McAfee Cloud Workload Security

确保您混合基础设施工作负载的安全。更安全，更快速，更简单。

随着公司数据中心的进化，每天都有更多工作负载迁移到云环境中。大多数组织是混合式环境，其中有不断变化的混合的内部和云端工作负载，包括容器。这会带来安全挑战，因为云环境（私有和公有）需要新的保护方法和工具。组织需要所有云工作负载的集中可见性，从而全面防范错误配置、恶意软件和数据泄漏造成的风险。

McAfee® Cloud Workload Security (McAfee® CWS) 可实现对弹性工作负载和容器的发现和防御自动化，从而消除盲点，提供高级威胁防护并简化多云管理。当您的工作负载通过虚拟私有、公共和多云环境转移时，McAfee 可通过单一自动化策略提供有效保护，让您的网络安全团队能够实现卓越运营。

现代化工作负载安全：用例

自动发现

未托管的工作负载实例和 Docker 容器会给安全管理造成裂隙，让攻击者找到潜入组织的突破口。McAfee CWS 可在 Amazon Web Services (AWS)、Microsoft Azure、OpenStack 和 VMware 环境中发现弹性工作负载实例和 Docker 容器，也将持续监控新实例。您将获得覆盖各个环境的集中而全面的视图，从而消除导致风险暴露的运营和安全盲点。

深入分析网络流量

通过利用来自云工作负载的本机网络流量，McAfee CWS 能够增强并应用来自 McAfee® Global Threat Intelligence (McAfee® GTI) 数据源的情报信息。丰富的信息能够显示诸如风险评分、地理位置和其他重要网络信息等指标。这些信息可用于创建自动补救操作以保护工作负载。

主要优势

- 弹性工作负载实例的持续可见性消除了运营“盲点”，能够自动实现过去繁复的策略部署。
- 集中式管理和自动化工作负载大幅降低了混合及多云环境的复杂性。
- 在不安装代理的情况下可视化和发现网络威胁。
- 经过虚拟机优化的威胁防御可提供多层对策。
- 与 Chef 和 Puppet 等自动化工具的集成在部署时给公共和私有云工作负载带来了安全性。

联系我们

集成到部署框架中

McAfee CWS 可创建部署脚本，以允许进行自动部署和 McAfee® 代理到云端工作负载的管理自动化。可以将这些脚本集成到 Chef、Puppet 等工具和其他 DevOps 框架中，以便将 McAfee 代理部署到由云提供商（例如 AWS 和 Microsoft Azure）运行的工作负载中。

整合事件

McAfee CWS 允许组织使用单一界面来管理内部和云端环境的各种对策技术。这也包括集成到其他技术中，例如 AWS GuardDuty、McAfee® Policy Auditor 和 McAfee® Network Security Platform。

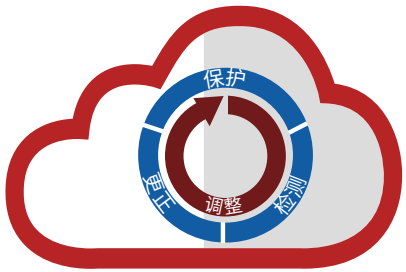
- 管理员可以利用持续监控和由 AWS GuardDuty 识别的未授权行为，提供另一级别的威胁监视。这一集成允许 McAfee CWS 客户直接在 McAfee CWS 控制台查看 GuardDuty 事件，包括 EC2 实例的网络连接、端口探查和 DNS 请求。
- McAfee Policy Auditor 根据已知或用户定义的配置审核来执行基于代理的合规性检查，例如 Health Insurance Portability and Accountability Act (HIPAA)、Payment Card Industry Data Security Standard (PCI-DSS)、Center for Internet Security Benchmark (CIS Benchmark) 或其他行业标准。McAfee CWS 会报告所有失败的审核，以便即时了解云中工作负载的错误配置。
- McAfee Network Security Platform 是另一个云安全平台，可对混合环境以及 AWS 和 Microsoft Azure 环境中的流量执行网络检查。该解决方案可对网络流量执行更为深入的数据包级别的检查，并通过 McAfee CWS 报告所有差异或发出警报，这样就针对多云环境的补救措施提供了单方面分析。

强制实施网络安全组策略

McAfee CWS 允许用户和管理员创建基线安全组策略，并根据这些基线审核在工作负载上运行的策略。与基线的任何偏差或更改都可能会在 McAfee CWS 控制台中创建警报，以进行纠正。管理员还可以通过 McAfee CWS 手动配置本机网络安全组，他们通过安全组能够直接控制云原生的安全组策略。

主要优势（续）

- 轻松实现对高级恶意软件和入侵的多层防范。
- 发现和监控 Docker 容器，并通过微分段保护其安全。
- 通过直接在解决方案中利用修正措施来保护您的环境安全。



Cloud Workload Security

全面的**可见性**
和**控制效果**

McAfee Cloud Workload Security 脱颖而出的原因：主要功能和技术

支持构建原生云

使用 McAfee CWS，客户可在单一管理控制台中集中管理多个公共和私有云，其中包括 AWS EC2、Microsoft Azure 虚拟机、OpenStack 和 VMware Vcenter。McAfee CWS 可以利用适用于 Amazon Elastic Container Service for Kubernetes (Amazon EKS) 和 Microsoft Azure Kubernetes Service (AKS) 的全新原生云构建支持功能，导入并允许客户在云中运行。

简化的集中式管理

单一的控制台跨服务器、虚拟服务器和云工作负载在多云环境中提供一致的安全策略和集中式管理。管理员还可以在 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件中创建多个基于角色的权限，使他们能够更具体、更恰当地定义用户角色。

利用微分段的网络虚拟化

原生云网络虚拟化、划分优先顺序的风险警报以及微分段功能提供认知和控制，以防范虚拟化环境中的横向攻击发展以及外部恶意源。一键关机或隔离功能有助于缓解配置错误的可能性，并提高补救效率。

出色的虚拟化安全功能

McAfee CWS 套件使用 McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) 来保护您的私有云虚拟机免受恶意软件的侵害。同时不会造成底层资源紧张，也不会有额外的运营成本。McAfee MOVE AntiVirus 允许组织将安全性转移到专用虚拟机上，以优化其虚拟环境的扫描。

用户可通过 McAfee® Endpoint Security for Servers 获得防恶意软件保护。此解决方案可智能地计划资源密集型任务（如按需扫描），以避免对关键业务流程产生影响。

对工作负载进行标记并自动确保其安全

利用将 AWS 和 Microsoft Azure 标记信息导入 McAfee ePO 软件并根据这些标记分配策略的功能，自动将权限策略分配给所有工作负载。现有 AWS 和 Microsoft Azure 标记会与 McAfee ePO 软件标记进行同步，以便实现自动管理。

自动修正

由用户来定义 McAfee ePO 软件策略。如果 McAfee CWS 发现了未受 McAfee ePO 软件安全策略保护，并且包含恶意软件或病毒的系统，则会自动隔离该系统。

自适应威胁防护

McAfee CWS 整合了全面的对策，包括机器学习、应用程序遏制、针对虚拟机进行了优化的防恶意软件、白名单、文件完整性监控和微分段，可防止您的工作负载遭到勒索软件和定向攻击等威胁的入侵。McAfee® Advanced Threat Protection 通过应用机器学习技术来根据恶意负载的代码属性和行为对恶意负载进行判定，从而战胜之前从未有过的复杂攻击。

应用程序控制

应用程序白名单功能只允许可信的应用程序运行，同时拦截一切未经授权的负载，从而能够防范已知和未知攻击。McAfee® Application Control 功能可根据本地和全球威胁情报提供动态保护，并且能够在无需禁用安全功能的情况下让系统保持最新。

文件完整性监控 (FIM)

McAfee® 文件完整性监控功能可持续进行监控，确保您的系统文件和目录没有受到恶意软件、黑客以及内部恶意人员的侵害。全面的审核详细信息提供有关服务器工作负载上文件如何变化的详细信息，并在检测到活跃攻击时向您发出警告。

适合多云环境的安全保护

McAfee CWS 可确保您在充分利用云的优势的同时，还能持续拥有最高级别的安全质量。它涵盖多种安全保护技术，可简化安全管理过程，并防止网络威胁对您的业务造成不良影响，从而让您集中精力发展业务。以下是可用软件包选项的特性比较。

特点	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
集中式管理（McAfee ePO 平台）	✓	✓	✓
支持多云（AWS、Microsoft Azure、VMware）	✓	✓	✓
使用微分段隔离工作负载和容器	✓	✓	✓
McAfee MOVE（无代理和多平台）	✓	✓	✓
适用于服务器操作系统（Windows 和 Linux）的 McAfee Endpoint Security 威胁防御	✓	✓	✓
基于主机的防火墙	✓	✓	✓
适用于 AWS 和 Microsoft Azure 的本地防火墙管理（安全组）	✓	✓	✓
主机入侵和漏洞利用防护	✓	✓	✓
将 AWS 和 Microsoft Azure 标记信息导入 McAfee ePO 软件	✓	✓	✓
对不符合要求的工作负载进行自动修正	✓	✓	✓
利用机器学习功能的自适应威胁防护		✓	✓
网络流量可视化和微分段		✓	✓
结合 McAfee GTI 信誉分数的原生云网络流量分析		✓	✓
McAfee® Virtual Network Security Platform (McAfee® vNSP) 集成		✓	✓
通过 McAfee Application Control 对服务器实施动态白名单技术			✓
通过 McAfee 文件完整性监控功能持续审核日志记录			✓
通过 McAfee® Change Control for Servers 保护文件和文件夹的安全			✓

了解更多

有关详细信息，请访问：
https://www.mcafee.com/enterprise/zh-cn/products/cloud-workload-security.html。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，
100013
电话：8610 8572 2000
www.mcafee.com/cn