

# 迈克菲恶意软件防护引擎： 价值与技术

迈克菲实验室 (McAfee Labs™) Christoph Alme 和 Declan Eardly

## 目录

<b>终端和网关协作型恶意软件防护</b> .....	<b>3</b>
终端恶意软件防护的价值 .....	5
网络网关恶意软件防护的价值 .....	6
<b>恶意软件检测基础</b> .....	<b>7</b>
准确检测与识别 .....	7
常规检测 .....	7
启发式检测 .....	8
<b>目前先进的恶意软件检测技术</b> .....	<b>9</b>
自动化智能感知 .....	9
降低风险 .....	10
防止误报 .....	10
代码安全 .....	10
基于云的检测 .....	10
模拟 .....	11
脱壳 .....	12
统计分类 .....	13
模糊指纹技术 .....	13
常规漏洞攻击检测 .....	14
行为分析 .....	15
<b>ProActive：基于行为的网关恶意软件防护插件</b> .....	<b>15</b>
ProActive 技术的作用 .....	17
<b>作者简介</b> .....	<b>21</b>
<b>参考文献</b> .....	<b>21</b>

本文档所提供的信息仅用于培训目的和为迈克菲用户提供便利。本文档包含的信息如有更改，恕不另行通知。这些信息按“现状”提供，对其准确性或这些信息对任何特定情况的适用性不做任何保证。

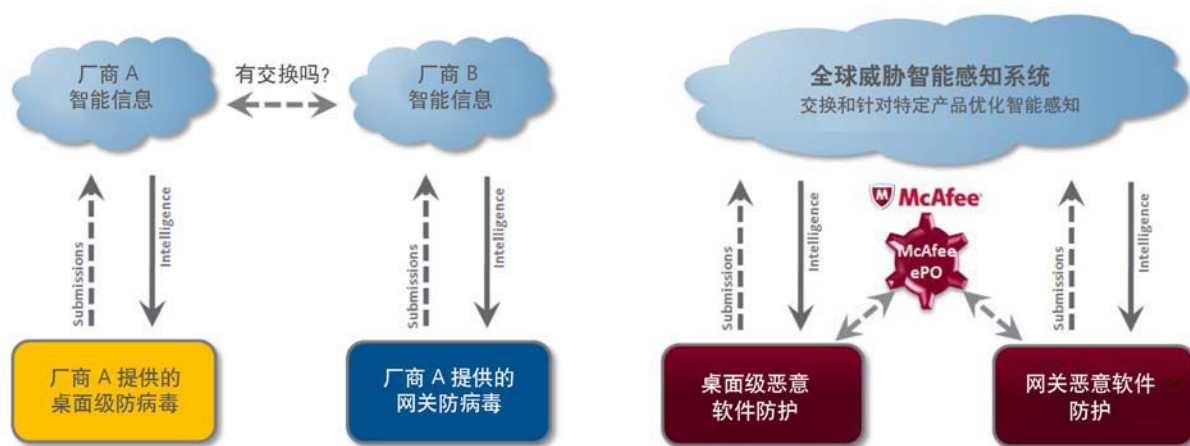
McAfee、McAfee 徽标、ePolicy Orchestrator 和 McAfee ePO 是 McAfee, Inc. 或其分支机构在美国及其他国家/地区的注册商标或商标。所有其他名称和品牌可能是其他公司的财产。版权所有 © 2010 McAfee, Inc.

## 终端和网关协作型恶意软件防护

在本报告中，我们将介绍迈克菲恶意软件防护引擎的核心技术、价值、ProActive 行为检测技术以及不同的引擎类型 — 终端恶意软件防护引擎和网关恶意软件防护引擎 — 如何结合成为专为企业优化的恶意软件防护架构。

市场出售的运行另一种防病毒引擎的基本网关在桌面系统中运行时，只可提供冗余的防病毒功能，但不具有上述网关恶意软件防护价值。防病毒软件厂商显然必须在其产品中实现类似的目的。厂商通常利用类似的技术（即使不是相同的技术）来解决相同的问题和实现相同的目的。因此，结合使用两种防病毒引擎除了运行两次相同或类似的技术外，很少能取得什么效果。这或许可以提供一些故障转移冗余，但无法提供更多价值，尤其是无法提供深层次防护。如 Gartner 发布的报告所述“对比基于签名的恶意软件防护引擎，在功效方面仅仅只有 2% 到 10% 的差异。因此，从基于签名的检测引擎转为使用另一种引擎仍然会留下防护缺口。” [1]

事实上，您通常会发现使用这一传统方法误报率上升了一倍。如果在一个设备（例如，网关）上混合使用两种类似的防病毒引擎，您还会发现内存的占用量提高了一倍，而性能则下降了。那么，让我们深入研究一下基于用户行为特征优化技术的协议遵从型恶意软件防护新方法如何真正提供更大价值。



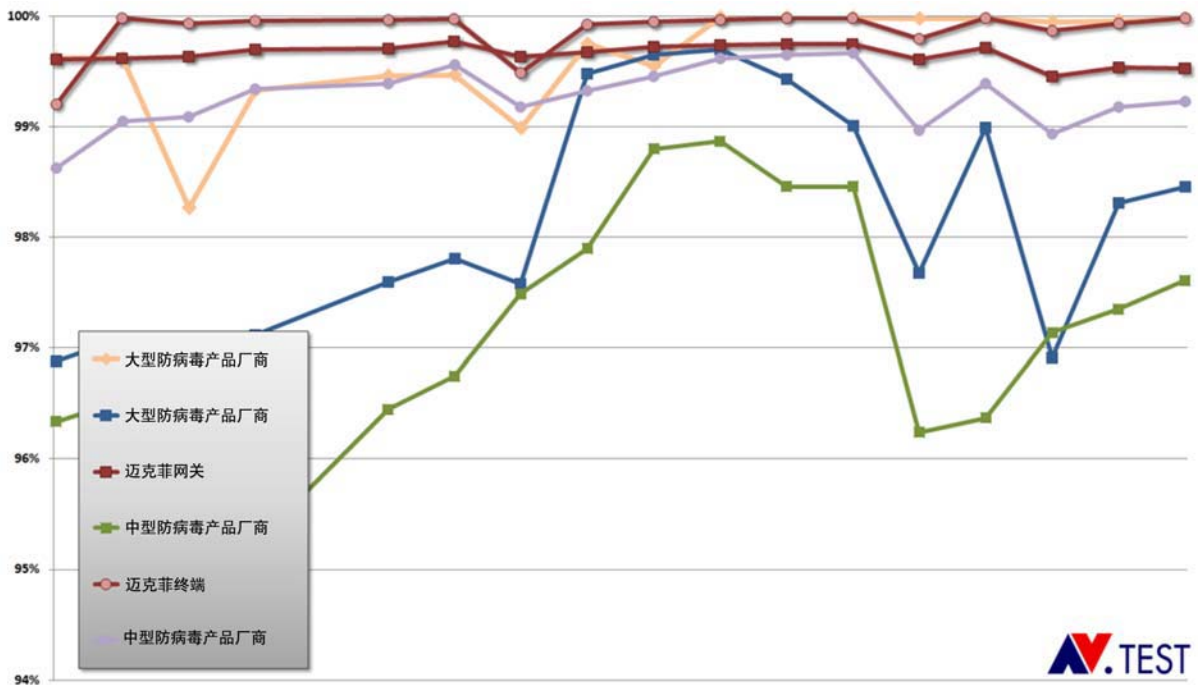
**双厂商设备安全防护：**这是智能感知的“黑洞”。从桌面防护中发现的可疑问题可能无法提高网关产品的检测效率，反之亦然。

**单厂商终端节点技术：**集成带来一流技术。在网络一端发现的可疑问题将有助于完善另一端的防护。

迈克菲网关恶意软件防护引擎利用独有的技术为网关提供了所需的更大价值：ProActive 基于协议规范，行为的恶意软件防护插件和 Artemis 基于云的防护。这些技术可帮助您的网络拦截绝大多数恶意软件。这种方法最大限度地降低了性能成本和管理成本，并且能在大多数威胁入侵

终端前在网络外围拦截它们。现在，我们一起来了解一下检测效率。

作为恶意软件防护测试标准组织 (AMTSO) 的创始成员，迈克菲一直致力于独立、公正地开展恶意软件防护测试。迈克菲终端和网关恶意软件防护引擎定期参加由 AV-Test GmbH 举办的测试，这是一个从德国马格德堡大学独立出来的全球知名病毒测试机构而且，享有声誉的 VirusTotal.com 网站也采用了我们的恶意软件防护引擎（两种）— 提供的免费 Web 服务被《PC World》杂志评为最佳“安全网站”产品之一。在 AV-Test 2009 年和 2010 年进行的迈克菲终端、网关恶意软件防护引擎与竞争对手引擎检测率对比测试中，迈克菲的引擎不仅在检测率方面全面领先，而且测试出的检测率非常一致，波动很小。对于任何企业而言，如果恶意软件防护引擎能够在数月和数年的时间稳定地保持高检测率，都将具有非常大的价值。

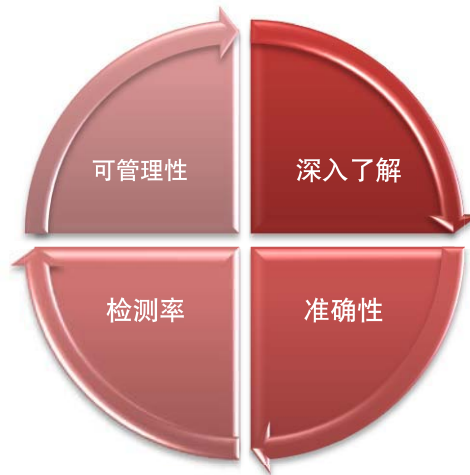


2009-2010 年大型厂商的检测率测试结果。数据由 AV-Test.org 提供。

通过结合使用终端和网关恶意软件防护技术，企业能够在网络外围严格执行安全策略，最大限度地提高主动捕获率，从而拦截大多数威胁，有效地为桌面系统提供帮助。我们将在后面的几章详细介绍所采用的引擎技术。

## 终端恶意软件防护的价值

当前，所有企业都必须在终端节点上运行恶意软件防护，这显然对恶意软件防护具有非常重要的价值。本章，我们将着重介绍在桌面环境运行恶意软件防护引擎的价值。



### 深入了解

如果运行在终端上，恶意软件防护引擎能够准确检测出威胁。它可以“现场”发现受保护系统中所有潜在的攻击媒介——来自网络（邮件、Web）和本地（CD 驱动器、U 盘）。通过按需扫描和内存扫描，可以深入了解威胁的真正运行时状况。例如，一些 rootkit 和后门程序只存在于内存中，不会在本地磁盘中出现。

### 准确性

据估计，全球用户安装的迈克菲恶意软件防护引擎每天扫描的文件数量超过了

**4.7 万亿个，**

这无疑突显了用户对引擎的准确性和可靠性的需求。业界享有声誉的组织（如：AV-Test、AV-Comparatives、Virus Bulletin 杂志等）一直在对恶意软件防护引擎的准确性进行公开、透明的测试。



### 检测率

恶意软件解决方案最重要的作用就是拦截恶意软件。有时，系统在恶意软件解决方案开始运行前可能就已经受到了感染。这时就需要恶意软件引擎具备杀毒功能，从而尝试在恶意软件发起攻击后尽可能多地清理用户数据（文档、媒体文件、可执行文件）。

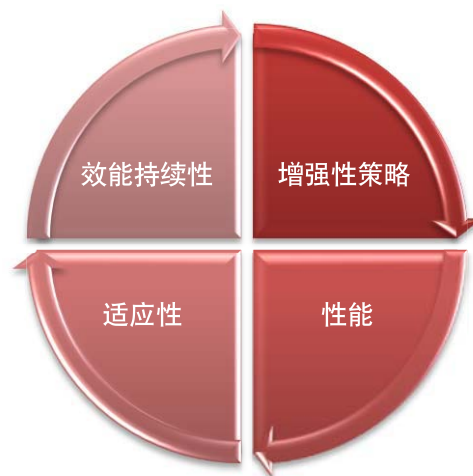
而且，只删除恶意软件文件本身还不够，任何使文件受到感染的恶意软件都必须清除。例如，W32/Conficker.worm 会将一个（经过伪装）autorun.inf — Windows CD AutoPlay 功能可以解释这种文件 — 放在任何与计算机连接的移动存储设备（例如，U 盘）上，以它作为媒介进行传播。

### 可管理性

虽然可管理性的价值可能对家庭用户无足轻重，但对企业用户却至关重要。借助一个中央管理控制台（例如，McAfee ePolicy Orchestrator）远程配置和控制数以千计的终端，得益于简单的部署、配置和监控，企业可大幅降低终端恶意软件防护解决方案的拥有成本。

## 网络网关恶意软件防护的价值

网关恶意软件防护可实施适用于网关的专用技术，提供的价值如下：



### 效能持续性

无论对于员工的笔记本电脑、访客的笔记本电脑，还是普及度较低的操作系统（Linux、Mac），确保在公司网络中每一个客户端上运行切实有效的最新恶意软件防护都是一项艰巨的任务。这一解决方案要求在网络外围集中执行恶意软件防护。

### 增强性策略

企业环境要求严格执行防护各种潜在有害程序和可疑行为的安全策略，有害程序和可疑行为也可能存在于不一定是恶意软件的软件中。网关恶意软件防护解决方案的误报率只有保持在较低水平才能确保其易管理、总拥有成本处于较低水平。不过，与桌面安全相比，网关误报不会对受感染的客户端产生任何负面影响（除了阻止访问邮件、网站或下载）。网关层的这一独有敏感性可确保严格、有效地执行安全策略。

**性能**

网关恶意软件防护 — 如果基于适用于网关的恶意软件防护技术 — 能以最低的成本提供真正的深层次防护：例如，结合使用 Web 网关的缓存功能，对于大型网络中的大量客户端而言，只需扫描一次资源，无需让每一台客户端 PC 自己运行相同的扫描。

**适应性**

鉴于任何安全解决方案都无法提供 100% 的保护，恶意下载或电子邮件仍然可以通过网关，感染桌面机。移动用户可能会在脱离公司的保护后受到感染。恶意软件通常会试图禁用桌面保护及相关更新机制。不过，通过安装 ProActive 插件，Web 网关不会受到恶意控制客户端 PC 的影响，仍然能检测出可疑的网络流量、拦截并隔离受感染的系统。为传出流量提供保护有助于减少公司承担的责任，例如，对访客已经受感染的笔记本电脑发起的攻击看起来似乎来自您的公司网络。

## 恶意软件检测基础

### 确切检测与识别

我们将重点介绍的常规检测和启发式检测技术在很大程度上基于经验和假设，而不是证据，由于知道什么是恶意软件，确切检测在拦截恶意软件方面似乎有着微弱的优势。确切检测通常基于签名扫描，能够尽可能准确、高效地提供值得用户信赖的恶意软件扫描结果。恶意软件防护引擎的修复功能也可以从对特定恶意软件的准确识别中获益。误报率保持在极低水平，从而使管理员无需手动维护白名单。不过，将数百条检测规则同时应用于接受扫描的文件这本身也是一种技术。这就要求将高度优化的算法和最佳代码执行用于存储并行检测规则，并将它们用于快速搜索和准确分类。

需要分析以进行彻底检测，达到上文所述的准确性，这也是这种方法的致命弱点。由于有针对性的短跨度，非典型性恶意软件的流行性比以往更强，恶意软件防护解决方案厂商可能永远也无法监测到特定恶意软件的样本，或者等到分析完成时和签名更新发布时，恶意软件可能已经离开了“作案现场”。这一流程的高度自动化和快速响应可以在一定程度上解决这个问题。（参见“[自动化智能感知](#)”）

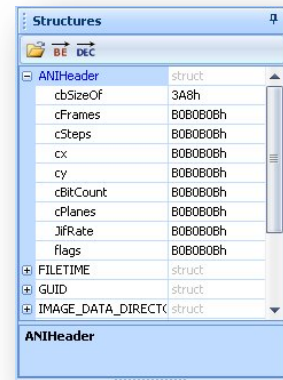
### 常规检测

管中窥豹，可见一斑：常规检测会提取一个或多个恶意软件系列样本或攻击样本的重要特征，生成的通用检测规则可以最大限度捕获同一系列的变体或相同漏洞的攻击。

常规检测规则采用类似于确切检测的技术，虽然误报风险略有上升，但我们从主动式保护中获益匪浅。

对新恶意软件做出的第一反应可能是指纹 — 或基于签名的检测，更多的常规检测规则将紧随其后，检测出即将出现的新恶意软件系列的变体或即将发起的攻击。

有时，我们甚至要到数月、甚至数年后才能看到常规检测的效果。臭名昭著的 Animated Cursor 漏洞的情况就是这样，它可能是 2007 年最流行的漏洞。原来“新”漏洞与 2005 年的 Animated Cursor 和 Icon Format Handling (MS05-002) 漏洞都是基于相同的 bug。两年后，攻击者只是稍作调整就触发了仍然存在于 Windows 的 user32.dll 文件中的漏洞。因此，对 2005 年漏洞所做的常规网关检测同样可以在两年后主动保护客户免遭利用 Windows Animated Cursor Remote Code Execution 漏洞 (MS07-017) 发起的攻击。



在 McAfee FileInsight 中打开的用来发起攻击的“anlh”头文件结构。[2]

## 启发式检测

无风不起浪。启发式检测结合一些已知的证据和经验来识别常见的分类。这一系列检测技术通常针对新恶意软件变体、新恶意软件系列、甚至未知漏洞，并提供了强大的主动检测功能。

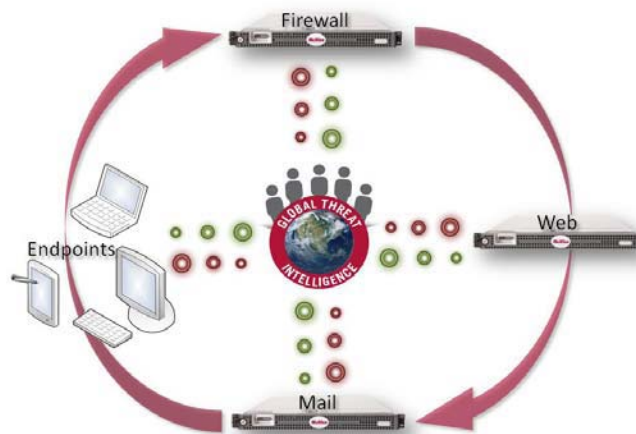
如果有如此强大的检测功能，即使误报率略微上升，也无法掩盖启发式检测出众的性价比。这种采用 ProActive 插件的网关恶意软件防护引擎误报率在 0.002%（一般网站）到 0.04%（可执行文件）之间，而且只需要网络管理员偶尔进行维护。主动式安全解决方案非常值得采用，客户可以获益非浅。虽然通常拦截用户根据需要发起的下载看起来好像是误报，但另一种检测行为却证明了这是一个正确合理的决定：反汇编防护、反调试技巧以及类似 rootkit 的隐藏文件行为是否可疑呢？是的，它们可疑；我们也可以认为它们存在恶意。然而，当我们通过游戏的版权保护模块或多媒体软件的数字版权管理组件 — 毫无疑问这两种应用程序本身都没有危害 — 来看待这类行为时，它们会因此而变得没有危害吗？这是网关感知误报的“灰色地带”。无论感知到什么，如果错误地拦截了下载或清理了网站，相比花数小时或数天时间来对受感染计算机进行取证分析以确定敏感数据是否遭窃和是否需要清理系统，将受影响的 URL 添加到白名单只需数分钟。

后者不仅使管理员始终处于繁忙状态，还使受影响的用户无法继续工作。每次感染所造成的财务损失视遭窃的数据或身份信息而定，从大概 50 美元 — 简单的感染 — 到数百万美元 — 公司高层的 PC 受到了信息窃取型恶意软件的攻击。例如，在 Google 受到 “Operation Aurora” 攻击期间，攻击者获得了 Google 源代码库的访问权限并窃取了该公司专有的代码和 Google Mail、Google Apps 等登录验证系统的代码。[3] 虽然只有 Google 才知道这次事件所造成的具体损失，但可以肯定的是损失绝对远大高于 50 美元。

## 目前先进的恶意软件检测技术

### 自动化威胁智能感知

迈克菲的解决方案会通过终端用户点和设备自动提交威胁信息（例如，新的潜在有害软件或可疑网站的样本）；对它们进行分析、分类和关联；并将它们整合到数据库更新中。用户还可通过 Artemis 云安全保护技术实时获取威胁信息。



*受恶意软件防护解决方案保护的终端和网络设备通过全球威胁智能感知系统获取数据，同时也向其提供数据。*

每周 7 天，每天 24 小时自动执行这一流程，生成多种防护措施，从适用于单个文件的最简单的指纹和签名、类似样本的通用描述，到通过提取不同系列恶意软件样本的共同行为特征建立的高级行为模式。

## 降低风险

### 防止误报

我们的自动化威胁智能感知可以为恶意软件防护引擎随后的数据库更新提供恶意软件检测数据，包括“正面”和“负面”培训。正面培训表示掌握了新的恶意软件检测规则，而负面培训表示会导致误报的检测规则自动删除和减少。

适用于网关的恶意软件防护技术还会考虑用户的上网行为和网站环境。具体分类取决于用户访问网站或可执行下载的方式。详细信息，参见“[环境](#)”。

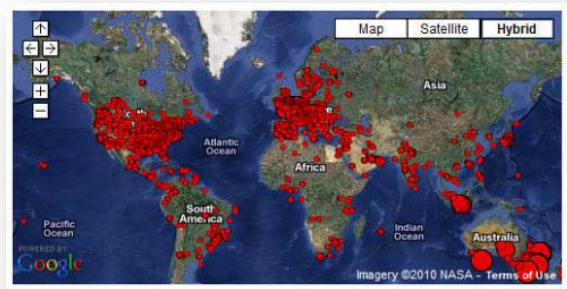
### 代码安全

新的软件代码是企业级恶意软件防护引擎必须保护的第二大风险区域，它可能存在 bug，从而导致潜在的安全漏洞。迈克菲将 coverity™ — 业界领先的代码工具和流程 — 应用于产品的整个生命周期。此外，迈克菲的专业团队还将执行安全审计，以确保迈克菲恶意软件防护引擎代码达到最高安全标准。最后，引擎二进制文件的 Authenticode™ 数字证书使用户和产品能够确保引擎未遭更改。

## 基于云安全的检测

恶意软件系列和变体的迅猛增长导致防病毒检测数据库保持着同步发展。迈克菲 Artemis 基于云的检测技术使我们能够利用云技术保存大量的检测规则，不仅减少恶意软件防护引擎的内存占用量，而且仍然能够访问全球恶意软件防护智能信息。如果没有 Artemis 这样的云安全技术，数据库更新所需的空间将比现在大约 6 倍，并且无法再高效地载入内存。

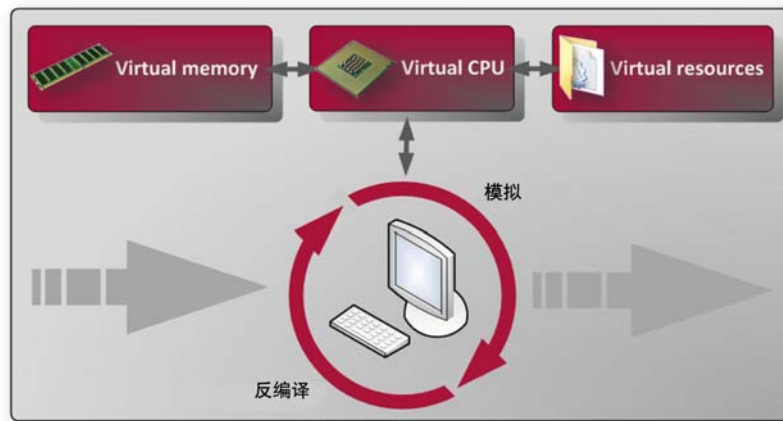
从保护的观点而言，云检测技术还使我们能够关联全球事件（例如，新的可疑文件的爆发）和提供实时保护。



迈克菲 Artemis 云技术跟踪新恶意软件的爆发。

## 虚拟复制

虚拟复制是恶意软件防护引擎打击多态恶意软件和提供准确的主动式检测的终极武器。多态恶意软件改变了加密方法和密钥，利用它加密原始病毒代码，虽然经历了每一个复制步骤，但原始病毒代码/病毒体却未发生变化。通过绕过加密和深入检测，我们的常规检测能够识别任何多态恶意软件系列。



模拟原理

虚拟复制的意思是引擎模拟一台虚拟计算机（它的 CPU、内存、操作系统 API 和资源），并在虚拟环境中模拟执行可疑文件。引擎像操作系统一样对可疑文件的代码执行反汇编，不过指令只会对软件模拟的安全数据结构产生影响。反汇编可以帮助我们深入了解可疑文件，从而做出准确的威胁预测。此外，模拟还是我们将在下一章中介绍的常规脱壳的基础技术。

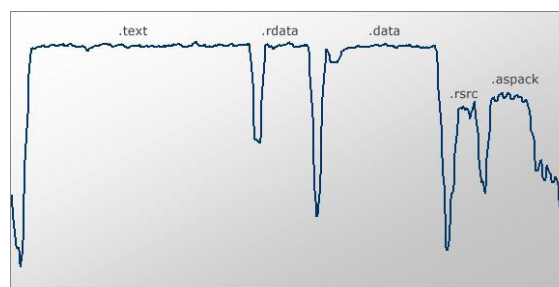
虚拟复制器必须应对所模拟计算机和操作系统的大量特性，如：进程和线程、文件以及反调试和反模拟手段。现有的反模拟方法：恶意软件编写者利用未记录的 CPU 指令（例如，salc、icebp）欺骗模拟器，并且当芯片中加入新指令时，新的恶意软件变体也会迅速获取这些指令。例如，新的 MMX 指令（被 Downloader.zq 和 Downloader.ash 变体利用）和 FPU 指令（W32/Alisa 和 W32/Sabia 病毒系列）。在 Windows 上使用的另一种常见方法是计时检查 — 检查执行一组指令所用的时间，如果计时检查失败，将立即或随后显示一个不同的代码路径（例如，W32/Volage 和 W32/Alisa 病毒系列）。还是在 Windows 上，通过使用 Structured Exception Handling (SEH)、Thread Local Storage (TLS) 回调，多数恶意软件都利用不常见的 Windows API 函数来使恶意软件防护引擎的模拟器失效。迈克菲的恶意软件防护引擎能够应对这类问题，并且我们的研究人员一直在跟踪这一领域的最新发展情况。

## 脱壳

恶意软件编写者经常利用运行时加壳工具来压缩恶意有效负载。已知的加壳工具和保护程序有 200 多种。运行时加壳工具可合法地用于最大限度降低可执行文件的下载大小，不过，多数情况下它们用于为程序代码添加混淆层。一旦开始后，可执行文件会运行一个解码器循环，先打开加壳的部分，然后转为执行（在内存中）未加壳的部分。

发现使用运行时加壳工具还不足以作为将程序识别为恶意内容的证据，这是因为没有危害的合法应用程序也会使用加壳工具。尽管如此，加壳工具的使用还是会引起恶意软件防护引擎的注意。如果还发现了其他可疑行为，启发式检测就会将其视为恶意软件。运行时加壳可执行文件会暴露一些显著特征，例如，加壳部分

的信息熵、解码器循环靠近可执行文件的入口点或跳转 — 将代码执行转入可写入（数据）部分。右图显示了信息熵随 Worm.NetSky.C（利用 ASPack 加壳工具进行运行时加壳的变体）部分的分布。从右往左看，在 .aspack 部分的末端开始执行，这部分未经过加壳，并且在图中记录了中熵。然而，这一部分包含的解码器循环会对左边三个部分中的恶意内容进行脱壳。由于经过加壳，这些部分显示了更高的熵。脱壳后，执行会转入（目前未加壳的）.text 部分。



信息熵在 NetSky.C worm 中的分布。

脱壳后，执行会转入（目前未加壳的）.text 部分。

恶意软件防护引擎应当包含对此类常用加壳工具（例如，ASPack、UPX、MEW、和 FSG 等）的脱壳支持。通过采用独有的常规脱壳技术，迈克菲恶意软件防护引擎实现了超越，甚至能够脱壳未知的、自定义运行时加壳工具 — 即使在隐藏或新的加壳工具上也可支持准确的主动式分类。

恶意软件目前利用许多其他形式的内容混淆手段，主要攻击静态/网关扫描，而不是运行时加壳。例如，利用 XOR、ROL 和其他简单的算法（为 Operation Aurora 攻击所用）来混淆攻击的可执行有效负载；base64 编码可执行有效负载，并将其直接置于 HTML 页面中（为大面积感染合法网站的 Gumblar 所用）；或者利用 GIF 或 JPEG stub 来隐藏经过混淆的可执行有效负载，从而使网络级扫描程序将它们视为合法的媒体文件（Mezzia 木马下载器所采用）。

```
eval(function(p, a, c, k, e, d) {
  e = function(c) {
    return (c < a ? '' : e(parseInt(c / a)) + ((c = c % a) > 35 ?
String.fromCharCode(c + 29) : c.toString(36))
  };
  if (!''.replace(/^/, String)) {
    while (c--) d[e(c)] = k[c] || e(c);
    k = [function(e) {
      return d[e];
    }];
    e = function() {
      return '\\w+'
    };
    c = 1;
  };
  while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b',
'g'), k[c]);
  return p
} ('2Z.34(32("33*p%2L4f%h%j%2Q%1%2L4f%4d ...
|document|length|substring|unescape|var|write'.split('|'), 0, {}))
```

经运行时加壳的恶意 Web 脚本（采用 Dean Edwards 加壳工具）。

长期以来，大多数攻击者都是利用加壳恶意代码的“成熟”理念来阻止扫描程序和分析人员进行分析。即使是采用 RSA 密码算法的真正加密也已经被 Web 恶意软件（例如，MMaxSploit 工具包）所利用。反模拟手段也丰富了脚本代码混淆，例如，使混淆密钥远离利用文档 URL (location.href) 或 HTTP 头信息值（Fragus 工具包使用最后修改的头信息）的内容，以携带该部分内容并使其可用于运行时重建。

## 统计分类

启发式检测技术会将一个新文件的属性或特征与从流行威胁库中收集的类似特征进行比较，从而确定一个与主动式模糊相匹配的属性或特征。特征是文件的基本属性，因文件格式、甚至是某些较小签名的不同而异。一些特征具有几何（或结构）性质，例如，我们在前面讨论的信息熵。其他特征从简单的文件大小属性 — 适用于任何文件 — 到高级 Authenticode™ 数字证书核查 — 仅适用于 Windows 可执行文件。

恶意软件的不断“商业化”导致重复使用代码部分、甚至大部分的二进制文件，仅对变体中的小部分数据进行更改。恶意软件防护引擎能够根据文件的特征和统计匹配启发式地将新的恶意软件变体与已知的恶意软件系列联系起来，从而对恶意软件不断商业化的这一趋势做出了强有力的反击，尤其是在木马、广告软件和间谍软件领域。例如，类似 Zlob 和各种 SpySheriff 恶意（假冒）防病毒软件的恶意软件系列因能够在短时间内生成新的变体而臭名昭著。

迈克菲对威胁态势的深入了解使我们能够将机器学习算法应用于这些巨大的恶意软件样本集合，并编译数据库（所谓的决策树）— 描述当前恶意软件系列，并支持根据这种形式的威胁智能信息来统计匹配任何新的可疑文件。



声称能在新安装的 Windows 中发现恶意软件的  
恶意防病毒软件。

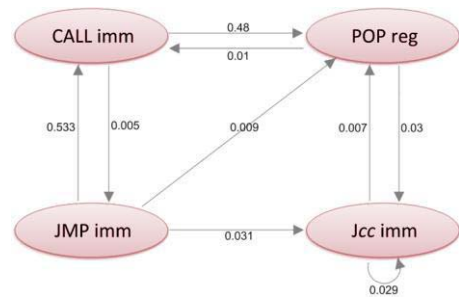
## 模糊指纹技术

恶意软件防护引擎支持大量待申请专利的高级模糊指纹技术。相比准确识别单个恶意软件文件

的哈希识别，得益于其所具有的模糊性，这些指纹还可以匹配变体。例如，使用操作码链、图形数据等来生成这类指纹。在 Web 网关，引擎还可以使用几何特征指纹。

### 常规漏洞攻击检测

无论是以企业为目标的攻击，还是快速传播的蠕虫（例如，Conficker），漏洞攻击往往是万恶之源。相比可执行的恶意软件文件，漏洞攻击通常以不起眼的文件格式（例如，JPEG、MP3、DOC 或 PDF）作为掩护。最早用于常规漏洞攻击检测的技术。X 光扫描能够探测一组已知的混淆方法（例如，XOR 和 ROL），搜索一组已知的签名。这显然会影响性能（支持更多的混淆方法会降低检测速度）的扩展和保护（基于签名）的增强。待申请专利的 McAfee XploitSeeker 漏洞攻击检测（是我们将在下一章详细介绍的 ProActive 插件的组成部分）则采用不同的方法——注重可扩展性。



x86 shellcode 的简化 Markov 模型

通过执行实时内容检测和虚拟机模拟，XploitSeeker 能在潜在的零日或有针对性攻击入侵客户端 PC 前检测出它们。XploitSeeker 采用一种称为 Markov 模型的统计方法来检测潜在机器代码行为的内容，而不使用任何签名。使用机器学习来“培训”模型。此外，这种检测方法还受文件格式限制，从而扩展了其应用范围。[4]

仅仅在 2009 年上半年，XploitSeeker 就成功地拦截了通过大多数致命零日漏洞发起的攻击，包括：Internet Explorer Buffer Overflow Zero-Day (MS09-002)、Adobe Reader getIcon() Stack Overflow Zero-Day (CVE-2009-0927)、PowerPoint Code Execution Zero-Day (MS09-017) 和 DirectShow Video ActiveX Zero-Day (MS09-032)。借助迈克菲的恶意软件防护解决方案，终端和网关都可以执行专为各自环境优化的检测方法。通过同时部署终端和网关防护解决方案，这些技术得到了增强，而且无需执行两次相同的扫描。

```

0.5      pop eax
0.5      pop eax
0.4      pop eax
0.4      pop eax
0.4      jmp loc_16

loc_6:
0.8      pop ebx
0.8      dec ebx
0.9      xor ecx,ecx
0.9      mov cx,0x3b8

loc_E:
0.9      xor byte [ebx+ecx],0xbd
1.0      loop loc_E
1.0      jmp loc_1B

loc_16:
0.6      call loc_6

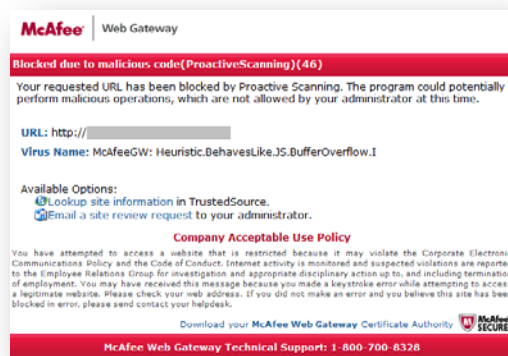
loc_1B:
...
    
```

x86 shellcode 的概率分类

## 行为分析

恶意软件检测领域存在两种形式的行为分析：动态分析和静态分析。在桌面机上运行时，动态分析能够监控应用程序和系统活动。如果检测到恶意或可疑的活动，引擎会及时拦截潜在的威胁。终端恶意软件防护的主机入侵防护系统 (HIPS) 功能（例如，运行时缓冲区溢出检测）就属于这一类型。

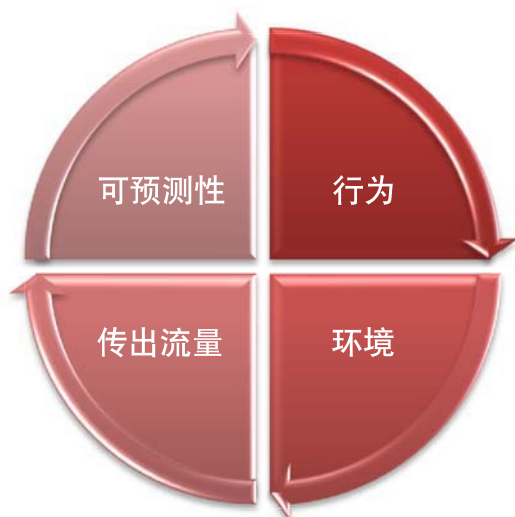
静态分析则能对磁盘上或内存中的文件进行解析、检测其代码部分，并对在计算机上实际执行将导致文件面临风险的行为进行尽可能的假设。网关恶意软件防护必须采用这种方法。roActive 是迈克菲用于在 Web 网关执行静态行为分析的技术，我们将在下一章对其进行详细介绍。ProActive 采用了前面介绍的模拟和静态分类技术。



预测 Internet Explorer XML Data Binding Zero-Day Vulnerability (MS08-078) 攻击的缓冲区溢出行为。

## ProActive：基于行为的网关恶意软件防护插件

我们所有的恶意软件防护技术都旨在提供预测性分析和主动采取应对措施。迈克菲待申请专利的 ProActive 技术提供了适用于 Web 网关的恶意软件防护功能，我们将通过其独有的四个技术特点来对其进行介绍。



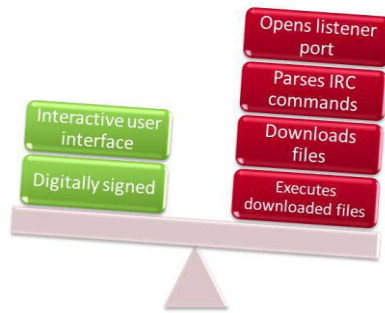
### 预测性

通过执行实时行为代码模拟和分类，ProActive 能够预测下载的文件和访问的

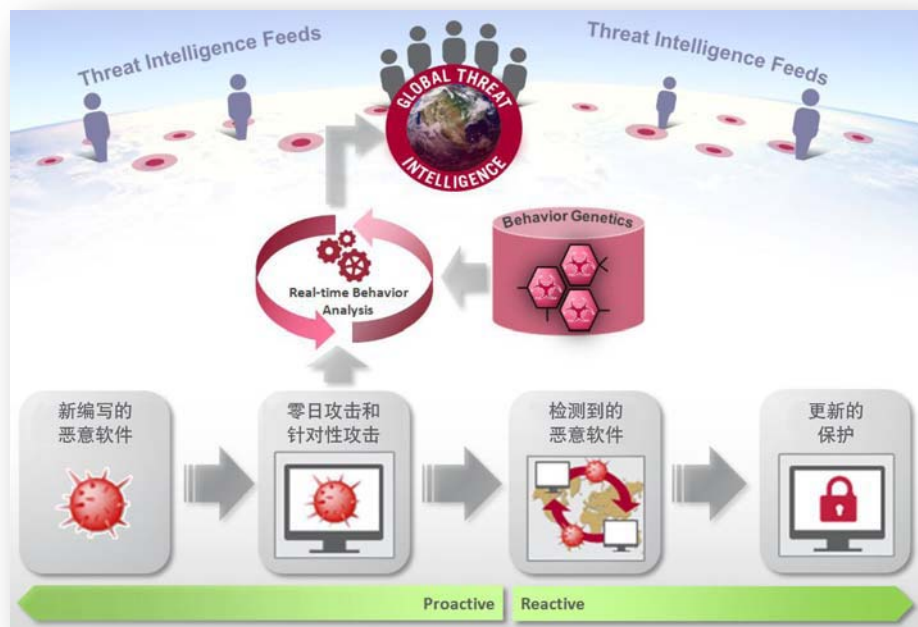
网站的行为以及在客户端 PC 上的执行时间。

行为

ProActive 完全以下载文件的行为特征为侧重点，这是因为行为是构建软件（包括恶意软件）的基础。无论恶意软件变体如何，以行为特征为焦点使迈克菲的解决方案能够在常见恶意行为（例如，密码窃取、后门通信、病毒复制）入侵桌面机前主动检测出它们。



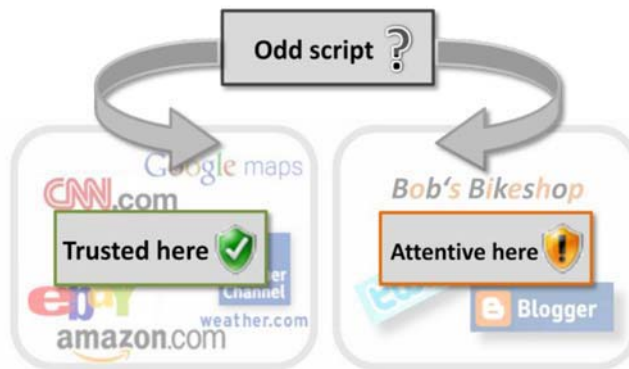
ProActive 会自动从我们的全球威胁智能感知系统数据库收集的威胁样本中提取行为特征。随后，会将这些特征与我们的机器学习算法培训数据库更新相关联。我们在一分钟内即可发布增量更新。迈克菲每周 7 天每天 24 小时不间断地为网关提供这种智能信息。



得益于全球威胁智能感知系统，ProActive 实时智能分析能在必要时终止恶意软件的生命周期。

行为

为确保在不失去对未知威胁的拦截能力的情况下实现最准确的分类，ProActive 技术会将用户的上网行为和网站环境考虑在内。用户如何触发了可执行下载？嵌入脚本的网站是什么类型？上网路径、点击行为、网站分类、下载的数字签名以及更多的因素都会影响整体分类。已知、可信的热门商业网站可能会允许执行看似奇怪的脚本，而用户被重新定向到的未知网站则会拦截它。



外发流量检查

待申请专利的 ProActive 网关恶意软件防护技术的第四个技术特点是检测可疑的内部网络外发流量。由于能够在网络外围及时检测出恶意“回拨”活动——发送窃取的密码或其他数据，这种检测方法使我们能够帮助漫游用户防止已受感染的笔记本电脑泄露数据，网关恶意软件防护解决方案可以拦截数据流，隔离客户端，防止其进一步访问网络，直到完成清理工作。



ProActive 技术的作用

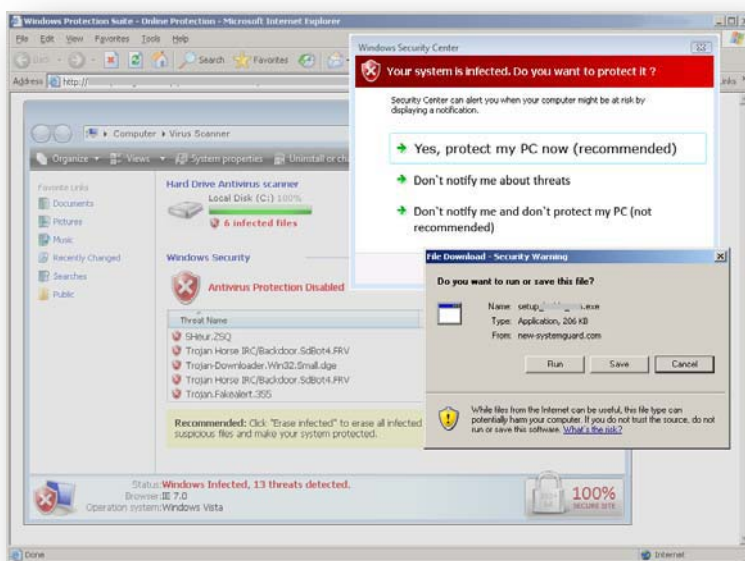
ProActive XploitSeeker  
检测

零日漏洞允许在 Microsoft DirectShow 的 Video ActiveX 控件 (MS09-032) 中远程执行代码，这一漏洞在 2009 年遭到攻击者的大肆利用。之所以出现漏洞是因为与受影响的 ActiveX 控件静态链接的基本 Active Template Library 中缺少数据验证检查。



广泛传播的恶意防病毒欺诈威胁 — 通知网站访问者他们的计算机受到了感染，并提供清理服务 — 同样利用交互型网站来吸引攻击对象的注意。

攻击者利用 Dean Edwards 脚本加壳工具对下图中的虚假防病毒页面所采用的脚本代码进行了运行时加壳。该脚本能够动态生成一个 Web 表单，并将下载的目标 URL 填写其中，然后提交表单，从而在无需用户交互操作的情况下触发路过式下载。传统的检测技术会将这种脚本分类为“可疑”，但却不会拦截它。这是为什么呢？原因在于 Web 2.0 站点普遍采用 Web 表单，而我们不想“伤及无辜”。

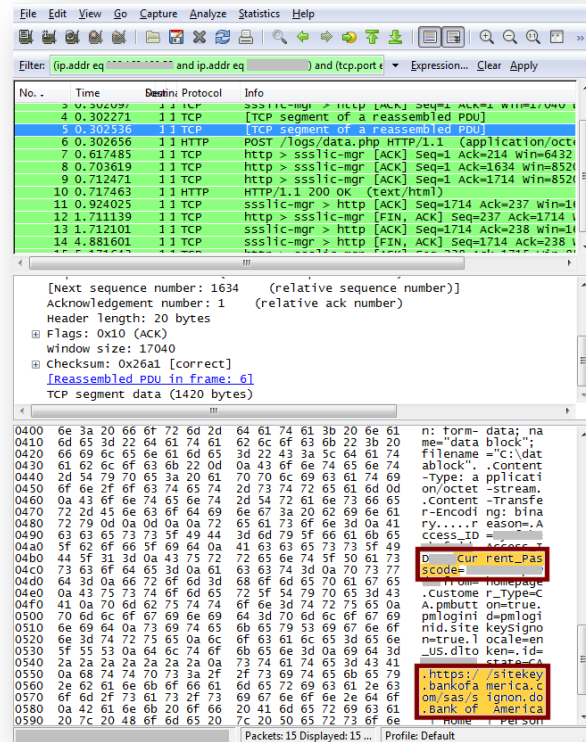


恶意虚假网站触发路过式下载恶意软件。

由于要下载的可执行文件采用了自定义运行时加壳，传统检测技术会将其列为可疑，但只凭这一点仍然无法证明是否应当拦截它。不过，我们现在可以将这三点结合起来：可疑的脚本、无需用户交互操作即可触发可执行文件下载的脚本、可执行文件的可疑“外观”。ProActive 能够在 LooksLike.Win32.Suspicious.C 这样的威胁攻击桌面系统前拦截它们，同时保持用户浏览合法 Web 2.0 站点所需的准确性。

## ProActive 传出流量分析

虽然存在多种密码窃取恶意软件系列和变体，但它们的行为通常可归结为“劫持”进程或操作系统以捕获数据，并发送回所捕获的数据。这就需要避开桌面防火墙或企业防火墙的“干扰”。为了达到这一目的，大多数恶意软件使用 HTTP，因为这是公司防火墙必须开放的几个端口之一。密码窃取者通常还会将他们的数据发送代码注入浏览器进程，从而使简单的桌面防火墙只能看到一个发送数据的合法浏览器进程。



SilentBanker 正在传回窃取到的网上银行帐户数据。

SilentBanker 密码窃取程序也不例外。这种恶意软件以网上银行凭据为目标，并且能够在 SSL 保护生效前捕获这些凭据。不过，其丢弃器组件被前瞻性地拦截为 LooksLike.Win32.Small.C，而丢弃的浏览器辅助对象则被前瞻性地来拦截为 BehavesLike.Win32.PasswordStealer.H。



确定这些客户端试图自动运行恶意软件，并锁定所有 Web 访问。

即使我们没有在这一阶段捕获恶意软件，迈克菲 ProActive 技术也会分析 SilentBanker 向外发送的数据（窃取的密码和用户数据）、区别合法 Web 流量未经请求提交的数据，并及时制止数据泄露。

## 作者简介



Christoph Alme 是迈克菲实验室的恶意软件防护引擎研发团队负责人。主要负责监督英国和德国的引擎团队的研究工作。Alme 在主动式恶意软件防护领域发明了多种待申请专利的关键技术。Alme 在迈克菲收购 Secure Computing 后加入迈克菲，此前，他曾就职于 SAP 和 BMW。



Declan Eardly 是迈克菲实验室的恶意软件防护引擎研发团队的负责人。主要负责领导英国的核心引擎团队。Eardly 拥有 15 年的恶意软件防护研发经验，涉及所有恶意软件主题，从 Microsoft Office 恶意软件到恶意软件统计分类的最新发展。他还曾为 Dr. Solomon's Software 工作。

## 参考文献

[1] Gartner, 《避免恶意软件感染的十大步骤》，2009 年 9 月。

[2] 迈克菲实验室, 《新版 McAfee FileInsight》。

<http://www.avertlabs.com/research/blog/index.php/2009/09/10/new-version-of-mcafee-fileinsight/>

[3] Network World, 《报告：Google 攻击以“Gaia”密码系统为目标》。

<http://www.networkworld.com/news/2010/042010-report-google-attack-targeted-gaia.html>

[4] 迈克菲实验室的 Christoph Alme 和 Dennis Elser, 《利用 Markov 模型检测代码执行攻击》，2009 年 CARO 会议。



McAfee, Inc.  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

本文档所提供的信息仅用于培训目的和为迈克菲用户提供便利。本文档包含的信息如有更改，恕不另行通行。这些信息“按现状”提供，对其准确性或这些信息对任何特定情况的适用性不做任何保证。

McAfee, McAfee 徽标和 McAfee ePolicy Orchestrator 是 McAfee, Inc. 或其分支机构在美国及其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。版权所有 © 2010 McAfee, Inc.

### 迈克菲（上海）软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室	邮编：100020	电话：(8610) 85722000	传真：(8610) 86752299
上海市卢湾区湖滨路 222 号企业天地 1 号楼 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