NetIQ

客户成功案例

Sentinel
Identity Manager
Access Manager

国家电网上海市电力公司

通过与 NetIQ Identity Manager 紧密集成，Sentinel 显著增强了安全性，从而提高生产力并节省成本.

概述

国家电网上海市电力公司 (SGCC) 负责生产和配送通过煤炭、天然气、整体煤气化联合循环 (IGCC)、风力和太阳能产生的电力。该公司于 1985 年在中国上海成立。上海市电力有限公司是中国国家电网公司的子公司。

挑战

上海电力长期以来一直使用 NetIQ Identity Manager 和 Access Manager 为其 3.4 万用户提供统一的身份管理解决方案。在近几年，安全性已成为日益严重的问题，而犯罪分子一直在通过数据漏洞主动收集信息，这造成了收入损失。

“通过引入 Sentinel，我们能够将 IT 安全人员从五人减少到仅两人。让安全数据触手可及意味着我们对任何安全漏洞的响应速度可以提高 80%，并且我们将安全事件总量减少了 50%。”

卢士达先生
总监
国家电网上海市电力公司

虽然上海电力已通过现有的安全系统来保护其业务系统和统一身份管理系统，但该解决方案并不能令人满意，正如上海电力总监卢士达先生所言：“我们无法以集中的方式报告数据，所有数据都分散在不同的系统当中。这意味着当我们发现安全威胁时，我们的安全管理员需要检查每个业务系统的日志。这样做需要太长的时间；在这段时间内，安全漏洞可能会对我们的业务造成不可估量的损害。这种耗时的手动流程意味着我们无法满足合规性监管要求，并因此受到了处罚。”

上海电力需要一种解决方案来帮助快速识别数据漏洞和数据窃取行为。它还需要支持突出显示帐户密码漏洞以及审计“僵尸”的帐户（未处于活动状态但面临安全风险的帐户）。作为现有的 NetIQ 身份和访问管理客户，它要求将安全解决方案与统一身份管理解决方案相集成，这一点至关重要。

解决方案

上海电力对市场进行了调查，旨在寻找一种可与 NetIQ 身份和访问管理系统相集成的敏捷式、可缩放的高性能安全解决方案。上海电力对 NetIQ Sentinel 以

国家电网公司 STATE GRID CORPORATION OF CHINA

概况：

- **行业：**
  公用事业
- **位置：**
  中国
- **挑战：**
  替换手动的且耗时的安全解决方案，它使上海电力面临违规并因此受到处罚的风险。新解决方案需要与负责管理 20 万用户的现有 NetIQ 统一身份管理系统紧密集成，可提供成熟的报告和审计功能。
- **解决方案：**
  使用 Sentinel 提供可缩放的高性能安全解决方案。
- **成果：**
  + 将 IT 安全人员从五人减少到两人
  + 将安全事件响应时间缩短了 80%
  + 将安全事件减少了 50%
  + 将安全原因导致的收入损失减少了 90%
  + 增强了合规性、监控和审计功能

“Sentinel 与 NetIQ 统一身份管理系统之间的本机集成使我们能够引入更多安全功能，而无须更改我们的体系结构。”

卢士达先生
总监
国家电网上海市电力公司

www.netiq.com

及 EMC eVision 和 IBM Qradar 进行了评估。EMC eVision 以折扣价格销售，因为该软件通常与 EMC 硬件捆绑在一起。它并不包含审计和报告模块，对于上海电力而言该模块非常重要，事实证明它是一种成本高昂的选项。虽然对 IBM 解决方案感兴趣，但上海电力还是担心 IBM 在中国缺少支持服务以及欠缺项目交付能力。

卢士达对决定采用 NetIQ Sentinel 评论道：“Sentinel 与 NetIQ 统一身份管理系统之间的本机集成使我们能够引入更多安全功能，而无须更改我们的体系结构。Sentinel 组件可以缩放并且可轻松扩展，能够满足我们的任何未来需求。实施 Sentinel 非常简单，我们能够快速启动并运行。”

该解决方案可以为关键的应用程序系统创建每日报告，并对绕过统一身份管理系统的用户进行审计，然后向安全小组发送警报。该系统会在每个季度生成一份报告来突出显示未使用的帐户，以便能够关闭这些“僵尸”帐户。

由于需要对 3.4 万用户进行管理，了解用户系统访问过程中的“人员、事件、时间、地点和方式”对于控制内部风险至关重要。Sentinel 将安全数据与唯一的用户身份信息相集成，以帮助上海电力快速识别存在风险的访问行为。为了对上海电力的合规性现状提供支持，Sentinel 简化了安全事件的收集，以便自动执行合规性审计和报告功能，并显著降低查找和准备审计员所要求数据的复杂性、时间和成本。

成果

增强了整个上海电力基础设施的安全性，同时降低了安全管理成本和人力成本，正如卢士达先生所言：“通过引入 Sentinel，我们能够将 IT 安全人员从五人减少到仅两人。让安全数据触手可及意味着我们对任何安全漏洞的响应速度可以提高 80%，并且我们将安全事件总量减少了 50%。这使得由安全漏洞造成的经济损失减少了 90%。”

他总结道：“通过实施 Sentinel，我们可以轻松确保始终遵循安全法规。借助清晰透明的系统，我们能够快速识别并响应任何安全威胁。监控和审计变得非常简单。通过 NetIQ 解决方案之间的关键集成，我们能够管理“僵尸”帐户并深入了解所运行的每个应用程序的用户访问权限。NetIQ 在整个过程中为我们提供支持，我们期待继续合作下去。”

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