NetIQ

客户成功案例

Sentinel
Sentinel Log Manager
Access Manager
Identity Manager
eDirectory

戴顿大学

由于该大学的计算环境十分多样化，IT 员工无法执行实时数据分析，也无法创建足够的报告来确保支付卡行业 (PCI) 安全合规性。戴顿大学在 NetIQ® Sentinel™ Log Manager 中找到了解决方案。它平均每天已经记录、分析和响应 300 万次安全事件。

概述

《美国新闻与世界报道》(U.S. News & World Report) 将戴顿大学誉为全国十佳天主教大学之一。戴顿大学于 1850 年建立，它通过基于社区的鞭策和鼓励，努力从各方面培养学生。

挑战

戴顿大学的 IT 部门负责保护敏感信息，如 12,000 多名学生和 3,000 多名教职工的信用卡交易信息和个人数据。“一次安全危害的财务成本可能就会非常巨大，”戴顿大学首席系统工程师 Randy Hardin 说道。“但同等重要的是，我们需要保护技术资源，而又不能防碍自由通讯，自由通讯可是教育体验必不可少的组成部分。”

“Sentinel 和 Sentinel Log Manager 的关键优势是明确将安全事件与单独身份关联的能力…”

RANDY HARDIN
首席系统工程师
戴顿大学

该大学有一台中央日志服务器，用来收集整个网络上的安全事件，但它无法汇总数据并执行实时分析。“我们有一大堆数据，但却无法找到对安全原因真正重要的那些数据，”Hardin 说道。该大学需要有效的方法来分析数据并简化报告创建，以符合支付卡行业 (PCI) 的相关法规。

解决方案

该大学平均每天已经使用 NetIQ Sentinel 来检测和记录 300 万次安全事件。IT 小组部署 Sentinel Log Manager 来简化并加快对日志数据的分析。

“我对 Sentinel Log Manager 的出现感到非常兴奋，”Hardin 说道。“这正是我们要找的解决方案，而且我们相信，它会在我们的环境中集成得很好。我们以前研究过一些开放源代码日志记录和分析产品，以及一些商业解决方案。很多其他的解决方案侧重于个别系统。这些解决方案的功能完全不够广泛，不适合我们多样化的计算环境。只有 Sentinel Log Manager 具备我们需要的灵活性。它使我们能按

UNIVERSITY of DAYTON

概况

行业
教育

地点
俄亥俄州

挑战
该大学需要有效的方法来分析日志数据并简化报告创建，以符合 PCI 的相关法规。

解决方案
使用 Sentinel Log Manager 轻松高效地分析日志数据。

成果
+ 提醒安全小组注意潜在威胁
+ 几乎瞬间即可执行审计

“由于实施了 Sentinel，我们能够更深入地了解潜在安全问题。”

RANDY HARDIN
首席系统工程师
戴顿大学

www.netiq.com

任何参数查看所有信息，以及提取至关重要的安全信息并理解其意义。”

戴顿大学对 Sentinel 同样印象深刻，它利用 Sentinel 从其防火墙、入侵检测系统、NetIQ eDirectory™ 条目、NetIQ Identity Manager 和 NetIQ Access Manager™ 中收集安全相关事件。“Sentinel 和 Sentinel Log Manager 以及 Identity Manager 结合的关键优势在于，能够明确地将安全事件与单独身份关联，这对实现 PCI 合规性而言非常重要，”Hardin 说道。

“Sentinel 和 Sentinel Log Manager 的自定义程度非常高，”Hardin 说道。“我可以选择对我而言重要的特定属性，并一眼看清发生了什么情况。我们还可以创建自定义仪表板来进行管理，这样就可以轻松了解我们的合规性状况和总体安全态势。”

成果

Sentinel 一直工作良好，提醒安全小组注意潜在威胁。“自实施 Sentinel 后，我们对潜在安全问题有了更好的了解，”Hardin 说道。“如果未授权人员试图访问服务器，我能够在几秒钟内看到整个事件。它如此出色的工作真令人兴奋。”

这个完全集成的解决方案快速分析海量数据，并聪明地只报告重要的安全事件。“有了 Sentinel 和 Sentinel Log Manager，我们可以非常快速地分析来自不同来源的数据，并将安全事件关联到单独的身份。”

以前，单独查询的审计要花 20 分钟时间，但现在，IT 员工几乎瞬间即可执行审计。因此，该大学的安全调查变得更加高效。“作为安全调查的一部分，每隔几个礼拜，我小组的几个成员就要花一整天时间手动关联事件，”Hardin 说道。“现在我们有了 Sentinel Log Manager，我们执行安全调查的速度加快高达 90%。”

戴顿大学对该解决方案的性价比非常满意。“Sentinel Log Manager 不仅出色完成了对我们扔给它的海量数据进行分析的工作，”Hardin 说道。“而且在今年内，它就能通过缩短的管理时间轻松收回成本。”

NetIQ
北京络威尔软件有限公司
中国北京市朝阳区东三环中路 7 号
北京财富中心写字楼 3603 室
电话：8610 65339000

info@netiq.com
www.netiq.com/communities
www.netiq.com

有关我们在北美，欧洲，
中东，非洲，亚太平洋和
拉丁美洲的办公室详细列表，
请访问 **www.netiq.com/contacts**

www.netiq.com