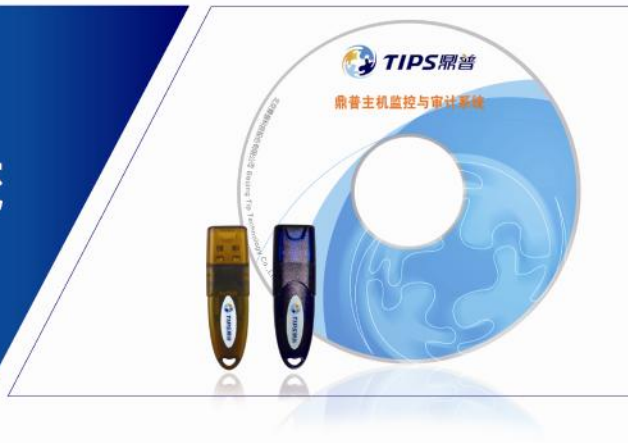
TIPS鼎普

鼎普主机监控与审计系统



中国信息防泄漏领航企业

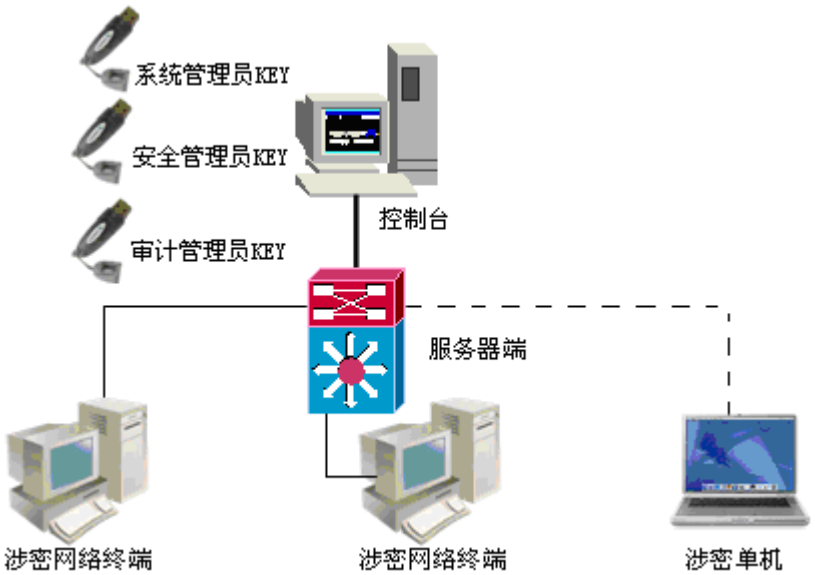
目 录

产品概述

在涉密信息系统领域，国家政策以分级保护的强制性测评为重点，对应的信息化建设以防止信息泄露为主，使失泄密事件在信息技术高速发展的信息系统中防患于未然；在非密信息系统领域，国家对信息系统推行分等级保护的政策和行动方兴未艾，信息化的管理维护既要便于应用又要保证系统安全可信。所有这些都离不开安全技术的应用，而其应用的便利性、实效性和可扩展性又是其中的关键。

北京鼎普科技股份有限公司经过多年的政策跟踪研究，以强大的驱动级内核加固技术作支撑，研发了“鼎普主机监控与审计系统”系列安全管理软件，用于监控和审计涉密计算机的数据输入/输出接口、设备以及被控端用户的敏感行为，从而加强涉对密计算机的安全管理，达到有效预防失、泄密事件发生的目的。本系统为计算机安全管理部门和安全检查机构提供了方便、准确、快捷的终端用户安全管理手段。

“鼎普主机监控与审计系统”采用 C/S 结构，模块化设计，由客户端、服务器、控制台三部分组成。综合运用底层驱动、驱动拦截、网络协议驱动过滤、文件驱动过滤、加密传输、身份认证多种技术。为用户提供了“从终端、网络到管理中心三点一线”的操作平台，实现对主机各种泄密途径实时控制，对网络运行安全、高效管理的一体化集中解决方案。系统结构图如下：



产品功能

1 监控终端各接口外设、打印输出

防止非授权人员随意使用单机的各种接口、外设拷入拷出信息、打印而泄露敏感信息，监控他们的使用过程，或直接禁用

2 非授权外部链接阻断

实时阻断终端联接互联网或其他未授权网络从而导致黑客入侵、泄密及严重保密违规事件的发生，并报警

3 终端接入网络认证

对接入内部网络的终端进行合法性认证，阻止外来的以及不健康的终端非法接入企业内网窃密和传播木马病毒

4 文件合规性操作

监控用户对文件的打开、修改、新建、删除、重命名、复制等操作行为，也可对指定盘符、文件类型、目录和文件进行监控。实时产生报警信息，保护敏感文件的安全性、可用性

5 U 盘防泄密管理

对 U 盘进行集中注册，提取台帐、打上安全标签。防止内外介质交叉使用而导致的泄密及木马病毒传播泛滥，指定介质的使用权限和范围，全程监控使用过程，实时产生报警信息

7 企业信息管理、变更报警

企业资产实际上就包含有大量的敏感信息，如硬盘、服务器等。对其进行统计、集中管理，实时报警其发生的任何变动，可对企业重要信息资产实施有效的管理

8 终端软件安装策略制订

管理员可制定强制策略，防止用户随意安装使用聊天、网络窃听、反卸载等各种软件工具，破坏运行环境、降低工作效率

9 终端、网络的流量监控

统计内部 IP、MAC 或用户的流量，包括总流量和应用协议流量，结合鼎普网络信息监测系统可以进行流量控制和负载均衡

10 端口协议审计

审计监督终端对端口的开启及使用状态，监控利用 HTTP、SMTP、POP3、TELNET 等协议传输行为

11 网络设备管理

通过集成的 SNMP 管理协议模块，实现对网络设备如交换机等的管理，绘制网络拓扑，联动网络接入认证模块

12 终端健康状态监测

动态监测入网终端的监控状态，对没有安装某强制软件或防病毒系统、密码设置不合要求、注册表关键项被篡改的终端实时报警，也可采取断网、软件推送安装等强制措施

产品优势

1 底层技术应用，自身安全性突出

1) 防绕过、防卸载: 国内首款基于驱动级技术开发的内网安全管理平台，核心功能不同于应用层的技术设计，终端防卸载能力突出，保密管理性强。

2) 防假冒、防窃听：终端代理核心实现在驱动级，控制台与服务器分离，部署位置不受限；控制台、服务器、终端代理之间连接采用数字证书，严防假冒；策略信息、报警日志加密传输，防止窃听

2 创新思维，安全性与管理性兼顾

1) 适用超大网络管理：采用多级分布式结构，系统各级管理中心建立了良

好的调度和通信机制，管理权限层层下发，管理逻辑清晰明确

2) 保密性管理性并重：系统通过多模块的组合应用，实现对主机防泄密监控、网络监控、数据库审计、网络管理、非法外联、可信健康接入认证、补丁分发、信息集中输入输出的内网安全一体化管理平台

3) 网络与单机兼管：系统总体基于网络进行管理；对不联网单机采用智能 KEY 本地管理，报警信息通过审计 U 盘本地查看，也可选择导入到服务器集中管理

4) 快速提取关注信息：根据实际管理需要，可自主定义各类报警信息、报警级别、报警方式、报警信息查询方式，在数据库的海量信息中快速提取、审计事件信息

3 遵循政策法规标准

1) 依据国家政策标准：“鼎普主机监控与审计系统”以 BMB17/20/22、27 号、66 号、43 号文件、ISO/IEC 27001 相关标准为功能开发依据

2) 以三员分离为原则：实现系统管理员、安全管理员、审计管理员的权限分离。既适应涉密系统对 BMB 相关标准的检测响应，也注重等级保护及信息安全管理的综合应用

关于鼎普

北京鼎普科技股份有限公司坐落于中关村软件园，是中国信息防泄漏的领航企业。鼎普科技创建于 2003 年，经过 8 年的快速成长，已成为国内信息防泄漏产品与解决方案的专业提供商，公司拥有 200 多人的专业团队，在全国各地拥有 5 家分公司和 7 个办事处，同时在北京、上海、成都、郑州、石家庄设立了五大客服中心，为众多的军队、军工企业、政府、高校、科研院所、金融系统和大型央企等客户提供及时、便利、真诚的服务。

鼎普科技拥有国际性标准水平的安全产品研发中心，中心设有信息安全攻防实验室、信息安全检查与评估实验室及新品研发等机构。在安全产品研发中心从事计算机、网络、电子信息应用等领域的顶级科技人才，通过长期对客户需求的理解与信息技术的研究，使鼎普科技的技术成为国内内网安全产品的标杆典范。专业从事信息安全的咨询顾问以其精湛的技术，帮助客户解决实际面临的安全问

题，为客户呈现具有鼎普产品个性化、高效率的解决方案。

卓越的管理团队使鼎普科技通过了 ISO9001 质量体系认证、CMMI 三级认证、军工保密二级资格认证，获得了涉密信息系统集成资质、计算机信息系统集成资质，成为商业密码定点生产单位。取得了权威机构的各类资质认证 70 余项、专利 26 项。

作为“中国计算机学会计算机安全专业委员会”、“中国计算机学会信息保密专业委员会”和“全国信息安全标准化技术委员会”的成员企业，鼎普科技荣获了最具成长科技型 100 强企业、北京市专利试点企业、国家互联网应急服务支撑单位等多项国家级荣誉称号。为国防、国家奥运、神舟飞船等大型信息安全项目提供高品质的产品及服务，更获得了高度评价及认可。

鼎普科技旗下拥有信息防泄漏领域的领军品牌“鼎普”，同时拥有信息安全检查类第一品牌“猎隼”，秉承“更底层、更安全”的技术创新理念，与客户共同分享信息安全时代的无限精彩！