

# McAfee Risk Advisor

不必依靠猜测即可在正确的位置采取安全措施



各企业通常部署多种安全单点产品来应对层出不穷和不断演进的威胁。但是，即便部署了所有这些技术方案，安全和 IT 人员也可能经常在星期二修补程序发布日那天坐在指挥室内，试图回答以下问题：“我们是否需要关闭业务，应用此修补程序？” McAfee® Risk Advisor 预先将威胁、漏洞和应对措施的信息整合在一起，以突出显示真正面临风险的资产。您不必依靠猜测，即可了解在何时何地采取安全措施，从而节省时间和资金。

## 主要优势

- 在企业生产力与适当的安全级别之间取得平衡
- 快速识别面临威胁风险的资产
- 消除了将威胁与面临风险的关键系统相关联的手动、耗时过程，直接指导补救工作的开展
- 使用 McAfee Labs 提供的威胁馈送保持最新状态
- 与核心迈克菲产品集成，例如 McAfee ePO 控制台、McAfee Vulnerability Manager、McAfee Host Intrusion Prevention、McAfee Network Security Manager、McAfee Policy Auditor 等

McAfee Risk Advisor 提供风险指标和分析，您不必推测即可在正确的位置实施补救工作，这一点为行业首创。

McAfee Risk Advisor 将威胁馈送与漏洞及应对措施信息关联起来，对面临风险的特定资产提供即时的评估。借助此信息，您可以立即获得有关威胁、严重性及其风险的信息，让您可根据资产的价值确定补救工作的优先顺序。

这种做法可产生明显的效果，因为某个资产可能易受威胁的攻击，但在相应的应对措施就位后，该资产可能不再有风险。了解哪些资产易受攻击和面临风险有助于安全部门将其工作集中在需要立即采取措施的资产上。

除了利用 McAfee Risk Advisor 节省成本和管理开销外，您还可以清楚地了解在应对措施上的投资所能产生的投资回报率。具体而言，利用 McAfee Risk Advisor，您可以将威胁与资产关联起来，并清楚了解保护这些资产的应对措施，而不管应对措施是否就位。此外，使用此信息可帮助确定在哪些应对措施上进行投资，以便在将来获得保护。

## 综合视图

Risk Advisor 威胁馈送查看器提供来自数千家供应商和行业收集点的有关新威胁和已更新威胁的最新信息。该查看器包括：

- 威胁描述和概述
- 详细的分析
- 补救和建议的操作

- 通知和漏洞利用讨论的链接
- 不同的风险计分方法
- 受影响的应用程序
- 威胁对各种法规要求的影响

此外，威胁馈送还包含可由 McAfee ePolicy Orchestrator® (ePO™) 集中式管理平台部署的特定迈克菲应对措施（如果需要）。Risk Advisor 查看器会计算当前接受管理且包含正确应对措施和没有应对措施的主机数量。应对措施合规性图表可直接在威胁视图中生成，用于说明针对威胁采取的应对措施。

## 规格

### 最低系统要求

- McAfee ePolicy Orchestrator 4.0 (修补程序 3)
- Microsoft Windows Server 2003 (SP2 或更高版本)
- Microsoft SQL Server 2005 (SP1 或更高版本)

### 可选的系统要求

- McAfee VirusScan® Enterprise 8.0/8.5
- McAfee Host Intrusion Prevention 7.0
- McAfee Rogue System Detection 2.0 (修补程序 2)
- McAfee Vulnerability Manager 6.7

## 风险摘要

除了与应对措施相关联外，Risk Advisor 还与 McAfee Vulnerability Manager 和 McAfee ePO 控制台集成，让您可以将漏洞配置文件绘制成图表，以确定要采取安全措施的位置。所生成的图表会简明扼要地反映资产面临风险的位置和方式。这个简单的布尔图表会显示“有风险”和“无风险”摘要。深入分析图表时，会显示一个“风险详细信息”图表，用于反映以下状态：

1. **绿色** - 无漏洞且受到保护（没有检测到漏洞并且采取了相应的应对保护措施）。
2. **黄色** - 有漏洞但受到保护（检测到漏洞，但采取了相应的应对措施以提供保护）。
3. **红色** - 有漏洞且未受保护（检测到漏洞并且没有采取相应的应对措施）。
4. **灰色** - 未知（没有可用于确定漏洞状态或应对措施的数据；一般认为这是路由器和打印服务器等设备所在的位置，因为应对措施对这些资产不适用）。

为确定“有风险”和“无风险”状态，Risk Advisor 采用了保守的方法。资产只有在“无漏洞且受到保护”的情况下，才能归为“无风险”类别。包括黄色（有漏洞但受到保护）、红色（有漏洞且未受保护）和灰色（未知）资产在内的其他所有资产都放在“有风险”组。

## 报告

借助简单的自上而下报告，您可以快速进行深入分析，以了解需要重点采取补救措施的位置。在综合信息显示板中，您可以查看有关威胁的细致、简洁的信息。所提供的详细程度可让您：

- 了解有关威胁及其工作原理的信息
- 查看首次宣布威胁的日期和时间，以及对该记录的最新内容更新
- 查看迈克菲提供的建议补救方法和应对措施
- 确定检测到漏洞的迈克菲解决方案

## 始终保持最新状态

为使您的企业保持最新状态，McAfee Risk Advisor 从世界级的研究组织 McAfee Labs 接收威胁更新。我们的企业级威胁馈送可提供简明、有意义的最新威胁数据，因为这些数据是从我们包含数百万个数据收集点的网络中收集来的。

该馈送包含有关威胁的新闻和补救信息以及指向泄露和漏洞利用信息的链接。此外，该馈送还使用 CVSS v2 模型提供图解说明的风险得分，以及特定威胁对行业法规的影响。

该馈送还包括 McAfee VirusScan、McAfee Host Intrusion Prevention 和 McAfee Network Security Manager 以及检测资产中漏洞的系统（例如 McAfee Vulnerability Manager）所提供的应对措施信息。

有关详细信息，请访问 [www.mcafee.com/cn](http://www.mcafee.com/cn) 或联系您当地的迈克菲代表。

### 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) 85752299

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

销售热线：800-810-0369 [www.mcafee.com/cn](http://www.mcafee.com/cn)

