Sécurité des clouds privés

Protégez votre cloud privé grâce à une approche intégrée de la sécurité.

Mis en place pour gérer et adapter les charges de travail dynamiques sur une infrastructure hautement virtualisée, les déploiements en cloud privé engendrent des problèmes de sécurité que les solutions de sécurité statiques traditionnelles n'ont pas été conçues pour résoudre. C'est pourquoi McAfee a développé des technologies de pointe et un modèle de déploiement intégré qui optimise la protection des instances de cloud privé, notamment les centres de données définis par logiciel (SDDC) et les environnements multiclients. Les entreprises et les fournisseurs de services managés (MSP) peuvent ainsi profiter de la flexibilité opérationnelle et des économies de coûts associées aux clouds privés, tout en protégeant leurs données clients et de propriété intellectuelle. Les solutions McAfee® protègent les clouds privés contre les menaces internes et externes, telles que les attaques ciblées et les logiciels malveillants (malware) et assurent dans le même temps la conformité aux réglementations publiques et sectorielles.

Les défis associés à la sécurité des clouds privés

De plus en plus d'entreprises de toutes tailles se tournent aujourd'hui vers les clouds privés. Leur objectif ? Réaliser des économies de coûts et tirer parti de l'agilité des clouds publics sans compromettre le contrôle et la sécurité informatiques. Selon une enquête, plus de 70 % des entreprises utilisent, mettent en œuvre ou évaluent actuellement des modèles de cloud privé[1]. Outre les avantages qu'ils offrent par rapport aux modèles de centre de données traditionnels, les clouds privés garantissent aux équipes informatiques un niveau de contrôle plus élevé que les clouds publics. Ils présentent toutefois des défis spécifiques en termes de sécurité, qu'il convient de résoudre en vue d'optimiser la protection et la conformité.

L'un des principaux problèmes est l'absence de visibilité sur l'ensemble du trafic qui permettrait de s'assurer que l'entreprise n'est pas la cible d'une attaque ciblée. Dans les environnements de cloud privé hautement virtualisés, le trafic réseau circule de plus en plus souvent latéralement entre les machines virtuelles (trafic est-ouest, entre serveurs). Les solutions de sécurité isolées traditionnelles ne sont pas conçues pour les environnements de centres de données virtualisés de ce type. En effet, elles protègent uniquement le trafic nord-sud, entre des instances internes et externes, qui traverse le périmètre du centre de données. Elles n'ont aucune visibilité sur le trafic au sein même du centre de données (trafic est-ouest), ce qui crée une faille dans la protection. En effet, l'absence d'inspection du trafic est-ouest permet aux menaces internes de se propager latéralement à l'intérieur du centre de données.

Un autre problème majeur lié au cloud privé consiste à assurer la sécurité à la vitesse du cloud tout en préservant la conformité. Compte tenu de l'adoption par les équipes informatiques d'un modèle informatique plus dynamique et agile, la sécurité réseau doit pouvoir s'adapter aussi rapidement que le cloud. Par ailleurs, l'équipe informatique est tenue de respecter certaines réglementations ou normes de conformité, par exemple la norme PCI DSS (Payment Card Industry Data Security Standard) ou la loi HIPAA (Health Insurance Portability and Accountability Act). Malheureusement, les solutions de sécurité isolées sont incapables d'évoluer et donc de migrer automatiquement avec les charges de travail virtualisées.

Enfin, un dernier problème de taille se pose, à savoir la capacité limitée des entreprises à gérer les stratégies de sécurité avec assurance et à garantir des accords de niveau de service (SLA) robustes en soutien des besoins métier. La pénurie d'experts en sécurité dont souffrent les départements informatiques les empêche de gérer la sécurité des clouds privés de manière efficace et rentable. L'effectif dont ils disposent utilise essentiellement des outils traditionnels et ne partage pas les informations sur les menaces suffisamment rapidement, si tant est qu'il le fasse.

Les objectifs de la sécurité des clouds privés

Il est désormais indispensable de protéger votre entreprise à la fois contre les attaques externes et les menaces internes. Cela signifie que la sécurité de votre cloud privé ne peut se permettre de présenter des failles. Dans le cas des attaques externes, votre objectif

est d'identifier et de bloquer les attaques entrantes au niveau du périmètre, mais aussi de détecter et neutraliser les communications sortantes avec des serveurs de commande et de contrôle. Pour ce qui est des menaces internes, vous devez pouvoir identifier les logiciels malveillants et les supprimer des serveurs virtualisés au sein du centre de données, ainsi que détecter et neutraliser les attaques émanant de comptes utilisateur dotés de privilèges.

Pour y parvenir, une visibilité complète sur la sécurité, une protection dynamique et une gestion efficace des stratégies à l'échelle de vos clouds privés sont autant d'impératifs. Une visibilité totale sur la sécurité des charges de travail des clouds privés est obligatoire pour protéger votre entreprise, dans la mesure où il est impossible de protéger des actifs que vous ne voyez pas. Une protection dynamique permet de sécuriser un environnement de cloud privé par des mécanismes de sécurité capables de s'adapter à un environnement en constante évolution, où les machines virtuelles sont sans cesse déplacées d'un hôte à l'autre. Enfin, vous avez besoin d'une gestion simplifiée de la sécurité pouvant exploiter les ressources en personnel et leur permettre de respecter les SLA tout en assurant la protection de l'entreprise.

Fonctionnement du modèle coordonné de McAfee

McAfee propose la solution de sécurité intégrée la plus complète du marché. L'objectif est d'aider les entreprises à assurer la protection et la conformité des environnements de clouds privés hautement virtualisés ou des centres de données définis par logiciel (SDDC) de manière efficace et rentable, sans sacrifier la flexibilité, l'efficacité opérationnelle et les économies de coûts.

Conçues pour fonctionner ensemble de manière harmonieuse et répondre aux défis spécifiques des déploiements en cloud privé hautement virtualisés et des SDDC, nos solutions offrent une protection optimale contre les attaques ciblées avancées. L'exemple suivant illustre le fonctionnement du modèle McAfee intégré en cas de menaces au niveau du périmètre du centre de données.

Neutralisation des menaces émergentes

Les clouds privés nécessitent des mécanismes spécifiques pour bloquer les attaques ciblées et empêcher leur propagation. McAfee Virtual Network Security Platform, un système de prévention des intrusions (IPS) virtuel en ligne, inspecte les fichiers au niveau du périmètre. Ces fichiers sont ensuite analysés à l'aide de divers moteurs sans signatures activés par la stratégie antimalware avancée de la solution. Si un fichier semble suspect mais que son statut ne peut pas être établi avec certitude, McAfee Virtual Network Security Platform l'envoie à McAfee Advanced Threat Defense, qui l'analyse et en transmet la réputation à McAfee Threat Intelligence Exchange. Cette information est partagée avec la solution McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) installée sur le serveur, qui prend alors des mesures et supprime le fichier.

Protection et conformité optimisées grâce aux solutions McAfee

Pour offrir ce niveau de visibilité, de protection dynamique et de gestion efficace des stratégies, la combinaison de solutions McAfee est la suivante :

McAfee Virtual Network Security Platform

Ce système IPS avancé, doté de fonctionnalités complètes, a été spécialement conçu pour répondre aux exigences des environnements virtuels. Cette instance virtuelle de McAfee Network Security Platform vous permet de déployer rapidement des sondes virtuelles en vue de protéger diverses architectures réseau. Son intégration étroite avec d'autres technologies, telles que Intel Open Security Controller et McAfee Advanced Threat Defense, permet de prendre des mesures immédiates dès lors que le caractère malveillant d'un fichier est établi. Une approche coordonnée de la sécurité vous permet de bloquer immédiatement toute autre copie de ce fichier qui entrerait sur le réseau, sans qu'il soit nécessaire de réanalyser le fichier. De plus, la solution peut mettre en quarantaine un hôte infecté, empêchant ainsi la propagation d'activités malveillantes sur le réseau.

McAfee MOVE AntiVirus

McAfee MOVE AntiVirus assure aux postes de travail et serveurs virtuels une protection optimisée contre les logiciels malveillants. Il élimine les goulots d'étranglement et les retards d'analyse en transférant les opérations d'analyse, de configuration et de mise à jour des fichiers DAT depuis les images des systèmes invités vers une appliance virtuelle renforcée ou vers un serveur d'analyse de déchargement. L'exploitation d'un cache global de fichiers analysés permet à McAfee MOVE AntiVirus de s'assurer qu'une fois un fichier contrôlé et son absence de contamination confirmée, les machines virtuelles qui y accéderont par la suite seront dispensées d'attendre l'exécution d'une analyse.

McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange assure une détection des menaces et une réponse adaptatives et collaboratives, offrant ainsi aux entreprises une visibilité et un contrôle accrus dans leur lutte contre les menaces émergentes et ciblées. Il combine des informations mondiales sur les menaces avec des données collectées en local pour opérationnaliser la cyberveille en temps réel sur l'ensemble des solutions de protection des serveurs, de la passerelle, du réseau et du centre de données. En partageant instantanément cette cyberveille, McAfee Threat Intelligence Exchange permet à vos solutions de sécurité de fonctionner de concert pour échanger des informations et réagir aux attaques. Ce type de protection adaptative réduit le délai entre la détection et l'endiguement des attaques à quelques millisecondes — au lieu de plusieurs jours, semaines ou mois dans le cas des modèles de sécurité traditionnels.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense permet non seulement de détecter les attaques ciblées avancées actuelles, mais aussi de traduire les informations sur les menaces en actions afin d'assurer à l'entreprise une protection immédiate. Par rapport aux environnements

sandbox conventionnels, McAfee Advanced Threat Defense comprend des fonctionnalités d'inspection supplémentaires qui élargissent le champ de la détection et identifient les menaces appliquant des techniques de contournement. La solution recourt à une approche multiniveau innovante pour détecter les logiciels malveillants de type « jour zéro ». La solution combine des signatures de virus à faible empreinte, l'analyse de la réputation et l'émulation en temps réel avec des fonctions d'analyse statique de code et d'analyse dynamique (sandboxing) pour décortiquer le comportement réel des logiciels malveillants. Pour neutraliser les menaces qui échappent aux mécanismes de détection des environnements sandbox, McAfee Advanced Threat Defense comprend des fonctions de décompression étendues qui contrent les techniques de dissimulation et exposent le code exécutable d'origine. Cette solution permet à l'analyse statique du code de rechercher des anomalies au-delà des attributs de fichiers de haut niveau, en analysant tous les attributs et jeux d'instructions afin de déterminer le comportement attendu.

Logiciel McAfee ePolicy Orchestrator® (McAfee ePO™)

Le logiciel McAfee ePO offre une sécurité intégrée et une gestion centralisée des stratégies pour tous vos déploiements dans le cloud. Il vous permet de découvrir et de visualiser toutes les machines virtuelles, ce qui simplifie la protection des clouds. Les administrateurs peuvent surveiller les relations entre hyperviseurs et machines virtuelles, le niveau de sécurité ainsi que l'état de l'alimentation quasiment en temps réel.

Répondre aux besoins en protection et conformité dans les clouds privés

L'exploitation de la gamme intégrée de solutions McAfee de protection des clouds privés vous permet d'atteindre tous vos objectifs critiques en matière de sécurité, parmi lesquels :

- Visibilité totale sur les ressources à protéger et les menaces avancées, pour une protection renforcée des clouds privés. Cette visibilité contribue à protéger les données clients et les éléments de propriété intellectuelle de l'entreprise hébergés dans le cloud privé.
- Des technologies de protection dynamique intégrées et adaptées à la flexibilité des environnements de cloud privé, pour vous protéger contre les menaces avancées et garantir la conformité, en plus de surveiller le trafic est-ouest au sein de ces environnements. Ce type de protection permet de préserver et de prouver la conformité avec les lois et réglementations publiques et sectorielles.
- Gestion avancée des stratégies au sein de l'infrastructure, avec des fonctions d'automatisation permettant de déployer des stratégies de sécurité pour les clouds privés de manière efficace. Une telle gestion réduit les coûts associés à la sécurité, à l'application de mesures correctives en cas d'attaque et à la maintenance dans le centre de données défini par logiciel (SDDC). Elle réduit en outre le délai entre la découverte des menaces et attaques externes et internes, et la mise en œuvre de mesures correctives.

Principaux avantages de McAfee

- **Une gamme complète :** Tirez parti d'une gamme complète de solutions conçues pour fonctionner ensemble de manière harmonieuse dans le but de répondre aux défis de sécurité spécifiques des environnements de cloud privé.
- **Protection et correction dynamiques :** Les services IPS de nouvelle génération vous permettent de protéger votre cloud privé de manière dynamique, d'assurer sa gestion et sa conformité et de mettre en œuvre les mesures de correction nécessaires.
- **Prévention des attaques externes :** Découvrez et bloquez les attaques, les logiciels malveillants et les menaces au niveau du périmètre du centre de données défini par logiciel (SDDC), de même que les communications entrantes avec un serveur de commande et de contrôle.
- **Prévention des menaces internes :** Identifiez les logiciels malveillants et supprimez-les des serveurs virtualisés de votre SDDC. Détectez et neutralisez les attaques émanant d'utilisateurs avec privilèges.
- **Renforcement de la conformité :** Assurez et prouvez la conformité de votre entreprise avec les lois et réglementations publiques et sectorielles.
- **Réduction du temps de réponse :** Mettez en place une protection adaptative capable de réduire le délai entre la découverte des menaces et attaques externes et internes, et la mise en œuvre de mesures correctives.
- **Réduction des coûts :** Abaissez les coûts associés à la sécurité, à l'application de mesures correctives et à la maintenance au sein du SDDC.
- **Amélioration de la visibilité :** Bénéficiez d'une visibilité immédiate sur la présence d'attaques ciblées avancées au sein de votre entreprise.

En savoir plus

Pour plus d'informations, consultez la page **www.mcafee.com/fr/solutions/secure-cloud/index.aspx**.

1. « State of the Market: Enterprise Cloud 2016 »
(État du marché : cloud d'entreprise 2016), Verizon, novembre 2015

McAfee
Together is power.

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