McAfee Public Cloud Server Security Suite

Segurança abrangente para cargas de trabalho em nuvem AWS e Azure

Principais vantagens

- Desenvolvido para cargas de trabalho AWS e Azure
- Descoberta instantânea
- Avaliação da segurança e remediação de ameaças
- Segurança expansível
- Proteção abrangente
- Aproveita o console de gerenciamento McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Inclui as opções de distribuição Chef, Puppet e OpsWorks
- Demonstre conformidade
- Integra-se com outras outras soluções da Intel Security

Conforme as empresas mudam sua estratégia de data center para incluir e, muitas vezes, liderar as instâncias de servidor em nuvem pública, elas estão cientes de que um modelo de responsabilidade compartilhada[1] para proteção é um fator-chave a ser considerado. Os fornecedores de nuvem pública, como Amazon Web Services (AWS) e Microsoft Azure, protegem o perímetro, enquanto os usuários cuidam da segurança do conteúdo. Entretanto, como empresas pioneiras protegem suas cargas de trabalho na nuvem contra ameaças persistentes avançadas (APTs) e de dia zero enquanto mantêm os custos alinhados com suas estratégias de nuvem? Alguns dos principais desafios para as empresas ao adotar a nuvem são:

- Está ficando difícil acompanhar ameaças avançadas e de dia zero.
- A falta de visibilidade e o gerenciamento centralizado tornam isso extremamente desafiador em infraestruturas de múltiplas nuvens.
- A degradação do desempenho é uma preocupação na segurança da carga de trabalho na nuvem.

O McAfee® Public Cloud Server Security Suite oferece descoberta instantânea e controle de ameaças e cargas de trabalho AWS e Azure para uma proteção completa, consistente e contínua, com o mínimo de impacto sobre o desempenho. Você pode descobrir múltiplos data centers na nuvem, contas na nuvem, máquinas virtuais e ameaças emergentes.

A segurança abrangente proporcionada pelo McAfee Public Cloud Server Security Suite inclui prevenção contra intrusões e antivírus em sua base, juntamente com lista branca avançada para proteger contra ameaças de dia zero, controle de alterações para cumprir com requisitos regulatórios de conformidade e gerenciamento de criptografia para proteção de dados. Um único console de gerenciamento facilita o gerenciamento de múltiplas nuvens e a imposição de políticas. Opções de distribuição flexíveis com as ferramentas Chef, Puppet e OpsWorks do DevOps proporcionam uma experiência descomplicada e com o mínimo de impacto.

Figura 1. Console de gerenciamento único para múltiplas infraestruturas de nuvem e múltiplas tecnologias da Intel Security.

intel Security

Plataformas compatíveis

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

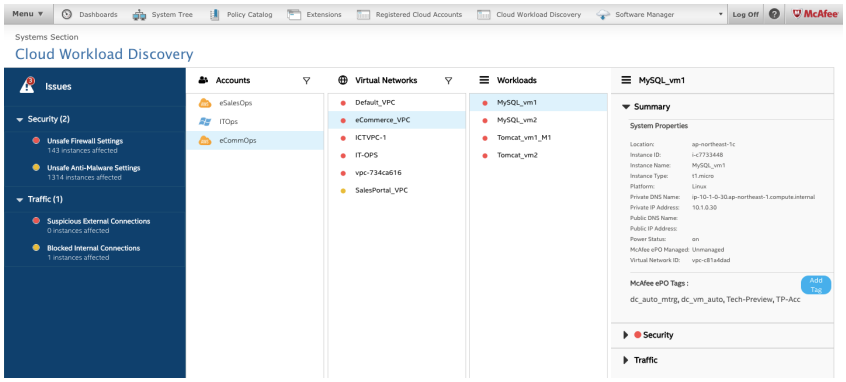

Figura 2. Descubra e monitore múltiplas infraestruturas de nuvem e ameaças emergentes

Descubra infraestruturas de nuvem e ameaças

Para ter um controle melhor sobre a infraestrutura de nuvem e as ameaças, você precisa de uma visibilidade melhor sobre elas.

- Descubra todas as redes virtuais ou nuvens privadas virtuais (VPCs), modelos e cargas de trabalho pela infraestrutura AWS e Azure em questão de minutos. Ter informações detalhadas sobre as contas da infraestrutura de nuvem, saber quais usuários têm acesso a quais partes da infraestrutura de nuvem, compreender como as cargas de trabalho são atribuídas a modelos e VPCs e ter uma visão rápida da árvore de sistema associada à infraestrutura de nuvem são as primeiras etapas para proteger devidamente a sua infraestrutura de nuvem.
- Obtenha visibilidade sobre a segurança de múltiplas nuvens de forma centralizada. Aproveite informações sobre ameaças de ponta a ponta, incluindo fontes de ataques, para um melhor controle da segurança.
- Visualize o tráfego pelas cargas de trabalho e gerencie a forma como as informações fluem entre elas e como são acessadas de fora da organização.

Monitore a nuvem e tome providências mais rápidas em relação a alertas de segurança

Como uma correção mais rápida é cada vez mais importante, com esta solução você pode determinar rapidamente os problemas de segurança em um nível mais profundo e tomar providências imediatas.

- Identifique problemas que exijam atenção urgente e tome as medidas apropriadas utilizando um código de cores para as ameaças.
- Crie rótulos personalizados e atribua-os às cargas de trabalho com base em seus requisitos específicos.
- Tome medidas corretivas para enfrentar os problemas de segurança e adote políticas ou defina reputações de ameaça para defender a infraestrutura contra futuros incidentes de segurança.
- Gerencie o firewall da nuvem com políticas personalizadas para cargas de trabalho individuais ou grupos de cargas de trabalho. Gerencie políticas para grupos de segurança AWS para controlar o tráfego em uma ou múltiplas instâncias.
- Identifique a ocorrência de tráfego suspeito em VPCs e tome providências de correção para impedir que informações críticas caiam em mãos erradas

Proteção abrangente contra ameaças

O McAfee Public Cloud Server Security Suite aproveita um único agente que proporciona múltiplas camadas de segurança que podem ser gerenciadas utilizando-se um único console de gerenciamento em múltiplas plataformas de nuvem. Essa solução também pode ser distribuída com ferramentas compatíveis com DevOps, proporcionando a melhor experiência possível.

Para saber mais

Visite a página do produto: **www.mcafee.com/br/products/public-cloud-server-security-suite.aspx**

Também disponível para compra no **AWS Marketplace**.

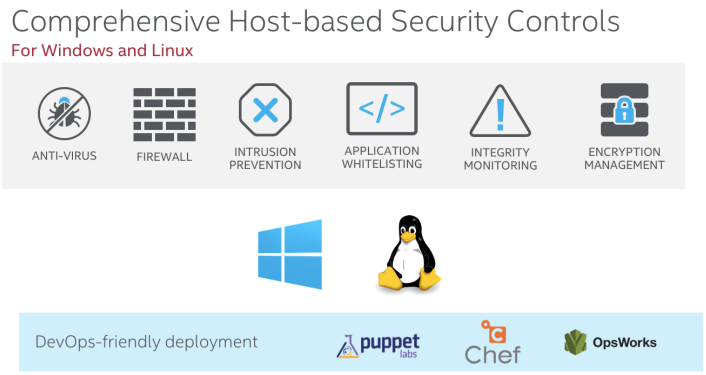

Figura 3. Segurança abrangente para cargas de trabalho de nuvem pública.

Recurso	Vantagens
Opções de distribuição Chef, Puppet e AWS OpsWorks	• As ferramentas de distribuição DevOps permitem que a segurança seja levada em consideração antecipadamente e com facilidade de distribuição. • A segurança pode ser incorporada como parte das operações.
Descoberta de cargas de trabalho na nuvem	• Visibilidade instantânea sobre as infraestruturas de nuvem para descobrir data centers virtuais, cargas de trabalho na nuvem e firewalls de nuvem. • Notificação rápida de alertas sobre ameaças com avaliação automática da postura de segurança. • Correção mais rápida das ameaças com alertas priorizados com base na criticalidade das ameaças e etapas para agir rapidamente em relação a esses alertas.
Console único de gerenciamento para múltiplas soluções de segurança da infraestrutura de nuvem (software McAfee ePO)	• Extremamente vantajoso para uma situação de ambiente híbrido. • Gerenciamento por um único painel para políticas e cargas de trabalho físicas, virtuais e em nuvem. • Integração entre tecnologias de segurança locais e na nuvem do parceiro e da Intel Security. • Reduz o custo total de propriedade com processos de segurança integrados e etapas de resolução rápida.
Antimalware	• Máxima defesa contra malware. Protege os sistemas e arquivos contra vírus, spyware, worms, cavalos de Troia e outros riscos de segurança. Detecta e remove malware, além de permitir que os usuários configurem com facilidade as políticas para gerenciar itens em quarentena.
Firewall de host	• Proteja as cargas de trabalho contra ataques e acesso não autorizado.
Prevenção de intrusões de hosts	• Bloqueia tráfego de rede indesejado ou nocivo e bloqueia proativamente ataques conhecidos e de dia zero com uma tecnologia premiada e patenteada. • Impede que alterações indesejadas sejam feitas nas cargas de trabalho ao restringir o acesso a portas, arquivos, compartilhamentos, chaves do Registro e valores do Registro especificados. • A proteção de memória evita que programas anormais ou ameaças estourem os limites do buffer e sobrescrevam a memória adjacente ao gravar dados em um buffer. A exploração de estouros de buffer pode resultar na execução de código arbitrário no seu computador.
Lista branca (whitelist) de aplicativos	• Protege contra ameaças persistentes avançadas e de dia zero sem atualizações de assinaturas. • Reforça a segurança e reduz os custos de propriedade com inserção dinâmica em lista branca, aceitando automaticamente software novo adicionado através de nossos canais confiáveis. • Reduz os ciclos de aplicação de patches utilizando listas brancas seguras de aplicativos e proteção de memória avançada.
Monitoramento de integridade de arquivos	• Oferece detecção contínua de alterações em nível de sistema em locais remotos ou distribuídos. • Evita adulterações através do bloqueio de alterações não autorizadas em diretórios, configurações e arquivos de sistema críticos. • Rastreia e valida todas as tentativas de alteração em tempo real na carga de trabalho, impondo uma política de alterações por janela de tempo, fonte ou tíquete de trabalho aprovado.
Gerenciamento de criptografia	• Criptografa dados armazenados em volumes AWS EBS com o padrão de criptografia avançada AWS Advanced Encryption Standard (AES). • Volumes com dados preexistentes podem ser criptografados convenientemente. • Integra-se com o serviço de gerenciamento de chaves Key Management Service (KMS) da Amazon para criptografia.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com

1. **http://www.mcafee.com/br/resources/white-papers/wp-cloud-security-primer-techtarget.pdf**