McAfee Cloud Workload Security

Sécurisez les charges de travail de votre infrastructure hybride 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 le cloud. 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 (McAfee® CWS) 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 multicloud, publics et privés virtuels. Cette approche garantit l'excellence opérationnelle en matière de cybersécurité.

Sécurité de pointe pour les charges de travail : cas d'utilisation

Découverte automatisée

Les instances de charge de travail et conteneurs Docker non managés créent des failles dans la gestion de la sécurité et peuvent offrir une porte d'entrée aux pirates. McAfee CWS découvre les charges de travail élastiques et conteneurs Docker hébergés dans les environnements Amazon Web Services (AWS), Microsoft Azure, OpenStack et VMware. En outre, 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 élastiques élimine les « zones d'ombre » opérationnelles, tout en automatisant la tâche laborieuse de déploiement des stratégies.
- La gestion centralisée et les charges de travail automatisées réduisent considérablement la complexité des environnements hybrides et multiclouds.
- Les menaces réseau sont visualisées et identifiées sans installer d'agent.
- Des mécanismes de défense contre les menaces optimisés par les machines virtuelles offrent des contre-mesures multiniveaux.
- 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

Visibilité sur le trafic réseau

Grâce au trafic réseau natif généré par les charges de travail de cloud, McAfee CWS est capable de compléter et d'exploiter les données de cyberveille McAfee® Global Threat Intelligence (McAfee® GTI). Les informations enrichies permettent d'afficher des propriétés telles que le score de risque et la géolocalisation, ainsi que d'autres informations importantes sur le réseau. Elles peuvent servir à mettre en place des mesures de correction automatisées afin de protéger les charges de travail.

Intégration avec des infrastructures de déploiement

McAfee CWS crée des scripts de déploiement pour permettre le déploiement de l'agent McAfee® vers les charges de travail de cloud et leur gestion. Ces scripts permettent une intégration avec des outils tels que Chef, Puppet et d'autres infrastructures DevOps pour le déploiement de l'agent McAfee vers des charges de travail exécutées par des fournisseurs de cloud, comme AWS et Microsoft Azure.

Consolidation des événements

McAfee CWS permet aux entreprises d'utiliser une interface unique pour gérer un éventail de technologies de contre-mesures pour les environnements sur site et de cloud. Il peut également intégrer des technologies supplémentaires, telles qu'AWS GuardDuty, McAfee® Policy Auditor et McAfee® Network Security Platform.

- Les administrateurs peuvent tirer parti de la surveillance continue et de l'identification des comportements non autorisés qu'effectue AWS GuardDuty, pour un niveau supplémentaire de visibilité sur les menaces. Grâce à cette intégration, la console McAfee CWS permet de visualiser directement les événements GuardDuty, notamment les connexions réseau, les sondages de ports et les requêtes DNS destinées aux instances EC2.
- McAfee Policy Auditor exécute des contrôles avec agent sur les audits de configuration connus ou définis par l'utilisateur, afin d'en vérifier la conformité avec la loi HIPAA (Health Insurance Portability and Accountability Act), la norme PCI DSS (Payment Card Industry Data Security Standard), les références CIS (Center for Internet Security Benchmark) ou d'autres normes du secteur. McAfee CWS signale les audits non conformes afin de vous offrir une visibilité instantanée sur les erreurs de configuration des charges de travail dans le cloud.
- McAfee Network Security Platform est une plate-forme de sécurité du cloud qui procède à l'inspection du trafic réseau dans les environnements hybrides, AWS et Microsoft Azure. Elle effectue une inspection plus approfondie du trafic réseau au niveau des paquets, et signale les divergences ou les alertes via McAfee CWS. Les utilisateurs bénéficient ainsi d'une visibilité centralisée sur les environnements multiclouds pour l'application de mesures correctives.

Mise en œuvre de stratégies pour les groupes de sécurité réseau

McAfee CWS permet aux utilisateurs et aux administrateurs de créer des stratégies de référence pour les groupes de sécurité, mais aussi de réaliser des audits des stratégies qui s'exécutent sur les charges de travail

Principaux avantages (suite)

- Vous bénéficiez d'une protection multiniveau contre les logiciels malveillants avancés et les intrusions.
- Vous découvrez et surveillez les conteneurs Docker, et vous les sécurisez grâce à la microsegmentation.
- Vous sécurisez votre environnement en appliquant directement des mesures correctives à partir de la solution.

Cloud Workload Security

Contrôle total et pleine **visibilité**

en les comparant à ce cadre de référence. Tout écart ou modification par rapport au cadre de référence peut générer une alerte dans la console McAfee CWS à des fins de correction. Les administrateurs peuvent également configurer manuellement des groupes de sécurité réseau natifs à partir de McAfee CWS, ce qui leur permet de contrôler directement les stratégies de groupe de sécurité natives au cloud.

Caractéristiques distinctives de McAfee Cloud Workload Security : principales fonctionnalités et technologies

Prise en charge de builds natives au cloud

Grâce à McAfee CWS, les clients peuvent consolider la gestion de plusieurs clouds publics et privés à l'aide d'une console de gestion unique, incluant notamment AWS EC2, les machines virtuelles Microsoft Azure, OpenStack etVMware Vcenter. McAfee CWS permet aux clients d'importer des builds et de les exécuter dans le cloud grâce à la prise en charge de builds natives au cloud pour Amazon Elastic Container Service for Kubernetes (Amazon EKS) et Microsoft Azure Kubernetes Service (AKS).

Gestion simple et 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. Les administrateurs peuvent également créer plusieurs autorisations basées sur les rôles dans McAfee® ePolicy Orchestrator® (McAfee ePO™), ce qui leur permet de définir des rôles d'utilisateur de façon plus précise et adéquate.

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.

Protection optimale des environnements virtualisés

La suite McAfee CWS protège les machines virtuelles de votre cloud privé contre les logiciels malveillants à l'aide de McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus), et ce sans solliciter les ressources sous-jacentes ni augmenter les charges d'exploitation. McAfee MOVE AntiVirus permet aux entreprises de transférer les fonctions de sécurité à des machines virtuelles dédiées pour une analyse optimisée de leur environnement virtualisé.

McAfee® Endpoint Security for Servers offre aux utilisateurs une protection antimalware. Cette solution permet de planifier intelligemment les tâches gourmandes en ressources, par exemple l'analyse à la demande, afin de limiter l'impact sur les processus métier critiques.

Marquage et automatisation de la sécurité des charges de travail

Attribuez automatiquement les stratégies appropriées à toutes les charges de travail : vous importez des marqueurs AWS et Microsoft Azure dans McAfee ePO, puis vous affectez des stratégies fondées sur ces marqueurs. Les marqueurs AWS et Microsoft Azure existants sont synchronisés avec ceux de McAfee ePO et sont ainsi automatiquement gérés.

Autocorrection

L'utilisateur définit les stratégies de McAfee ePO. Si McAfee CWS identifie un système qui n'est pas protégé par les stratégies de sécurité de McAfee ePO et qu'il s'avère que celui-ci contient un logiciel malveillant ou un virus, le système sera automatiquement mis en quarantaine.

Protection adaptive contre les menaces

McAfee CWS 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 antimalwares optimisées pour les machines virtuelles, les listes blanches, la surveillance de l'intégrité des fichiers et la microsegmentation. McAfee® Advanced Threat Protection neutralise les attaques sophistiquées encore inconnues en appliquant des techniques d'apprentissage automatique pour identifier les charges actives malveillantes par leur comportement et les caractéristiques de leur code.

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. McAfee® Application Control 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.

Surveillance de l'intégrité des fichiers

La fonction de surveillance de l'intégrité des fichiers assure un contrôle continu. 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.

Protection adaptée à votre environnement multicloud

McAfee CWS 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	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
Gestion centralisée (plate-forme McAfee ePO)	✓	✓	✓
Prise en charge multicloud (AWS, Microsoft Azure, VMware)	✓	✓	✓
Utilisation de la microsegmentation pour la mise en quarantaine des charges de travail et des conteneurs	✓	✓	✓
McAfee MOVE (sans agent et multiplate-forme)	✓	✓	✓
McAfee Endpoint Security - module Prévention des menaces pour les systèmes d'exploitation serveur (Windows et Linux)	✓	✓	✓
Pare-feu basé sur l'hôte	✓	✓	✓
Gestion de pare-feu native pour AWS et Microsoft Azure (groupes de sécurité)	✓	✓	✓
Prévention des exploits et des intrusions sur l'hôte	✓	✓	✓
Importation de marqueurs AWS et Microsoft Azure dans McAfee ePO	✓	✓	✓
Autocorrection des charges de travail non conformes	✓	✓	✓
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 McAfee GTI		✓	✓
Intégration de McAfee® Virtual Network Security Platform (McAfee® vNSP)		✓	✓
Listes blanches dynamiques pour les serveurs via McAfee Application Control			✓
Journalisation d'audit continue avec la fonction de surveillance de l'intégrité des fichiers			✓
Protection des fichiers et des dossiers avec McAfee® Change Control for Servers			✓

En savoir plus

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

Les avantages et fonctionnalités des technologies McAfee dépendent de la configuration système et peuvent nécessiter la présence de certains éléments matériels ou logiciels ou l'activation de services particuliers. Pour en savoir plus, consultez le site www.mcafee.com/fr. Aucun système informatique ne peut être totalement sécurisé.

McAfee Together is power.

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