医疗防统方系统

**防“非法统方”、完整追踪取证**

**产品概述**

捷普医疗防统方系统是交大捷普自主研发的专业医疗防统方产品，该产品结合了捷普在众多医疗反统方项目的实践经验和多年数据库安全领域的技术积累，完全符合卫计委对医疗统方行为的监管要求。

捷普医疗防统方系统提供事前、事中、事后三个层次的统方行为识别与监控，能够检测、记录、审计、还原各类统方访问行为，包括HIS应用访问、系统维护人员访问以及对服务器的远程telnet、ftp访问等，及时发现、告警并阻止各类违规操作，杜绝恶意人员非法统方行为。



**医院防统方面临困境：**

**统方回扣诱惑大：**统方回扣往往会达到药品零售额的10%至30%，非法获利空间非常大，导致医疗从业人员愿意铤而走险获取统方信息。

**非法“统方”途径多：**非法统方可能是医院工作者、医疗系统开发维护人员、医院数据库管理员，或者黑客，堵漏难度很大。

**国家政策要求日益严格：原**卫生部曾在2006、2010、2012、2014年数次发文，明确要求加强信息系统监管，防止非法统方，并追究刑事责任。

**产品特点**

**传统防护手段捉襟见肘：**传统采用数据库自身审计功能，这对系统性能影响较大，且审计权限和操作权限没有分离，维护人员众多，导致审计工作繁琐、不准确，审计信息易被篡改和泄漏。



**全面的统方身份判断**

捷普医疗防统方系统能够结合认证系统及访问请求信息，全面的定位出违规统方的人员信息，包括：医院内部人员违规操作、第三方开发或维护人员安全隐患、内部系统管理员和超级用户等操作、远程或移动终端接入违规操作、黑客入侵访问等。

**专业的统方手段识别**

捷普医疗防统方系统实时监控来自各个层面的统方行为，可准确识别各种统方手段，如：来自HIS应用程序发起的数据库操作请求、来自数据库客户端工具的操作请求等、来自专业医疗统方工具的数据库请求以及通过远程命令行方式运行的SQL命令。

**精准的统方人员定位**

捷普医疗防统方系统可以对IP、MAC、操作系统用户名、数据库账户、应用账号、使用的工具、等一系列要素进行关联分析，从而精准追踪到具体科室、姓名、位置等信息。

**完整的统方行为还原**

捷普医疗防统方系统通过定向行为分析，可以明确出在某段时间内所有的统方操作，并进行完整的过程回放。通过对特定行为精确回放，如执行删除表、文件命令、数据搜索等，真实再现完整操作过程，进行电子取证，为违规统方溯源提供有力的证据。

**易用的设备运维管理**

捷普医疗防统方系统提供向导帮助和规则模板服务，0基础客户也能快速完成自助化配置上线服务；同时提供可视化统方报表，帮助管理人员快速掌握统方事件风险现状和综合态势。

**产品功能**

* **“八元组“精确定位统方人员**

同时支持业务系统帐号、数据库帐号、操作系统用户名、客户端主机名、客户端程序名、IP、MAC、时间等”八元组“信息采集，在复杂环境下也能够精确定位到具体人员。

* **访问控制防止非法统方**

通过字段组访问控制实现“统方”防御。对同时出现“药品”+“剂量”+“医生”或“单价”+“总价”+“医生”等查询进行授权控制，防止非法统方。

* **操作回放防止抵赖行为**

对于可疑统方操作，通过回放整个过程，可以看到真实输入及屏幕显示内容，提供对特定行为精确回放，如执行查询、增加、删除等，防止对违规统方的抵赖行为。

* **全面的统方识别能力**

支持识别和审计各种常见的医院应用系统及医疗终端应用统方行为，能够对HIS、LIS、PACS、RIS、健康档案等医疗应用全面审计，统方识别能力业界领先。

* **细粒度的操作行为审计**

能够识别HIS等应用系统和移动端数据库操作的全部要素，基于数据库语义的深度分析，能够对请求、执行、返回等内容提供双向的全面深度审计，准确的定位违规统方行为。

* **强大专业的统方审计能力**

同时支持C/S和B/S架构HIS应用，能够对二层和三层架构同时审计，具备捷普独有的三层审计智能关联技术专利，通过多层关联技术，能够快速还原用户行为，锁定异常统方行为；同时支持对SSL加密流量、绑定变量、64K超长SQL进行审计，审计专业性行业领先。

* **全方位实时风险控制**

内置专门的统方知识库，能够根据姓名、工号、IP、药品、剂量、时间、命令等多种要素来灵活制定风险事件和控制策略；支持通过自动建模的方式快速识别异常违规“统方”行为；提供实时的短信、邮件、Syslog、SNMP等多种告警方式，及时预警和控制风险行为。

* **自助化的设备配置向导**

提供向导帮助和规则模板服务，利用基本向导、业务向导、统方知识库、审计模板等功能帮助零基础客户快速完成自助化配置上线服务。

* **简单智能的审计报表**

提供预定义和自定义报表模块，快速生成统方事件报表和风险趋势报告，同时支持输出防统方综合报表，支持以PPT、PDF、WORD、EXCEL、HTML等格式导出相关报表。

* **分布式集中监控**

提供防统方统一监管平台，防统方系统支持分布式部署和集中监控，在满足各家医疗单位自身反统方保护要求的同时，也能很好的满足卫生监管部门对下辖的各个医院的非法统方行为集中监管和审计需求。

**典型部署**

捷普医疗防统方系统采用旁路部署，它直接在核心交换机上旁路镜像所有往返医疗应用系统和后台数据库的数据流量，不改变原有网络结构，运行中无需在医疗信息系统服务器上安装任何代理插件 ，无需提供医疗信息系统的任何管理账号和密码，不占用系统服务器资源，无需重启被审计系统及服务，对医疗应用系统应用零影响。



捷普医疗防统方系统旁路部署示意图

捷普医疗防统方系统支持分布式部署和集中管理，通过在区县或市级卫生局部署捷普防统方集中监管平台，可以满足对下级医院防统方设备的统一监管需求，实时接收下级防统方监控节点的事件日志，及时处置各下辖医院的违规统方行为，确保医疗防统方监管要求能够真正落地。捷普医疗防统方集中管理平台的部署能帮助卫生监管部门有效解决以下几个问题：

* 下辖医院不上报、私自隐瞒、私自处理统方风险日志问题；
* 下辖医院解决缺少指导、规则设置不规范、无法有效处理问题；
* 下辖医院风险处理不及时或很少上线查看防统方系统审计信息问题；
* 下辖医院设置白名单、免审计规则，逃避医疗防统方系统审计问题；
* 下辖医院让防统方系统处于闲置状态，为应付上级检查才上线等问题。



捷普医疗防统方系统分布式部署和管理示意图