McAfee Active Response

全面的终端检测和响应

注重安全的实体目前所面临的威胁形势纷繁复杂、变幻莫测。攻击的创建和传播速度与日俱增。“设计者”利用专业知识，以单个组织为攻击目标，以此来提高攻击效率并最大限度地降低被检测到的风险。攻击者也正在更加频繁地渗透防御技术。高瞻远瞩的组织需要简单易用的集成式工具，帮助他们更加有效地检测存在的攻击者，随后开展快速调查和补救。最佳的检测和响应解决方案可提高安全效率，但它们同时也需要从不断增多的系统中捕获越来越多的信息。McAfee® Active Response 开箱即用，性能优越，可与现有的安全管理解决方案进行自动交互，而且支持用户自定义，从而能够极大地降低攻击者趁虚而入损坏您的计算资产和公司品牌的风险。

主要优势

- **自动化：**捕获并监控环境和系统状态，以便找出可能为 IoA 的一些更改，同时发现休眠的攻击要素，并将情报发送给分析、运营和鉴证团队。
- **适应性：**收到警报时，您可以根据攻击方法的改变而做出调整，针对感兴趣的对象自动收集数据、发出警报和做出回应，以及自定义您对客户工作流的配置。
- **持续性：**持续工作的收集器会在检测到攻击事件时激活触发器，将您一直在监控的攻击活动情况通知给您和您的系统。

不断演变的威胁形势

企业开始意识到自己随时有可能遭到攻击者的入侵，因此必须通过及早地检测攻击、检测正在进行的活动或发现攻击指标 (IoA)，做好充分准备来高效应对此类入侵。与此同时，人们还认识到必须使用新技术来弥补当前在监控、发现、检测和响应方面存在的缺陷。

当前的事件响应方法存在的局限性

当事件响应者和安全管理员按要求在整个组织内调查可疑或已知事件时，通常会受到两个关键因素的制约：时间和规模。虽然现有的系统或工具可收集大量详细信息，但是收集并分析此类信息却需要花费很长时间。速度是数据收集工作的关键性要求，所以一些重大的威胁往往会隐匿在所收集的数据，以及用于收集数据的各种系统中。此外，收集到的数据鱼龙混杂，必须经过筛选方能识别关键信息，且收集到的数据量非常庞大，处理难度也日益提升。

人们最常使用的事件响应工具是由响应者自己编写的脚本。这些工具构成了数据收集的基础，可用于更广泛的分析中。这套知识体系以及相关的工具已经相当成熟，但是大规模地快速使用这些知识及工具的能力却非常有限。正是因为无法在整个组织内针对特定的 IoA 开展实时调查，所以往往会导致响应者在发现攻击和做出响应的过程中缺乏远见。通常，上述工作会受到人为的时间要求限制，这可能会导致在事件响应过程中出现重大缺陷。这为响应者带来了极大的困扰，因为他们的工作在当前工具的局限下，又受到了人为限制。

全面的终端检测和响应

McAfee Active Response 能够持续检测高级安全威胁并做出响应，从而帮助安全从业人员监控安全状态、改进威胁检测，并且从前瞻性发现、详细分析、鉴证调查、全面报告以及优先警报和操作方面，全面扩展事件响应能力。McAfee Active Response 经过优化，符合严格的终端检测和响应 (EDR) 标准，它采用支持用户自定义的预定义收集器来深入搜索所有系统，不仅能够从正在运行的进程中找到存在的 IoA，而且还能够发现处于休眠状态甚至已经删除的 IoA。此外，McAfee Active Response 使用户不仅能够搜索目前存在的 IoA，而且还能够通过可在将来出现 IoA 时给出指令的触发器，根据安全目标发出警报并采取操作。

McAfee Active Response 有力地证明了 McAfee 集成安全体系结构的有效性，它的目的是为了在更复杂的网络世界利用更少的资源更快地解决更多威胁问题。通过 McAfee Active Response，您可以持续监控并有效了解您的终端，从而更快地识别攻击入侵。它还为您提供了所需的工具，以便更快地纠正问题，同时为您的业务创造最为有利的条件。所有这些强大的功能均通过 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件进行管理，同时利用了 Data Exchange Layer，这可提供统一的可伸缩性和可扩展性，而无需增加产品管理人数。

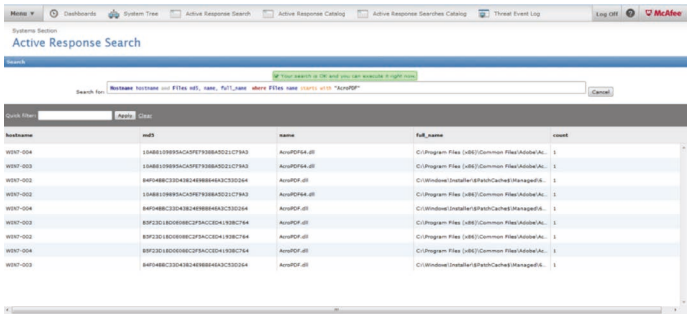

图 1. McAfee Active Response 搜索用户界面。

系统要求

最低硬件要求

如有必要，该服务器可在虚拟机上安装。McAfee Active Response 服务器运行的推荐最低硬件要求如下：

- 4 Intel Xeon CPU X5675，3.07 GHz
- 8 GB RAM
- 120 GB 固态磁盘

要求的服务基础设施

- McAfee ePO 5.1.1 或更高版本
- McAfee Agent 5.0 扩展或更高版本
- Data Exchange Layer 2.0.0.405 代理或更高版本

支持的 Web 浏览器

- Microsoft Internet Explorer 9 或更高版本
- Google Chrome 17 或更高版本
- Mozilla Firefox 10.0 或更高版本

要求的客户端基础设施

- 适用于 Linux 终端的 McAfee Agent 5.0.0.2710 或更高版本
- 适用于 Microsoft Windows 终端的 McAfee Agent 5.0.0.2610 或更高版本
- Data Exchange Layer 2.0.0.405 客户端或更高版本 (在所有受管终端上)

支持的客户端操作系统

- Microsoft Windows
  - Microsoft Windows 8.0、Base；32 位和 64 位
  - Microsoft Windows 8.1、Base、U1；32 位和 64 位
  - Microsoft Windows Server 2012 Base、R2、U1；64 位
  - Microsoft Windows Server 2008 R2 Enterprise、SP1，64 位
  - Microsoft Windows Server 2008 R2 Standard、SP1，64 位
  - Microsoft Windows 7 Enterprise，最高 SP1；32 位和 64 位
  - Microsoft Windows 7 Professional，最高 SP1；32 位和 64 位
- CentOS 6.5，32 位
- RedHat 6.5，32 位

功能	优势	客户利益	特色
收集器	收集器使用户能够找到并查看其系统中的数据。	收集器提供了搜索功能来深入检查系统。通过收集器，可以监控重要的入侵或潜在的攻击，从而收集并查看这些系统中的数据。用户可以从多种常用的脚本语言中任选一种，轻松自定义自己的收集器和响应，从而实现最佳的可配置性和适应性。	McAfee Active Response 能够在可执行文件或正在运行的文件以外查找处于休眠状态的代码，甚至还有那些为了掩饰攻击者的动向而已经删除的代码。McAfee Active Response 可以搜索文件、网络流、注册表和流程图。
触发器	触发器使安全从业人员能够利用一套指令，持续监控现在和将来的重要事件或状态变化。	采取的操作是由事先设定的触发器发起的，随之会生成一个事件或执行响应。McAfee Active Response 能够超越静态的“窥视”，实现连续的响应模式。	McAfee Active Response 既可以发现当前的威胁，也能够在将来出现威胁时触发操作。
反应	在满足触发器条件的情况下，反应会给出一系列预先配置且可自定义的操作，让您能够搜寻并消除威胁。	反应允许用户采取操作，例如搜索通过文件哈希（MD5 和 SHA1）从系统中删除的文件，查看是否有任何主机主动连接到某个 IP 地址或过去曾连接到某个 IP 地址，或者搜索系统中未被访问或触发过且并非基于 PE 的恶意文件（在系统中搜索被复制到文件系统但是没有打开过的恶意 PDF）。	McAfee Active Response 预先配置为针对搜索结果采取操作，并调整用户指定的自定义操作以满足用户定义的特定需求。
通过 McAfee ePO 软件进行集中式管理	该单一控制台环境提供了全面的管理和自动化操作。	管理员可以将 McAfee ePO 软件用作 McAfee 集成安全体系结构的一部分，以促进对触发器和搜索的自动响应，并应对和缓解威胁。通过单一控制面板进行管理，能够在不增加额外管理负担的情况下，实现更好的安全监控。这能够为管理人员简化操作并减少时间投入。	通过单一控制台进行管理并采取操作，是一个非常明显的特色。使用单一控制台，我们能够通过一套强大的安全控件（包括 McAfee Active Response），为各种平台提供独特的保护。
集成安全体系结构	利用 Data Exchange Layer，简化了与 McAfee 旗下其他产品的通信。	作为 McAfee 集成安全体系的一部分，McAfee Active Response 通过该平台的创新型概念、优化的流程及实用的建议，可降低风险、缩短响应时间，并减少开销和运营人员成本。	

了解更多信息

要详细了解 McAfee Active Response 的优势，请访问 **www.mcafee.com/cn/products/active-response.aspx**。

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