bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息教育业防勒索软件解决方案

佰倬信息科技有限公司

2021 年 5 月

目　录

一、 高校校园信息化发展现状

受疫情影响，在线教育愈加火热。作为全国教育战线抗疫工作的重要组成部分，各高校通过教育信息化手段尤其是在线教学的推进，维系了高校教学秩序的稳定。截至 5 月初的统计表明，全国 1454 所高校开展在线教学，103 万教师在线开出了 107 万门课程，合计 1226 万门次。参加在线学习的大学生共计 1775 万人，合计 23 亿人次。

（一）高校信息化发展现状

我国高校信息化建设近年来取得了突破性的进展，各大高校主管部门对于高校自身的信息化建设工作非常重视，不管是在人力还是财力上都不断增大着投入比例。总体来看，包含了以下几个方面：

(1)我国高校信息化建设一直处于高速发展阶段。众多高校拥有了基础网络建设和硬件设施，基础设施正朝着不断更新换代的新要求上继续发展。几年前，教育部科技发展中心展开的一项调查显示(243 所高校参与调查)，90% 的高校已建立校园一卡通系统，88% 高校建立了覆盖全校校园安全监控系统，82% 的高校提供带校名后缀的电子邮件系统，74% 的高校建立了统一的身份认证系统，近 80% 的高校采购了全校性网络教学平台。

(2)教育信息化发展至今，已经被各大高校和教师逐渐接受和采用。从幻灯片教学到以教学电视投影设备为主的多媒体教学，从多媒体再到网络教学和远程教学，传统黑板面授教学模式逐渐被新型技术模式所取代。信息技术的引入所带来的教学形式的多样化和教学内容的充实化，大大提升了高校教师在教学中的质量，而信息技术中的通讯技术的应用，也增进了师生之间的互动与交流。

(3)随着高校信息化建设的不断深人，信息技术使高校内的各大领域之间得到了整合。高校信息化建设在高校建设中发挥着非常重要的作用，它使得高校在教学质量与教学效率上得到了极大的提高。统计信息化、金融信息化、管理信息化、电子商务等高校的许多学科建设与计算机技术之间的结合变得愈发普遍。

(4)信息技术在科研、财务、管理等领域发展迅猛。我国在高校信息化建设方面发展至今，除了大力发展了教育信息化以外，信息技术也在学校文化、科研、管理、财务等领

域得到了迅猛的发展势头，并且大部分的高校已经在上述技术上领先于教育信息化建设工作方面的步伐。

(5)高校管理决策层对信息化建设上的重视程度越来越高，并且校方对于信息化建设的经费投入上也越来越大。据教育部数据，截至 2020 年 6 月 30 日，全国高等学校共计 3005 所。据公开资料数据显示，我国高校平均每年的教育信息化建设投入在 1000 万元左右。照此计算，我国高校信息化建设的学校投入经费在 2020 年将达到 300 亿元左右。因此，业内人士也认为，大数据在高校信息化的运用将在 2020 年左右迎来爆发期，届时，高校信息化将再“升级”。

（二）、高校信息化发展面临的挑战与机遇

(1)问题与挑战

虽然近年来高校信息化发展取得了一定的成绩，但同样还存在着诸多问题与挑战：

信息技术人才竞争激烈

随着互联网迅速发展，社会上对互联网人才尤其是高端人才竞争激烈，学校难以吸引到高水平信息技术人才。

教育信息化产品成熟度不高、国产化不够

大量高水平信息技术人才和信息技术公司聚集到互联网行业，面向教育行业的软件公司水平普遍不高、服务能力弱、产品成熟度不高。国外高水平软件与国内高校实际需求存在差异，国产化、定制化不够。

网络与信息安全形势严峻

学校重要信息系统存储着学校重要信息及大量教职工敏感个人信息，确保学校网络信息安全是信息化建设的首要任务。网络攻击、网站篡改、信息窃取等仍然不断威胁着学校网络与信息安全，信息安全专业技术人员短缺，形势严峻。

信息技术发展迅速，产品更新换代频繁

信息技术发展迅速，一方面为信息化建设不断提供新的技术，另一方面，信息技术更新换代过快，信息化产品的开发成本高，可持续性难以保障。

(2)机遇

国家高度重视教育信息化

《国家中长期教育改革和发展规划纲要》关于推进教育信息化进程独立成章;《教育信息化十年发展规划(2011-2020 年)》正式颁布;教育部制定印发《教育信息化“十四五”规划-教育信息化 2.0 行动计划》。

信息技术日益成熟

当前，信息技术发展迅速，大数据、物联网、虚拟化、云计算、移动互联、万物互联、泛在接入等技术不断革新，日益成熟，有力推动着信息化发展，为高校实现高水平的信息化建设提供了技术上的可行性。

学校及师生对信息化需求强烈

国家"双一流"大学大多已确立到本世纪中叶建成世界一流大学的宏伟目标，世界一流大学必然是信息化一流的大学，对信息化支撑保障能力提出了更高的要求;学校各单位对学校信息化基础平台的服务能力提出了明确需求;师生已具有较高的信息化素养，希望学校提供更加优质的信息化服务，对高水平的信息化应用需求强烈。

疫情倒逼推动高校信息化发展

教育部印发《关于在疫情防控期间做好普通高等学校在线教学组织与管理工作的指导意见》，遴选了 37 家在线课程资源平台和技术平台供高校选择使用，开放在线课程资源，保障高校和职业学校在线教学。疫情防控期间，高校的信息化工作都不同程度地面临着一定的压力，但同时也倒逼信息化部门对未来做出思考。

二、 未来高校信息化的发展趋势

近几年来我国的信息技术发展主要影响了教学管理方面，从日前的情况来看，高校的教学管理信息化主要呈现以下发展趋势：

(1)数字化发展趋势

在高校的教学管理中需要处理多样化的，数量庞大的信息，这些信息包含了“数字化信息”和“非数字化信息”。而从目前发展的现状来看，教学管理信息系统已然给非数字化信息转换工作来了很大的便利，其让信息系统中的各项事务都将以数字化的形式出现在管理者面前，因而方便存储与调用。

教学管理信息化体系的广泛应用，让教学过程中的庞大信息基本都被数字化，其不但降低了信息整理和存储的成本，也方便了高校各职能部门和教师对相关数据的调用，同时又能借助网络不限时间、不限空间地随时调用教学信息，方便了信息的传播和利用，让教学信息能够最大程度地实现共享，提高信息的使用效率。

(2)网络化发展趋势

网络化是信息技术的灵魂，如果高校内的各信息单位没有网络的连接，那么其只能利用信息技术进行信息收集与整理，并且信息收集方式也会是脱离了信息化技术的、传统的、费时费力的方式，信息化建设就没有意义。

网络化指的是将高校内的各部门、各院系，以及高校与高校之间通过计算机网络进行联系，从而搭建出一个信息化教学管理平台。在各平台中的各个用户都可以通过客户端登录平台进行信息查阅、传送和利用。另外，网络化还包含着学校建设的校园网，在一个信息化系统之中实现对教师、学生、课程等的管理，且这些系统之间能够很方便地对信息数据进行交流。

(3)智能化发展趋势

智能化是指由现代通信与信息技术、计算机网络技术、行业技术、智能控制技术汇集而成的针对某一个方面的应用。而高校教学管理的信息化系统发展至今，其运用了多种信息技术，如数据库技术、人工智能技术和多媒体技术、计算机网络技术等，因此让其逐渐呈现出智能化的发展趋势。

并且，当代社会对于智能化的需求越来越迫切，高校教学管理环境也应该顺应时代融人智能化。教学管理信息化系统在未来对其结构进行设计时，将会充分运用人工智能技术，能方便搜索推理的实现，借助先进的模块管理技术和数据库技术，联系教学管理中的各个相对独立的教学环节，从而实现综合管理。

(4)扁平化发展趋势

在传统高校教学管理中一般是垂直化的管理模式，而随着高校信息化教学管理的发展，让高校的教学管理模式开始向扁平化发展。在传统的教学管理中一般是按照科层制而组织的，在这种组织框架之下，资源、信息与权力之间往往呈现出一种垂直的格局。而随着信息化系统的应用，在教学管理当中的大量中间层级逐渐被去掉，信息传递模式由以往的垂直模式渐渐变为扁平模式，教学管理的框架也渐渐被扁平化趋势所取代。

(5)合作化发展趋势

以往传统教学管理中，教学组织会按照各自的分工原则来进行工作的分配，也就是由不同部门来分管各自的工作，因此各部门之间存在着缺乏合作的现象。而随着信息化教育时代的到来，将以往垂直化教学管理信息系统转变为扁平化，传统的按工作职能分配任务的组织框架便不可能适应信息化教学管理活动的需要。

因为在高校教学管理信息化体系之下，需要相关管理人员具有较高层度的专业知识、综合素质以及技能，这往往就需要教学管理系统以任务中心来进行工作的安排，从而构成一个有效的任务网，教学管理人员便是这个任务网上的各个节点，任何一个节点之间都可以实现即时的信息沟通，即实现了真正意义上的合作化。因此，合作化也是信息化教育的未来发展趋势之一 。

智慧校园将成为高校信息化的发展新方向

在高校信息化发展的背景下，智慧校园作为教育信息化的重要组成部分，越来越多高校加以部署，这也将成为未来高校信息化发展的新方向。

高校信息化已迈入智慧校园建设阶段

我国高校信息化建设与应用大体经历了三个阶段。第一阶段是从 20 世纪 90 年代起步的校园网建设阶段;这一阶段，IDC 建设和基地 IT 应用等信息化硬件设施是主要建设核心。

从 2000 年左右开始，由于互联网和计算机的进一步发展和普及，高校信息化建设进入以数字校园为主的第二阶段，建设的侧重点逐渐从信息基础设施转向各类信息系统，各高校先后开发了人事管理、财务管理、教务管理、科研管理等一系列管理信息系统和以身份认证、数据交换、集成门户为特征的数字校园运行管理平台。与此同时，高校也开始联合优质社会力量、在信息化服务商的技术支持下搭建符合学校需求的数字校园网络。

自 2015 年左右开始，大数据、云计算、人工智能、移动互联等新兴技术开始渗透和应用于高校信息化建设，国内高校信息化发展进入全新的智慧校园阶段。智慧校园是高校信息化的更高级形态，是数字校园的扩展与升级;它综合运用人工智能、大数据、移动互联等新一代信息技术，有效衔接校园现实空间和数字空间，优化师生与学校环境、资源的交互方式，为师生建立智能的教育、教学和生活环境。

三、 高校数据安全防护需求分析

高校信息化体系的建设，必然带来大量数据的集中存储与使用。在一体化综合信息平台的运行过程中，存储了大量的敏感数据，包括且不限于：

- ✓ **高校核心运营数据**
  综合事务服务中心与教务、学工、人事、科研、财务等十几个业务系统对接，项目管理信息化平台，这些业务系统中包含大量的财务、人事敏感信息，一旦泄露，会给学校的声誉造成影响。
- ✓ **师生员工个人敏感信息**

2020 年 10 月，《中华人民共和国个人信息保护法（草案）》征求意见稿（以下简称《个人信息保护法》）出台，就个人信息保护有关的立法问题向社会公开征求意见。个人信息保护立法迎来元年。校园网业务系统中存储着大量的师生员工个人信息，如何保证这些个人敏感信息的安全，防止个人隐私被侵犯，成为校园信息化建设中必须解决的问题。

- ✓ **高校科研成果或数据**

  科研系统中所涵盖的科研团队阶段性研究成果或技术理念，这些信息拥有巨大的价值，属于特殊的无形资产。

与校园信息化建设平台的不断进步相比，资金、技术、人员、管理等各种因素制约了校园网络安全防护与建设的速度。与之相对的，则是网络攻击手段层出不穷，操作系统漏洞、勒索病毒攻击、黑客恶意入侵……这些都可能导致校园网各业务系统被攻击，数据被勒索，业务被迫中断，或者学校运营数据、院系科研成果或广大师生员工的个人信息被泄露，严重威胁学校的正常运行或师生员工的安全。

针对以上数据安全问题，学校迫切需要在信息化建设中加强数据安全防护体系建设，加强各系统的数据安全管理与维护，防止敏感信息泄露，保障学校和师生的数据安全，创建安全、可信的教育和科研环境。

四、 佰倬信息数据安全解决方案

佰倬信息数安解决方案提供“以数据为中心，以数据流动为线索”的数据自保，通过“后量子密钥管理”和“强制访问控制”的智能集成，实现数据自保，使服务器和终端数据能够抵御勒索软件、恶意软件、内鬼等已知未知威胁而带来的数据安全问题。

结合学校现有信息化建设的应用场景和数据安全（严峻的安全形势：网站被篡改、信息被窃取等）需求，解决学校信息化体系中服务器端访问控制和信息存储机密性的问题，有效增强其服务器端操作系统的安全性，提升校园信息化建设体系的数据安全性，为学校的正常运行保驾护航。

1) 系统整体架构

网络拓扑图

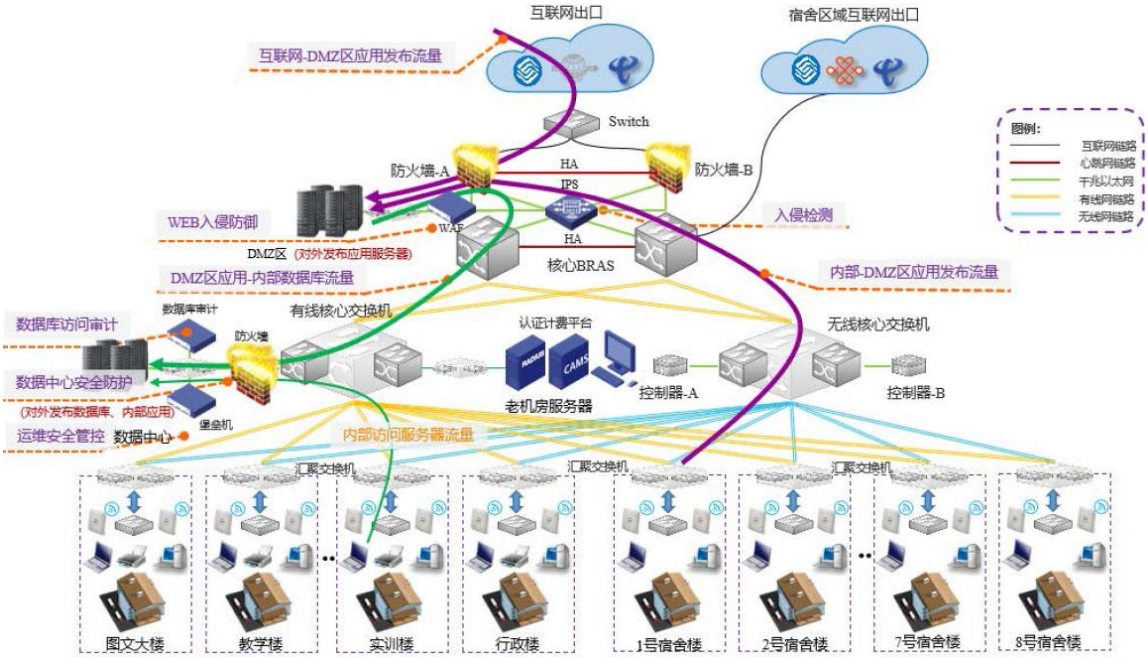


图 1 校园网拓扑图

从上图可以看出，学校校园网架构中的数据存储分布在以下区域：

序号	分布	待保护设备	说明
1	DMZ 区	对外发布应用服务器	应用服务器中的配置参数、临时文件等（非结构化数据）
2	数据中心	对外发布数据库服务器	业务系统对应的敏感信息（结构化数据）
3		内容应用服务器	业务系统中的配置参数、文件等（非结构化数据）
4		认证计费平台服务器	认证计费平台对应数据库、文件等（结构化数据+非结构化数据）

2) 佰卓数据安全防护

佰卓数据安全防护的主要目标包含以下三类：

1、 学校信息化体系各业务应用系统运行过程中提交或上传的文件的安全性，如：业务办理所需材料、机要文件、财务报表、邮件附件等；

2、 信息化体系各业务系统运行配置文件，如：应用系统的配置文件；

3、 业务系统运行所依赖的数据库数据

在校园网现有架构体系中的数据存储位置，推荐安装部署佰卓数安服务器版，实现对服务器端的数据库文件的安全防护；

此外，安装部署数安岗哨平台，实时监控各服务器端数据访问情况，实现数据安全集中管控。

3) 系统整体架构

部署佰卓数安系列防护系统后，系统架构如下图所示（红色标识）。

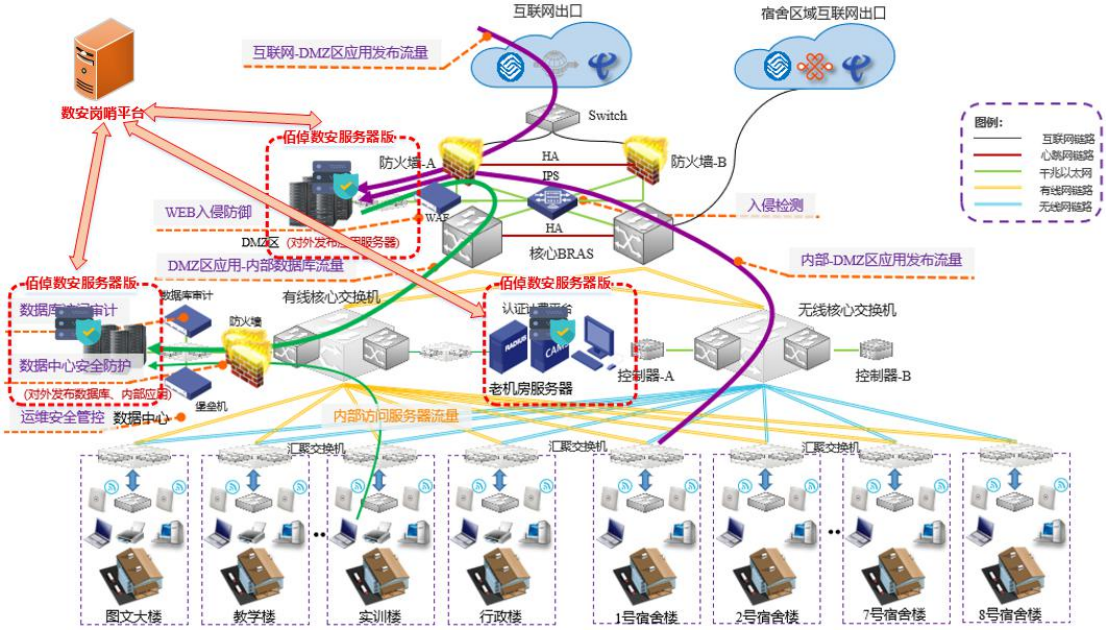


图 2 安装部署佰卓数据安全防护产品

- **佰卓数安服务器版**
  - ✓ DMZ 区—对外发布应用服务器（部署在现有设备上）
  - ✓ 数据中心—对外发布数据库服务器（部署在现有设备上）
  - ✓ 数据中心—内部应用服务器（部署在现有设备上）
  - ✓ 数据中心—认证计费平台服务器（部署在现有设备上）
- **佰卓数安网宝**
  - ✓ DMZ 区—对外发布 Web 应用服务器（部署在现有设备上）
- **佰卓数安岗哨平台**

  建议使用单独的服务器安装部署岗哨平台，岗哨平台与各服务器上部署的佰卓数安服务器版中的安全岗哨连接，实现集中管控。

4) 安全防护方案

佰卓数据安全防护方案中，在各待保护服务器（实体机/虚拟机均可）安装部署佰卓数安服务器版，加强操作系统数据安全，对服务器上的结构化数据（比如：数据库中存储的**师生一卡通消费数据、水电费消费数据、**）或非结构化数据（比如：应用系统中的临时文件、配置文件；文件服务器中的存储的身份证信息、财务报告等）进行加密存储和强访

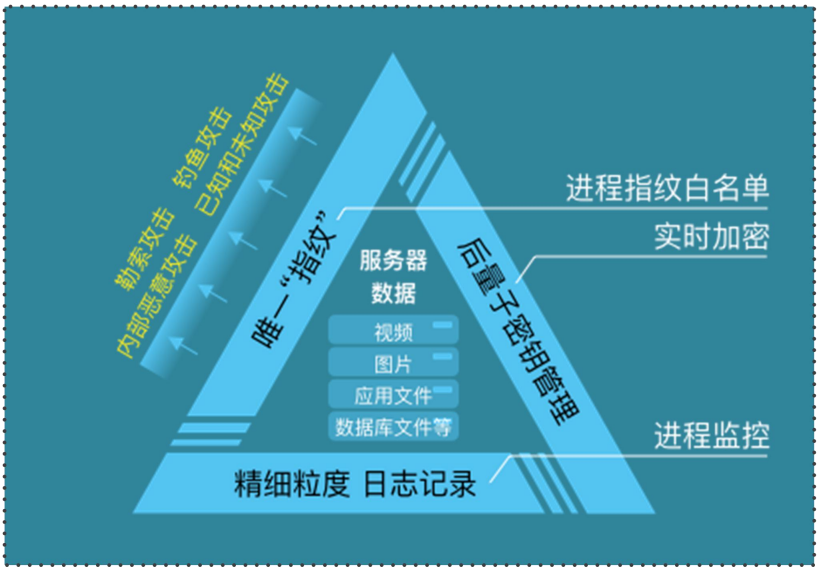
问控制，仅允许授权进程对文件进行读写操作，实时阻断未授权进程的非法操作，打造完整的数据生命周期可信安全链，提升数据安全防护能力，确保校园信息化体系中数据存储和访问的安全性。

5) 技术特性

佰倬公司的“**数据自保**”理念是以数据为核心，利用三大核心技术构架全球最先进的数据全程安全系统：

- 基于数据的**操作系统内核层的透明加密**，在大数据环境下，对各种专业格式数据与非结构化数据进行全面支持。
- 根据自身专利，开发个性化、密码学的**强访问控制技术**，建立从用户到框架层、内核层、基于硬件的可信计算区域的完整的可信安全链。真正实现数据所有人对数据的全面掌控。
- 建立全球唯一的**零感知量子安全密钥管理系统**，率先构建密钥共享可信链，实现内核层加密，传输加密，数据进程指纹控制，无泄漏密钥管理，授权共享与可控溯源融合一体，形成全新的数据全程安全系统。

本系统中文件存储安全防护推荐使用的数据安全产品是佰倬数安服务器版，其技术架构如下：



6）功能介绍

6.1. 佰倬数安服务器版，实现数据文件存储、使用安全

6.1.1. 与等保 2.0 政策匹配

等保 2.0 三级安全通用要求中在数据完整性和数据保密性方面提出了明确的要求。

- **数据完整性**
  - ✓ 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
  - ✓ 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
- **数据保密性**
  - ✓ 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

简而言之，就是要采用加解密或校验码技术保证重要数据在传输和存储过程中的完整性；采用加解密技术保证重要数据在存储过程中的保密性。

6.1.2. 数安服务器版产品功能介绍

佰倬数安服务器版是一款“以数据为中心，以数据流动为线索”的数据自保软件产品。通过“后量子密钥管理”和“强制访问控制”的智能集成，实现数据自保，使服务器数据能够抵御勒索软件、恶意软件、内鬼等已知未知威胁，满足等保 2.0 中对重要数据的存储过程中的完整性和保密性需求。

其主要功能如下：

➢ **低资源消耗**

被保护数据为数据库时，数据自保软件的内核模块对数据库吞吐量的影响要低于 5%。

➢ **强制访问控制和加密智能相结合**

对需要保护的数据进行自动加密保护，基于进程指纹信息和加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只授权合法进程访问被加密保护的数据，拒

绝非法进程访问被加密保护的数据。即使非法或恶意内部人员将强制访问控制强行关掉，数据仍一直保持被加密状态，无明文泄漏。

- **操作系统内核层的文件系统数据透明加密与数据访问控制紧密结合**

在操作系统内核层的文件系统中实现数据加密，此加密机制对合法进程透明，即加密机制不改变合法进程对数据的访问方式。同时，文件系统使用强制访问的授权判定信息决定是否对数据进行加解密，从而保证在系统漏洞/系统后门被利用时数据仍不会泄露。

- **零知识数据保护**

作为数据保护服务的提供者，不收集关于用户的网络、系统和数据的任何信息。在提供服务的同时对用户的网络、系统和数 据一直保有零知识。

- **数据防泄漏、防破坏**

能够保证在非易失性存储介质(如服务器硬盘)由于种种可能而脱离数据保护系统控制后，所存储的数据内容仍然安全而不会被窃取或泄露。

- **抵御已知未知的外来恶意软件攻击(防勒索攻击、防钓鱼攻击等)**

能够做到服务器系统对恶意软件的性质种类毫不知情的情况下，保护数据不被窃取、破坏、劫持及勒索。被保护数据免疫已知和未知病毒，可抵御已知和未知的外来恶意攻击，不惧怕系统漏洞和后门，防勒索、破坏、和泄漏。

- **抵御内部恶意攻击(防内鬼攻击)**

支持禁止操作系统用户及系统管理员使用未授权程序对被保护数据文件进行复制、移动、删除、或修改，防内部攻击。

- **用户对加解密过程无感知**

运行在操作系统的内核层，用户无需关注加解密的过程。

- **对系统计算性能进行实时监测**

安全岗哨对系统的关键计算性能指标实时做出完整的记录，并上传至中央岗哨平台。

- **对软件自身的运行情况的监察**

对软件自身的运行情况和工作状态做出完整的记录，从而保证整体系统的安全性。

➢ **边缘安全自保与中央管控监察的完美结合**

各个服务器上的安全岗哨自动与数安岗哨平台连接，将岗哨记录和系统性能实时汇总到数安岗哨平台。

6.2. 佰卓数安网宝，实现网页防篡改

佰卓数安网宝主要采用文件系统内核层的强访问控制，所有对 Web 服务器上的文件操作都需要经过我们的授权。该产品能防止网页内容被黑客、系统漏洞、网页木马以及后门等已知未知攻击，有效应对各种内、外部篡改风险，实现高可靠的网页防篡改方案，保障业务的持续稳定运行。

6.2.1. 数安网宝产品功能介绍

（1）强访问控制

通过操作系统内核层强访问控制，确保从被保护的网页服务进程向外发布的网页内容不被篡改。具体地：

- 禁止网页内容文件被除指定的数据同步进程之外的任何其它的进程（包括暴露在网络攻击之下可能被网络攻击劫持的网页服务器进程）修改；
- 禁止网页服务器的配置文件被未授权进程修改；
- 禁止未授权进程向网页服务器指定的网页内容目录中写入任何新内容。

由此保护网页不被篡改，确保网页内容的正确发布。

（2）数据同步

由专门的数据同步进程提供安全的文件同步方案，确保网页内容从内容生产服务器到多台网页服务器的及时的同步发送。

（3）零知识数据保护

作为数据保护服务的提供者，不收集关于用户的网页文件的任何信息。在提供数据保护服务的同时对用户的网络、系统和数据一直保有零知识。

（4）无额外的响应延迟

受保护的网页服务器对正常的网页访问没有额外的响应延迟。

6.3. 佰倬数安岗哨平台，实现系统集中管控

6.3.1. 等保 2.0 政策匹配

等保 2.0 在三级以上安全要求中明确提出了“集中管控”的要求，包括是否使用了加密的方式进行远程管理，是否部署了综合网管系统、综合审计系统、集中防病毒系统、补丁管理系统，集中的安全事件识别、报警和分析系统等等。

“集中管控”的含义：

- “集中”是指通过集合 IT 资产安全基础信息、系统风险检测等安全信息，进行统一配置，从而达到降低成本、高效管理。
- “管”代表“可管”，旨在通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行安全策略管理，从而保证信息系统安全可管。
- “控”代表“可控”，是指以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。

6.3.2. 数安岗哨平台产品功能介绍

佰倬中央岗哨平台（以下简称 CSP），力求对各服务器的数据安全及其性能进行管理、控制、感知、分析、预警、和可视化展示，通过集中管理模式，进行统一配置，为管理员构建一个可进行安全策略管理的平台，从而满足等保 2.0 三级安全要求中在“安全管理中心”部分提出的集中管控合规要求。

具体功能如下：

- **岗哨的远程安装、配置、和管理**

  在中央岗哨平台上，可以对各个服务器的岗哨进行远程安装、配置、和管理。岗哨的安全配置的调整有严格的授权、分权管理流程。操作既便利，又安全。

- **精细粒度的安全感知**

  包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等在内的岗哨记录，以及包括 CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息实时汇总到中央岗哨平台，进行归一化处理加工，实现实时监察和全面审计。

- **数据与系统安全的专业指数分析**

  通过建模，定义了系列数据与系统安全的专业指数，包括**系统生命力**、**负载突变指数**、**攻击突变指数**等，并可直观展示。

- **实时安全告警**

  在保障数据安全的同时，根据数据与系统安全的专业指数分析，对系统健康安全进行等级划分，并做到实时预警。

- **大屏可视化集中展示**

  把高度凝炼的数据与系统安全整体态势，用大屏/全屏直观展示，为运营监控、分析、决策支持提供精准信息。

- **动态可视化安全报表**
  对于数据自保情况和系统健康安全状态，进行动态、自定义条件组合查询，支持搜索结果的图表化呈现。

五、 成功案例 (江苏信息职业技术学院)

学校简介

江苏信息职业技术学院是江苏省人民政府批准、教育部备案的国有公办普通高等学校，是江苏省示范性高等职业院校。学校的前身苏南工人技术学校创建于 1953 年，是新中国第一所电子类中等专业学校，1960 年更名为无锡无线电工业学校。2002 年 8 月，国家级重点中专无锡无线电工业学校和创建于 1997 年的国家级职教中心无锡市锡山职教中心合并，实现了人才培养层次的提高和建制的升格，迈上了高等职业教育的新征程。68 年来，学校始终与国家和民族的命运休戚与共，走出了一条坚持与探索、继承与创新、奋斗与超越交相辉映的科学发展之路，8 万多名校友秉承“养正修能”的校训，弘扬“立德树人”的校风，生生不息，薪火传承，展示了学院的文化底蕴和办学理念，反映了学校的整体价值追求。新的历史时期，学校正努力建设以物联网技术融合现代制造业和现代服务业的发展，信息特色鲜明、一流企业认可、人民满意的高水平高职名校。

学校坐落在美丽的太湖之滨无锡市，现设有藕塘和东亭两个校区，占地面积 1165 亩，建筑面积 34 万平方米，拥有实验实训教学仪器设备 1.8 亿多元，图书 75 万多册，目前注册在校生 12000 多人，现有教职工 620 人，其中高级职称 198 人，具有硕士、博士学位教职工 398 人,专业课教师“双师素质”比例达 90%以上。

面临挑战

信息技术发展迅速，一方面为信息化建设不断提供新的技术，另一方面，信息技术更新换代过快，信息化产品的开发成本高，可持续性难以保障。

学校一些重要信息系统存储着学校重要信息及大量教职工敏感个人信息，确保学校网络信息安全是信息化建设的首要任务。网络攻击、网站篡改、信息窃取等仍然不断威胁着学校网络与信息安全，信息安全专业技术人员短缺，形势严峻。如下图所示，“校园一卡通”是“数字化校园”中的重要组成部分，它主要具有综合消费类、身份识别类、金融服务类等功能，整个系统与银行系统、学校原有的系统和学校管理信息系统都有衔接，可谓

系统平台	小额支付	身份识别	水电管理	第三方接入
能源综合分析系统	食堂消费系统	多媒体教室管理系统	分体水控系统	网络计费系统
网银转帐充值系统	银行圈存转账管理系	机房管理系统	一体化水控系统	教务管理系统
在线支付平台	班车车载刷卡管理系	指纹认证校园应用方	预付费水表系统	图书馆系统
系统管理平台	校园自助复印打印系	指纹认证系统	联网型水表系统	
财务结算平台	自助洗衣机控制器	RFID远距离识别系统	远传水表管理系统	
卡务管理平台		车辆出入管理系统	集中电能计量控制系	
设备集控平台		无障碍通道系统	预付费电能表系统	
密钥管理平台		身份识别系统	联网电表控制系统	
统一门户平台		门禁控制系统		
综合自助服务平台		考勤系统		
增值服务综合平台		会议签到系统		

集各种数据于一体的系统。因此此系统中存储了大量的重要的数据并需要进行严格的保护。

实施方案

佰倬信息的 佰倬数安服务器版、佰倬数安网宝（网页防篡改）、佰倬数安岗哨平台三位一体的新一代的数据安全产品，“以信息数据安全为中心，以数据可控使用技术为支撑，以数据安全管理为保障，以业务需求为导向”。从数据安全角度出发，在 Web 应用层、承载数据库的操作系统层全方位的超强访问控制与数据文件加密集成，对已知、未知威胁实现防御。

在学校的对外官网、校内网站服务器上部署佰倬数安网宝（网页防篡改），防止黑客利用未知的 Web 漏洞对学校的网站进行破坏。在学校的一卡通系统的数据库服务器上部

署了佰倬数安服务器版，成功地防范当黑客提权后对数据库进行拖库以及加密勒索、防范内部系统用户对数据库文件的不合理操作，大大提高了一卡通系统的数据的安全级别。佰倬数安岗哨平台则实现了全天候地对未授权的访问告警的监控与准实时告警，使得学校可以实时发现发生在这些服务器上的对数据文件的攻击与未授权的访问，在保护数据的安全的情况下能及时处理安全事件，大大提高了对网络安全事件的响应、处理速度。

项目收益

通过部署了佰倬数安服务器版、佰倬数安网宝（网页防篡改）、佰倬数安岗哨平台，实现了 Web 前端服务器、数据库服务器的数据安全保护：

- **强制访问控制和加密智能相结合**
- **操作系统内核层的文件系统数据透明加密与数据访问控制紧密结合**
- **数据防泄漏、防破坏**
- **抵御已知未知的外来恶意软件攻击(防勒索攻击等)**
- **抵御内部恶意攻击(防内鬼攻击)**
- **用户对加解密过程无感知**
- **对系统计算性能进行实时监测**
- **对软件自身的运行情况的监察**
- **边缘安全自保与中央管控监察的完美结合**