McAfee ePolicy Orchestrator

激励并助力安全专业人员

安全管理需要在不同的工具和数据之间处理繁琐的事务。这会让攻击者占得先机，他们有更多时间来利用工具之间不可见的缺口，并造成更大损害。此外，网络安全工作人员资源有限，需要具备精深的安全专业技能才能轻松协调复杂的网络安全环境。

企业需要快速响应任何类型设备上的威胁以便最大程度地减轻损害，并且管理层通常会要求安全专业人员提供安全管理有效性的证据。McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理平台可通过内部部署和云部署两种方式访问，避免了耗时的人工操作和人工操作可能出现的错误，还可以帮助安全专业人员更快速更高效地做出响应。

基本的安全保护功能

首先从必备的安全功能说起。监测和控制设备与系统运行状况的能力是所有安全基础设施的核心。行业标准，例如互联网安全中心 (CIS) Controls™ 和 Benchmarks，以及美国国家标准与技术研究院 (NIST) SP 800-53 安全与隐私控件均要求必须对安全基础设施进行监测和控制。McAfee ePO 控制台可让您获得关键可见性并设置和自动执行策略，以确保整个企业健康的安全态势。通过单一控制台对整个企业环境进行策略管理并实施安全策略，消除了协调多款产品的操作复杂性。这一基本的安全管理功能是确保 IT 安全合规的基础。

主要优势

- 业界推崇的集中式管理解决方案，具有独特的集成式单一管理控制台，操作非常简单，可通过内部部署或云部署两种方式进行访问
- 自动化工作流可简化管理工作并提高效率
- 集成了 McAfee 和 150 多款第三方安全解决方案的综合性开放式平台，可以更快速更准确地针对威胁做出响应
- 通用的安全管理功能，适用于市场上大部分设备
- 可利用并增强操作系统中内置的本机安全控件（例如 Windows Defender）
- 安全保护范围可扩展到数千台设备，全面覆盖设备和云端

联系我们

经过实践验证且操作简单的高级安全管理解决方案

全球有 36,000 多家企业和组织信赖 McAfee ePO 控制台，用它来管理安全，简化和自动化合规流程，并全面提升设备、网络和安全运营的可见性。大型企业依靠 McAfee ePO 控制台的高度可扩展架构，通过一个集成式控制台即可管理数十万个节点。此信息显示板视图可帮助您确定风险管理任务的优先级顺序，并在一个新的安全保护工作区中用一个图形化的视图向您提供有关您整个数据环境的安全态势摘要信息。

管理员可以深入了解特定事件以获得更多见解。此摘要视图可减少创建报告和整理手头数据所需的时间，还可避免因手动操作而带来的潜在错误。McAfee ePO 控制台让企业安全管理员有机会简化策略维护过程，利用我们业界领先的消息传递结构 Data Exchange Layer (DXL) 引入第三方威胁情报，并将策略与一系列安全产品进行双向集成。这些高效运营削减了流程和数据共享开销，可实现更迅速、更精准的响应。

开放式平台高效管理，从容应对无序增长

ESG研究显示，40%的企业使用10到25种工具，而30%的企业使用 26 到 50 种工具来管理数十亿种针对设备的新威胁。像这样使用多种安全产品不仅造成了操作复杂性，还使从安装到报告的统一管理体验的运营成本翻倍。超过一半的企业预计，通过集成安全工具可节省 20% 以上的时间（2018 年 MSI研究）。McAfee采用开放式平台的安全管理方法来满足这些要求，让您能够整合扩展，同时还能全面保护各类资产的安全，支持威胁情报收集，管理开源数据并集成第三方产品。McAfee 可集中控制各种安全产品的合规性并对这些设备进行管理。分析人员能够迅速透视各种产品，找到关键数据并采取必要的策略措施。McAfee ePO 控制台还可让您为下一代技术投资，并在单一框架中将它们与现有资产集成。

我们的开放式平台提供了一系列集成方法（脚本编写、API、不带 API，以及可最大限度减少用户操作的开源 DXL 消息传递结构），让您能够选择可满足企业需求的最佳安全管理方法，而无需进行大量的自定义或其他服务。通过 McAfee® Security Innovation Alliance 计划，我们能够加快可互操作的安全产品的开发，简化这些产品与复杂客户环境的集成，并提供真正意义上的集成式互联安全生态系统，从而帮助客户最大限度地实现其现有安全投资的价值。McAfee Security Innovation Alliance 计划拥有 150 多个集成合作伙伴。

业内分析人士表示，McAfee ePO 软件是许多客户购买 McAfee 解决方案并始终选择 McAfee 产品的原因所在。

集成式平台的优势

与没有使用集成式平台的企业相比，使用集成式平台的企业不仅能够获得更好的安全保护，而且还能更快地做出响应。

使用集成式平台的企业

- 78% 的企业在过去一年遭遇的泄漏在五次以下。
- 80% 的企业可在八小时内发现威胁。

没有使用集成式平台的企业

- 仅 55% 的企业在过去一年遭遇的泄漏在五次以下。
- 仅 54% 的企业可在八小时内发现威胁。

资料来源：2016 Penn Schoen Berland

此外，Data Exchange Layer (DXL) 通信架构还可以将多个供应商的产品、内部开发的产品，以及开源解决方案整合到一起，优化安全操作。通过将 Cisco pxGrid 和 DXL 相集成，您可以访问来自 50 多种其他安全技术解决方案的任何数据。McAfee ePO 是管理我们功能强大的开放式平台的关键组件。

扩展了对设备的安全保护：管理本地安全工具

可扩展的 McAfee ePO 平台能够管理多种设备，包括设备附带的本机安全控件。McAfee 可增强并协同管理 Microsoft Windows 10 中内置的安全功能，以提供优化的安全保护，同时支持企业充分利用 Microsoft 系统中的本机安全功能。McAfee ePO 软件可管理 McAfee® MVISION Endpoint，后者集成了专门为 Microsoft 操作系统 (OS) 本机安全功能优化了的高级机器学习功能，并且无需任何额外的复杂操作和管理控制台成本。McAfee ePO 软件使用适用于企业异构环境中 Microsoft Windows 10 设备和所有设备的共享策略，可提供通用管理体验，进而确保策略一致性和操作简便性。

通过自动化工作流确保一致性

McAfee ePO 软件提供了灵活的自动化管理功能，您可以通过单一控制台迅速确定、管理和响应安全漏洞、安全态势的变化以及已知威胁。McAfee 于 2018 年委托 MSI 研究开展的一项调查发现，企业期望通过自动执行重复性任务，每天节省大约 25% 的时间。使用 McAfee ePO 软件，您只需单击几个操作步骤即可从单一控制台轻松部署并实施安全策略。在您完成任务，并查看每个步骤以了解步骤之间的相互关联时，这个单一的管理平台视图会提供相关上下文。这有助于降低操作复杂性并最大限度地降低发生错误的可能性。您可以确定 McAfee ePO 控制台应如何根据环境的安全事件类型和严重性以及策略和工具指示发布警告和做出安全响应。为了支持开发运营和安全运营，McAfee ePO 平台可让您在自己的安全和 IT 操作系统之间创建自动化工作流以迅速修复问题。您可以使用 McAfee ePO 控制台来触发 IT 操作系统的补救措施，例如分配更严格的策略。利用其 Web 应用程序编程接口 (API) 减少手动工作。您可以选择在推出全新或更新策略或任务之前设置一个批准流程，以降低错误风险并确保质量控制。

节省时间

MSI 研究于近期完成的 2018 年调查显示，客户认为如果采用集成式安全工具，将会节省多达 20% 的时间。

集成的价值

- 提高工具和流程的效率：61%
- 降低复杂性并减少手动操作，让安全专业人员能够将更多精力放在需要谨慎思考的任务上：61%
- 通过在图形和上下文中显示数据，加强对威胁的监测：58%
- 简化工作流以加速响应：57%

资料来源：2018 年 MSI 研究

常见使用案例

- 通过计划安全合规性报告以满足各个利益相关方的需求，节省时间并消除冗余和劳动密集型工作。
- 利用其强大的应用程序编程接口 (API) 集，将 McAfee ePO 控制台轻松集成到企业已有的业务流程和功能中，以获取更多洞见并加快工作流。例如，它可与票证发放系统、Web 应用程序或自助门户相集成。
- 在借助 McAfee ePO 控制台与 Microsoft Active Directory 的同步将新计算机添加到公司网络时，通过部署代理或机器学习安全解决方案来维持良好的安全态势。

快速缓解和补救

McAfee ePO 平台具有内置的高级安全功能，可提高安全运营人员在缓解威胁或进行更改以恢复合规性时的效率。McAfee ePO 的自动响应功能可根据发生的事件触发相应操作。操作可以是简单的通知或已批准的补救措施。

适用于自动响应的常见使用案例

- 根据预先确定的阈值，通过电子邮件或短信将新威胁、失败的更新或高优先级错误通知管理员
- 根据客户端或威胁事件应用策略，如在主机可能受到感染时阻止外部通信（以拒绝命令和控制活动）的策略，或者是阻止数据泄漏/出站传输，直至管理员重置策略为止
- 标记系统并运行额外的任务以进行补救，如检测到威胁时的按需内存扫描
- 触发注册的可执行文件以运行外部脚本和服务器命令，例如在服务台生成票证或集成到其他业务流程中
- 使用更严格的策略自动隔离工作负载或容器（任何设备）

基于云的安全管理

企业需要简化部署高级威胁解决方案的过程并加快其速度。许多企业正逐渐意识到，基于云的安全管理可消除内部部署基础设施的成本并且免于维护，因而在效率方面具有优势。McAfee ePO 软件可通过以下两种方式随时随地从云端进行部署：将 McAfee ePO 软件部署在 Amazon Web Services (AWS) 中或者 McAfee MVISION ePO 中。这两种部署方式都能在一小时内完成并运行。

- 在 AWS 中部署的 McAfee ePO 软件支持企业利用多项本机 AWS 服务，例如自动扩展和 Amazon RDS，无需购买和管理单独的数据库。这样管理员就能专注于关键安全任务而不是基础设施。在 AWS 中部署的 McAfee ePO 软件可管理 McAfee® Endpoint Security、McAfee® Data Loss Prevention、McAfee® Cloud Workload Security、Data Exchange Layer，以及已集成到 McAfee ePO 软件中的第三方安全解决方案。

> “McAfee ePO 是将安全自动化与协调功能相集成的开创性产品之一。... 当今的安全专业人员需要安全产品既具有传统 ePO 的强大功能，同时还要简单易用，让他们能够既安全高效又务实有效地工作... 作为一款以 SaaS 方式交付的解决方案，MVISION 集分析、策略管理和事件响应功能于一身，能够满足企业和中型市场的需求。”
>
> — IDC 安全产品研究副总裁 Frank Dickinson

- McAfee® MVISION ePO 是以 McAfee ePO 为基础构建的一款软件即服务 (SaaS) 解决方案。它可显著简化平台的管理工作，让管理员能够重点关注关键安全任务。平台更新采用持续交付模式，十分透明。部署代理之后，设备安全功能会在整个企业中自动部署，不需要为每台设备进行手动安装或更新，可确保更强有力地实施安全策略以应对威胁。这让企业能够使用单一控制台从任何位置管理 McAfee MVISION Endpoint 和 Data Exchange Layer。McAfee MVISION ePO 使您的设备能够向安全信息和事件管理 (SIEM) 解决方案提供重要的分析结果，确保分析人员能够轻松访问这些重要信息，以改进威胁追踪和补救工作。

McAfee ePO 管理的 McAfee 产品

McAfee 产品*
McAfee® Endpoint Protection（威胁防护、防火墙、Web 控制）
McAfee MVISION Endpoint 凭借高级威胁防护功能有效弥补了 Windows Defender 的不足
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention (McAfee DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

*适用于内部部署 McAfee ePO

灵活的部署方式

部署方式	主要优势
McAfee ePO 内部部署	完全控制数据和功能集
在 AWS 中部署 McAfee ePO	免除了内部部署解决方案所需的硬件维护
McAfee MVISION ePO ePO 软件即服务*	多租户的 SaaS 产品，无需对基础设施进行维护和升级

*并非所有 ePO 功能在 McAfee MVISION ePO 上都可用

“McAfee ePO 软件和其他解决方案相比更出色。它是我们终端保护的一站式方案。我可以通过一个管理面板查看有关我们所有 McAfee 产品的信息。其简单易用的信息显示板和内置的功能让我们的一切操作都变得更加轻松，包括监测、报告、部署、更新、维护和决策。”

- Computer Sciences Corporation 信息安全工程师 Christopher Sacharok

使用案例：McAfee ePO 控制台如何实现集中式安全管理

产品和技术	使用案例	优势
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO 软件可管理 McAfee MVISION Endpoint，通过高级安全保护功能增强了 Microsoft Windows 10 本机安全控件的功能。您可以通过适用于 Microsoft Windows 和 McAfee Endpoint Security 的通用管理平台和一致的策略，轻松发现并管理高级威胁。	增强了对 Microsoft Windows 本机控件的安全保护，并且经过实践验证可提高管理效率。
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security 可发现终端上已知的恶意文件。McAfee ePO 控制台可在终端上设置更严格的策略来隔离恶意文件。使用一个通用的管理界面即可完成上述操作。	快速遏制受感染的终端
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager 可检测终端上的重大数据泄露事件，并在 McAfee ePO 控制台中进行标记。McAfee ePO 控制台通过应用数据丢失防护策略来阻止数据泄露并告诉用户此操作不合规。	自动实施数据丢失防护策略

集成示例

产品和技术	有关集成的使用案例	优势
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security 会标记可疑主机。McAfee ePO 控制台可触发额外的扫描。这会通过 PxGrid 和 DXL 交换（借助 McAfee ePO 控制台）告知 Cisco ISE。Cisco ISE 可将主机隔离，直至该主机被认为可接受为止。	增加主动保护
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO 会将资产列表共享给 Nexpose。这样您就能从 McAfee ePO 控制台了解危险态势并制定相应的策略。将安全漏洞数据与供应商的 DXL 社区共享。	▪ 降低复杂性 ▪ 通过一个信息显示板获取全面而可靠的安全态势，并将行动划分优先级以便将风险降至最低
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	该集成有助于网络和终端之间的双向和实时情报共享。 同时与 DXL 社区共享安全事件。 Check Point Anti-Bot 软件刀片可阻止命令和控制 (C&C) 流量，并向 McAfee ePO 软件和其他集成的第三方安全解决方案发送关于常见 DXL 问题的警报。McAfee 可根据这一情报自动启动对终端设备的相关补救工作流。Check Point 软件和 McAfee 解决方案还能检测和阻止零日攻击，并将这些攻击转化为已知攻击，无论这些攻击源自网络还是终端均是如此。此集成通过实时交换与任务相关的重要情报，让我们的相关产品能够自动检测、阻止和修复威胁。	▪ 缩短检测时间 ▪ 阻止和修复攻击

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