FICHE TECHNIQUE

Protection McAfee contre les fuites de données, des équipements jusqu'au cloud

Protection des données unifiée

Des entreprises de toutes tailles adoptent aujourd'hui des services dans le cloud, notamment Microsoft Office 365, pour garantir à leurs employés une plus grande flexibilité et un accès aisé aux applications métier essentielles. Or, les solutions de protection des données sur site ne disposent généralement pas de visibilité sur les données des services de cloud tels qu'Office 365, pas plus qu'elles ne peuvent contrôler la collaboration ou le partage au sein du cloud. De nombreuses entreprises envisagent d'ajouter une solution de protection des données distincte pour leur environnement cloud, mais ce faisant, elles risquent de fragmenter leurs stratégies, la génération de rapports et la réponse aux incidents. Une telle approche entraîne une augmentation des coûts opérationnels et une incohérence dans la protection des données au niveau des équipements, des réseaux et des services de cloud.

McAfee offre une protection unifiée contre les fuites des données sur les terminaux, les réseaux et dans le cloud grâce à l'intégration de deux technologies de pointe : McAfee® Data Loss Prevention (McAfee DLP) et McAfee® MVISION Cloud. Cette intégration offre aux entreprises une expérience de protection des données unifiée et transparente, qui minimise le risque de fuites tout en optimisant l'efficacité opérationnelle.

Inefficacité des solutions de protection des données fragmentées

Par le passé, l'implémentation d'une solution de protection contre les fuites de données (DLP) dans le cloud impliquait de recréer entièrement les règles DLP déjà définies pour l'environnement sur site. De plus, les règles DLP applicables aux systèmes sur site ne tenaient pas compte de la collaboration et du partage natifs avec des tiers propres aux services de cloud. Par conséquent, non seulement les équipes passaient énormément de temps à répliquer des tâches déjà réalisées pour la protection des données sur les équipements et le réseau, mais la mise en œuvre des stratégies risquait d'être incohérente en raison des différents moteurs DLP utilisés. Les éventuelles fuites de données dues aux liens partagés ou à la collaboration dans le cloud étaient invisibles pour les systèmes DLP sur site.

Principaux avantages

Intégration transparente

- Établissez des classifications de vos données une seule fois dans McAfee ePO, puis utilisez-les dans tous les contextes : équipements, réseau et cloud.
- La connexion des solutions DLP sur site et dans le cloud peut être effectuée en un clic et en moins d'une minute.

Prévention systématique des fuites de données

- La solution utilise un moteur partagé de classification et de stratégies pour les différents environnements.
- Il n'est pas nécessaire d'apporter des modifications dans différentes consoles.

Gardez le contact

Connexion et synchronisation de la prévention des fuites de données — sur site et dans le cloud

McAfee® ePolicy Orchestrator® (McAfee ePO™) simplifie la mise en œuvre d'une protection unifiée contre les fuites de données, des équipements jusqu'au cloud. Grâce à l'alliance de MVISION Cloud et de McAfee ePO, vous pouvez protéger les données de tous les services de cloud bien plus rapidement, en disposant d'informations contextualisées sur la collaboration et le partage natifs au cloud. Il est possible de connecter les deux solutions en un seul clic et en moins d'une minute[1]. Les règles DLP définies dans McAfee ePO pour le réseau et les équipements sont transmises à MVISION Cloud, où elles peuvent être appliquées à n'importe quel service de cloud et au trafic natif au cloud qui contourne votre réseau. Les classifications de données sont synchronisées, ce qui garantit une prévention des fuites de données cohérente sur les terminaux et dans le cloud. Tous les incidents sont communiqués à McAfee ePO pour que vous disposiez d'un workflow DLP unifié, des équipements jusqu'au cloud.

Gain d'efficacité opérationnelle, des équipements jusqu'au cloud

Les clients qui utilisent McAfee ePO tirent parti de cette intégration pour faciliter la mise en œuvre de la protection contre les fuites de données dans les services de cloud et pour simplifier leurs opérations. Illustrons ceci par un exemple. Un important fabricant de produits alimentaires qui utilisait McAfee DLP sur ses terminaux et partages de fichiers réseau devait déterminer où résidaient ses données dans le cloud et mettre au point une stratégie pour les protéger. L'entreprise a d'abord exécuté McAfee® Web Gateway pour analyser le trafic web et déterminer les principales destinations utilisateur, ainsi que les emplacements de stockage des données d'entreprise dans le cloud. À la suite de cette analyse, l'entreprise a découvert que la majorité de ses données étaient en fait concentrées dans Microsoft Office 365.

Les exigences en matière de protection des données étaient identiques pour le cloud et les emplacements sur site, mais des différences contextuelles telles que le partage de fichiers et la collaboration dans le cloud soulevaient de nouvelles difficultés. Par exemple, l'entreprise devait analyser ses données dans Office 365 à la demande, de la même façon que sur site. Par contre, elle devait également appliquer des règles DLP pour les données entrantes et sortantes d'Office 365, une opération propre au cloud et échappant à la visibilité réseau. Elle a ainsi déterminé qu'une solution CASB (Cloud Access Security Broker) serait idéale pour répondre à ces besoins et a donc évalué diverses offres disponibles sur le marché. En fin de compte, elle a adopté MVISION Cloud en raison de son intégration étroite avec les règles DLP existantes de McAfee ePO. À partir de McAfee ePO, l'équipe de sécurité a pu transférer les classifications de données sur site vers MVISION Cloud, puis créer des stratégies pour Office 365 en utilisant ces classifications prédéfinies. À présent, l'entreprise dispose d'un emplacement de gestion unique pour les classifications de données, les incidents de fuites de données liés aux équipements et au cloud, ainsi que la génération de rapports sur le trafic web provenant de McAfee Web Gateway. Toutes ces possibilités sont réunies dans McAfee ePO.

Principaux avantages (suite)

Vue unique pour la gestion des incidents et la génération de rapports

- Vous bénéficiez d'une gestion centralisée des incidents dans plusieurs environnements.
- Il est inutile de basculer d'une console à l'autre pour consulter les incidents et les rapports.

« Nous avons choisi McAfee MVISION Cloud comme solution CASB en raison de la visibilité qu'il nous procure sur les déplacements de nos données et les utilisateurs qui y accèdent, mais aussi pour la facilité avec laquelle il nous permet de percevoir le risque lié à un service de cloud. »

— RSSI d'un fabricant international d'appareils IoT

Gestion des incidents et génération de rapports centralisées

McAfee ePO offre une console unique pour la gestion centralisée de toutes les violations DLP et la génération de rapports. Il n'est pas nécessaire de passer d'une console à une autre pour voir les incidents et générer des rapports, que les violations proviennent d'équipements professionnels ou d'applications de cloud. Cette console centralisée contribue également à réduire la complexité en matière d'audits et de conformité réglementaire en offrant une visibilité sur les données sensibles dans les différents environnements.

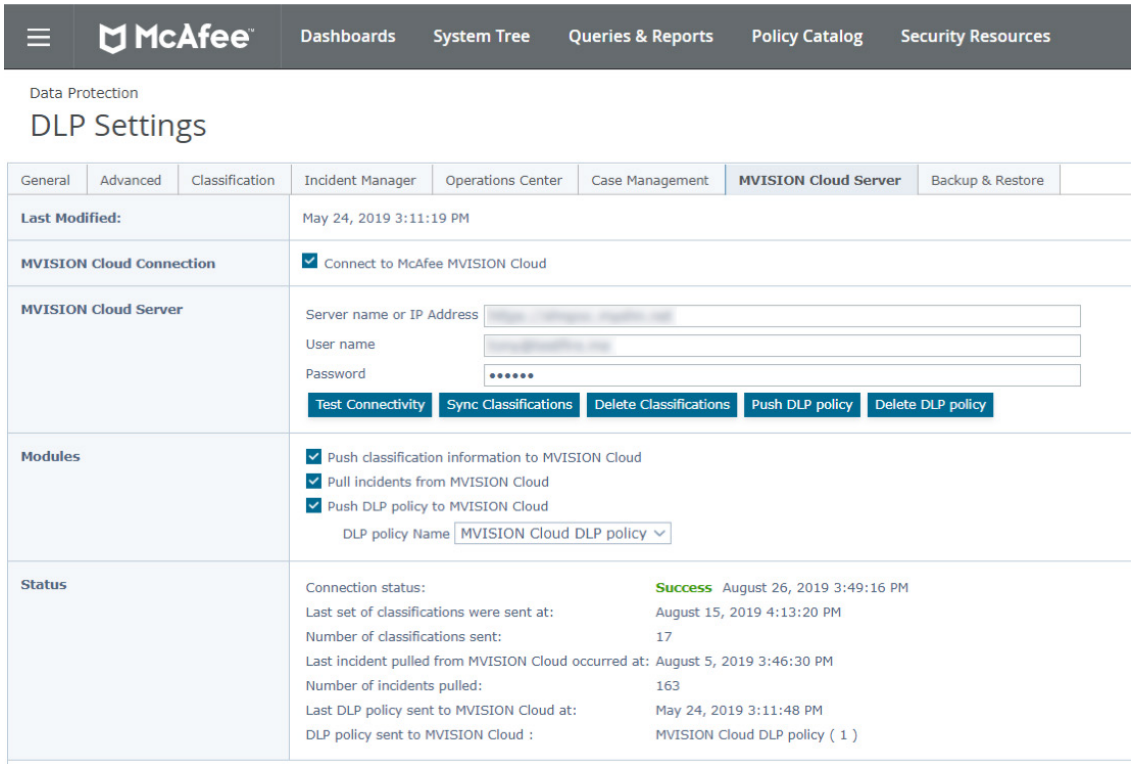

Figure 1. Synchronisation des stratégies DLP avec MVISION Cloud dans McAfee ePO.

Résumé

Face au volume croissant de données créées et envoyées chaque jour dans le cloud, il est plus important que jamais de disposer de stratégies DLP cohérentes pour protéger les données sur tous les vecteurs de fuites, qu'il s'agisse de terminaux d'entreprise, d'équipements non managés, du réseau ou d'applications de cloud.

L'extension des capacités DLP de McAfee des équipements jusqu'au cloud assure aux entreprises une expérience transparente et unifiée pour la protection des données dans de multiples environnements. Une telle approche permet de gagner un temps précieux grâce à une meilleure efficacité opérationnelle et contribue à limiter le risque de fuites de données.

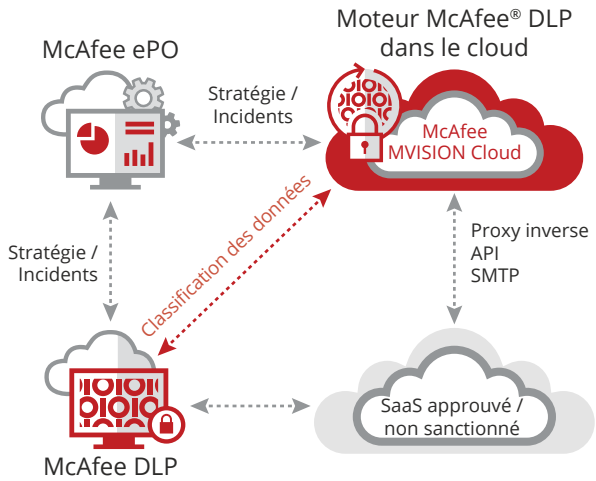

Figure 2. Architecture globale de gestion des incidents de la protection McAfee contre les fuites de données, des équipements jusqu'au cloud.

En savoir plus

Pour en savoir plus, consultez notre site à l'adresse **www.mcafee.com/enterprise/fr-fr/products/data-protection-products.html**.

1. Sur la base de tests internes systématiques réalisés en laboratoire par McAfee.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr