McAfee Application Data Monitor

利用应用层检测功能监视数据和检测隐藏的威胁

McAfee® Application Data Monitor 设备通过全程监控应用层的所有内容，可以使安全性和合规性不仅限于日志管理。您可以全面检查应用程序内容，以获得对网络使用情况最深入的了解。

McAfee Application Data Monitor 设备将整个应用程序会话解码到第 7 层，可提供从基础协议和会话完整性到应用程序本身的内容（如电子邮件的文本或其附件）等所有部分的完整分析。这一级别的详细信息可让您准确地分析真实的应用程序使用情况，同时还能让您实施应用程序使用策略，并检测出隐蔽的恶意流量。

这种深入检测通过跟踪网络上敏感数据的所有使用情况来实现合规性。当 McAfee Application Data Monitor 设备检测到违规行为时，将会保留该应用程序会话的所有详细信息，以用于事件响应、取证或合规性审核要求。

同时，通过 McAfee Application Data Monitor 设备可以查看可能伪装成合法应用程序的威胁：

- 高级应用层威胁
- 在未经授权的情况下使用或窃取机密数据
- 在安全“盲点”上发生或从安全“盲点”发出的攻击
- 使用危险的遗留代码
- 窃取或滥用用户凭据
- 通过任何应用程序传输敏感数据
- 业务流程中断

数据丢失和违反合规要求

McAfee Application Data Monitor 设备可以对电子邮件附件、即时消息、文件传输、HTTP POST 或其他任何应用程序中传输的敏感信息进行检测，并立即通知您以减轻损失。

主要优势

- 对数百个应用程序的整个应用程序会话进行解码，直到第 7 层
- 包含适用于受监管数据和敏感数据的预置检测规则
- 支持用户可定义的字典和规则以实现自定义
- 生成应用程序事件的完整审核记录以证明其合规性
- 被动式运行以避免应用程序干扰
- 与 McAfee Enterprise Security Manager 集成，从而允许在应用程序内容与事件和其他数据源之间建立关联
- 灵活的混合交付选项包括物理设备和虚拟设备

您可以使用现成的功能来检测敏感数据(如信用卡信息和身份证号),也可以通过定义您自己的敏感和机密信息字典,来对 McAfee Application Data Monitor 设备的检测功能进行自定义。McAfee Application Data Monitor 设备将检测这些敏感的数据类型,向相关人员发出警报,以及记录违规行为以维护审核记录。

文档发现

McAfee Application Data Monitor 设备可发现 500 多种文档类型,这些文档在网络上通过电子邮件、聊天、P2P、文件共享及其他方式进行交换。不论文档采用何种扩展名,McAfee Application Data Monitor 设备都能发现,包括伪装成其他类型并试图绕过邮件网关和入侵检测系统 (IDS)/入侵防御系统 (IPS) 设备的文档。即便是嵌入到其他文档中的文档,以及经过存档、压缩和编码的文档均可借助具有可操作性的指标(如文件名和所执行的操作)来发现。

应用层威胁

复杂的新型威胁可以利用常见企业应用程序中的漏洞渗透到您的网络并导出敏感数据。虽然这些应用层威胁很难使用传统防火墙、IDS 和 IPS 检测出来,但 McAfee Application Data Monitor 设备能够监视应用程序的完整内容(包括基础协议),从而检测出隐藏的负载、恶意软件甚至隐蔽的通信通道(例如 PDF 文档中嵌入的可执行文件)。

协议异常

异常检测可以主动识别即将发生的威胁,从而降低风险和最大限度地减少损失。某些传统安全解决方案仅对网络流进行分析,而 McAfee Application Data Monitor 设备将此方法推向了更高层级。我们通过查看过去的网络行为来检测应用程序和协议中的异常,从而提供了一套更强大、更具前瞻性的风险检测方法。

不会对应用程序产生任何干扰

由于 McAfee Application Data Monitor 设备在 SPAN 端口上运行,因此不会对应用程序性能或可靠性造成干扰,也不会导致延迟。

与您的基础设施集成

大多数网络监控解决方案都是单独运作的,而 McAfee Application Data Monitor 设备可与其他信息安全系统协同工作。借助 McAfee Enterprise Security Manager,它可以与安全基础设施的其他组件建立连接,以简化安全操作、提高整体效率并降低成本。您可以将数据丢失和欺诈检测与强大的分析、网络检测及数据库事件监控等功能集成在一起。

示例用例

McAfee Application Data Monitor 设备可以检测各种未经授权的活动、违反策略、窃取和欺诈行为。以下是一些示例。

支持 500 多种应用程序和协议

- **底层网络协议:**TCP/IP、UDP、RTP、RPC、SOCKS、DNS 等
- **电子邮件:**MAPI、NNTP、POP3、SMTP、Microsoft Exchange
- **Web 邮件:**AOL Webmail、Hotmail、Yahoo! Mail、Gmail、Facebook 和 MySpace 电子邮件
- **即时消息:**AOL、ICQ、Jabber、MSN、SIP 和 Yahoo
- **文件传输协议:**FTP、HTTP、SMB 和 SSL
- **压缩和解压缩协议:**BASE64、GZIP、MIME、TAR、ZIP 等
- **存档文件:**RAR 存档文件、ZIP、BZIP、GZIP、二进制到十六进制文件和 UU 编码存档文件
- **安装包:**Linux 安装包、InstallShield CAB 文件、Microsoft CAB 文件
- **映像文件:**GIF、JPEG、PNG、TIFF、Auto CAD、Photoshop、位图、Visio、数字原始图像和 Windows 图标
- **音频文件:**WAV、MIDI、RealAudio、Dolby Digital AC-3、MP3、MP4、MOD、RealAudio、SHOUTCast 等
- **视频文件:**AVI、Flash、QuickTime、Real Media、MPEG-4、Vivo、Digital Video (DV)、动态 JPEG 等
- **其他应用程序和文件:**数据库、电子表格、传真、Web 应用程序、字体、可执行文件、Microsoft Office 应用程序、游戏和软件开发工具
- **其他协议:**网络打印机、Shell 访问、VoIP 和 P2P

窃取机密信息

某位员工使用 zhangsan@company.com 登录后，向 lisi @gmail.com 发送了一封电子邮件。该电子邮件包含一个名为 shoo.doc 的文件，而文件中含有“秘密配方”字样。该电子邮件于中午 12:20 通过 SMTP 服务器 (10.0.2.13) 从主机台式机 0232 (192.168.0.36) 发出，主题为：got it（拿到了）。

使用未经授权的应用程序

某位员工违反策略，使用自己安装的对等文件共享应用程序传输音乐文件。他在工作时间发送大文件，结果占用了宝贵的带宽。而进一步调查显示该员工经常违反策略。他在自己的桌面机上使用 Jabber 和 IRC，并且运行未经授权的 Web 服务器。

在工作场所办私事

某位员工偷偷在网上进行短线当日交易。在工作日，她每天上午和下午都会平均花一个小时连接到金融交易网站。她还利用公司的 VoIP (SIP) 系统平均每天拨打六次电话，并且在 Yahoo! Messenger 上以“张三”的身份与“李四”和“王五”交谈好几个小时。

使用强度较弱的密码

您公司的安全策略要求所有用户系统和应用程序帐户都必须使用高强度密码。Microsoft Active Directory 帐户已受到严格管理。但是在不使用 Active Directory 的面向外部的 FTP 服务器、邮件服务器和关键 Web 应用程序上，使用了许多强度较弱的密码。

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

61322ds_app-data-monitor_0914
2014 年 9 月