McAfee Cloud Workload Security

Sécurisez vos charges de travail de cloud public et privé à l'aide d'une solution sûre, simple et rapide.

Avec l'évolution des centres de données d'entreprise, un nombre croissant de charges de travail sont migrées chaque jour vers les clouds. La plupart des entreprises possèdent un environnement hybride composé de charges de travail sur site et dans le cloud, notamment des conteneurs, suivant une proportion qui ne cesse de fluctuer. Cette évolution représente un nouveau défi pour la sécurité car la protection des environnements de clouds (publics et privés) exige des approches et outils différents. Les entreprises ont besoin d'une visibilité centralisée sur toutes leurs charges de travail de cloud, doublée d'une défense complète contre les risques d'erreurs de configuration, d'attaques de logiciels malveillants et de compromission de données.

McAfee® Cloud Workload Security automatise la découverte et la protection des conteneurs et des charges de travail élastiques pour éliminer les zones d'ombre, contrer efficacement les menaces avancées et simplifier la gestion multicloud. McAfee permet de sécuriser vos charges de travail à l'aide d'une seule stratégie automatisée lorsqu'elles sont déplacées entre vos environnements hybrides, publics et privés virtuels. Cette approche garantit l'excellence opérationnelle en matière de cybersécurité.

Visibilité en temps réel

Découverte automatisée

Si certaines instances de charge de travail et conteneurs Docker échappent à votre contrôle, ils peuvent créer des failles dans la gestion de la sécurité et offrir une porte d'entrée aux pirates. McAfee Cloud Workload Security découvre les charges de travail élastiques et conteneurs Docker hébergés dans les environnements Amazon Web Services (AWS), Microsoft Azure et VMware. De plus, il surveille constamment l'apparition de nouvelles instances. Vous bénéficiez ainsi d'une vue centralisée et complète de vos environnements. De plus, vous éliminez les zones d'ombre opérationnelles et de sécurité susceptibles d'accroître votre niveau de risque.

Principaux avantages

- Une visibilité constante sur les instances de charges de travail flexibles élimine les « zones d'ombre » opérationnelles, tout en automatisant la tâche laborieuse de déploiement des stratégies.
- Découvrez et surveillez les conteneurs Docker, et sécurisez-les grâce à la microsegmentation.
- Des mécanismes de défense contre les menaces optimisés par les machines virtuelles offrent des contre-mesures multiniveaux.
- La gestion centralisée et les workflows automatisés réduisent considérablement la complexité des environnements hybrides et multiclouds.
- L'intégration avec des outils d'automatisation comme Chef et Puppet permet de sécuriser les charges de travail des clouds privés et publics au moment du déploiement.

Gardez le contact

Sécurité de pointe pour les charges de travail

Protection contre les menaces avancées

McAfee Cloud Workload Security intègre des contre-mesures qui protègent les charges de travail contre les menaces telles que les ransomwares et les attaques ciblées. Au nombre de celles-ci, citons l'apprentissage automatique, le confinement d'applications, les fonctions antimalware optimisées pour les machines virtuelles, les listes blanches, la surveillance de l'intégrité des fichiers et la microsegmentation. Les fonctions de protection contre les menaces avancées, notamment l'apprentissage automatique, neutralisent les attaques sophistiquées encore inconnues et identifient les charges actives malveillantes par leur comportement et les caractéristiques de leur code.

Consolidation des événements

McAfee Cloud Workload Security permet aux entreprises d'utiliser une interface unique pour gérer tout un éventail de technologies de contre-mesures pour les environnements sur site et de cloud, y compris des technologies tierces telles qu'AWS GuardDuty. Les administrateurs peuvent tirer parti de la surveillance continue et l'identification des comportements non autorisés par AWS GuardDuty, pour un niveau supplémentaire de visibilité sur les menaces. Grâce à cette intégration, la console McAfee Cloud Workload Security permet de visualiser directement les événements GuardDuty, notamment les connexions réseau, les sondages de ports et les requêtes DNS destinées aux instances EC2. Les événements de connexion réseau GuardDuty sont cartographiés dans un organigramme lorsque le trafic correspond au trafic découvert par McAfee Cloud Workload Security.

Protection optimale des environnements virtualisés

McAfee Cloud Workload Security protège les machines virtuelles de votre cloud privé contre les logiciels malveillants sans solliciter les ressources sous-jacentes ni augmenter les charges d'exploitation. La protection antimalware intelligente permet de planifier les tâches gourmandes en ressources, par exemple l'analyse à la demande, au moment où l'hyperviseur n'est pas surchargé.

Visualisation du réseau grâce à la microsegmentation

La visualisation du réseau native au cloud, les alertes de risques priorisées et la microsegmentation offrent la connaissance de la situation et le contrôle nécessaires pour prévenir la progression des attaques latérales dans les environnements virtualisés et bloquer les sources malveillantes externes. Les fonctionnalités d'arrêt en un clic ou de mise en quarantaine permettent de réduire le risque d'erreurs de configuration et améliorent l'efficacité des mesures correctives.

Principaux avantages (suite)

- Dotez-vous d'une solution de protection multiniveau conviviale contre les logiciels malveillants avancés et les intrusions.
- Visualisez et identifiez les menaces réseau sans installer d'agent.
- Sécurisez votre environnement en appliquant directement des mesures correctives à partir de la solution.

Cloud Workload Security

Contrôle total et pleine **visibilité**

Surveillance de l'intégrité des fichiers

Cette fonction assure une surveillance continue. Elle vérifie que les systèmes de fichiers et les répertoires n'ont pas été compromis par des logiciels malveillants, des cyberpirates ou des utilisateurs internes animés d'intentions malveillantes. Un rapport d'audit complet fournit des informations sur les modifications apportées aux charges de travail serveur et vous avertit de la présence d'une attaque active.

Contrôle des applications

Les listes blanches d'applications préviennent les attaques connues et inconnues en autorisant uniquement l'exécution des applications approuvées et en bloquant les charges actives non autorisées. Cette fonction offre une protection dynamique basée sur une cyberveille locale et mondiale et permet d'assurer la mise à jour des systèmes sans désactiver les fonctions de sécurité.

Gestion simplifiée

Des stratégies cohérentes grâce à une gestion centralisée

Une console unique permet de gérer les stratégies de sécurité de façon centralisée et systématique sur les serveurs, les serveurs virtuels et les charges de travail de cloud des environnements multiclouds.

Déploiement automatisé

Grâce à la prise en charge d'outils de déploiement automatisés comme Chef, Puppet et Ansible, vous pouvez déployer automatiquement des technologies de sécurité dans des environnements multiclouds.

Protection améliorée

McAfee Cloud Workload Security vous permet de bénéficier d'une sécurité hors pair tout en profitant des avantages du cloud. La solution offre une couverture intégrale de vos technologies de protection et simplifie la gestion de la sécurité. De plus, en empêchant les cybermenaces de nuire à vos activités, elle vous permet de vous consacrer au développement de l'entreprise. Le tableau ci-après illustre les fonctions disponibles dans les différentes éditions.

FICHE TECHNIQUE

Fonctionnalités	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Gestion centralisée (plate-forme McAfee® ePO™)	✓	✓	✓
Prise en charge multicloud (AWS, Azure, VMware)	✓	✓	✓
Utilisation de la microsegmentation pour la mise en quarantaine des charges de travail et des conteneurs	✓	✓	✓
Prévention des menaces pour les systèmes d'exploitation serveur (Windows et Linux)	✓	✓	✓
Prévention des exploits et des intrusions sur l'hôte	✓	✓	✓
Gestion du chiffrement dans le cloud	✓	✓	✓
Gestion de pare-feu native pour AWS et Azure (groupes de sécurité)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (sans agent et multiplate-forme)	✓	✓	✓
Pare-feu basé sur l'hôte	✓	✓	✓
Protection adaptative contre les menaces avec apprentissage automatique		✓	✓
Visualisation du trafic réseau et microsegmentation		✓	✓
Analyse native du trafic réseau dans le cloud, alliée au score de réputation Global Threat Intelligence		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
Intégration de McAfee® Virtual Network Security Platform		✓	✓

En savoir plus

Pour plus d'informations, consultez le site : **https://www.mcafee.com/fr/products/cloud-workload-security.aspx**.

McAfee
Together is power.

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