McAfee Cloud Workload Security

保护私有和公共云工作负载。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 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、公共和混合环境转移时，McAfee 无可匹敌的保护可通过单一自动化策略提供有效保护，让您的安全团队实现运营卓越性。

实时监控

自动发现

不可见的工作负载实例和 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 Cloud Workload Security 可跨 Amazon Web Services (AWS)、Microsoft Azure 和 VMware 环境发现弹性工作负载实例和 Docker 容器，并持续监控新实例。您将获得跨各个环境的集中而全面的视图，消除导致风险暴露的运营和安全盲点。

现代化工作负载安全

高级威胁防护

McAfee Cloud Workload Security 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。先进的威胁防护（包括机器学习）通过应用机器学习技术战胜之前从未有过的复杂攻击，根据这些工具的代码属性和行为判定恶意负载。

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。
- 发现和监控 Docker 容器，并通过微分段保护其安全。
- 经过虚拟机优化的威胁防御可提供多层对策。
- 集中式管理和自动化工作流大幅降低了混合及多云环境的复杂性。
- 与 Chef 和 Puppet 等自动化工具的集成在部署时给公共和私有云带来了安全性。

联系我们

整合事件

McAfee Cloud Workload Security 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。这包括第三方技术，如 AWS GuardDuty。管理员可以利用连续监控和由 AWS GuardDuty 识别的未授权行为，提供另一级别的威胁可视性。这一集成允许 McAfee Cloud Workload Security 客户直接在 McAfee Cloud Workload Security 控制台查看 GuardDuty 事件，这包括 EC2 的网络连接、端口探查和 DNS 请求。当流量对应 McAfee Cloud Workload Security 已发现的流量时，GuardDuty 网络连接事件会映射在流量图形中。

出色的虚拟化安全

McAfee Cloud Workload Security 保护您的私有云虚拟机免受恶意软件侵害，同时不会造成底层资源紧张，没有额外的运营成本。您可以得到智能地计划资源密集型任务的防恶意软件保护（如按需扫描），同时虚拟机监控程序不会过度负载。

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，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。

文件完整性监控 (FIM)

FIM 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、黑客以及恶意内部人员的侵害。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，并就活跃的攻击向您发出警告。

Application Control

应用程序白名单防范已知和未知攻击，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。应用程序控制根据本地和全球威胁情报提供动态保护，并且让系统保持最新状态而无需禁用安全功能。

简化管理

通过集中式管理实现一致性

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。

自动部署

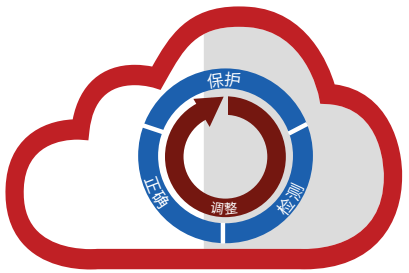
凭借 Chef、Puppet 和 Ansible 等组织提供的自动化部署工具，您可在多云环境中自动部署安全技术。

改善安全覆盖范围

McAfee Cloud Workload Security 确保您维持最高的安全质量，同时利用云。它涵盖多种保护技术，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。

主要优势（续）

- 实现了对先进恶意软件和入侵的多层防范，并且更加易用。
- 在不安装代理的情况下可视化和发现网络威胁。
- 通过直接在解决方案中利用修正措施来保护您的环境。



Cloud Workload Security

全面**可见性**和**控制力**

功能	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
集中式管理（McAfee® ePO™ 平台）	✓	✓	✓
多云支持（AWS、Azure、VMware）	✓	✓	✓
使用微分段隔离工作负载和容器	✓	✓	✓
服务器操作系统的威胁防护（Windows 和 Linux）	✓	✓	✓
主机入侵和漏洞利用防护	✓	✓	✓
云加密管理	✓	✓	✓
适用于 AWS 和 Azure 的本地防火墙管理（安全组）	✓	✓	✓
McAfee® Management for Optimized Virtual Environments（无代理和多平台）	✓	✓	✓
基于主机的防火墙	✓	✓	✓
利用机器学习的自适应威胁防护		✓	✓
网络流量可视化和微分段		✓	✓
结合 Global Threat Intelligence 信誉分数的云原生网络流量分析		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
McAfee® Virtual Network Security Platform 集成		✓	✓

了解更多信息

有关详细信息，请访问：**https://www.mcafee.com/cn/products/cloud-workload-security.aspx**.

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