solarwinds®

# SolarWinds Log & Event Manager（日志与事件管理器）

基于TriGeo®


## 您的日志文件看起来从未这么好过...或提供过如此多的信息！

会见我们家庭的最新成员：SolarWinds Log & Event Manager（日志与事件管理器），一款基于TriGeo®技术的新产品。这款强大的产品结合了实时日志分析、事件关联以及特别查询，以提供您所需的可视化、安全性和控制功能。

最后，您可以宣称此款产品部署起来如此简单却完全能胜任IT运营、合规性以及安全性挑战，您势必会雀跃万分。忘掉昂贵、复杂的解决方案，同时仍可拥有日志采集、日志分析和事件管理等丰富功能——而且价格实惠到让您大跌眼镜！

## SolarWinds Log & Event Manager（日志与事件管理器）的亮点：

- 解决性能和可用性问题，针对数以百万计的文件与事件提供可见性，迅速地识别异常情况。
- 利用“经审计验证”符合每个审计机关施加的安全性监控和日志管理需求的合规方案，确保符合PCI、HIPAA、NCUA、GLBA、NERC-CIP、FISMA、SOX等要求或自己公司的政策。
- 通过300多份报告和开箱即用的合规数据包快速、方便地生成合规报告
- 横贯整个基础设施执行积极的日志分析和实时事件关联，快速识别攻击，突出威胁，并查出违反政策的行为。
- 通过前所未有的关联引擎对网络、系统、应用程序、虚拟机和存储设施中数以百万计的事件以实时、内记忆、非线性和多维式的方式进行关联
- 采用Word Cloud（词汇云）、树图、气泡式图表和柱状图等形式提供直观的搜索界面，可视化搜索数据以及了解如何采取行动
- 通过Active Reponses，自动采取行动对服务、流程、账户和特权进行隔离、阻断、选择路径以及控制，保护您的基础设施，从而减轻威胁
- 通过实时检测和弹出USB驱动器的方式保护敏感数据
- 采用高性能、高压缩数据模式，以60:1的比例存储数据，实现TB级日志数据存储无需购买额外的存储设备
- 部署SolarWinds Log & Event Manager（日志与事件管理器）可在几小时内完成——无需顾问的帮助
- 享受对数十家厂商、数百种产品以及上千款模型的支持

# SolarWinds Log & Event Manager（日志与事件管理器）的特点

## 主动的日志分析

在如今的IT环境下，您一不小心就会淹没在浩瀚的日志数据中。您的基础设施中的众多分布系统、应用程序和网络都有相关联的日志文件，但是，如果您不能有效地对其进行收集和分析，这些信息便毫无价值。

SolarWinds Log & Event Manager（日志与事件管理器）不仅提供实时记录分析，同时还传送可视化的交互式数据和内置知识，对各种设备和应用程序的日志进行自动收集、标准化和翻译处理。这意味着您能立刻识别出感兴趣的事件并采取行动。告别成堆无用的数据，迎来简化的日志分析！

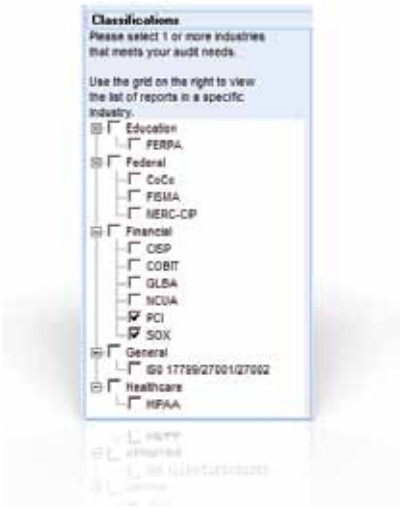
## 实时事件关联

对网络、系统、应用程序、虚拟机和存储设施成千上万的事件实施关联是多么可怕的工程...但有了SolarWinds Log & Event Manager（日志与事件管理器），动动指尖即可轻松实现。前所未有的关联引擎竭尽全力为您服务，它是实时、内记忆、非线性和多维的方式协助工作。此等价位绝没有其他解决方案能保证有如此的功效和灵活性！

内置近700种关联规则，SolarWinds Log & Event Manager（日志与事件管理器）提供开箱即用的可见性，减少您的工作时间。但我们理解您同样需要适合您的具体环境的规则。于是我们创建了令人难以置信的简单关联规则生成器，采用图形界面让IT管理员轻松快速地建立自定义规则。最后，您完全可以毫无费力地获取强大的关联性！

## 专门的IT搜索

我们理解您没有时间筛选海量的日志事件和数据源...同时也了解很多工具仅仅提供令人失望的搜索工具栏，并没能真正地识别重要数据。SolarWinds Log & Event Manager（日志与事件管理器）通过升级工具栏为您提供高级搜索功能，确保您能对事件实施有效精细的分析。




利用直观的搜索界面，您能够立即洞察一些通常被忽视的活动。独一无二的Word Cloud（词汇云），加上树图、气泡式图表和柱状图的使用，SolarWinds日志与时间管理器（Log & Event Manager）提供一个完全交互式的搜索环境，使可视化数据搜索与理解如何采取行动变得容易，工作起来事半功倍。另外，得益于我们在数据族聚、归档和加密上的创新手段，完成TB级数据搜索的速度之快（和安全性）定会令您惊叹不已。

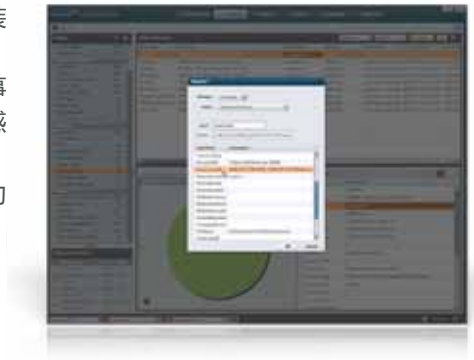
## 合规报告

我们理解合规报告是您最不喜欢的活动之一，因此我们建立了300多份“经审计验证”的合规报告，必令您惊喜万分。无论所需遵守的是哪项缩写法案 （PCI DSS、GLBA、SOX、NERC CIP或HIPAA，等等）内置报告控制台均能轻松地生成报表并提供图形摘要。您甚至可以定期生成报告，并以多种格式导出，让您的工作更轻松。并且您可以放心，SolarWinds Log & Event Manager（日志与事件管理器）同样符合所有主要审计机构施加的安全性监控和日志管理规定。

### 积极响应与减轻威胁

若检测到威胁，您必须立即作出响应，以防止灾难出现。SolarWinds Log & Event Manager（日志与事件管理器）的诞生将成为恶意程序、零日攻击和蠕虫病毒这些给基础设施造成严重破坏的黑客行为的倒霉时刻。内置Active Responses，需要减轻威胁和采取行动时即可自动响应，诸如隔离受感染机器、阻止IP地址、禁用用户账户、终止未授权进程、重启服务，等等。

### USB检测与防护



USB设备是IT管理员的噩梦；千兆字节的敏感数据可以装在地铁代币大小的设备上带出门。为了防止数据丢失，我们给SolarWinds Log & Event Manager（日志与事件管理器）植入了跟踪USB活动和辨别未授权运行或敏感文件复制的技术。事实上，该产品可以支持实时通知、禁用用户账号、隔离工作站或甚至自动弹出USB驱动等功能。它就像无声的守卫者，捍卫您最宝贵的数据！

### 长期日志存储

如何存储TB级的日志数据，是众多IT部门的一大难题。然而，花更多的钱来购买更多存储设备，可不是闹着玩的。SolarWinds Log & Event Manager（日志与事件管理器）采用高性能、高压缩的数据模式，以60:1的比例和极快的速度存储数据。这意味着能够解决存储大量合规性数据的需求，同时消除添购额外储存设备的烦恼。此外，还能享受多年在线数据存取服务！

### 快速与轻松的执行

我们以提供可轻松、快速部署的产品为骄傲，SolarWinds Log & Event Manager（日志与事件管理器）也不例外。启动和运行此产品无需借助顾问团队或花费周末时间来通读枯燥的用户指南。通常被描述为“以午餐为生”，SolarWinds Log & Event Manager（日志与事件管理器）只需花几小时即可开始提供可见性和完成需要的保护。

### 直观的界面

直观的界面是简化产品使用的关键。SolarWinds Log & Event Manager（日志与事件管理器）提供您所渴望的优越的可用性与易用性。控制台的设计旨在给您提供可视化的日志和时间数据，从而能直接采取行动而无需花数小时来筛选数据。它同时还支持拖放和点击功能，数据分类更简单，无需学习复杂的查询语句。

### 全面支持种类众多的数据源

SolarWinds Log & Event Manager（日志与事件管理器）内置多样性支持，符合当今IT环境的主题。支持数十家厂商、数百种产品以及上千款模型。SolarWinds Log & Event Manager（日志与事件管理器）集成了每个主要类别中最佳的产品功能，而且每周都进行添加更新。

“这是迄今为止我见过最好的SEIM系统，更谈不上拥有了。各个方面都完全符合产品描述，甚至超出预期！采购、安装、支持和培训等各方面都令我非常满意。”

- Lou Porreco,
Windsor管理集团 技术总监