McAfee Cloud Workload Security

Proteja suas cargas de trabalho de infraestrutura híbrida. Com mais segurança, rapidez e simplicidade.

Com a evolução dos data centers corporativos, mais cargas de trabalho migram para ambientes de nuvem a cada dia. A maioria das organizações tem um ambiente híbrido com uma mistura de cargas de trabalho no local e na nuvem, incluindo contêineres, os quais estão em fluxo constante. Isso constitui um desafio para a segurança, visto que os ambientes de nuvem (privada e pública) exigem novas abordagens e ferramentas para proteção. As organizações precisam de visibilidade central sobre todas as cargas de trabalho de nuvem, com defesa completa contra o risco de má configuração, malware e violações de dados.

O McAfee® Cloud Workload Security (McAfee® CWS) automatiza a descoberta e a defesa de contêineres e cargas de trabalho elásticas para eliminar pontos cegos, proporcionar defesa contra ameaças avançadas e simplificar o gerenciamento de múltiplas nuvens. A McAfee oferece uma proteção que possibilita que uma única política automatizada proteja eficazmente as suas cargas de trabalho enquanto estas passam pelos seus ambientes virtuais privados, públicos e de múltiplas nuvens, viabilizando uma excelência operacional para as suas equipes de segurança cibernética.

Segurança moderna para cargas de trabalho: casos de uso

Descoberta automatizada

Contêineres do Docker e instâncias de cargas de trabalho não gerenciados criam brechas no gerenciamento de segurança e podem permitir que os atacantes estabeleçam a presença necessária para se infiltrar na sua organização. O McAfee CWS descobre contêineres do Docker e instâncias de cargas de trabalho elásticas em ambientes Amazon Web Services (AWS), Microsoft Azure, OpenStack e VMware. Ele também monitora continuamente novas instâncias. Você obtém uma visão centralizada e completa dos ambientes e elimina pontos cegos operacionais e de segurança que resultam em exposição a riscos.

Principais vantagens

- A visibilidade contínua sobre instâncias de cargas de trabalho elásticas elimina os “pontos cegos” operacionais enquanto automatiza distribuições de políticas, antes trabalhosas
- O gerenciamento centralizado e as cargas de trabalho automatizadas reduzem consideravelmente a complexidade dos ambientes híbridos e de múltiplas nuvens
- Visualize e descubra ameaças à rede sem instalar um agente
- Defesas contra ameaças, otimizadas para máquinas virtuais, oferecem contramedidas em múltiplas camadas
- A integração com ferramentas de automação, como Chef e Puppet, proporciona segurança às cargas de trabalho de nuvem pública e privada no momento da distribuição

Conecte-se conosco

Obtenção de insights sobre o tráfego de rede

Ao utilizar o tráfego de rede nativo oferecido pelas cargas de trabalho na nuvem, o McAfee CWS consegue complementar e aplicar inteligência a partir de feeds de dados do McAfee® Global Threat Intelligence (McAfee® GTI). As informações enriquecidas podem mostrar propriedades como pontuação de risco, geolocalização e outras informações de rede importantes. Essas informações podem ser utilizadas para criar ações de correção automatizadas para proteger as cargas de trabalho.

Integração em estruturas de distribuição

O McAfee CWS cria scripts de distribuição para possibilitar a distribuição e o o gerenciamento automáticos do agente McAfee® para cargas de trabalho na nuvem. Esses scripts permitem integração em ferramentas tais como Chef, Puppet e outras estruturas de DevOps para distribuição do agente McAfee para cargas de trabalho executadas por provedores de nuvem, como AWS e Microsoft Azure.

Consolidação de eventos

O McAfee CWS permite que as organizações utilizem uma única interface para gerenciar diversas tecnologias de contramedidas para ambientes no local e na nuvem. Isso também inclui integração em tecnologias adicionais, como AWS GuardDuty, McAfee® Policy Auditor e McAfee® Network Security Platform.

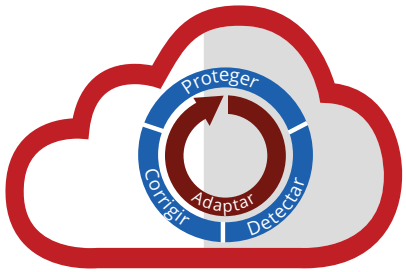
- Os administradores podem aproveitar o monitoramento contínuo e os comportamentos não autorizados identificados pelo AWS GuardDuty, o que proporciona mais um nível de visibilidade sobre as ameaças. Essa integração permite que os usuários do McAfee CWS visualizem eventos do GuardDuty, os quais incluem conexões de rede, sondagens de portas e solicitações de DNS para instâncias EC2, diretamente de dentro do console do McAfee CWS.
- O McAfee Policy Auditor realiza verificações com base em agente relacionadas a auditorias de configuração conhecidas ou definidas pelo usuário para fins de conformidade, como Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Center for Internet Security Benchmark (CIS Benchmark) ou outros padrões setoriais. O McAfee CWS informa quaisquer auditorias falhas, proporcionando visibilidade instantânea sobre más configurações de cargas de trabalho na nuvem.
- O McAfee Network Security Platform é uma outra plataforma de segurança de nuvem que realiza inspeção de rede no tráfego de ambientes híbridos, bem como AWS e Microsoft Azure. Ele realiza inspeções mais profundas em nível de pacote no tráfego de rede e informa quaisquer discrepâncias ou alertas através do McAfee CWS. Isso proporciona visibilidade de painel único sobre ambientes de múltiplas nuvens para fins de correção.

Imposição de políticas de grupo para segurança de rede

O McAfee CWS permite que usuários e administradores criem políticas de grupo de referência para segurança e auditem as políticas que são executadas nas cargas de trabalho em relação a essas referências. Quaisquer

Principais vantagens (continuação)

- Tenha uma proteção multicamada fácil contra intrusões e malware avançado
- Descubra e monitore contêineres do Docker e proteja-os com microssegmentação
- Proteja o seu ambiente adotando ações corretivas diretamente de dentro da solução



Cloud Workload Security

Visibilidade
e **controle** abrangentes

desvios ou alterações em relação à referência podem gerar um alerta no console do McAfee CWS para fins de correção. Os administradores também podem configurar manualmente grupos de segurança de rede nativa, a partir do McAfee CWS, que lhe permitam controlar diretamente políticas de grupo de segurança nativas da nuvem.

Qual é o diferencial do McAfee Cloud Workload Security: principais recursos e tecnologias

Suporte para compilação nativo na nuvem

Utilizando o McAfee CWS, os usuários podem consolidar o gerenciamento de múltiplas nuvens privadas e públicas em um único console de gerenciamento, incluindo AWS EC2, máquinas virtuais do Microsoft Azure, OpenStack e VMware Vcenter. O McAfee CWS pode importar e permitir que os usuários executem na nuvem com o novo suporte de compilação, nativo na nuvem, para Amazon Elastic Container Service for Kubernetes (Amazon EKS) e Microsoft Azure Kubernetes Service (AKS).

Gerenciamento simples e centralizado

Um único console oferece gerenciamento centralizado e uma política de segurança consistente em ambientes de múltiplas nuvens, abrangendo servidores, servidores virtuais e cargas de trabalho na nuvem. Os administradores também podem criar múltiplas permissões com base em funções no software McAfee® ePolicy Orchestrator® (McAfee ePO™), o que lhes permite definir as funções dos usuários de maneira mais específica e apropriada.

Visualização da rede com microssegmentação

Capacidades de microssegmentação, alertas de risco priorizados e visualização de rede nativas da nuvem oferecem conscientização e controle para prevenir o avanço de ataques laterais dentro de ambientes virtualizados e oriundos de fontes maliciosas externas. A capacidade de desligamento ou colocação em quarentena com um único clique diminui a possibilidade de erros de configuração e aumenta a eficiência da correção.

Melhor segurança para virtualização

O McAfee CWS protege as suas máquinas virtuais de nuvem privada contra malware utilizando o McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus). Ele faz isso tudo sem consumir os recursos subjacentes ou exigir custos operacionais extras. O McAfee MOVE AntiVirus permite que as organizações transfiram a carga da segurança para máquinas virtuais dedicadas para uma varredura otimizada de seu ambiente virtualizado.

Os usuários obtêm proteção antimalware com o McAfee® Endpoint Security for Servers. Essa solução pode agendar, de maneira inteligente, tarefas que utilizam recursos intensivamente, como varreduras solicitadas, para evitar impacto sobre processos empresariais críticos.

Tags e automatização na segurança das cargas de trabalho

Atribua automaticamente as políticas certas a todas as cargas de trabalho, com a capacidade de importar informações de tags do AWS e do Microsoft Azure para o software McAfee ePO, e atribua políticas com base nesses tags. Os tags existentes do AWS e do Microsoft Azure são sincronizados com os tags do software McAfee ePO, sendo gerenciados automaticamente.

Autocorreção

O usuário define as políticas do software McAfee ePO. Se o McAfee CWS encontrar um sistema que não esteja protegido pelas políticas de segurança do software McAfee ePO e que contenha um malware ou vírus, esse sistema será colocado em quarentena automaticamente.

Proteção adaptável contra ameaças

O McAfee CWS integra contramedidas abrangentes, incluindo autoaprendizagem, contenção de aplicativos, antimalware otimizado para máquinas virtuais, listas brancas, monitoramento de integridade de arquivos e microssegmentação, para proteger as suas cargas de trabalho contra ameaças como ransomware e ataques direcionados. O McAfee® Advanced Threat Protection derrota ataques sofisticados e nunca antes encontrados aplicando técnicas de autoaprendizagem para condenar cargas maliciosas com base em seu comportamento e nos atributos de seu código.

Controle de aplicativos

A inclusão de aplicativos em uma lista branca previne ataques tanto conhecidos quanto desconhecidos, só permitindo a execução de aplicativos confiáveis e bloqueando quaisquer cargas não autorizadas. O McAfee® Application Control proporciona uma proteção dinâmica com base em inteligência local e global contra ameaças, bem como a capacidade de manter os sistemas atualizados sem desativar recursos de segurança.

Monitoramento de integridade de arquivos (FIM)

O monitoramento de integridade de arquivos da McAfee monitora continuamente os arquivos e os diretórios do seu sistema para assegurar que eles não foram comprometidos por malware, hackers ou elementos internos maliciosos. Detalhes de auditoria abrangentes proporcionam informações sobre como os arquivos nas cargas de trabalho dos servidores estão sendo modificados e alertam quanto à presença de ataques ativos.

Cobertura de segurança apropriada para o seu ambiente de múltiplas nuvens

O McAfee CWS mantém uma segurança da mais alta qualidade, ao mesmo tempo que aproveita as vantagens da nuvem. Ele abrange múltiplas tecnologias de proteção, simplifica o gerenciamento da segurança e impede que ameaças cibernéticas afetem os seus negócios, para que você possa se concentrar em seu crescimento. Veja a seguir uma comparação dos recursos das opções de pacotes disponíveis.

Recursos	McAfee® Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
Gerenciamento centralizado (plataforma McAfee ePO)	✓	✓	✓
Suporte para múltiplas nuvens (AWS, Microsoft Azure e VMware)	✓	✓	✓
Uso de microssegmentação para colocar em quarentena cargas de trabalho e contêineres	✓	✓	✓
McAfee MOVE (sem agente e multiplataforma)	✓	✓	✓
Prevenção de ameaças do McAfee Endpoint Security para o SO do servidor (Windows e Linux)	✓	✓	✓
Firewall com base em host	✓	✓	✓
Gerenciamento de firewall nativo para AWS e Microsoft Azure (grupos de segurança)	✓	✓	✓
Prevenção de explorações e intrusões no host	✓	✓	✓
Importação de informações de tags do AWS e do Microsoft Azure no software McAfee ePO	✓	✓	✓
Autocorreção em cargas de trabalho fora de conformidade	✓	✓	✓
Proteção adaptável contra ameaças, com autoaprendizagem		✓	✓
Visualização do tráfego de rede e microssegmentação		✓	✓
Análise do tráfego de rede nativo da nuvem combinada com avaliação de reputação do McAfee GTI		✓	✓
Integração com o McAfee® Virtual Network Security Platform (McAfee® vNSP)		✓	✓
Listas brancas dinâmicas para servidores por meio do McAfee Application Control			✓
Registro de auditoria contínuo com o monitoramento de integridade de arquivos da McAfee			✓
Proteção de arquivos e pastas com o McAfee® Change Control para servidores			✓

Saiba mais

Para mais informações, visite: **www.mcafee.com/br/products/cloud-workload-security.aspx**.

Os recursos e vantagens das tecnologias da McAfee dependem da configuração do sistema e podem exigir a ativação de hardware, software ou serviços. Saiba mais em www.mcafee.com/br. Nenhum sistema de computador é absolutamente seguro.

McAfee Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br