解决方案简介

防范规避恶意软件

如 McAfee Labs 威胁报告：2017 年 6 月所详述，规避恶意软件可以逃避检测。它通过冒用或滥用合法的应用程序进行隐藏。这种恶意软件知道自己将在沙盒中进行分析，它会延迟执行，等待几天、几周甚至几个月的时间寻找机会发起攻击。

构建安全程序来防范规避恶意软件，应以三个基本构成要素为基础。

- **人员**：安全从业人员必须经过培训才能妥善应对安全事件，并妥善管理当前安全技术。攻击者通常使用社会工程来感染用户。如果没有内部意识和培训，用户会给攻击者留下一些漏洞。
- **流程**：必须具备清晰的结构和内部流程，安全从业人员才能有效率地工作。最佳安全做法（更新、备份、管理、情报、事件响应计划等）是强大高效的安全团队的关键要素。
- **技术**：技术是团队和流程的支柱。应该开发和增强技术，使其适应新的威胁。

防范规避恶意软件的可行策略和规程

- 最重要的恶意软件感染防御资源是用户。用户必须知道，下载和安装可能有风险的来源中的应用程序存在风险。用户还必须了解，浏览恶意软件时可能会不慎下载。
- 始终保证浏览器和附加项是最新版本，并将终端上的防恶意软件和网络网关升级和更新为最新版本。
- 不允许使用不是企业 IT 安全团队分发和认证的受信任的网络上的系统。规避恶意软件可通过与受信任的网络连接的未受保护的系统进行传播。

McAfee
Together is power.

- 规避恶意软件可以隐藏在之前因受黑客攻击感染特洛伊木马的合法软件中。为阻止这类攻击成功，我们强烈建议实施严格的软件传播和分发机制。建议创建企业应用程序中央存储库，用户可以从此库下载经过批准的软件。
- 在授权用户安装之前未经 IT 安全团队验证的应用程序的实例中，指导用户仅安装已知供应商提供受信任特征码的应用程序。在线提供的“无害”应用程序有嵌入式规避恶意软件是很常见的。
- 切勿从非 Web 来源下载应用程序。从 Usenet 组、IRC 通道、即时消息客户端或 P2P 系统下载到恶意软件的概率非常高。IRC 和即时消息中指向网站的链接也经常会连接到被感染的下载项。
- 针对阻止网络钓鱼攻击问题，实施教育计划。恶意软件通常是通过网络钓鱼攻击进行分发的。
- 结合防恶意软件技术，利用威胁情报源。这样有助于加快威胁检测速度。

McAfee 产品如何防御规避恶意软件

McAfee 提供了新一代的安全功能，旨在抵御最善于规避的现代威胁。利用强大的机器学习分析和应用程序遏制工具，组织可以更快捷地找出隐藏的威胁并根据它们的踪迹阻止威胁。

这些功能通过以下 McAfee 产品交付：

Real Protect

Real Protect 是 McAfee Endpoint Protection 解决方案的一部分，它结合了执行前静态分析和执行后行为分析，与任何基于特征码或只有静态分析的解决方案相比，该功能可阻止更多恶意软件，所有功能均集成在 McAfee 生态系统中。Real Protect 运用最先进的机器学习方法根据其静态特征（执行前分析）的深入评估及其具体行为（动态行为分析）识别恶意代码 - 所有内容都无需特征码。Real Protect 功能可以识别最新的模糊处理技术，找出隐藏威胁，让零日恶意软件无处藏身。

动态应用程序遏制

动态应用程序遏制 (DAC) 也是 McAfee Endpoint Protection 解决方案的一部分，用于保护“第一感染源”终端免受新零日恶意软件的感染。当终端检测到可疑文件时，DAC 将立即阻止恶意软件经常使用的行为（例如，更改注册表、写入临时目录或删除文件）。与其他技术不同，DAC 不会耽搁终端（以及用户）的时间，在文件可疑的情况下，会让可疑文件加载到内存，但不允许它对终端进行特定更改或感染其他系统。

Real Protect 和 DAC 可相互集成，也可与其他第三方安全解决方案（例如，SPLUNK、Avecto 和 ForeScout）和 McAfee Endpoint Protection 集成，从而针对最隐蔽的威胁提供多层防御。这些功能可让您的安全团队以一种快速自动的方式应对威胁防御生命周期的所有阶段（检测、纠正和主动防御）。

Real Protect 和 DAC 可用于：

- 通过消除模糊处理技术来找到攻击，进而发现更多恶意软件威胁。
- 限制攻击的影响：在攻击发生之前或攻击造成无可挽回的损害之前，遏制、防护和阻止系统遭到破坏。
- 跟踪和适应：使用自动化集成防御执行范围更广的安全操作，无需考虑或手动激活操作。

请参阅使用 Real Protect 和 DAC 遏制规避恶意软件的演示视频。

动态应用程序遏制配置最佳做法

McAfee Default 策略中的 DAC 规则设置为只报告，因此可降低误报。自适应威胁防护另外提供了两种预定义 DAC 策略：McAfee Default Balanced 和 McAfee Default Security。这些策略设置了一系列建议规则，将根据以下安全配置文件进行阻止：

- McAfee Default Balanced 提供基本级别的保护，可将很多常见的未签名安装程序和应用程序的误报降至最低。
- McAfee Default Security 提供严格的保护，但可能会导致未签名安装程序和应用程序的误报频频发生。

使用规则设置为“报告”的 McAfee Default 策略评估 DAC 规则的影响。要确定是否将规则设置为“阻止”，请监控日志和报告。收集完允许的 DAC 违规（事件 ID 37280）后，请在执行 McAfee Default Balanced 策略前设置企业级信誉或 DAC 排除。

DAC 可以根据名称、MD5 哈希、签名数据和路径从遏制中排除进程。如果您的组织对内部部署的工具进行签名，请将这些签名添加为排除项，以降低误报。

DAC 规则提供了洪泛控制，可将生成的事件数量限制为每小时一次、每个规则一次和每个进程一次。DAC 洪泛控制根据进程 ID 跟踪进程。当进程重新启动时，操作系统会为其分配一个新 ID，此操作将重置洪泛控制，即使进程名称完全相同。例如，如果进程 A 每小时违反 DAC 规则 A 100 次，您每小时只会收到一个事件。如果进程 A 在这一小时内重新启动，洪泛控制将重置进程 A，如果该进程仍然违反 DAC 规则 A，您会收到另一个事件。如果进程 B 违反同一 DAC 规则 A，您将收到第二个事件（带有进程 B 的详细信息）。阅读此内容以了解有关 McAfee 定义的 DAC 规则的特定最佳做法的更多信息。

在生产系统的部署基本映像上运行 McAfee GetClean 工具，以确保将干净的文件发送到 McAfee Global Threat Intelligence (GTI) 进行分类。该工具可帮助确保 McAfee GTI 不会为您的文件提供错误的信誉值。有关详细信息，请参阅《GetClean 产品手册 (PD23191)》。

McAfee Cloud Threat Detection

利用 McAfee Cloud Threat Detection (CTD) 可轻松增强 McAfee 保护，识别高级恶意软件和曝光规避威胁。访问 McAfee ePO Cloud，启用 McAfee CTD 并将其与 McAfee 产品进行集成。

要结合使用 McAfee CTD 功能和 McAfee 安全产品，请采取以下操作：

- 在 McAfee ePO Cloud 中启用 McAfee CTD。
- 在 McAfee 安全产品界面中启用 McAfee CTD 并获取配置密钥。
- 在 McAfee ePO Cloud 界面中使用配置密钥生成激活密钥。
- 使用激活密钥激活您的 McAfee 安全产品。

获取配置密钥和激活产品的详细说明有所不同。请参阅产品手册以了解有关集成 McAfee CTD 和 McAfee 产品的详细信息。

当集成产品开始向 McAfee CTD 发送文件，以便进行分析时，您可以在 McAfee ePO Cloud 中的“订购”页面上查看您的使用信息。

McAfee Active Response

- McAfee Active Response 用于查找和响应高级威胁。当结合威胁源（例如 McAfee GTI、Dell SecureWorks 或 ThreatConnect）使用时，可搜索到规避威胁，并在这些威胁伺机扩散之前将其扼杀。
- 自定义收集器可用于构建专用工具，以查找和识别与感染特洛伊木马的应用程序相关的迹象。
- 用户可构建触发器和反应来定义满足特定条件时的操作。例如，发现特定哈希或文件名时，可自动触发“删除”操作。

进一步阅读

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (消除高级威胁：采用分层防御以实现全面的恶意软件防护)

安全建议中心：抵御恶意软件和特洛伊木马程序的 10 大方法

McAfee Endpoint Security：常见问题

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/cn