

Tivoli Security Operations Manager 产品解决方案:

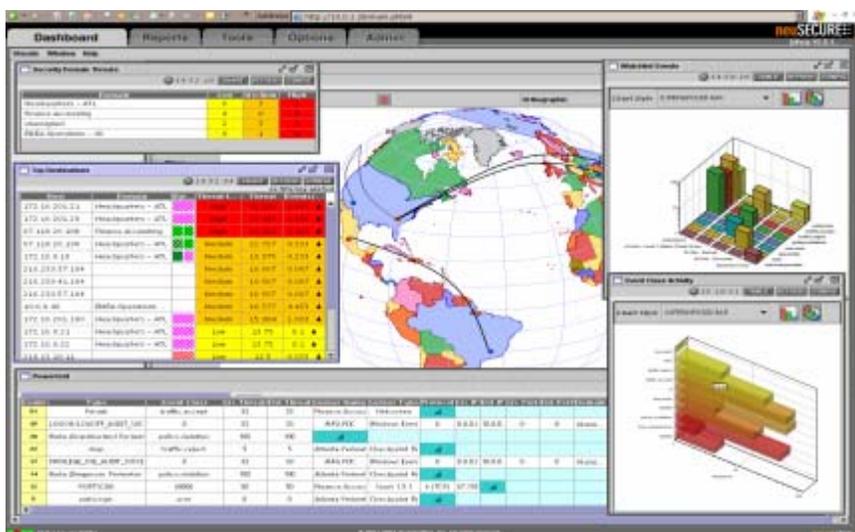
集中企业的安全性和遵从性管理，提供强大的风险可视性

由于不具备可视性和完整的解决方案，企业在进行安全和风险管理时可能遇到如下的问题：

- 难以对访问系统的用户及其行为进行全程的监控、追踪、与定位
- 无法对所有用户进行监控和审计，难以及时的发现入侵与违规行为
- 难以对现有的安全日志和收集的事件进行综合的分析，以发现潜在的安全隐患和满足制度法规遵从与审计的需求

解决方案的价值

- 即时、跨资源的企业安全信息的平台
- 提高信息安全和风险管理工作的效率和可视性
- 评估企业IT资源的总体安全性和制度遵从状态



安全事件管理解决方案

- 整合的安全视图来管理复杂的安全环境
- 即时、跨资源的安全事件收集和关联分析能力来提高安全事件的认识度，实时发现潜在的安全隐患
- IT 流程优化:信息共享(NOC, SOC, Help Desk) 将安全运行与其它 IT 部门紧密集成在一起

● 实现功能

智能显示板来管理复杂的安全环境

跨设备的实时事件关联可提高事故辨别能力

安全事件集中收集和标准化

基于规则和数据模型进行事件关联分析，包括

- ✓ 基于统计的关联
- ✓ 基于规则的关联
- ✓ 基于安全漏洞的关联
- ✓ 基于敏感性的优先级关联处理

自动响应和故障报警处理

通过自动化来提高安全操作人员的工作效率

客户化的审计报告，趋势分析和依从性报告