

应用 McAfee Host Intrusion Prevention

快速成功部署的最佳实践

目录

摘要	3
引言	
基础须知	5
第一步：策略制定	6
第二步：准备试用环境	10
第三步：安装与初始配置	12
第四步：初始调整	13
第五步（可选）：激活自适应模式	17
第六步：增强防护和高级调整	18
第七步：维护与扩展	19
后续步骤	20
关于 McAfee, Inc.	20

摘要

现在，混合攻击和零日漏洞攻击带来的风险比病毒更高。为保护业务连续性、保持数据机密和减少补丁程序的压力，企业必须通过基于系统的细致保护来增强基于网络的保护。利用正确的试用策略和一些直观调整，可以有效地部署 McAfee® Host Intrusion Prevention（主机 IPS），在不中断业务运营的情况下为此系统提供保护。本文介绍为顺利推进从试用到广泛成功部署 McAfee 主机 IPS，每位管理员所应采取的一系列步骤。本文并非旨在替代《迈克菲安装和产品指南》，而是要介绍整体应用策略以及应用过程中经现场检验的最佳实践。

引言

通过操作主机 IPS，可以降低安装补丁程序的频率和紧迫性，保持业务连续性和员工工作效率，保护数据机密以及支持法规遵从性，从而为您的组织提供更大价值。它结合了签名和行为入侵防护系统 (IPS) 保护与状态防火墙和应用程序拦截功能，可以为所有终端提供保护——台式机、笔记本电脑和服务器——不受已知和未知威胁的攻击。

不过，为了避免中断业务，任何与最终用户和关键业务应用相关的事项都需要谨慎部署。极具风险敏感性的安全技术专业人员将主机 IPS 部署细分为多个可管理的小段，小心地提升防护级别，允许微调策略以支持业务的细微差异，以及实现最终用户变更的最小化。这种慢而稳妥的方法以最少的管理工作提供最大的保护益处，所需时间为一到三个月。

主机 IPS 中的 IPS

主机 IPS 包括三个功能组：IPS、防火墙和应用程序拦截。显然，所有三个功能都会对您有所助益。但是，最好不要同时启动所有这些功能。

建议您从 IPS 功能开始，除非出于法规或风险原因，必须将防火墙作为首要任务。IPS 功能可提供针对已知威胁和零日漏洞威胁的需要普遍应用的关键防护。通过迈克菲预定义的策略设置和及时适当的投资，您可以快速启动主机 IPS，保护您的系统免遭漏洞和攻击。

使用本指南中的策略成功部署和优化 IPS 后，您将能够集中精力、信心倍增地激活防火墙以及启用符合您的系统和业务需求的任意应用程序拦截功能。由于所有三个功能都是单个软件包的组成部分，该软件的这些附加功能都已安装。尽管具体策略、反应响应和规则各有不同，此处介绍的试用策略将适用于防火墙和应用程序拦截部署。

提示：如果您希望从部署防火墙开始，以保护笔记本电脑或支持遵从支付卡行业 (PCI) 法规，则可使用本指南中的策略，但有关定义和激活防火墙策略的详情，请参阅产品手册。

大多数管理员可自行执行这些步骤。如果您需要，迈克菲合作伙伴和服务专家可以为您提供帮助。这些专家对本指南做出了重大贡献。他们遵循相似的流程，因为它可靠地激活了多数企业所需的风险缓解。

现在我们开始吧。

一些简单的阶段

建议遵循以下七个步骤完成试用：

1. 战略和规划
2. 准备环境
3. 安装与配置
4. 初始调整
5. 可选自适应模式
6. 增强防护和高级调整
7. IPS 之外的维护与扩展

桌面机和服务器均遵循相似的部署过程。但是，建议对较复杂和任务关键型高级用户桌面机和服务器实施较保守的保护起始点和阶段定时。有关实施方面的差异，也是基于此思路。

有关定时和期望的说明

对于成功的部署——困难最小，最大程度缓解风险——应用过程为期一到三个月。在此期间，现场操作工作仅需几天，但必须在各阶段之间预留时间，使产品能够收集使用情况数据，作为调整的依据。

实施时间的最大可变因素是系统的范围和您的站点的用户配置文件。用户群越多样，在所有目标系统上实施主机 IPS 所花的时间就越长。您必须在不影响用户工作效率和应用程序功能的情况下激活保护。每个重要的系统和用户配置文件都会从调整和测试中受益。

许多环境都需要 IT 管理人员审批部署、迁移至拦截模式以及使用防火墙。将这些审批所需的额外时间计算在内。

注意：本指南中的所有参考信息都来自《McAfee Host Intrusion Prevention 产品指南》，除非另有说明

IPS 部署的潜在困难严禁事项

建议的最佳实践

1. 在未首先登录以便对情况有所了解的情况下，阻止中等严重性、高严重性签名。	最初仅阻止高严重性签名。此级别可防护最严重的漏洞，但会产生一些错误事件。中等严重性的签名根据行为运行，通常至少需要进行一些调整才能限制支持呼叫。
2. 假定所有系统都将使用相同的策略。	隔离桌面机以反映应用程序和权限。从最简单的系统开始，并为主要组创建标准使用配置文件。在学习过程中逐步添加更多的用户和更多的使用配置文件。
3. 对用户体验进行的测试太少	挑选一些重要的用户组，对致力于提供反馈的代表用户提供试用，测试应用程序是否仍正常运行，然后在经验证策略可以在不影响工作效率的情况下正常使用时进行广泛部署。您希望给用户留下良好的第一印象。
4. 视主机 IPS 为“即设即忘”。	和病毒防护不一样，要保持准确而高效的保护，需要进行定期监控和定期维护。完成部署后，要预先安排时间，至少每周查看一次日志和更新一次规则。
5. 同时启动 IPS、防火墙和应用程序拦截。	从 IPS 开始，然后添加防火墙，并根据需要添加应用程序拦截功能。您将了解如何创建策略，对合适的保护类型更加熟悉，以及能够更轻松地将变更与相应的结果联系起来。
6. 将主机 IPS、防火墙或应用程序拦截功能无限期地保持在自适应模式中。	当您有时间监控创建的规则时，请在短时间内使用自适应模式。
7. 立即阻止系统检测为入侵的所有行为。	请花时间确认您看到的流量确实是恶意的。使用数据包捕获、网络 IPS 或任何您拥有的方式。

基础须知

对 IPS 功能如何保护系统以及基本策略设置和调整概念有一个明晰的了解是成功应用的第一步。

IPS 在主机上是究竟如何运行的？

IPS 功能监控系统和应用程序编程接口 (API) 调用。它还可检查流进或流出系统的流量，并检查应用程序和操作系统的行为。通过结合使用签名和行为防护，它可识别并阻止恶意攻击以及以系统漏洞为目标的攻击行为防护可封闭应用程序，使每个应用程序只可访问自己的资源并防止其他应用程序访问这些资源。有人称此隔离为“行为泡沫”。如果某应用程序通过尝试渗透到其他应用程序的文件、注册表项或内存空间来试图打破其泡沫，IPS 客户端可阻止该操作和/或记录事件。此外，迈克菲获得专利的通用缓冲区溢出防护可防止通过非法内存位置执行代码，这是最常见的服务器攻击之一。

这些类型的 IPS 可一起防止系统受到针对新漏洞的零日漏洞攻击 — 无需进行更新 — 并且在您部署之前为您提供测试补丁程序的时间。

什么是签名和严重性级别？

IPS 使用签名 —— 字符模式和行为模式 —— 识别并防止恶意行为。签名在数据库中按严重性级别分类，反映攻击带来的危险。

- **高** —— 大多数可明确识别的安全威胁或恶意操作的非行为签名，包括充分识别的攻击。在每个系统上设置这些防护规则。
- **中** —— 应用程序在其封装外部运行的行为活动的签名。在关键系统上设置这些防护规则，尤其是 Web 服务器和 SQL Server 上。
- **低** —— 应用程序和系统资源被锁定无法更改的行为活动的签名。设置这些防护规则可提高基础系统的安全，但需要再进行一些微调。
- **信息** —— 应用程序和系统资源已修改的行为活动的签名。更改可能表示良性的安全风险或试图访问敏感系统信息。此级别的事件在正常系统活动期间发生，通常不表示攻击。

McAfee Labs™ 研究人员为特定应用程序和操作系统设计了 IPS 规则，这些签名通过 McAfee ePolicy Orchestrator® (McAfee ePO™) 基础设施分布并保持在 IPS 客户端。自动更新会刷新最新防护内容很多签名保护整个操作系统，但有些签名只保护经常被攻击的应用程序。例如，桌面机 IPS 客户端包含对 Internet Explorer 和 Microsoft Outlook 的目标防护。如果 Internet Explorer 尝试安装后门程序，IPS 将截获并拒绝该应用程序的“写文件”命令。对于服务器，特殊行为签名针对常见 Web 和数据库服务器攻击，如目录遍历和 SQL 注入式攻击。

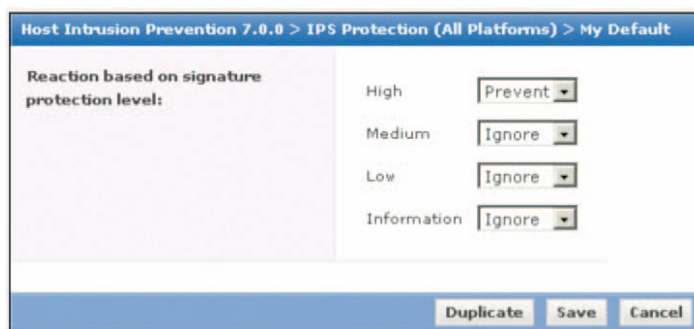
什么是策略和防护级别？

对于每种严重性级别，IPS 策略均定义相应的应对措施：阻止、记录或忽略。每种策略均包含定义行为和选项的规则，用于启用或禁用这些反应规则的应用程序策略按防护级别分组。迈克菲提供预设的基本和高级防护级别，或者您也可以定义自己的防护级别。

预配置的策略包括:

- **基本防护** (迈克菲默认) —— 阻止高严重性级别的签名并忽略其余签名
- **增强防护** —— 阻止中、高严重性级别的签名并忽略其余签名
- **最全面防护** —— 阻止中、低、高严重性级别的签名并记录其余签名
- **准备增强防护** —— 阻止高严重性级别的签名并记录中严重性级别的签名以及忽略其余签名
- **准备最全面的防护** —— 阻止中、高严重性级别的签名, 记录低严重性级别的签名, 以及忽略其余签名
- **警告** —— 记录高严重性级别的签名并忽略其余签名

通过自定义防护, 您可以创建或编辑策略, 使用 ePO 控制台定义您自己的 IPS 防护策略。您可以将任何级别的严重性与**阻止**、**记录**或**忽略**选项相结合, 并根据需要调整规则的严重性。



配置对攻击或可疑行为的响应

例如, 安全策略可能表明, 当客户端识别中严重性级别的签名时, 将记录该签名事件, 并允许操作系统处理此进程, 而当识别高严重性级别的签名时, 将阻止此进程。

多实例策略使您可以将多个设置分组到一个策略伞下, 以满足不同的系统和用户类型的需要。您可以定义每个应用程序的特定策略, 然后将其放在一起以适合各个系统配置。例如, 可以定义两个自定义策略, 一个用于邮件服务器, 另一个用于数据库服务器。然后通过多实例策略, 将这两个策略分配给同时安装 Microsoft Exchange 和 SQL Server 的系统。

第一步: 策略制定

第一阶段的第一步是集中。全面思考您的系统防护策略, 设立切实可行的目标以及制定相符的试用和部署计划。

确定试用的优先级

确保了解您的安全目标并调整试用流程与其相匹配。您可能需要根据学习曲线仔细权衡紧迫性。您可能确定一些要立即阻止的具体问题, 或者允许一般监控期限, 只是为了了解有关客户群中真实情况的详细信息。每个组织都会在防护和工作效率之间实现不同程度的平衡。在一开始就确立明确的优先级可简化整个过程。

思考以下问题：

- 哪些是特定安全隐患区域或标记为审核的最新事件？
- 哪些系统最易受攻击？
- 移动笔记本电脑是不是优先考虑对象？
- 进行控制是否意味着我必须减少关键用户群或系统组中的漏洞？

对于许多客户而言，最大的漏洞莫过于离开受控企业环境的笔记本电脑上的漏洞。这些系统是 IPS 的最佳首要目标。有些客户想加强重要服务器的防护。建议这些关键业务系统以较慢的速度进行试用。写下您的主要目标，接下来的一些步骤将帮助您确定优先级。

概览

在本指南中，我们的重点是 IPS，但也可能有助于了解整个主机 IPS 部署的环境。在下面的例子中，IPS 分阶段部署，并在特定系统类型上充分考虑添加防火墙和应用程序拦截功能。

- 笔记本电脑和标准桌面机上的 IPS
- 关键服务器上的 IPS
- 高级用户桌面机上的 IPS
- 笔记本电脑上的防火墙
- 扩展服务器 IPS 部署（添加防火墙、更多的服务器）
- 为高级用户桌面机添加防火墙
- 研究基本应用程序拦截功能（了解/黑名单）
- 设置防护（执行/白名单）

这只是一个例子。您可以重新排序这些步骤以反映对防火墙更紧急的需求或跳过不相关的步骤。符合您的企业的目标和风险。

定义环境

建议您选择一组小型试用系统来运行测试应用。通过在三个子网上选择不超过 100 个节点，您将能够从最初保守的防护级别逐渐升级。通过步进式扩展，您可以轻松处理出现的任何问题。问题依然存在：哪些计算机？

确定系统类别

区分系统的主要类别并有选择性地包括在您的试用中。从低到高的实施复杂性，IPS 可支持：

- 标准化最终用户桌面机或笔记本电脑，一般群体型最终用户不具有在这些系统上安装或删除应用程序的管理权限。您可以创建多个用户配置文件，每个配置文件具有一个定义的标准应用环境。
- 自定义高级用户桌面机或笔记本电脑，专门用户保留安装其自己的应用程序的管理权限。高级用户通常包括管理员和软件开发人员。有时，管理权限似乎是企业的工件。在理想的情况下，不真正需要管理控制的所有系统都应消除这些权限，以缩小必须归档和调整的系统类型的范围。
- 运行专用数据库、Web、电子邮件或其他应用程序的服务器，以及打印和文件服务器。

实验室还是真实世界？

许多企业在安装新产品以前，必须对其进行实验室测试，这已经成为一种标准步骤。他们构建生产机器的映像（通过公司映像或使用公司软件的全新版本），并在部署之前在受控环境中测试这些映像。

借助 IPS，此方法提供了最快的初始规则基准，但整体效果最差，因为没有考虑到用户变化。测试人员人工模拟用户行为，但不可能捕获合法活动的真实详情。用户和恶意软件始终寻找新的用例，生成不必立即处理的事件，或在无意间作为“正常行为”的例外而避开检测。这两种结果都需要大量时间，并且会产生问题。

根据我们的经验，学习的主要部分在于生产环境中的实时系统。最佳生产测试使用挑选出的机器，而目标用户执行日常任务。由于实际用户确实在操作其系统和应用程序，因此该方法提供最可靠的基准。他们可即时提供对更改防护级别和策略的影响的反馈。但是，这也通常意味着部署速度降低。

对于具有时间和资源的用户，可采用结合这两种模式的折衷方法。实验室测试期间可使您熟悉主机 IPS 的流程和策略，建立信心。测试一些使用配置文件后，这些配置文件可移到生产系统试用中。可能错过了实验室测试的任何活动或应用都可在生产试用中进行测试。此两步过程适合非常保守的企业。

提示：管理员应该能够轻松访问试用系统，他们通常可从初始试用组中消除防护薄弱的办公和家庭用户。

确保合适的用户表示

了解系统类型后，接下来就应该在您的试用中识别用户配置文件和机器。包括最终目标用户群内的多种用户类型。这种广度将帮助您创建反映正常业务需求和使用的规则与策略。例如，在标准化呼叫中心或支持中心，您将拥有管理员、前线支持人员和后备支持。请确保包括至少其中一个使用配置文件，以便 IPS 将遇到并建立可全面使用的策略。

确认您的部署策略

选项 1：“最简单的先行”

对于初始防护的快速实施和高级防护的低压学习曲线，建议仅在标准化桌面机和笔记本电脑上激活基本防护，然后激活登录高级用户桌面机和服务器。

基本防护是 IPS 的默认策略。它将阻止触发高严重性级别签名的活动，不需要进行调整，并且生成少量事件。其设置包括：

- IPS 防护已启用；触发高严重性级别签名的活动被阻止，以及所有其他签名被忽略
- 迈克菲应用程序作为除 IPS 自我防护规则之外的所有规则的可信应用程序列出；作为可信应用程序，它们的运行不产生异常事件
- 防火墙、隔离和应用程序拦截防护未启用

尽管桌面机和笔记本电脑的品牌和型号各不相同，但差别相对较小。丰富的经验使 IPS 可非常准确地解决高严重性级别的问题。例如，在过去的几年里，迈克菲表示，90% 或以上的 Microsoft “补丁日” (Patch Tuesday) 问题使用现有的基本防护级别防范。即使是激活默认防护功能也会产生巨大的直接价值。

我们强烈推荐此“最简单的先行”策略。服务器可能是要防护的最关键系统，但也可能是最棘手的。部署服务器需要更加谨慎，因为必须对 IPS 规则进行调整，以允许合法应用运行，并反映对大多数服务器精心优化性能和系统。测试并找出错误然后进行调整的相关规则可能会对实时的任务关键系统很危险。

同样，高级用户系统往往有一组不同的应用程序和特殊权限，如运行脚本的权限。激活 IPS 可能会产生大量事件，需要仔细检查这些事件才能确保适当的权限或拦截。高级用户和服务器利用额外时间来了解合法使用情况。

监控和记录

在标准桌面机上激活基本防护时，也可在这些计算机上启动中等严重性问题的日志记录。在开始更紧密地锁定控制时，此监控功能将帮助您发现 IPS 将标记的其他事件。在日志记录模式下，可以查看使用量和使用类型，因此您可以真实了解系统行为。建议在这第一阶段进行记录以确保不会出现异常或中断。最好记录事件一个完整的业务周期，至少一个月或一个季度，以查看完整一系列的应用和活动。使用准备增强防护策略来自动完成此操作。此设置将防止高严重性级别并记录中严重性级别的签名，但忽略其余签名。

对于其他系统、服务器和高级用户桌面机，则设置中和高严重性级别的监控与记录。没有同时记录中严重性级别和高严重性级别的默认设置，因此您将需要复制现有策略并对其进行自定义。仅观察中、高严重性级别事件可提供较充分的相关信息，而不会使您陷入大量细节当中。您将发现根据每个特定应用程序实例调整服务器平台时的系统差异，或者开发人员有其喜爱的工具和秘密的编译器时的系统差异。

提示：激活监控和日志记录功能不应影响系统或应用程序操作，但在 IPS 激活后，即使在仅日志模式下，密切监控系统也始终是明智的做法。由于 IPS 通过低级别交互与应用程序和操作系统一起工作，因此总有可能影响一些应用程序的性能。

计划扩展

随着在试用过程中越来越有信心，您可以根据系统类别将签名从记录转为主动实施，在了解哪些活动合法时调整规则和优化策略。我们将在本指南的稍后部分描述此过程。

选项 2：基本防护无处不在

在某些环境下，合法方法是利用默认设置中打包的迈克菲专业技术并在所有系统上部署预先配置的基本防护配置文件。此方法适用于不希望进行大量调整或付出太多精力就能得到 IPS 核心防护的用户。如果 IPS 不是您购买产品的主要原因，则此策略可提供需要最少工作的部署，可以针对大型攻击激活即时防护。

做出决策

选项 1 帮助您从 IPS 投资中获得最大防护益处。选项 2 提供可靠的轻型策略。请根据您的风险状况做出选择。

第二步：准备试用环境

在确定优先级、目标和防护策略后，应检查您的环境是否符合技术先决条件，并在安装前消除任何系统问题。这一前期工作将使您能够集中精力部署 IPS，并避免与 IPS 软件无关的潜在问题。

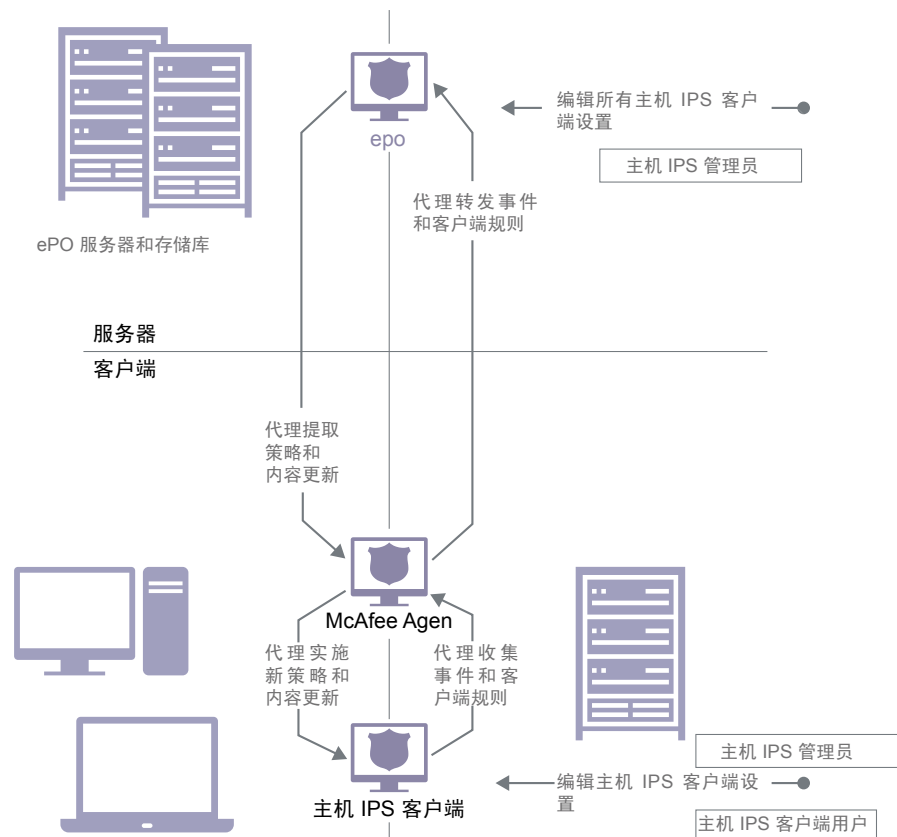
安装/更新 McAfee ePO 软件

在安装 IPS 之前，必须先安装 ePO 服务器，并在目标主机上安装 McAfee Agent。

不仅仅是使用 ePO 软件安装此应用程序，您还需要了解使用 ePO 软件进行策略实施，这样才能成功应用主机 IPS。如果您还不熟悉使用 ePO 软件创建策略，请参阅《McAfee ePolicy Orchestrator 产品指南》获取详细信息。

为何选择 ePO 软件？

主机 IPS 需要 ePO 软件。和迈克菲防病毒系统不同，其自动签名 DAT 更新基础设施意味着 ePO 软件为可选（“即设即忘”模型），主机 IPS 部署依赖特定于组织的策略和规则，这些策略和规则根据业务和用户群的变化而定期调整。为通过这些转型支持明智而高效的策略维护，主机 IPS 利用 ePO 软件成熟的基础设施。使用 ePO 软件可提高策略应用的一致性、减少错误以及增强管理员的可见性和控制。



过程概述：使用 ePO 软件安装和维护 IPS。

- ePO 服务器在每个主机上使用 McAfee Agent 在每个目标系统上安装 IPS 客户端
- 在 ePO 管理控制台内创建并维护 IPS 策略
- ePO 服务器将策略传送至主机系统的代理
- IPS 客户端实施策略并生成事件信息，再将事件信息提供给代理
- 代理将事件信息传输回 ePO 软件
- 在预定间隔或根据需要，ePO 服务器将从迈克菲存储库提取内容以及更新功能，然后代理从服务器中提取它们以更新 IPS 客户端
- 随着策略更改，代理将提取这些信息以更新 IPS 客户端

使用 ePO 软件设置使用配置文件和客户端

对于每种不同的使用类型 —— Web 服务器、笔记本电脑、自助服务终端 —— 应创建不同的 ePO 使用配置文件。最终，您将这些配置文件与特定 IPS 策略关联，并且在您需要管理异常时提前准备好配置文件很有用。

提示：ePO 软件允许对系统进行逻辑标记。标记是可手动或自动应用于一个或多个系统的标签。根据标记将系统分类为试用组，并将标记用于报告标准。

以逻辑方式分组客户端。可根据适合 ePO 系统树层次结构的任何标准对客户端进行分组。例如，可以按地理位置分组第一层，按操作系统平台或 IP 地址分组第二层。建议您按照主机 IPS 配置标准来分组系统，包括系统类型（服务器或桌面机）、关键应用程序（Web、数据库或邮件服务器）以及具有战略意义的位置（DMZ 或内部网）。

命名规则很重要。理想情况下，应建立任何人都可以解释的简单命名规则。客户端是由系统树、某些报告和客户端上活动生成的事件数据中的名称来识别。

检查试用系统的运行状况

现在您已标识客户端，请确保没有会中断部署的先前系统问题。检查 ePO 服务器的相关日志文件和系统事件日志。查看表示配置不正确的错误或故障以及可能影响成功安装主机 IPS 的系统异常。必须在安装主机 IPS 之前补救错误。要查找的一些重要因素：

- **补丁等级** —— 是否所有驱动程序和应用程序都是最新的？大家都知道，较旧的介质和音频播放器、Internet Explorer 以及网卡驱动程序会产生中止安装的不一致性。请应用最新的补丁程序和修补程序。
- **不兼容的软件** —— 主机上是否正在运行其他入侵检测或防火墙应用程序？您需要禁用或删除它们。
- **管理访问权限** —— 您必须具有对系统的管理访问权限。还需注意用户是否拥有管理访问权限。原因何在？用户在测试期间安装新应用程序时可能会删除测试流程，因此您应该注意这些权限。如果无法消除最终用户的管理访问权限，则考虑作为高级用户将此系统置于其他使用配置文件中。
- **组织注意事项** —— 有些计算机扩大应用程序、使用其他语言、特定于位置的应用程序和本土应用程序，因此需特别加以注意。考虑阻止这些系统直到部署的第二阶段，或从 IPS 防护中排除这些专用应用程序，直到您有时间记录并分析其行为。（请参阅下一部分的可选基本策略配置。）

第三步：安装与初始配置

您已计划完毕，并已准备就绪。最后，是部署的时候了。

在 ePO 服务器上安装主机 IPS 管理软件并将主机 IPS 客户端软件导入 ePO 存储库

在 ePO 服务器系统上，安装主机 IPS 管理组件，该组件为 ePO 控制台中的主机 IPS 策略管理提供接口。将主机 IPS 客户端导入服务器上的 ePO 存储库。

记住在迈克菲服务门户上查看任何补丁程序或知识库文章，网址为：<https://mysupport.mcafee.com/Eservice/Default.aspx>。从 <http://www.mcafee.com/us/downloads/> 下载更新内容。有关详细信息，请参阅《*McAfee Host Intrusion Prevention 安装指南*》。

设置初始防护级别和响应

您早期对策略和使用配置文件的投入现在派上了用场。通过定义防护级别或将防护级别与每个使用配置文件相关联来实施策略。如果您遵循“最简单的先行”策略，您将激活标准桌面使用配置文件的基本防护。

有关说明，请参阅使用 *IPS 防护策略*。

优化基准策略（可选）

有些管理员在开始部署前会立即调整防护默认值。您可以选择自动防护高风险应用程序（那些作为服务或面向网络的开放式端口启动的应用程序）和本土应用程序。内部开发的应用程序通常在开始部署时从 IPS 中排除，在侦听网络连接时尤其如此。内部软件开发人员可能不像商业开发人员那样对预期编程和安全行为要求严格。例如，链接至 *Internet Explorer* 的程序在发生错误行为时，可能会无意中触发 *Internet Explorer* 防护签名。由于内部开发的应用程序不是典型的攻击目标，黑客看不到也不知道它的存在，因此它们的漏洞风险较低。

考虑在您的可信网络列表中添加漏洞扫描程序的 IP 地址。您的现有 ePO 平台和安全策略可能会提供有关拦截或允许各个使用配置文件的额外指导。最后，您可以使用自适应模式，有选择性地定义适用于被排除应用程序和实施防护的规则。在您建立基本防护并熟悉 IPS 签名和策略后，可执行此步骤。

有关详细信息，请参阅 *策略管理*。

通知最终用户并计划安全窗口

在激活 IPS 前，通知用户他们将收到新的防护措施，并且在某些情况下提供安全窗口。这一沟通方式将降低对最终用户工作效率的感知风险，对于在出行途中携带笔记本电脑的用户来说尤其重要。在试用过程中，用户可通过三种方式改写 IPS 拦截。管理员可：

- 生成限时密码
- 委派给最终用户禁用模块的特定能力
- 必要时，允许最终用户完全删除主机 IPS

您不能太随意地分发这些资源：您不希望用户破坏部署。其中两个门将在试用的后期关闭。请参阅使用客户端 *UI 策略*。

取得支持中心团队的支持

让您的支持中心了解您即将激活主机 IPS。只要有问题，就应该时刻准备识别问题。您最终可能会证明主机 IPS 在某种情形下是安全的，但这才是安全软件管理的正常环境。

安装主机 IPS 以试用主机

从小处开始，仅安装几个客户端，然后随着把握性越来越大，以较大的增量逐渐扩展至更多系统。从 1 开始，然后 10、20、50 直到 100 个系统。下面是部署顺序：

1. 确保目标主机已开机、联网并与 ePO 软件通信
2. 通过 ePO 部署任务，将主机 IPS 代理推向试用组中的一小组主机
3. 验证安装是否成功：根据需要进行故障排除和调整
4. 扩展到更多系统

在安装过程中，检查用于正确操作新软件的试用系统并监控服务器事件和对网络性能产生任何重大影响 ePO 日志。可能会出现几个问题：这正是试用和逐步部署为何至关重要的原因。

1. 检查主机 IPS 服务和框架服务是否已启动
2. 关键 — 运行简单应用程序，例如会计、文档编辑、电子邮件、Internet 访问、多媒体或开发工具，测试其是否正常运行。您的用户是否可执行其标准工作？您希望证明并验证正确的操作检测。
3. 如果您在客户端发现问题，可以检查 IPS 客户端日志和客户端操作系统日志，查看是否有错误。请参阅使用主机入侵防护客户端。

重复以上步骤以扩展到更多系统，直到植入试用组。

提示：请记住测试每次安装或策略更改，确保最终用户能够成功执行他们的工作。此测试可能是在确保成功部署方面最有价值的活动。

第四步：初始调整

随着试用组的不间断运行，您现在可以稍候并观察一段时间。预留两天到一周的时间累积事件，但不要忽视试用。回应所有支持呼叫。

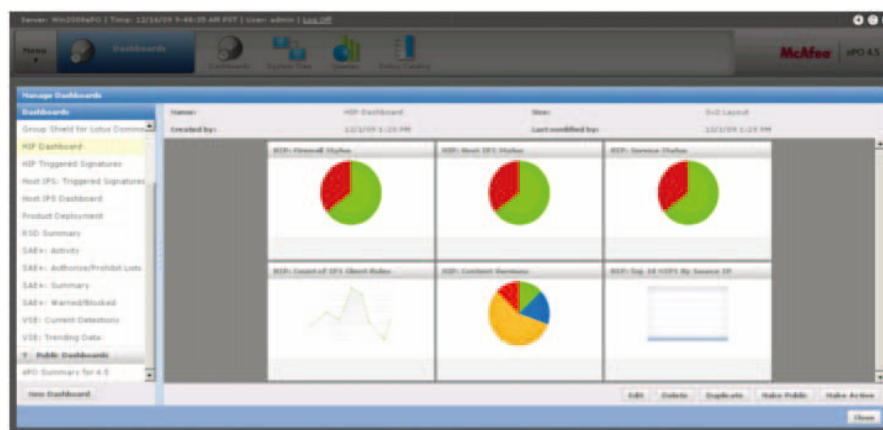
每日监控

管理员务必明白，IPS 不同于病毒防护或在他们自主管理威胁时安装但通常被忽略的设备。在一开始，每天花数分钟查看 IPS 事件日志并监控活动量和类型。这种习惯可帮助您获得正常操作级别和活动模式的基准。例如，在每日监控中，您应注意服务器维护 and 应用程序更新的定期进程和活动级别。了解基本活动后，您就可以立即识别出现的任何异常活动。

最终，您的每日检查将包括在出现新事件时优化规则、策略和异常。主机 IPS 提供精确控制，因为其可以监控所有系统和 API 呼叫，并阻止可能导致恶意活动的呼叫。类似于网络 IPS 系统，随着应用、业务和策略要求的更改，有时也会需要进一步调整规则。

提示：人们在扫描日志时，对于重复操作和可能导致不同规则决策的遗漏细节会感到麻木倦怠。在全面检查期间，可偶尔中断并重新开始。

主机 IPS 部署的持续维护包括监控、分析、对活动做出响应、更改和更新策略以及执行系统任务，例如设置用户权限、服务器任务、通知和内容更新。需要在操作级别上对这些活动进行预估，以保持 IPS 功能的运行状态和效率。



使用 ePO 信息显示板监控事件和趋势。

几天之后，查看日志

不断累积的事件日志将帮助您优化策略，以便在自由访问信息和应用程序和安全防护之间取得平衡。这种平衡对于每个用户类型来说通常都是不同的。在此阶段，您将通过 ePO 软件手动调整策略。稍后，我们将讨论使用自适应模式自动生成策略。

首先分析日志。在 ePO 软件中，查看“报告”下“主机 IPS”选项卡中的“事件”选项卡。您可以深入分析事件的详情，例如触发事件的进程、生成事件的时间以及生成事件的客户端。您正在查找红色标记，例如具有欺骗性的误报率或高严重性级别的触发签名。

检查进程和服务是否正确无误。您期望运行的应用程序应正在运行，而您不希望看到的应用程序则不应出现。如果您发现根据合法活动记录的事件（这对于内部开发的应用程序来说最常见），这些误报率将在下一步得到解决。

提示：通常，生成或阻止事件对于最终用户或应用程序的操作无明显影响。例如，VMware 封装和 Adobe 应用程序经常会出现这种行为。如果您能确认用户体验没有变化，则忽视这些事件是安全的。您可以关闭漏洞，例如有可能以其他方式被攻击的跨站点脚本漏洞。

开始调整以加强防护并实现合法业务运营

对于上面所列的触发事件，您现在应当：

- 提升对应当拦截的已记录事件的防护
- 消除基于合法业务活动的误报率

应告知客户以下列三种方式之一做出反应：

- **忽略** —— 无反应；事件未被记录，并且进程未被阻止。
- **记录** —— 事件被记录，但进程未被阻止。
- **阻止** —— 事件被记录，且进程被阻止。

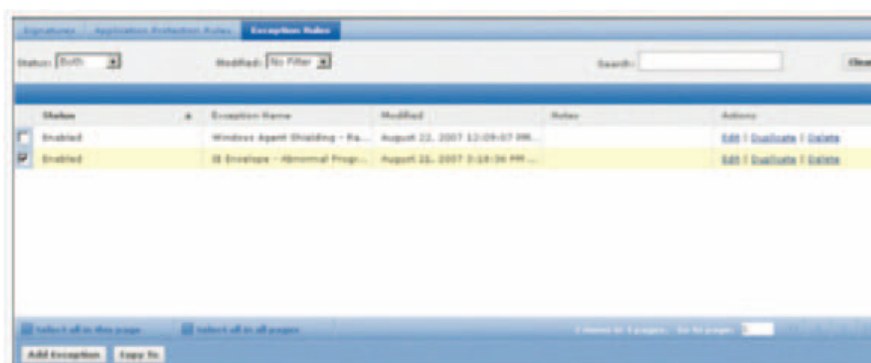
提示：保持浏览器窗口或选项卡对 ePO 控制台的 IPS “事件” 部分开放，并使用单独的窗口管理 IPS 产品。当您来回跳转时，不会在系统树或策略中失去定位。

调整反应规则

首先，对于那些在登录模式下监控的系统，应该调用对任何 1 级严重性签名的防护模式。

创建异常

其次，识别标记应该允许或可能允许并已记录的合法行为的事件。您可以通过创建异常规则和可信应用程序，或通过简单调整反应响应来降低这些误报率。



编辑异常规则以管理行为。

创建异常规则以在特定环境中覆盖安全策略。您可以设置忽略的反应响应，将不再记录事件。例如，尽管某个策略可能认为某些脚本处理为非法行为，但是您的工程组中的一些系统需要运行脚本。为工程系统创建异常，使其在策略继续阻止其他系统上的脚本时可正常运行。使这些异常成为服务器要求策略的组成部分，以仅涵盖工程。

异常使您能够降低误报警报，并最大限度地减少不必要和不相关的数据流入控制台。通过降低干扰，您将更轻松地识别每日监控中的重要事件。

提示：使异常足以通用，可在相同或相似环境下的所有类似系统中使用。

创建可信应用程序

可信应用程序是始终可访问的应用程序进程。可信应用程序因使用配置文件不同而不同。公司某些领域的正常业务可能需要某些软件应用程序，而在其他领域则不需要。例如，您可能在技术支持部门允许即时消息，但阻止其用于金融部门。您可能在允许使用的技术支持部门的系统上建立可信应用程序。有关详细信息，请参阅产品指南中的配置可信应用程序策略。

使用查询获取有关特定项目的数据并过滤该数据特定子集中的数据：例如，指定时间段内由特定客户端报告的高级事件。查找最常触发的签名。是否应允许这些日常合法业务功能？将这些签名的严重性级别调整为较低的级别。有些桌面机异常证明是合法应用程序的错误行为，您无需允许这些行为。验证用户应用程序功能是否正确并继续拦截。

最后，定性因素：您是否收到任何用户投诉？您应直接与用户交谈，以验证他们的应用程序是否正常运行。

在试用期间进行调整决策时，您应遵循以下过程：

- **编辑策略** —— 使用 ePO 软件编辑并创建策略和反应
- **选择性地应用规则** —— 使用 ePO 软件将规则应用到目标系统（非自动）
- **激活更改** —— 在 ePO 控制台中更改主机 IPS 策略时，这些更改会在下一个代理服务器通信时对受管理的系统生效。默认情况下，此间隔为每 60 分钟一次。要立即实施策略，您可以通过 ePO 控制台发送代理定时
- **测试更改** —— 重新验证这些更改是否成功应用，包括与业务系统的兼容性（允许合法活动）。确保 IPS 网络流量已最小化并且您正在降低目标的误报率
- **更广泛地应用规则** —— 如果新规则奏效，则在相关系统中应用
- **继续每日监控**

请参阅使用 *IPS 规则策略*、*处理 IPS 异常*和*管理 IPS 事件*了解有关策略调整的特定说明。

配置信息显示板和报告

现在您的事件已进行得更加有序而准确，您可以使用 ePO 软件改善企业和 IPS 信息通信。

- 如果您正在使用 ePO v4 软件，则配置 ePO 信息显示板以快速了解持续策略遵从性、事件趋势、查询结果和问题。保存唯一的信息显示板以反映每日监控、每周检查以及任何管理报告。
- 配置通知，在发生特定事件时对特定个人发出警报。例如，在特定服务器上触发高严重性的事件时可发送通知。
- 安排报告自动运行并作为电子邮件发送至相关方

有关详细信息，请参阅*管理主机 IPS 事件的信息和通知*。

等待并观察

每隔两周或更长时间监控每日事件，检查支持中心电话、异常和误报率。通过相对保守的部署策略，应该不会有太多支持电话或问题，因此不需要进行重大调整。

禁用安全窗口

禁用以下解决办法。此步骤有助于防止用户和恶意软件避开 PS 防护。

- 委派给最终用户禁用模块的特定能力
- 必要时，允许最终用户完全删除主机 IPS

第五步（可选）：激活自适应模式

与此同时，您的较复杂的自定义系统可能处于*日志模式*。一旦您完成了一个日志记录业务周期，即可开始实施有针对性的规则，为这些系统创建自定义策略集。这些策略可手动定义，但*自适应模式*为创建基于主机活动的*IPS*规则提供了功能强大的工具，无需管理员操作。当使用应用程序时，将创建规则以允许进行各种操作。自适应模式不触发*IPS*事件，也不拦截活动，恶意攻击（高严重性的签名）除外。然而触发规则的异常将由*ePO*软件记录为*IPS*客户端规则，因此您可以监控进程。通过在试用期间在自适应模式下设置代表主机，您可以为每个使用配置文件或应用程序创建调整配置。然后通过*IPS*，您可以采用任意、全部或不采用客户端规则并将其转换为服务器授权的策略。完成调整后，关闭自适应模式以增强系统的入侵防护。（除了自适应模式，防火墙和应用程序拦截功能还具有记忆模式，在实施前需要管理员或最终用户审核规则。）

日志记录模式帮助您了解活动的频率。相应地，自适应模式告知您活动的完整范围和类型。一起使用这两个工具可为贵公司的合法商业活动提供良好的功能基准。然而，您应当预期到，在试用周期中不会捕获不正常活动，因此时刻准备不时查看异常和手动创建规则。例如，某用户可能每四个月运行一次本土应用程序，并遗漏日志记录模式和自适应模式周期。

请注意，自适应模式在默认情况下拦截所有高严重性警报。如果您仅监控到这一点，请警惕此新的实施影响系统行为，特别是影响本土应用程序。

使用自适应模式管理中、高严重性的签名。该组合为您提供良好的活动概述，无过多干扰。

自适应模式创建异常规则效率很高。然而，给定系统上不可能允许所有活动，否则您不会考虑新的防护措施。出于这个原因，您应在有限的时间内使用自适应模式，必须密切查看创建的各个规则（每个规则只有一个实例），并且必须停用自适应模式创建的不可接受的规则。

当您激活自适应模式时，选择策略选项以保留客户端规则。否则，新规则将在各个策略执行间隔被删除，并将需要重新学习。最终，当您选择关闭自适应模式并转至实施时，您将需要关闭保留客户端规则并消除不是由*ePO*提供的策略声明的所有规则。

顺序应为：

1. 在特定时期激活自适应模式（至少一周，至多 30 天）
2. 评估异常和自适应规则
3. 停用不适当的规则
4. 在*IPS*客户端规则选项卡上，直接将合法规则迁移到其他客户端的应用程序策略
5. 停用自适应模式
6. 关闭保留客户端规则（如果设置了此选项）

重要须知：自适应模式允许合法活动和不适当的活动。将创建接受这些活动的规则，无需管理员审批。每个创建的规则只能记录一个异常事件，因此在创建规则之后无法记录相同的活动。您只能收到一份通知，因此必须坚持查看并做出响应，以阻止不可接受的规则。

自适应模式的最佳实践

为了得到最全面的防护，必须预先确保从未覆盖某些签名。仅编辑这些签名的规则以禁用允许客户端规则选项。

- 在自适应模式或记忆模式下运行客户端至少一周，以遇到所有正常活动。选择计划活动次数，例如备份或脚本处理。
- 和日志记录一样，您可以在 ePO 控制台中跟踪客户端异常，在常规视图、筛选视图和聚合视图中查看这些异常
- 对每个异常使用自动创建的规则以定义更加详细的新策略，或在现有策略中添加新规则，然后对其他客户端应用更新的策略。
- 当您启用自适应模式时，选择策略选项以保留客户端规则。如果不启用，将在每个策略实施间隔后删除规则。
- 使用自适应模式一段时间，在此期间，您可以查看异常和创建的规则。如果无法查看规则，则停用自适应模式以避免允许有风险的活动。
- 当您需要为新应用程序创建规则时，自适应模式很有用。短暂启动自适应模式以执行该应用程序，然后推广合适的规则。

提示：请记得要停用自适应模式，这样就不会在您不知情的情况下创建规则。

请参阅使用 *IPS 策略* 或联系迈克菲合作伙伴或服务专家，获取有关微调策略和使用自适应模式的详细帮助。

第六步：增强防护和高级调整

至此您已建立并调整基本活动响应，可以开始提高防护和实施等级。可以在日常监控环境中执行这些调整步骤，也可选择重复试用的正式迭代步骤。执行每个步骤之后，先至少等待两周再考虑做出其他更改。这段时间可确保系统在其现有级别的防护下正常运行。

通过准备增强防护将标准化桌面机从基本防护迁移至增强防护

增强的防护级别将阻止中、高严重性级别的签名并忽略其余签名。通过使用准备增强防护，可先采取记录中等严重性级别的中间步骤。正如我们讨论服务器和高级用户桌面机一样，日志记录提供在您提升防护级别时将受影响的活动的详细信息，引导准确的策略管理并限制异常。

当您对业务将继续而不中断感到满意时，移动设置以增强防护。对网络中的其他系统重复此循环。最全面的防护适合大多数专用和增强操作环境。由于最全面的防护甚至会拦截低严重性级别的签名，因此应在全面测试后明智部署。重申一下，可使用准备最全面的防护作为在激活最全面防护之前发现变更影响的试验场。

极其保守的企业可以在防护级别将每个更改部署为自己的试用，按照我们讨论过的迭代步骤操作。请记住在验证更改的测试周期前后启用或禁用安全窗口和自适应模式。

继续调整

查看异常和出现的所有问题。按照初始调整步骤中所讨论的管理这些问题。

- 监控服务台电话和用户对由拦截的访问、误报率或新应用程序活动引发的任何投诉或业务问题的意见。这些问题应最大程度地减少，但是总会有新的要求。
- 定期检查生成的异常
- 相应调整策略。请记住使用 ePO 软件向主机系统发送策略更新。您要有意识地将其应用到您希望影响的系统。

第七步：维护与扩展

上述步骤概述了基本部署过程。如果您的系统部署了中等防护级别，则已拥有高级系统防护。您可能需要继续定期监控、更新策略和维护系统。当前，还应考虑扩展受保护的系统并增强防护以包括更严格的策略和其他主机 IPS 功能。

维护

迈克菲经常发布新签名的内容更新，偶尔发布功能更新和补丁程序。最佳实践建议包括：

- 制定定期更新计划，以便 ePO 软件对迈克菲存储库中的更新进行轮询，并且您的客户端收到这些更新。
- 如果您在初始部署期间发现大量的自定义应用程序需要调整，则可能希望提取主机 IPS 内容到存储库的评估分支机构，根据系统的试用组进行测试。在您的试用组认证新的内容之后，可将其迁移到当前分支机构，进行全面部署。
- 如果您正在使用 Microsoft 产品，可在补丁日发布时，同时排定下载内容。
- 新的应用程序在某些计算机上可能需要定期安装，而您可能没有时间或资源立即对其进行调整。对配置文件特定的计算机使用自适应模式，并向服务器转发产生的客户端规则。您可以向现有或新的策略推广这些客户端规则，然后对其他计算机应用策略以便处理新软件。
- 在您的变更管理和软件发布流程中插入 IPS 测试。当您准备部署 Microsoft 补丁、Service Pack 或产品时，在 IPS 系统上测试并试用，以便在批量部署前可以进行合适的调整。

通常，当新应用程序、用户或使用配置文件出现时，最好在少数几台计算机上执行小型试用以定义并测试策略，然后更广泛地部署这些增强功能。

扩展

根据贵公司的具体情况，考虑以下任一选项扩展您的部署。请记住继续认真而稳妥地部署更改，以便最大限度地减少用户中断，并快速诊断异常。缓慢变更胜过出错或遗漏实用防护选项按此顺序，您可以：

- 使用测试的使用配置文件向其他系统部署相同的防护。您可以轻松管理对数以千计的计算机部署主机 IPS，因为大多数计算机适应几个使用配置文件。管理大规模部署减为维护少数策略规则
- 如果您只试用标准化桌面机，则对高级用户和服务器重复该流程，从日志记录开始并充分利用自适应模式

- 添加新的使用配置文件和用户群
- 实施防火墙规则，然后按此顺序考虑应用程序拦截。遵循试用流程，但参阅产品指南获取有关规则和记忆模式的详细信息。
 - » 防火墙是分层安全产品至关重要的组成部分。它对系统拦截所有未经请求的流量，从而显著降低远程攻击的机会。笔记本电脑应优先部署防火墙。
 - » 部署应用程序拦截通常极具选择性，但其有助于进行基本了解，即使您认为不需要。如果出于隐私或法规原因，您必须立即拦截一个特定威胁或应用程序，应用程序拦截是一个关键工具。

后续步骤

本指南提供成功应用主机 IPS 的产品发布计划。通过认真周密地应用 IPS 功能和调整策略，管理员能够以最少的返工部署 IPS，不会使自己或其用户有挫败感。请参阅安装和产品指南获取详细信息，并通过从迈克菲服务门户和下载网站的下载内容，确保得到最及时的防护。如果您希望获得实际帮助，请联系迈克菲合作伙伴或服务专家。

关于 McAfee, Inc.

迈克菲公司 (McAfee, Inc.) 总部位于美国加利福尼亚州的圣克拉拉市，是全球最大的专注于安全技术公司。致力于解决安全领域最艰巨的挑战。迈克菲所提供的具有前瞻性且经实践验证的解决方案和服务，为全球范围内的系统和网络提供安全保护，同时使用户能够安全地在网上冲浪和购物。依靠屡获殊荣的研究团队，迈克菲为家庭用户、企业、公共机构和服务提供商开发了创新的产品，让他们能够实现法规遵从，保护数据、预防网络中断、识别安全漏洞，并持续监测和改善他们的安全状况。<http://www.mcafee.com/cn>

迈克菲(上海)软件有限公司

北京市朝阳区外大街 16 号中国人寿大厦 1709 室	邮编: 100020	电话: (8610) 85722000	传真: (8610) 85752299
上海市卢湾区湖滨路 222 号 1 号楼企业天地 1101 室	邮编: 200021	电话: (8621) 23080699	传真: (8621) 63406606
广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室	邮编: 510620	电话: (8620) 38860668	传真: (8620) 38860638

迈克菲销售热线: 800-810-0369 www.mcafee.com/cn

