McAfee Advanced Threat Defense

检测高级恶意软件

McAfee® Advanced Threat Defense 使组织不仅能够检测高级规避新恶意软件，而且还可以将威胁信息即时转化为措施并实现保护。与传统的沙盒不同，它提供了额外的检测功能，能够扩展检测范围，并且发现善于躲避的威胁。从网络和终端到调查，安全解决方案相互紧密集成，以便在整个环境中即时共享威胁信息，从而提高保护和调查能力。灵活的部署选项，几乎支持任何网络。

不同于以往的检测方式，我们的技术通过终端从网络边缘将高级恶意软件分析功能与现有的防御解决方案相结合，并且能够在整个 IT 环境中共享威胁情报。通过在生态系统中共享威胁情报，集成的安全解决方案可以相互协作，即时关闭命令和控制通信，隔离受破坏的系统，阻止其他同类或类似威胁的实例，评估影响，执行调查并采取应对措施。

McAfee Advanced Threat Defense：检测高级威胁

McAfee Advanced Threat Defense 通过创新的分层途径，可检测当今隐匿的零日恶意软件。它将低接触分析引擎（如防病毒特征码、信誉和实时模拟）与动态分析（沙盒）相结合，以分析实际行为。调查继续进行用以检查文件属性和指令集的深度静态代码分析，以确定预期或规避行为并且评估与已知恶意软件系列的类似性。在分析中的最后一步，McAfee Advanced Threat Defense 专门查找已经通过机器学习确定的恶意指标（通过深度神经网络）。通过结合可实现市场中最强大的高级恶意软件安全防护技术，并有效地平衡深度检查和性能这两方面的需求。借助捕获更容易识别的恶意软件的特征码和实时模拟等较低强度的分析方法对性能有益，而将深入的静态代码分析和通过机器学习获得的洞察力添加到沙盒则可提供详细的恶意软件分类信息，并拓宽针对高度伪装且善于躲避的威胁的检测。可以通过解包、深度静态代码分析和机器学习洞察力来识别可能不会在动态环境中执行的恶意指标。

McAfee Advanced Threat Defense 的关键特色

解决方案广泛集成

- 与现有 McAfee 解决方案、第三方电子邮件网关和支持开放式标准的其他产品集成
- 缩短了从遭遇威胁到遏制威胁并对组织实施全面保护的时间
- 简化工作流程，以加速响应和补救过程
- 实现自动化

强大的分析功能

- 深入静态代码分析、动态分析和机器学习相结合，利用无可匹敌的分析数据提供更准确的检测
- 高级功能支持 SOC 和实现调查

联系我们

恶意软件作者通过打包更改代码的组成或将其隐藏以躲避检测。大多数产品无法正确解包全部原始（源）可执行代码以供分析。McAfee Advanced Threat Defense 包括大量解包功能，可消除混淆，暴露原始可执行代码。它能让深入的静态代码分析在高级文件属性以外查找异常，从而分析属性和指令集以确定预期行为。

与此同时，深入的静态代码分析、机器学习和动态分析还能对可疑恶意软件实施完善的全方位评估。无可比拟的分析输出生成摘要报告，这些摘要报告提供全面理解和操作优先级，还可生成更详细的报告以提供有关恶意软件的分析师级别数据。

增强的保护

McAfee Advanced Threat Defense 和安全设备（从网络边缘到终端）之间的紧密集成使您能够在 McAfee Advanced Threat Defense 证实文件存在恶意时立即采取措施。检测和保护之间这种紧密的自动化集成至关重要。

McAfee Advanced Threat Defense 可以以不同方式集成：直接与安全解决方案集成，通过 McAfee Threat Intelligence Exchange 来继承或者通过 McAfee Advanced Threat Defense Email Connector 来集成。

这种直接集成使安全解决方案能够对 McAfee Advanced Threat Defense 认定的文件采取行动。这些解决方案可立即将威胁情报纳入现有的策略实施流程，并阻止其他同类或类似的文件实例进入网络。

McAfee Advanced Threat Defense 认定的内容出现在集成产品的日志和信息显示板中，就像整个分析已经完成载入，从而并且简化工作流，使管理员能够通过单个界面有效地管理警报。

与 McAfee Threat Intelligence Exchange 集成，将 McAfee Advanced Threat Defense 功能扩展到其他防御解决方案（包括 McAfee Endpoint Protection），确保各类集成安全解决方案均可访问分析结果和攻击信号。倘若 McAfee Advanced Threat Defense 证实某个文件存在恶意，McAfee Threat Intelligence Exchange 将立即通过信誉更新向组织内的各项综合对策发布威胁信息。

启用 McAfee Threat Intelligence Exchange 的终端可以阻止安装 patient-zero（第一传染源）恶意软件，并在未来出现该文件时提供主动防护。启用 McAfee Threat Intelligence Exchange 的网关可以防止文件进入组织。此外，启用 McAfee Threat Intelligence Exchange 的终端还能在脱机情况下继续接收最新文件裁决结果，消除带外负载传输的盲点。

灵活的集中式部署

- 通过支持多种协议的集中式部署降低成本
- 灵活的部署选项，几乎支持任何网络

集成解决方案

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

McAfee Advanced Threat Defense Email Connector 使 McAfee Advanced Threat Defense 能够从电子邮件网关接收电子邮件附件以进行分析。McAfee Advanced Threat Defense 分析附件中的文件，并且在邮件标题中将结论返回到转发电子邮件网关。电子邮件网关随后可以采取基于策略的操作，比如删除或隔离附件，以防止恶意软件感染和传播到内部网络。一种离线模式，可在使用 McAfee Advanced Threat Defense 对带附件的电子邮件进行扫描时将其交付到最终用户。电子邮件网关不会等待对附件的判定结果。管理员通过 McAfee Advanced Threat Defense 或 McAfee Threat Intelligence Exchange 查看附件扫描结果。为了加强电子邮件服务器的检测，McAfee Advanced Threat Defense 通过 McAfee Threat Intelligence Exchange 集成了 McAfee Security for Email Servers。

共享威胁以增强和自动化调查

要对攻击进行调查和补救，组织需要具有可行情报的全面监控能力，以便组织更好地做出决策并采取相应的行动。McAfee Advance Threat Defense 可以产生深度威胁情报，并在您的整个环境中轻松共享，以增强和自动化调查。对 Data Exchange Layer (DXL) 和 REST 应用程序编程接口 (API) 的支持有助于与其他产品和广泛使用的威胁共享标准（如 Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII)）集成，从而进一步支持组织创建、支持和扩展协作式安全生态系统。

在 McAfee 生态系统中，McAfee Enterprise Security Manager 利用并关联 McAfee Advanced Threat Defense 及其他安全系统提供的详细文件信誉和执行事件，提供高级警报和历史视图，从而加强安全情报、风险优先级和实时态势感知。利用 McAfee Advanced Threat Defense 提供的威胁数据指标，McAfee Enterprise Security Manager 将回查六个月的数据，搜索它保存的网络或系统数据中的此类漏洞的指示。它可以揭示之前与新识别的恶意软件源进行过通信的系统。与 McAfee Endpoint Protection、McAfee Threat Intelligence Exchange 和 McAfee Active Response 紧密集成，从而优化安全运营响应以及可见性和操作的效率，如发布新配置、实现新策略、删除文件以及部署可主动消除风险的软件更新。当 McAfee Active Response 识别出网络中被感染的终端并将其列入 McAfee Advanced Threat Defense 报告中时，可以轻松执行通知的操作。从 McAfee Active Response 中的单一工作区查看这些详细的报告可以提高分析师的效率。

高级功能支持调查

McAfee Advanced Threat Defense 提供了很多高级功能，包括：

- **可配置操作系统和应用程序支持：**通过选择环境变量定制分析映像以验证威胁和支持调查。
- **用户交互模式：**支持分析师直接与恶意软件样本交互。
- **大量解包功能：**将调查时间从数天缩短为几分钟。
- **完整逻辑路径：**通过强制执行典型沙盒环境中处于休眠状态的额外逻辑路径，实现更深的样本分析。
- **将样本提交给多个虚拟环境：**通过确定需要执行文件的环境变量加快调查速度。
- **详细报告，涵盖了从反汇编输出和内存转储直至图形函数调用关系图及已嵌入或已丢弃的文件、用户 API 日志和 PCAP 信息：**提供关键信息以供开展分析师调查。威胁时间线有助于实现攻击执行步骤的可视化。
- **Bro Network Security Monitor 集成：**将 Bro 传感器部署到可疑网段，以监控和捕获流量，并将文件转发到 McAfee Advance Threat Defense，以便进行检测。

部署

灵活的高级威胁分析部署选项，几乎支持任何网络。利用对 Azure Marketplace 中提供的私有和公共云的支持，McAfee Advanced Threat Defense 可作为内部部署设备或虚拟外形规格提供。

了解更多信息

有关开始评估 McAfee Advanced Threat Defense 的信息，请与您的代表联系，或访问 www.mcafee.com/cn/products/advanced-threat-defense.aspx。

McAfee Advanced Threat Defense 规格

物理外形规格	ATD-3100 1U 机架安装	ATD-6100 1U 机架安装
虚拟外形规格	v1008 VMware ESXi 5.5、6.0、6.5 Microsoft Hyper-V Server 2012 R2、Windows Server 2016	v1008 VMware ESXi 5.5、6.0、6.5 Microsoft Hyper-V Server 2012 R2、Windows Server 2016
检测		
支持的文件样本类型	PE 文件、Adobe 文件、MicroSoft Office 套件文件、镜像文件、存档、Java、Android Application Package、URL	
分析方法	McAfee Anti-Malware Engine、McAfee GTI 信誉(文件/URL/IP)、Gateway Anti-Malware（模拟和行为分析）、动态分析（沙盒）、深入的代码分析、自定义 YARA 规则、机器学习：深度神经网络	
支持的操作系统	Windows 10（64 位）、Windows 8.1（64 位）、Windows 8（32 位和 64 位）、Windows 7（32 位和 64 位）、Windows XP（32 位和 64 位）、Windows Server 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008、Windows Server 2003、Android 支持所有语言的 Windows 操作系统。	
输出格式	STIX、OpenIOC、XML、JSON、HTML、PDF、文本	
提交方法	单点产品集成、RESTful API、手动提交和 McAfee Advanced Threat Defense Email Connector (SMTP)	

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