New York City Health and Human Services

The agency wanted to break down the information silos around its nine agencies. It needed a way to monitor security events to prevent policy violations and ensure regulatory compliance. With the use of NetIQ® Sentinel™ Enterprise and Micro Focus® Log Manager, the agency has significantly improved their reporting and auditing capabilities while minimizing the risk of security breaches.

Overview
New York City Health and Human Services maintains software and technology platforms that support 80,000 people in nine agencies, each operating its own solutions. The agency needs to demonstrate compliance with numerous state and federal regulations that protect personal information.

Challenge
New York City Health and Human Services Connect (HHS-Connect) needed to break down the silos between the nine agencies for which it develops and maintains applications and technology platforms. "Each agency built its own solutions to suit specific business problems," said Lou Sell, chief architect for New York City Health and Human Services. "We needed to monitor security events from all of these systems to prevent policy violations, but manually reviewing and correlating logs would have taken an inordinate amount of time."

Multiple laws govern the proper use of the agency's data. "To ensure compliance with these regulations, we needed to correlate security logs and transactions across systems to gain a comprehensive view," said Joe Fleischman, project manager in the office of the CIO for New York City Health and Human Services. "We also have many security filtering policies that determine which individuals at which agencies can access certain data. We needed a way to effectively track those policies.

Solution
After researching a number of commercial and custom solutions, HHS-Connect chose Sentinel Enterprise and Sentinel Log Manager to monitor its IT systems in real time. "Building a custom solution would have cost hundreds of thousands of dollars, and would have been extremely difficult and costly to maintain," said Fleischman. "Plus we would very likely have had to replace the custom solution after a few years when it no longer fulfilled our need. We found Sentinel and Sentinel Log Manager to be extremely customizable. We can easily pull in the right data fields and correlate that data to glean the information we need."

“Tracking these logs manually would have required a minimum of 20 additional staff and would have been far less effective.”

JOE FLEISCHMAN
Project Manager, Office of the CIO
New York City Health and Human Services

At a Glance
- **Industry**: Healthcare and Medical
- **Location**: United States
- **Challenge**: The organization needed to monitor security events from all of these systems to prevent policy violations.
- **Products and Services**: Sentinel Enterprise
  Sentinel Log Manager
- **Results**: + Provided the ability to quickly identify and respond to any system anomalies and potential policy violations + Improved reporting and auditing capabilities + Reduced IT workload through automation
HHS-Connect worked with Accenture, a global market leader in technology, consulting and outsourcing and a business partner, to implement the solution. “We have hundreds of different logs being generated across our systems,” said Fleischman. “Accenture devised a strategic plan to identify the most valuable logs and highest severity events to monitor. The Accenture team built the connectors to various application databases so we can centrally monitor security activities. The project was a success and was completed on time. We attribute that to Accenture and to the solutions.”

HHS-Connect now uses Sentinel Enterprise to detect and log daily security events, including application transactions, web service calls and authentication events. The agency uses Sentinel Log Manager to collect and analyze its log data. The software makes it easy to quickly recognize anomalies and potential policy violations. “We now have a single point of control for collecting and analyzing logs,” said Fleischman. “That makes it much easier to gain a holistic view of our environment and proactively monitor any potential security issues.”

**Results**

“Sentinel and Sentinel Log Manager help us make sense of data from myriad sources, so we can quickly identify and respond to any system anomalies and potential policy violations,” said Fleischman. “I don’t know how we would have accomplished this type of sophisticated monitoring solution without them.”

The solutions work well in the agency’s heterogeneous IT infrastructure. They also proved to be a good investment for HHS-Connect’s complex environment. “Sentinel and Sentinel Log Manager have already paid for themselves,” said Fleischman. “Tracking these logs manually would have required a minimum of 20 additional staff and would have been far less effective for safeguarding data and ensuring security.”

HHS-Connect has also improved its reporting and auditing capabilities. “Using Sentinel and Sentinel Log Manager, we’re better prepared for audits and can minimize the risk of security breaches,” said Fleischman. “If, for example, an authorized user misuses our systems, we can quickly identify and stop this behavior.”

换句话说：

HHS-Connect与Accenture合作，Accenture是一家全球领先的科技公司，提供咨询服务和外包业务。Accenture是一家业务合作伙伴，共同实施解决方案。“我们有数百种不同的日志被跨系统生成。”Fleischman说。“Accenture制定了一项战略计划，以识别最有价值的日志和最高严重性事件进行监控。Accenture团队建立了到各种数据库的连接器，以便我们能够集中监控安全活动。项目取得了成功，并按时完成。我们把这归功于Accenture和解决方案。”

HHS-Connect现在使用Sentinel Enterprise来检测和记录每日的安全事件，包括应用程序交易、Web服务调用和身份验证事件。该机构使用Sentinel Log Manager来收集和分析其日志数据。软件使快速识别异常和政策违规变得容易。

**结果**

“Sentinel和Sentinel Log Manager帮助我们从众多来源中整理数据，因此我们可以快速识别并响应任何系统异常和政策违规。”Fleischman说。“我不确定没有它们我们如何能够实现这种复杂的监控解决方案。”

这些解决方案在该机构的异构IT基础设施中运行良好。它们也被证明是该机构复杂环境中的一项良好投资。“Sentinel和Sentinel Log Manager已经支付了自己。”Fleischman说。“手动跟踪这些日志需要至少20名额外的人员，并且效果远不如能够有效保护数据和确保安全。”

HHS-Connect还提高了其报告和审计能力。“使用Sentinel和Sentinel Log Manager，我们为审计和可以减少安全漏洞的风险进行了更好的准备。”Fleischman说。“例如，如果授权用户误用我们的系统，我们可以快速识别并阻止这种行为。”