# McAfee Advanced Correlation Engine

## 以您的侧重点为依据来检测威胁

当今各种捉摸不定的威胁给标准的基于规则的威胁检测带来了挑战。将 McAfee® Advanced Correlation Engine 解决方案与 McAfee Enterprise Security Manager 一起部署，可以通过基于规则和基于风险的逻辑对威胁事件进行实时识别和评分。只要您告诉 McAfee Advanced Correlation Engine 解决方案哪些是您的重要资产（用户或群组、应用程序、特定的服务器或子网），它就会在这些资产受到威胁时向您发出警报。审核跟踪和历史重播支持取证、合规及规则调整。

借助两种专门的关联引擎和针对特定用途的性能，McAfee Advanced Correlation Engine 解决方案对 McAfee Enterprise Security Manager 的事件关联功能进行了补充：

- 使用无规则的风险分数关联来生成风险分数的风险检测引擎
- 通过传统的基于规则的事件关联检测威胁的威胁检测引擎

独立的 McAfee Advanced Correlation Engine 解决方案提供了支持您整个企业中丰富的事件关联所需的处理能力。其数据引擎可以灵活扩展，即便是面对规模庞大的网络，也能够适应。

### 实时和事后威胁检测

既可以在实时模式下，也可以在历史模式下部署 McAfee Advanced Correlation Engine 解决方案。在实时模式下，McAfee Advanced Correlation Engine 解决方案一边收集事件一边对事件进行分析，以便能够即时检测到威胁和风险。

- 对实时事件数据的基于规则的关联可在威胁发生时检测到威胁
- 对实时事件数据的无规则关联可在威胁形成时检测到威胁

在历史模式下，收集的任何数据都能通过两种关联引擎进行“重放”，以实现递归的威胁和风险检测。当发现零日攻击时，McAfee Advanced Correlation Engine 解决方案可以回溯以确定您的组织在过去是否遇到过此类攻击，从而实现子零日威胁检测。

### 主要优势

- 简化启动过程：不需要进行规则更新、调整特征码或其他繁琐的操作
- 在发现针对您的优先用户、资产、应用程序和活动的威胁时发出警报
- 通过同时进行的基于规则和无规则的关联进行准确评分
- 可让您检查历史记录中新的攻击和漏洞，从而检测出过去的事件
- 向 McAfee Enterprise Security Manager 添加特殊化关联和处理资源
- 在设备和虚拟部署中均可用

## 按需分配性能

由于 McAfee Advanced Correlation Engine 解决方案是独立式设备或虚拟产品，因此在事件收集和事件管理方面，绝不会对 McAfee Enterprise Security Manager 的性能有丝毫影响。您可以完全充分地利用 McAfee Advanced Correlation Engine 应用程序的所有功能，同时最大限度地发挥 McAfee Enterprise Security Manager 这个实用工具的作用。

## 基于规则的事件关联

基于规则的关联采用传统的关联逻辑来实时分析收集到的信息。所有日志、事件和网络流都关联在一起，再结合上下文信息（如身份信息、角色、漏洞等），以检测出表明有更大威胁的模式。尽管所有 McAfee Enterprise Security Manager 解决方案均已直接支持整个网络中基于规则的关联，然而 McAfee Advanced Correlation Engine 解决方案提供了专门的处理资源可以关联更多数据，因此既可作为现有关联工作的补充，也能完全取代它们。

## 无规则的风险分数关联

尽管基于规则的关联对于任何传统的安全信息和事件管理 (SIEM) 而言都是一项必要且重要的功能，但这些系统只能检测已知的威胁模式，因此需要不断进行特征码调整和更新才能维持有效运作。解决方法是采用“无规则”关联技术作为传统事件关联的补充。在无规则的关联系统中，用简单的一次性配置替代检测特征码：只需告知 McAfee Advanced Correlation Engine 解决方案哪些是您企业的重要资产即可。这可以是特定的服务或应用程序、一组用户或者特定类型的数据。

## 实时跟踪和警报

在了解您企业的重要资产后，McAfee Advanced Correlation Engine 解决方案便开始跟踪这些项目的所有相关活动，以生成可根据实时活动而变化的动态风险分数。当风险分数超出某个阈值时，McAfee Advanced Correlation Engine 解决方案内会生成一个事件。此事件可用来提醒安全分析人员日益加剧的威胁状况，也可以被基于规则的传统关联引擎用作更大事件的条件。McAfee Advanced Correlation Engine 解决方案会保留风险分数的完整审核记录，以便能对一段时间内的威胁情况进行全面分析和调查。

## 使用案例

### 为企业风险建模

McAfee Advanced Correlation Engine 解决方案提供了一个平台，可有效地为企业风险建立模型。具有高级权限的员工访问高度机密的文档可能会对国防机构造成风险；而被诊断患有重大疾病的名人的病历如果泄露则可能对医院构成风险。McAfee Advanced Correlation Engine 解决方案通过对重要属性打分（制定一个基准并在超出正常阈值时发送通知），从而为您的组织提供无懈可击的风险模型。

### 对关键数据进行前瞻性风险评估

McAfee Advanced Correlation Engine 解决方案可监控实时数据，允许您同时使用两种关联引擎来检测风险和威胁，防患于未然。您可以在传统的关联逻辑中使用风险分数。例如，基于规则的传统威胁检测特征码可能是“发生在暴力登录事件之后的恶意软件事件”。一般情况下，当此特征码触发时，事件早已发生了。而现在，借助 McAfee Advanced Correlation Engine 解决方案，您可以引入一个风险系数，例如在发生暴力登录事件后将风险分数提高 20%。当系统注意到该事件时，McAfee Advanced Correlation Engine 解决方案可以针对即将发生的事件发出前瞻性警报，以便在造成损害之前采取干预措施。

### 递归威胁评估

识别威胁或发现数据泄露不算难事，只是我们不知道这些问题是否一直存在。只需在历史模式下部署 McAfee Advanced Correlation Engine 解决方案，便可通过传统关联引擎和无规则关联引擎重放其中设置的任何历史数据。

通过确定新发现的威胁是在何时首次出现的，就更有可能找出发生此状况的根本原因。

## 工作模式

**实时关联模式**

- 对实时事件数据的基于规则的关联可在威胁发生时检测到威胁
- 对实时事件数据的无规则关联可在威胁形成时检测到威胁

**历史关联模式：**

- 对历史事件数据的基于规则的关联可实现递归威胁检测
- 对历史事件数据的无规则关联可实现递归威胁评估

## 关联功能

- 同时使用基于规则的关联和无规则关联
- 为来自任何受支持数据源的数据建立关联
- 为各个分布式网络和收集器中的数据建立关联
- 包含数百种预定义的事件关联规则
- 包含适用于无规则关联的配置编辑器
- 包含易于使用的图形用户界面（GUI）事件关联规则编辑器，可用于自定义规则或创建新规则

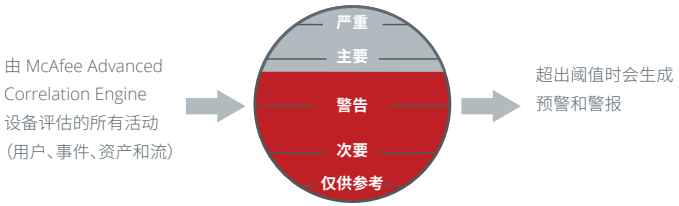


**图 1.** 基于风险的关联可帮助您检测优先资产中出现的威胁。

## 了解更多信息

有关详细信息，请访问 **www.mcafee.com/cn/products/siem/index.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

McAfee 和 McAfee 徽标是 McAfee, LLC 或其分支机构在美国和/或其他国家/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。
Copyright © 2017 McAfee, LLC. 41606ds_adv-corr-engine_1112B
2012 年 11 月