校园网络时钟系统（GPS北斗卫星授时）

产品名称	校园网络时钟系统（GPS北斗卫星授时）
公司名称	安徽京准电钟电子科技有限公司
价格	8500.00/台
规格参数	品牌:京准 型号:HR-906A 产地:合肥
公司地址	安徽省合肥市瑶海区长淮街道临泉路新安罗马花园7幢203室（注册地址）
联系电话	13295517758

产品详情

校园网络时钟系统（GPS北斗卫星授时）

智慧校园建设是近年来高校信息化建设的一个重要方向，随着智慧校园建设的不断深入，信息系统面临的信息安全威胁也在不断增长，信息安全风险日益突出。快速有效的发现智慧校园各业务系统存在的安全威胁，进而采取有效的预防和处置措施，是高校建设智慧校园过程中面临的急需解决的问题。

安全挑战

高校网络日益成为攻击者攻击的对象和各种病毒的温床，高校常见的安全事件包括门户、招生网站被攻击、篡改、挂马、钓鱼等，学生成绩单被篡改，攻击者入侵高校数据中心利用服务器的高性能高带宽对外发动攻击等。

智慧校园安全解决方案

高校智慧校园安全挑战主要包括：

1. 边界安全威胁

由于校园网与外部网络互联，不可避免的受到外部的各种入侵和攻击，由于校园网边界只部署传统防火墙作为防护设备，对外攻击抵御能力有限。

2. 系统漏洞风险

校园业务信息系统面临着安全漏洞的威胁，存在缺乏必要的入侵防护手段、缺乏必要的系统漏洞控制措施、业务系统权限控制不合理等问题。

3. 网站安全风险

高校网站主要面临被挂马被篡改、被DDoS攻击的风险，网站极易成为攻击者侵入校园内网的跳板。

4. 上网行为失控风险

校园网用户上网带来的风险，包括个人账号密码疏于管理、敏感言论、攻击者攻击工具在校园内传播等。

5. 安全管理手段缺失

智慧校园信息化管理工作繁重，传统的安全解决方案往往大幅增加安全管理工作的难度，导致问题处理不及时、响应缓慢等问题。随着高校系统、网络规模的扩大，设备的增多，设备管理人员也相应的增多。由于运维工作的复杂性，带来的用户角色、账号管理混乱，违规操作和越权访问事件频发，并且无法实现有效的监管。

解决方案

智慧校园安全解决方案以全面、整体、长期地满足高校安全保障为目标，以体系化建设为手段，结合重点安全保护对象，实现高校信息安全建设顺利开展。

1. 高校网络出口安全防护

在高校网络出口部署捷普防火墙系统，防止外部攻击者通过互联网业务系统攻击高校内网，进行数据窃取和数据破坏。通过防火墙的边界隔离和访问控制功能，实现对非法或危险行为进行实时拦截，保护高校内网业务安全。

部署捷普入侵防御系统，可以准确监测网络入侵行为和异常流量，自动对各类攻击性的流量、尤其是应用层的威胁进行实时阻断，避免或减缓攻击可能给高校网络带来的运行风险捷普入侵防御系统具备双向防护功能，可以有效阻断内网发起的恶意攻击流量。

2. 安全分域管理

为了更好的保障高校业务的稳健运行、避免高校业务信息系统间的恶意信息的传播扩散，采用安全分域的管理办法，建议高校安全域划分为学生域、教学域、科研域、财务域、资产域、校务职能域和技术支撑域等。安全域之间的边界保护，可以通过捷普防火墙访问控制列表来实现访问控制，通过捷普入侵防御系统阻止恶意入侵行为的发生，提高这些安全域的安全性。

对于保密要求比较高的安全域，需要在系统终端上安装捷普终端安全管理系统，监控终端的违规外联、违规开启服务端口的违规行为，控制终端外设端口的使用等。同时对终端的补丁、病毒库同步进行统一管理，强化终端主机安全保护，保障安全域内各终端安全。

针对Web服务器安全域，需要在Web服务器前部署捷普Web应用防火墙系统，实现应用服务器防护，保护网站Web服务器免受应用级入侵，同时弥补了防火墙、入侵防御类安全设备对Web应用攻击防护能力不足的问题。

3. 高校网络中心安全运维

在高校网络中心部署捷普网络脆弱性智能评估系统，帮助高校管理员能够很直观地了解网络中各系统的安全状况，及时发现网络中核心设备的漏洞及修复情况，避免由于网络系统漏洞问题引发信息安全事件。

部署捷普高性能网络信息审计系统，有效监控业务系统访问行为和敏感信息传播，准确掌握网络和各业务系统的安全状态，及时发现违反安全策略的事件并实时告警、记录，同时进行安全事件定位分析，方便事后追查取证。

部署捷普安全运维管理系统（堡垒机），建立面向安全运维的集中、有序、主动的运维安全管控平台。该系统基于为一身份标识的集中帐号与访问控制策略，与各服务器、网络设备等实现无缝连接，实现集中化、精细化运维操作管控与审计。

4. 安全一体化集中管理

智慧校园信息化管理工作繁重，建议部署捷普信息一体化集中管理系统，实现安全设备的统一管理，设备状态集中监控，安全策略集中下发，对海量 安全日志进行集中采集、分析、关联、汇聚和统一处理，实时输出分析报告，通过大屏展示的态势感知系统分析安全威胁的总体趋势，利用态势感知的大数据分析能力，实现失陷主机的确定与加固，实时快捷地发现校园的安全总体安全情况。

客户价值

■ 高校内部网络得到充分保护，有效阻止外部入侵行为、恶意攻击造成的严重后果。

■ 高校门户网站安全性得到加强，有效提高网站服务质量。

■ 智慧校园各业务系统得到安全保障，避免由于攻击者攻击造成“ 校园一卡通 ”、“ 数字图书馆 ”、“ 学生档案信息 ”等重要数据的破坏。

■ 规范学生上网行为，规避了学生恶意攻击造成的不良社会影响，很好的满足监管部门的相关要求。

■ 实现全网中的不同IT资产进行事件采集、分析和处理，构建统一的安全管理平台。

■ 通过系统和应用脆弱性检测探针来自动化智能化的实现脆弱性的闭环管理, 解决
资产多、资产环境复杂、资产难以管理的问题。