurisation de l'accès distant pour votre équipe
- Mise en quarantaine automatique des emails malveillants qui contournent les défenses périmétriques

Les plates-formes cloud telles qu'Amazon Web Services (AWS) ont transformé les méthodes de travail des entreprises. Elles permettent aux collaborateurs de travailler à distance dans le cloud, et aux entreprises de réduire les coûts, d'accroître leur agilité et d'accélérer l'innovation. Face à cette évolution, les cybercriminels ont délaissé l'ancien périmètre réseau pour se concentrer sur les personnes, ainsi que les données, les systèmes et les ressources auxquels elles accèdent. Dans ce contexte mouvant, vous devez sécuriser l'accès aux ressources AWS, prévenir les fuites de données et préserver votre conformité. La gamme de produits Proofpoint vous permet d'atteindre ces objectifs.

Nos solutions vous aident à gérer les problèmes suivants :

- Applications non approuvées (Shadow IT)
- Comptes compromis
- Violations de la conformité
- Usurpations de comptes de messagerie
- Accès non autorisés
- Fuites et exfiltrations de données
- Menaces internes
- Activités réseau suspectes

Identification des ressources et comptes AWS

Proofpoint Cloud App Security Broker (CASB) combine des contrôles centrés sur les personnes et des fonctionnalités de détection des comptes cloud compromis, de prévention des fuites de données (DLP) et de gestion des applications cloud et tierces. Il vous aide à sécuriser des plates-formes cloud telles qu'AWS. Notre solution CASB multimodale prend en charge les modèles de déploiement basés sur API et proxy.

Proofpoint CASB simplifie la sécurité et la conformité multirégion d'AWS grâce à une gestion centralisée. Vous bénéficiez d'une visibilité sur l'ensemble de vos applications SaaS (Software-as-a-Service) et de vos ressources IaaS (Infrastructure-as-a-Service) dans AWS.

Notre solution vous offre les possibilités suivantes :

- Visualiser les tendances en matière de création de ressources et rechercher les anomalies telles que la création ou la suppression excessives de ressources
- Explorer les ressources découvertes et vous assurer que les comptes sont mis en service conformément aux réglementations et aux bonnes pratiques
- Auditer les journaux de trafic réseau et identifier les applications cloud et les comptes AWS qui accèdent à votre réseau

Prévention des menaces dans le cloud

Les contrôles d'accès adaptatifs de Proofpoint CASB permettent une évaluation en temps réel de la sécurité, en fonction du rôle, du contexte et du niveau de risque. Ils bloquent automatiquement l'accès par des cybercriminels connus ou depuis des emplacements et réseaux dangereux, et appliquent aux utilisateurs à haut niveau de risque et de privilèges des contrôles basés sur les risques. Ceux-ci peuvent inclure une authentification renforcée, des règles pour les terminaux gérés et la mise en œuvre de réseaux privés virtuels (VPN).

Les contrôles d'accès adaptatifs bloquent les connexions suspectes. Ils empêchent la prise de contrôle de comptes de vos ressources AWS.

Ces contrôles vous offrent les possibilités suivantes :

- Bloquer l'accès aux comptes des utilisateurs les plus exposés par des connexions suspectes
- Créer une liste de blocage reprenant les pays où votre entreprise n'est pas présente

Identification des services mal configurés

Proofpoint CASB intègre la gestion du niveau de sécurité cloud, ce qui vous permet de gérer le niveau de sécurité dans votre environnement cloud. Vous pouvez ainsi organiser, configurer et assurer la maintenance de vos ressources cloud, afin de mieux respecter les normes de conformité.

Cette fonctionnalité vous offre les possibilités suivantes :

- Identifier les configurations et les paramètres qui s'écartent des normes publiées
- Recommander de bonnes pratiques pour corriger les problèmes de configuration identifiés qui présentent un risque de sécurité
- Simplifier la sécurité et la conformité cloud grâce à la gestion centralisée de toutes les ressources cloud, indépendamment du compte et de la région

Protection des données sensibles

Proofpoint Enterprise Data Loss Prevention (DLP) regroupe nos solutions DLP pour la messagerie électronique, le cloud et les endpoints. La solution combine les données d'analyse des contenus, des comportements et des menaces de ces canaux. Cela vous permet d'aborder tout le spectre des scénarios de fuites de données centrées sur les personnes.

Proofpoint Enterprise DLP vous aide à identifier les données sensibles et à les classifier dans les référentiels de stockage cloud.

Proofpoint Enterprise DLP vous offre les possibilités suivantes :

- Surveiller les activités des fichiers afin de détecter les infractions aux règles DLP
- Surveiller les buckets S3 pour prévenir le partage excessif
- Créer des règles de sécurité des données (Cette solution s'appuie sur 240 classificateurs DLP intégrés, notamment des identifiants intelligents intégrés, des dictionnaires, des règles et des modèles partagés avec d'autres produits DLP Proofpoint.)

Protection de vos comptes AWS

Amazon GuardDuty s'appuie sur Proofpoint Emerging Threats (ET) Intelligence pour protéger les instances AWS.

Proofpoint ET Intelligence est la source la plus précise et opportune de threat intelligence du secteur. Il combine base de données des menaces observées au niveau mondial, analyse des malwares et flux de réputation des adresses IP et des domaines en temps quasi réel. Cette solution fournit à vos équipes de sécurité les informations et le contexte nécessaires pour enquêter sur les attaques et les neutraliser.

Nous proposons des produits et solutions de nouvelle génération axés sécurité, conformité, gestion des risques numériques et réponse aux incidents. Nos informations sur la réputation des adresses IP et des domaines sont fondées sur l'une des gammes les plus complètes de technologies de protection. Elles couvrent la messagerie électronique, les terminaux mobiles, les réseaux sociaux, les services SaaS et les environnements réseau.

Gestion des menaces internes

Proofpoint Insider Threat Management (ITM) fait partie de la plate-forme Proofpoint Information and Cloud Security. Il vous protège des fuites de données, des actes malveillants et des atteintes à la marque d'origine interne. Proofpoint ITM vous protège contre les utilisateurs autorisés qui pourraient faire preuve de malveillance ou de négligence. Par ailleurs, la solution met en corrélation les activités des utilisateurs et les mouvements de données, de façon à vous protéger contre les compromissions de données induites par des utilisateurs internes.

Proofpoint ITM offre une visibilité sur les activités des utilisateurs et les mouvements de données dans les instances AWS EC2 et Amazon WorkSpaces.

Proofpoint ITM vous offre les possibilités suivantes :

- Bénéficier d'une visibilité totale sur les activités des endpoints et obtenir des informations contextuelles complètes sur les incidents imputables aux utilisateurs
- Visualiser le contexte des menaces ciblant des groupes d'utilisateurs spécifiques de façon à mieux gérer les risques posés par les utilisateurs

Sécurisation de l'accès distant aux applications cloud

Proofpoint Zero Trust Network Access (ZTNA) constitue une alternative Zero Trust et centrée sur les personnes aux VPN. Il sécurise l'accès distant à n'importe quelle application d'entreprise, peu importe son emplacement. Proofpoint ZTNA offre à vos utilisateurs un accès sécurisé microsegmenté à des centaines d'instances cloud. Vous pouvez automatiser la connexion de cloud à cloud et autoriser une mise en réseau de cloud hybride entre les serveurs sur site et les clouds publics.

Proofpoint ZTNA offre à vos collaborateurs, sous-traitants, partenaires et clients un accès distant sécurisé aux applications hébergées sur AWS.

Proofpoint ZTNA vous offre les possibilités suivantes :

- Gérer les règles d'accès distant aux ressources de l'entreprise stockées dans le centre de données ou le cloud AWS depuis une console unique
- Bénéficier d'une alternative Zero Trust qui offre un accès segmenté, vérifié et audité à chaque utilisateur

Amélioration de la fiabilité de la messagerie

Proofpoint Email Fraud Defense (EFD) protège votre entreprise de la fraude par email. Il vous offre une visibilité totale sur les domaines similaires et les emails envoyés via votre domaine. Il réduit également les risques que peuvent poser vos fournisseurs. Il identifie vos fournisseurs et les domaines similaires enregistrés par des tiers.

Proofpoint EFD sécurise les emails provenant d'Amazon SES. Il vous offre la visibilité, les outils et les services nécessaires pour autoriser les messages légitimes.

Proofpoint EFD vous offre les possibilités suivantes :

- Corriger les systèmes d'envoi d'emails mal configurés et les problèmes de remise liés aux erreurs de validation de l'authentification des emails
- Identifier et signaler les usurpations de comptes de messagerie
- Exposer les problèmes liés aux signatures DKIM et aux enregistrements SPF tels qu'observés par les destinataires des emails

Mise en quarantaine automatique des emails malveillants

L'appliance Proofpoint Threat Response Auto-Pull (TRAP) peut être hébergée sur AWS. Elle permet à vos équipes de sécurité d'analyser les emails et de supprimer automatiquement les messages malveillants. Elle met également les emails indésirables en quarantaine après leur remise.

Proofpoint TRAP simplifie votre processus de réponse aux incidents liés à la messagerie électronique. Vous bénéficiez d'une solution puissante, qui permet de réduire le temps que les équipes chargées de la sécurité consacrent au nettoyage des emails malveillants et indésirables.

Proofpoint TRAP vous offre les possibilités suivantes :

- Surveiller automatiquement les boîtes email
- Réduire de manière exponentielle le temps que les équipes chargées de la sécurité et de la messagerie consacrent à l'orchestration de la sécurité de la messagerie électronique et à la réponse aux incidents
- Mettre en quarantaine les messages transférés à d'autres personnes ou à des listes de distribution

Pour en savoir plus sur le partenariat entre Proofpoint et AWS, consultez la page **proofpoint.com/us/partners/aws**.

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. 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.

0201-023-01-01 9/21