Proofpoint Cloud App Security Broker IaaS Protection

Identification des services cloud mal configurés et protection des données sensibles dans les stockages IaaS

DÉFIS

- Erreurs de configuration
- Ressources et comptes IaaS inconnus
- Fuite de données et conformité
- Prise de contrôle de comptes cloud

PRINCIPAUX AVANTAGES

- Sécurité multicloud et conformité simplifiées grâce à la gestion centralisée de toutes les ressources IaaS, indépendamment du fournisseur, du compte et de la région
- Identification des paramètres de sécurité mal configurés qui s'écartent des normes publiées
- Surveillance et analyse du comportement des utilisateurs pour détecter et bloquer les connexions et les activités administratives non autorisées
- Protection des données sensibles dans les stockages IaaS
- Découverte et gestion des comptes IaaS non approuvés
- Déploiement rapide dans le cloud

PRODUITS

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint CASB IaaS Protection

L'adoption du cloud s'accélère. En choisissant de déployer des applications SaaS pour améliorer l'agilité, la flexibilité et l'évolutivité, les équipes métier et informatique ont ouvert la voie aux équipes DevOps. Elles sont en effet de plus en plus nombreuses à développer de nouveaux services et applications sur une infrastructure cloud.

Votre entreprise compte peut-être des dizaines, voire des centaines, de comptes IaaS dont les charges de travail sont déployées sur un ou plusieurs services cloud. Et peut-être devez-vous stocker vos données dans des référentiels cloud situés dans différentes régions du monde en raison des réglementations en matière de protection des données. Le manque de visibilité sur les failles de votre dispositif de sécurité cloud peut compliquer la gestion de la sécurité et de la conformité de l'environnement IaaS. En outre, les menaces liées au cloud, telles que la compromission de comptes, et la pénurie de personnel qualifié peuvent ajouter à la complexité.

Les erreurs de configuration, de gestion ou autres commises par les clients peuvent entraîner des compromissions de grande ampleur. Les attaques contre les services cloud tels qu'Amazon Web Services (AWS), Microsoft Azure ou Google Cloud (GCP) peuvent être dues à ce type d'erreur. Les responsables de la sécurité et de la gestion des risques doivent identifier et réduire ces risques. Par ailleurs, les comptes IaaS, les ressources et les données sensibles stockées dans le cloud telles que les informations clients ou les dossiers de patients doivent impérativement être sécurisés.

Pour protéger vos environnements IaaS et assurer la conformité, Proofpoint CASB IaaS Protection (IaaS Protection) offre les fonctionnalités suivantes :

- Découverte des ressources IaaS
- Gestion du niveau de sécurité cloud
- Sécurité des données
- Protection contre les menaces
- Contrôles adaptatifs de l'accès

IaaS Protection est une fonctionnalité de Proofpoint CASB proposée sous forme de module complémentaire.

Identification des erreurs de configuration dans les environnements IaaS

IaaS Protection vous aide à gérer le niveau de sécurité dans votre environnement multicloud. Cette fonctionnalité de Proofpoint CASB identifie les configurations et paramètres qui s'écartent des normes publiées dans les services IaaS. Il peut par exemple s'agir de paramètres tels qu'un compte utilisateur racine qui n'applique pas l'authentification à plusieurs facteurs.

IaaS Protection évalue vos paramètres liés aux machines virtuelles, au stockage, au réseau et aux contrôles d'accès par rapport aux quatre normes de sécurité suivantes :

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

Lorsqu'il identifie des configurations erronées qui présentent un risque pour la sécurité, il recommande les bonnes pratiques pertinentes pour les corriger.

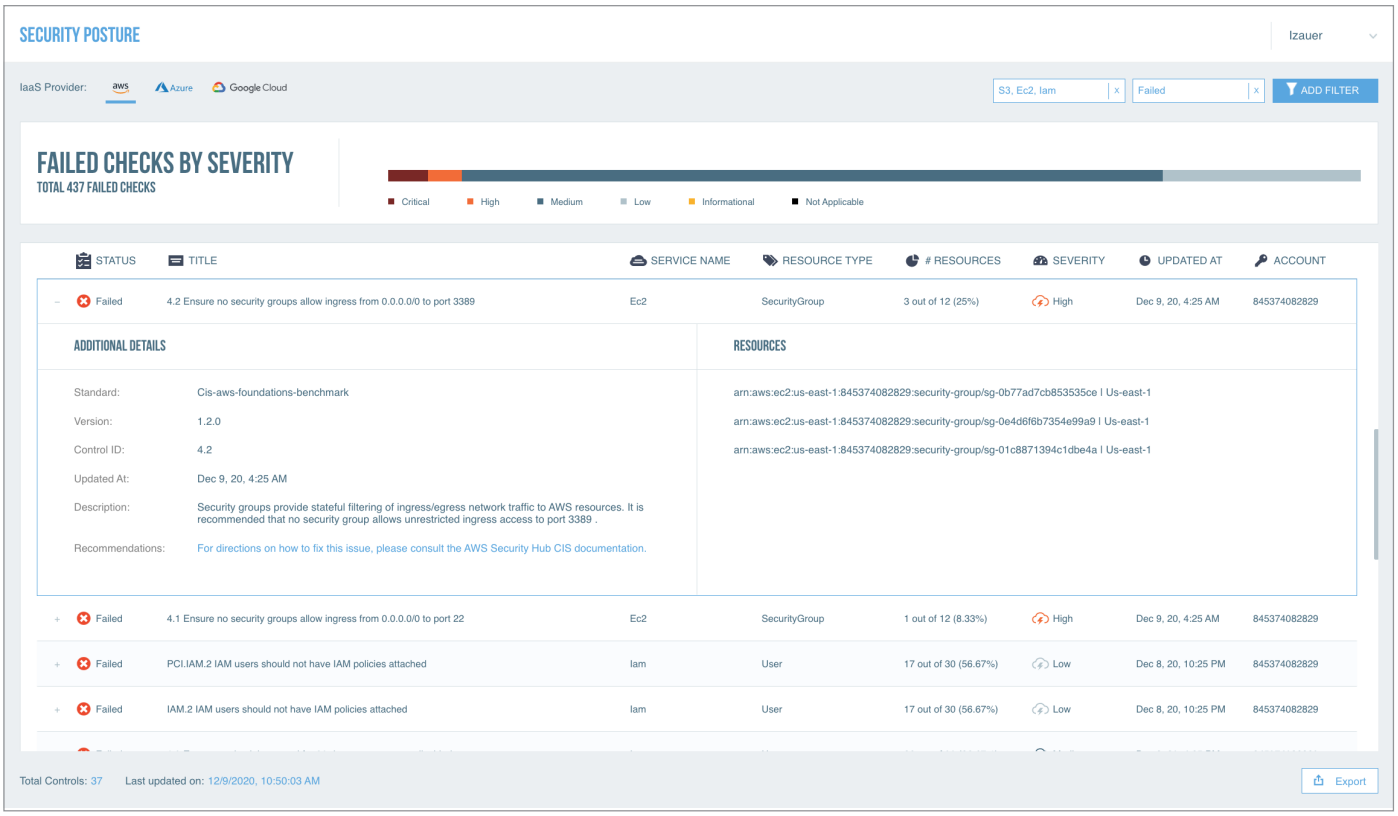

Figure 1. Tableau de bord du niveau de sécurité présentant une configuration erronée, les instructions sur les mesures à prendre pour respecter les normes de sécurité et une liste des ressources qui ne répondent pas aux normes

Surveillance et contrôle des activités des utilisateurs à privilèges

Contrairement aux applications SaaS, la plupart des utilisateurs IaaS sont des utilisateurs à privilèges, tels que des ingénieurs DevOps ou des développeurs de logiciels. Ils peuvent déployer, supprimer et configurer des ressources IaaS telles que des machines virtuelles et le stockage dans le cloud. Ils peuvent en outre attribuer des privilèges d'administration. C'est pourquoi la surveillance des activités des utilisateurs à privilèges est essentielle.

Combiné à Iaas Protection, Proofpoint CASB vous permet de définir des règles centrées sur les personnes (Figure 2). Ces règles sont basées sur un contexte enrichi et vous avertissent en cas d'activités non autorisées d'un utilisateur à privilèges. Le contexte fournit notamment des informations sur les risques liés à l'utilisateur, l'emplacement, le terminal et le réseau, ainsi que sur l'application cloud à laquelle l'utilisateur tente d'accéder. Vous pouvez par exemple empêcher les activités d'administration telles que la modification des autorisations liées aux buckets à partir de pays figurant sur liste de blocage.

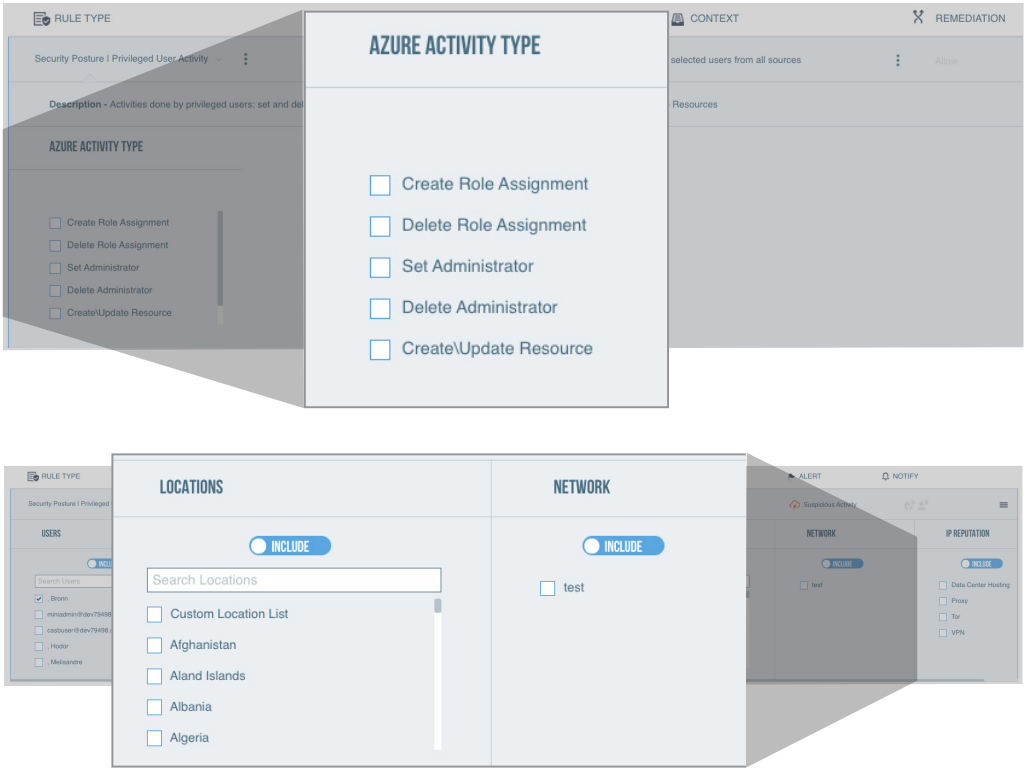

Figure 2. Modèle de règles pour les activités des utilisateurs à privilèges

Découverte de l'ensemble des ressources IaaS

Proofpoint CASB simplifie la sécurité et la conformité de l'environnement IaaS multicloud et multirégion grâce à une gestion centralisée. Vous bénéficiez en outre d'une visibilité complète sur toutes les applications SaaS et ressources IaaS, indépendamment du fournisseur, du compte et de la région (Figure 3).

Vous pouvez visualiser les tendances en matière de création de ressources et rechercher les anomalies telles que la création ou la suppression excessives de ressources. Vous pouvez également explorer les ressources découvertes par type et par région et vous assurer que les comptes sont mis en service conformément aux réglementations et aux bonnes pratiques. Par exemple, si vous êtes une entreprise multinationale ou européenne, vous pouvez surveiller les buckets déployés en dehors de l'UE pour prévenir les infractions au RGPD.

Découverte des comptes IaaS non approuvés

Proofpoint CASB vous procure une visibilité sur les applications non approuvées (Shadow IT) dans toute l'entreprise. Cela inclut les comptes IaaS qui n'ont pas été approuvés ou documentés par l'équipe informatique (Figure 4). Nous vous aidons à auditer les journaux de trafic réseau. Vous pouvez ainsi découvrir les applications cloud et les comptes IaaS qui ont été utilisés sur votre réseau. Il peut s'agir de comptes IaaS approuvés par l'équipe informatique, non documentés ou même privés. La console CASB vous permet de suivre directement l'état des comptes lors de l'audit des comptes non approuvés. Par exemple, si vous découvrez des comptes non documentés après une fusion, vous pouvez les mettre en service en fonction de critères de sécurité spécifiques afin d'assurer la conformité.

Figure 3. Tableau de bord de découverte des ressources IaaS indiquant les tendances, les emplacements et les types de ressources

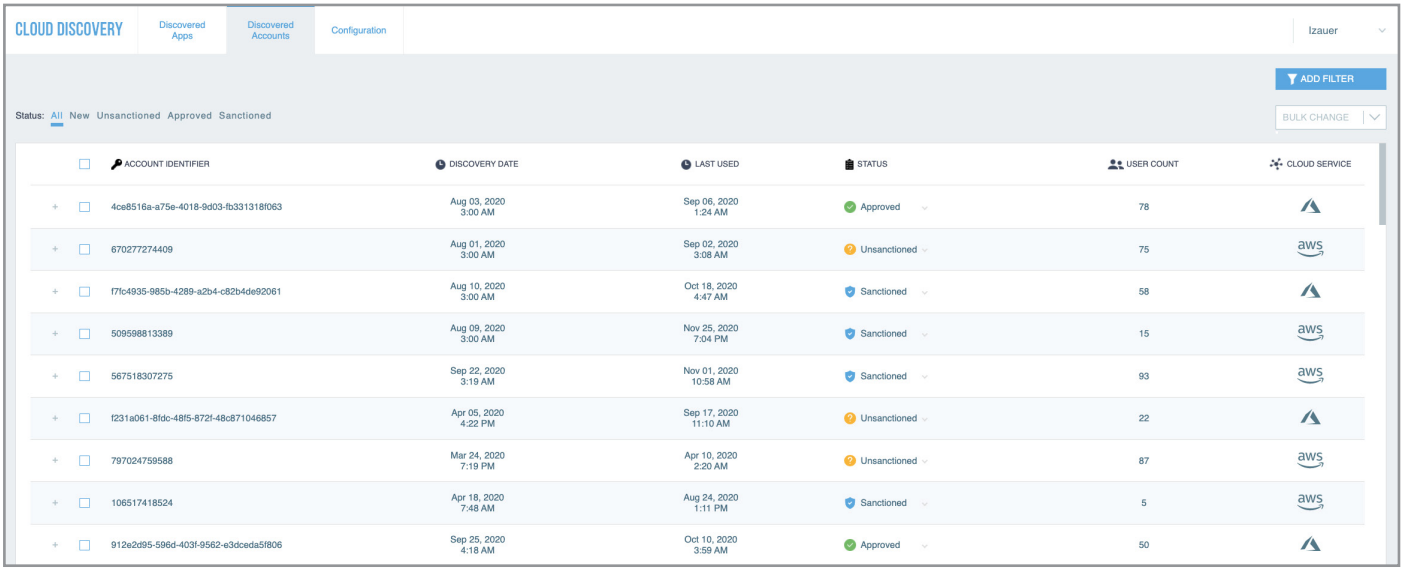

Figure 4. Tableau de bord indiquant l'état des comptes IaaS découverts sur le réseau d'entreprise

Protection des données sensibles dans les stockages cloud

Associé à IaaS Protection, Proofpoint CASB vous permet d'identifier et de classer les données sensibles contenues dans vos référentiels de stockage cloud, tels que les buckets AWS S3 et les conteneurs Azure Storage Blob. Il assure également les tâches suivantes :

- Surveillance des activités des fichiers afin de détecter les infractions aux règles DLP
- Surveillance des buckets et conteneurs pour détecter tout partage excessif
- Création de règles de sécurité des données fondées sur les classificateurs DLP, notamment les identifiants intelligents intégrés, les dictionnaires, les règles et les modèles partagés avec d'autres produits DLP Proofpoint

Nos classificateurs prêts à l'emploi vous permettent de réduire le temps de découverte et de protection des données réglementées présentes dans le stockage cloud. Ils vous permettent en outre de préserver votre conformité. En effet, en tant que composant de la solution Proofpoint Enterprise DLP, Proofpoint CASB vous permet de déployer des règles DLP cohérentes qui s'appliquent à la fois aux applications SaaS, aux buckets IaaS, à la messagerie et aux endpoints. De plus, vous pouvez centraliser la gestion des incidents DLP pour ces canaux depuis une console unique. En combinant les données d'analyse du contenu, du comportement et des menaces sur plusieurs canaux, vous pouvez déterminer si l'utilisateur qui a déclenché l'alerte DLP a été victime d'une compromission, a des intentions malveillantes ou est simplement négligent.

Fonctionnalités DLP de Proofpoint CASB :

- 240 classificateurs intégrés couvrant la norme PCI, le code PII, la loi PHI et le RGPD
- Dictionnaires et fonctions de mise en correspondance basée sur la proximité pour améliorer la prévention des fuites de données
- Correspondances exactes de données permettant d'automatiser le chargement de dictionnaires ou identifiants personnalisés afin de détecter les informations propres à votre entreprise (p. ex., les numéros de compte et d'autres données structurées issues des bases de données)
- Analyse de l'empreinte numérique des documents afin de détecter les données sensibles dans du contenu non structuré (formules, code source, formulaires, contrats, propriété intellectuelle, etc.)
- Prise en charge de 300 types de fichiers et outil de profilage des types de fichiers prenant en charge des types de fichiers nouveaux, personnalisés et propriétaires

Des modèles de règles flexibles vous permettent de définir des règles prenant en compte le contenu, le comportement de l'utilisateur et le type de menace (Figure 5). Vous pouvez ainsi contrôler la façon dont vos données sont partagées, chargées et téléchargées. Vous pouvez limiter automatiquement les autorisations de partage des buckets afin de préserver votre conformité. Vous pouvez par exemple surveiller le partage de buckets et interdire tout partage excessif à partir de pays figurant sur liste de blocage.

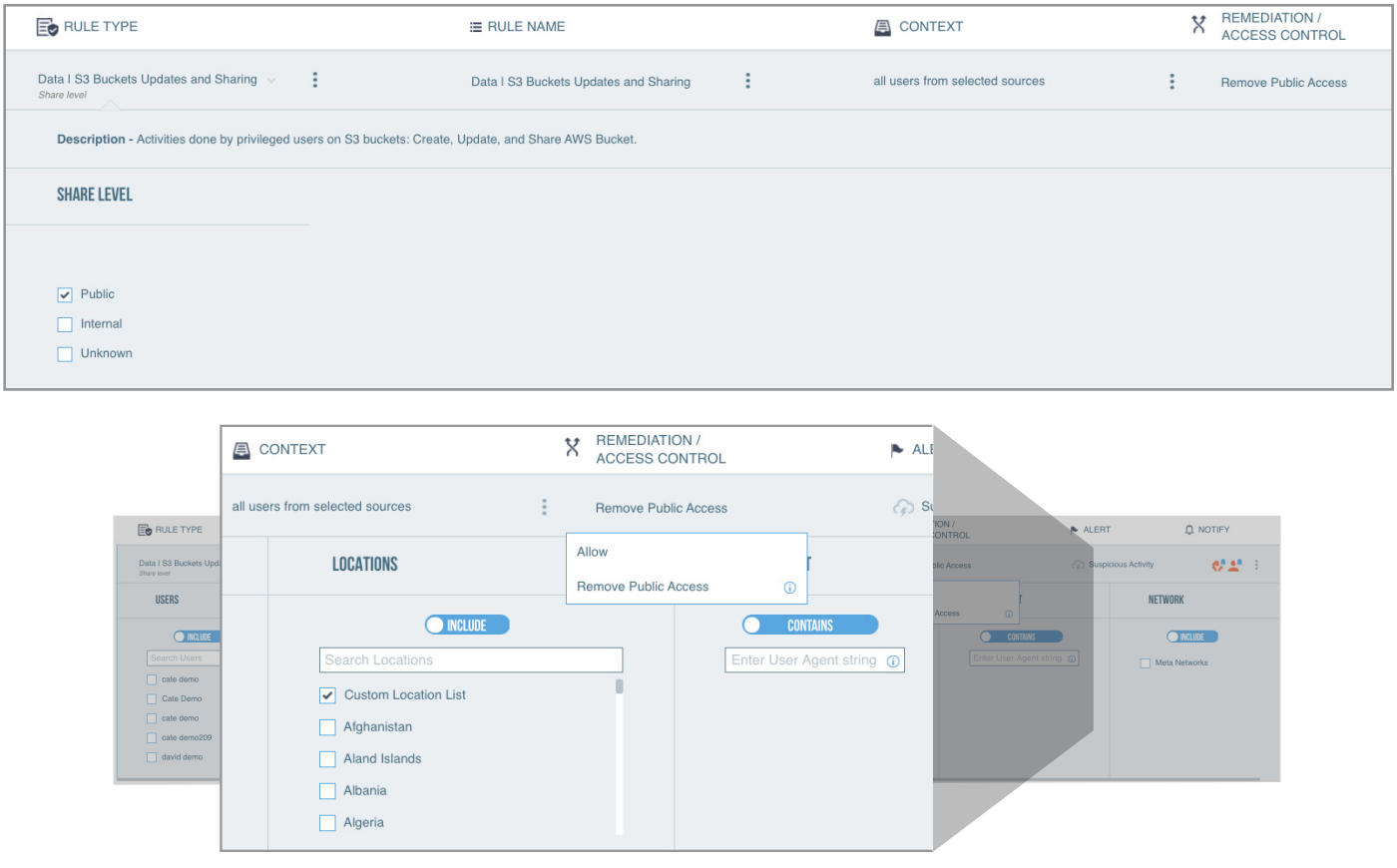

Figure 5. Modèle de règles pour la surveillance des autorisations de partage de buckets/containers

L'investigation des incidents DLP est également simplifiée, étant donné que vous pouvez mettre en corrélation les connexions suspectes ou les buckets mal configurés avec les incidents DLP. Vous pouvez également filtrer les événements et les alertes à des fins de génération de rapports, et surveiller la conformité de près en vous abonnant aux alertes.

Contrôles d'accès adaptatifs et protection contre les menaces

La console de gestion IaaS est une application Web utilisée pour créer et gérer les ressources cloud. Les entreprises doivent surveiller et contrôler l'accès à ce puissant outil. 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. Vous pouvez ainsi :

- Protéger votre environnement IaaS en définissant des règles visant à bloquer l'accès depuis des emplacements et réseaux à risque et par des cybercriminels
- Appliquer aux utilisateurs à haut niveau de risque et de privilèges des contrôles basés sur les risques, notamment l'authentification renforcée, des règles pour les terminaux gérés et la mise en œuvre de réseaux privés virtuels (VPN)

Proofpoint CASB tire parti d'informations de threat intelligence très complètes collectées sur plusieurs vecteurs (cloud, messagerie et autres) et synthétisées dans le graphique des menaces Proofpoint Nexus, qu'elle associe à des données contextuelles propres aux utilisateurs. Nous appliquons des algorithmes d'apprentissage automatique à ces données afin d'analyser le comportement des utilisateurs et de détecter les anomalies sur l'ensemble des services et locataires cloud. Nous vous aidons à différents égards :

- Détection des compromissions de comptes cloud
- Analyse des activités et alertes passées, notamment les accès suspects à vos services IaaS fédérés

EN SAVOIR PLUS

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