McAfee Public Cloud Server Security Suite

Protection complète des charges de traitement de cloud AWS et Azure

Les entreprises changent leurs stratégies de mise en œuvre des centres de données pour se tourner de plus en plus, et parfois massivement, vers des instances de serveur de cloud public. Cela soulève dès lors la question essentielle de l'efficacité du modèle[1] de responsabilité partagée. Les fournisseurs de clouds publics, tels qu'Amazon Web Services (AWS) et Microsoft Azure, assurent la protection du périmètre et laissent aux utilisateurs le soin de sécuriser le contenu. Dans ce contexte, les entreprises prévoyantes s'interrogent sur la marche à suivre pour protéger leurs charges de traitement de cloud contre les attaques de type « jour zéro » et les menaces APT, tout en maintenant les coûts à un niveau acceptable compte tenu de leur stratégie de cloud. Voici quelques exemples des principaux défis auxquels sont confrontées les entreprises qui adoptent le cloud :

- Lutter efficacement contre les menaces avancées et de type « jour zéro » devient de plus en plus difficile.
- La sécurisation des infrastructures à plusieurs instances de cloud est compliquée par le manque de visibilité et de gestion centralisée.
- La dégradation des performances qu'entraînent les solutions de protection des charges de traitement de cloud est problématique.

Figure 1. Console de gestion unique pour infrastructures à plusieurs instances de cloud et technologies McAfee multiples

Principaux avantages

- Conçue pour les charges de traitement AWS et Azure
- Découverte instantanée
- Évaluation de la sécurité et neutralisation des menaces
- Sécurité évolutive
- Protection complète
- Exploitation de la console de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Options de déploiement telles que Chef, Puppet et OpsWorks
- Démonstration de la conformité
- Intégration avec d'autres solutions McAfee

McAfee® Public Cloud Server Security Suite garantit une découverte et un contrôle instantanés des menaces et des charges de traitement AWS et Azure, et assure ainsi une protection complète, constante et permanente, avec un impact minimal sur les performances. Vous pouvez donc détecter de multiples centres de données et comptes de cloud, machines virtuelles et menaces émergentes.

La protection complète qu'offre McAfee Public Cloud Server Security Suite comprend des fonctions essentielles d'antivirus et de prévention des intrusions couplées à des listes blanches avancées pour mettre en échec les attaques de type « jour zéro », des technologies de contrôle des modifications pour assurer le respect des obligations réglementaires et une fonction de gestion du chiffrement pour protéger les données. La gestion de plusieurs instances de cloud et la mise en œuvre des stratégies sont en outre facilitées par l'utilisation d'une seule et unique console de gestion. Par ailleurs, les options de déploiement flexibles que proposent les outils DevOps, tels que Chef, Puppet et OpsWorks, offrent une expérience transparente avec un impact minimal.

Découverte des infrastructures de cloud et des menaces

Pour mieux contrôler vos infrastructures de cloud et les menaces auxquelles elles sont exposées, vous devez disposer d'une bonne visibilité.

- Détectez tous les réseaux virtuels ou clouds privés virtuels (VPC), modèles et charges de traitement sur les infrastructures de cloud AWS et Azure en quelques minutes seulement. Disposer d'informations détaillées sur les comptes d'infrastructure de cloud, savoir qui

Plates-formes prises en charge

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

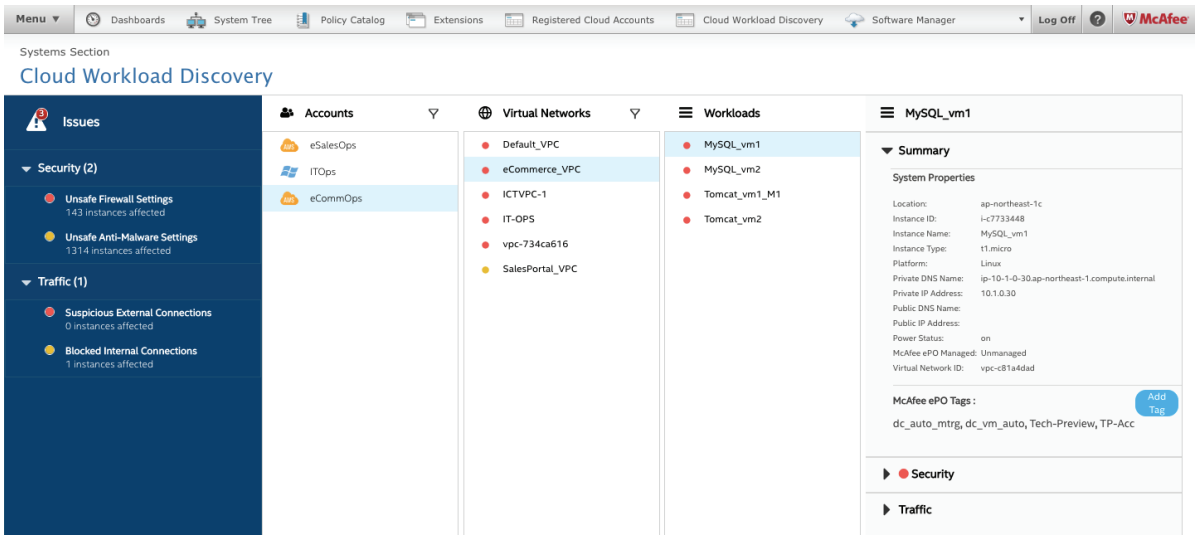

Figure 2. Découverte et surveillance de multiples infrastructures de cloud et menaces émergentes

a accès aux différentes parties de ladite infrastructure, comprendre la manière dont les charges de traitement sont attribuées aux modèles et VPC, et pouvoir bénéficier d'un aperçu rapide de l'arborescence des systèmes associés à l'infrastructure constituent les premières étapes pour une protection adéquate de votre infrastructure de cloud.

- Bénéficiez d'une visibilité centralisée et complète sur la sécurité de vos différentes instances de cloud. Profitez d'informations de bout en bout sur les menaces, ainsi que de données sur l'origine des attaques pour une meilleure gestion de votre sécurité.
- Surveillez le trafic sur l'ensemble de vos charges de traitement et gérez la manière dont les flux de données circulent entre ces différentes charges, ainsi que leurs accès à partir d'emplacements externes à l'entreprise.

Surveillance du cloud et réponse rapide aux alertes de sécurité

Dans un contexte où la vitesse d'intervention devient primordiale, cette solution vous permet de procéder à une évaluation plus rapide et approfondie de la gravité des problèmes de sécurité de sorte à pouvoir y remédier immédiatement.

- Identifiez les problèmes qui exigent une attention immédiate et prenez les mesures appropriées en vous aidant d'alertes avec code de couleur.
- Créez des marqueurs personnalisés et attribuez-les aux différentes charges de traitement selon vos besoins.
- Prenez des mesures correctives pour endiguer les problèmes de sécurité, et adoptez des stratégies ou définissez des scores de réputation en termes de menaces afin de protéger votre infrastructure contre de futurs incidents de sécurité.

Contrôles de sécurité complets, basés sur l'hôte

Pour Windows et Linux

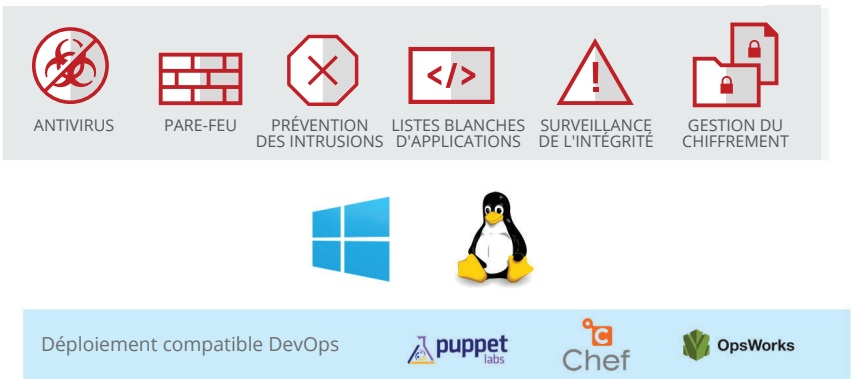

Figure 3. Protection complète pour les charges de traitement des clouds publics

- Gérez votre pare-feu de cloud au moyen de stratégies personnalisées adaptées à des charges de traitement spécifiques ou à des groupes de charges de traitement. Gérez les stratégies des groupes de sécurité AWS de façon à contrôler le trafic d'une ou plusieurs instances.
- Identifiez tout trafic suspect sur les différents VPC et prenez des mesures correctives pour empêcher que vos données critiques ne tombent entre de mauvaises mains.

Protection complète contre les menaces

McAfee Public Cloud Server Security Suite repose sur un agent unique qui fournit une sécurité multiniveau, elle-même gérée au moyen d'une seule console de gestion couvrant plusieurs plates-formes de cloud. La solution peut également inclure des outils compatibles DevOps pour des performances optimales.

Fonctionnalité	Avantages
Options de déploiement Chef, Puppet et AWS OpsWorks	▪ Protection de pointe grâce aux outils de déploiement DevOps faciles à configurer ▪ Intégration totale de la sécurité dans vos activités
Découverte des charges de traitement de cloud	▪ Visibilité instantanée sur les infrastructures de cloud pour une découverte efficace des centres de données virtuels, des charges de traitement de cloud et des pare-feux de cloud ▪ Notifications immédiates des menaces avec évaluation automatique de l'état de sécurité ▪ Neutralisation rapide des menaces avec priorisation des alertes en fonction de la gravité des menaces et marche à suivre
Console de gestion unique pour plusieurs solutions de sécurité des infrastructures de cloud (logiciel McAfee ePO)	▪ Solution extrêmement pratique pour les environnements hybrides ▪ Gestion unifiée via une seule console des stratégies et charges de traitement physiques, virtuelles et de cloud ▪ Intégration des technologies de sécurité sur site et dans le cloud de McAfee et de ses partenaires ▪ Réduction du coût total de possession grâce aux processus de sécurité intégrés et aux mesures rapides de neutralisation des menaces
Protection antimalware	▪ Défense optimale contre les logiciels malveillants ▪ Protection des systèmes et fichiers contre les virus, les logiciels espions (spywares), les vers, les chevaux de Troie et d'autres risques ▪ Détection et suppression des logiciels malveillants, avec stratégies définis par les utilisateurs pour la gestion des éléments en quarantaine
Pare-feu au niveau de l'hôte	▪ Protection des charges de traitement contre les attaques et les accès non autorisés

Fonctionnalité	Avantages
Prévention des intrusions sur l'hôte	▪ Blocage du trafic réseau indésirable ou nuisible et blocage proactif des attaques inconnues (de type « jour zéro ») et des attaques connues, à l'aide d'une technologie brevetée et primée ▪ Prévention des modifications indésirables au niveau des charges de traitement via la restriction de l'accès aux ports, aux fichiers, aux éléments partagés et aux clés et valeurs de Registre spécifiés ▪ Protection de la mémoire pour empêcher les menaces ou programmes anormaux de dépasser la limite de la mémoire tampon et d'écraser la mémoire adjacente lors de l'écriture de données dans une mémoire tampon. Les débordements de mémoire tampon exploités peuvent exécuter un code arbitraire sur votre ordinateur.
Listes blanches d'applications	▪ Protection contre les attaques de type « jour zéro » et les menaces persistantes avancées sans nécessiter de mises à jour de signatures ▪ Renforcement de la sécurité et réduction des coûts de possession au moyen d'une technologie de liste blanche dynamique qui valide automatiquement les nouveaux logiciels ajoutés via les sources de confiance définies ▪ Réduction des cycles d'application de patchs grâce à une liste blanche sécurisée et à la protection avancée de la mémoire
Surveillance de l'intégrité des fichiers	▪ Détection continue des modifications apportées aux systèmes sur les sites distants et distribués ▪ Blocage des modifications non autorisées des configurations, des répertoires et des fichiers système critiques pour empêcher les tentatives d'altération ▪ Suivi et validation de chaque tentative de modification en temps réel sur la charge de traitement, grâce à la mise en œuvre de la stratégie de modifications par période, source ou ticket d'approbation de modifications
Gestion du chiffrement	▪ Chiffrement des données stockées dans des volumes AWS EBS avec AWS Advanced Encryption Standard (AES) ▪ Chiffrement aisé des volumes contenant des données préexistantes ▪ Intégration du service KMS (Key Management Service) d'Amazon dédié au chiffrement

En savoir plus

Consultez la page de la solution : **www.mcafee.com/fr/products/public-cloud-server-security-suite.aspx**.

Également disponible à l'achat sur **AWS Marketplace**.

1. http://www.mcafee.com/fr/resources/white-papers/wp-cloud-security-primer-techtarget.pdff

McAfee
Together is power.

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