McAfee ePolicy Orchestrator

激励和助力安全专业人员

安全管理需要在工具和数据之间频繁处理事务，通常对外部威胁的可见性有限。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，从而造成更大损害。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。他们需要变被动为主动，先发制人。

组织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，而高级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™) 管理平台可以在内部部署，也可以在云端部署（有两种模型可供选择：SaaS 或 IaaS）。该平台可以帮助避免耗时的人工操作以及人工操作可能出现的错误。它还可以帮助负责管理安全响应的安全专业人员更快速高效地主动做出响应。McAfee ePO 控制台的独特之处在于 McAfee® MVISION Insights，这是一种首创性的技术，可在威胁入侵之前主动确定威胁和攻击活动的优先级，并预测您的对策是否可以阻止威胁，同时规定如果不能阻止，您需要采取哪些措施。

基本安全

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) 控制和基准，以及美国国家标准与技术研究院 (NIST) SP 800-53 安全与隐私控制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，帮助您设置和自动执行策略，以确保整个企业健康的安全状态。通过单一控制台对整个企业环境进行策略管理和实施安全策略，消除了协调多款产品的操作复杂性。MVISION Insights 扩展提供前瞻性强化建议和能力以及

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
- 前瞻性行动情报，让您先发制人
- 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

行动情报。这一基本的安全管理功能是确保 IT 安全合规的基础。

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的优先级，并在全新的安全保护工作区中用图形化视图向您提供关于整个数据环境的安全态势摘要。此外，凭借 MVISION Insights，您可以独特地获得对组织至关重要的外部预计威胁的前瞻性视图，以及关于您需要采取哪些措施的先占式指导。这可以提高您的端点安全性，变被动为主动，减轻安全管理压力。此外还提供了一个安全资源区域，通过该区域，最新的威胁信息和研究唾手可得。

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 控制台为企业安全管理员简化了策略维护工作。此外，它还可以吸收第三方威胁情报，从而利用我们业界领先的消息传递结构 Data Exchange Layer (DXL)。它也可以将策略与一系列产品双向集成。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。

支持中心让您可以轻松访问有关 McAfee 产品的信息，并提供客户环境中 McAfee ePO 服务器运行状况的概要信息。这在内部部署 McAfee ePO 控制台和 Amazon Web Services (AWS) 上部署的 McAfee ePO 控制台上均有提供。您可以主动接收支持和产品通知，搜索 McAfee 内容存储库，也可以从 McAfee ePO 控制台访问“最佳实践”和“操作指南”资源。您还可以轻松评估健康状况和接收改善健康状况的建议步骤，从而管理 McAfee ePO 基础设施的运行状况。

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

具有集成平台的组织得到更好的保护，并且比没有平台的对手实现更短的响应时间。

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。

（來源：2016 Penn Schoen Berland）

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。超过一半的组织预计，通过集成安全工具可节省 20% 以上的时间（来源：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、应用程序编程接口 (API)、无 API，以及可最大限度减少用户操作的开源 DXL 消息传递结构），让您能够选择最能满足企业需求的方法，而无需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 计划目前有 150 多个集成合作伙伴。

此外，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 控制台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 控制台可管理 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。

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%

（来源：2018 年 MSI 研究）

通过自动化工作流确保一致性

McAfee ePO 控制台提供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，您只需单击几个展开式逻辑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 运营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。

MVISION Insights 开创了独特的前瞻性自动化工作流程。从一般观点来看，通过基于行业和地理位置情报的 MVISION Insights 信息显示板，可以自动警示外部和已知威胁以及攻击活动，并确定其优先级。对于您当前的安全状态是否能够抵御该威胁，这可以提供预测性评估。更重要的是，它提供了具体的操作，如更新 .DAT 或执行隔离。

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。
- 通过利用 MVISION Insights，对于预计的威胁，在您的行业或地区如何跟踪这些威胁，您当前的安全状态是否可以防御这些威胁，以及如果不能，需要采取哪些措施，全部可通过 MVISION Insights 获得前瞻性的行动见解。
- 利用强大的 API 集可将 McAfee ePO 控制台轻松集成到现有的业务流程和功能中，从而获取更多见解并加快工作流。例如，McAfee ePO 可与票证发放系统、Web 应用程序或自助门户集成。
- 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。

> “McAfee ePO [软件]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既需要传统 [McAfee] ePO [软件]的强大功能，也需要简单易用，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等功能于一身，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

快速缓解和修复

McAfee ePO 平台具有内置的先进功能，在安全运营人员缓解威胁或进行更改以恢复合规性时提升效率。McAfee ePO 控制台的自动响应可根据发生的事件触发操作。操作可为简单的通知或得到批准的修复。

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 SMS 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。
- 标记系统并运行额外的任务以进行修复，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 控制台可通过以下两个可选部署选项随时随地从云端进行部署：将 McAfee ePO 软件部署到 AWS 或 McAfee® MVISION ePO™ 上。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 软件支持组织利用多项本机 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、DXL，以及集成到 McAfee ePO 软件的第三方解决方案。
- 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，不需要为每台设备手动安装或更新安全功能，确保更强有力地实施应对威胁的安全策略。这让企业能够使用单一控制台从任何位置管理 McAfee MVISION Endpoint 和 DXL。

> “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。我可以通过单个窗格看到自己需要的一切，查看我们的所有 McAfee 产品。其易用的信息显示板和内置的功能让一切都变得容易许多，包括可见性、报告、部署、更新、维护、决策。”
>
> —Christopher Sacharok，Computer Sciences Corporation 的信息安全工程师

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。此外，现有的本地部署或混合云 McAfee ePO 软件客户现在可以快速轻松地迁移到 MVISION ePO，并充分利用基于 SaaS 的安全管理平台的许多效率和优势。

McAfee ePO 软件管理的 McAfee 产品

McAfee 产品*
McAfee® Endpoint Protection（威胁防护、防火墙、Web 控制）
McAfee® MVISION Endpoint 利用高级威胁防御为 Microsoft Windows Defender 提供补充功能
McAfee® MVISION Mobile
McAfee® MVISION Insights
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)

**适用于内部部署的 McAfee ePO 软件。*

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
AWS 上的 McAfee ePO	免除了内部部署解决方案所需的硬件维护
McAfee® MVISION ePO 软件即服务*	多租户的 SaaS 产品，无需对基础设施进行任何维护和升级

**McAfee MVISION ePO 中并非所有 McAfee ePO 软件功能均可用*

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
MVISION ePO MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO 软件可管理 McAfee MVISION Endpoint，通过高级保护增强了 Microsoft Windows 10 本机控件。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 在终端上发现已知的恶意文件。McAfee ePO 控制台在终端上制定更严格的策略来将其隔离。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 检测终端上明显的数据渗漏并在 McAfee ePO 控制台中进行标记。McAfee ePO 控制台应用数据丢失防护策略来阻止数据并建议用户该数据不合规。	自动实施数据丢失防护策略
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insights	McAfee MVISION Insights 提供关于区分优先级和预计的外部威胁的可行信息。MVISION Insights 转向 McAfee® MVISION EDR 以提供攻击指标 (IoC)，并通过搜索来确定当前调查的环境中是否存在这些威胁。如果存在，则会提供相关攻击活动的详细信息和应对措施。	加快调查和解决速度

集成示例

产品和技术	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 标记可疑的主机。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，直至其看上去可接受。	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态势，并将行动划分优先级以最小化风险
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

2020 年 6 月