校宝在线信息安全白皮书

2020年3月

校宝在线

校宝在线(杭州)科技股份有限公司

目录

一、概述

- *校宝在线是谁?*
- *校宝是如何实现行业信息安全最高标准的?*

1.1 校宝在线信息安全体系概述

校宝在线成立于2010年，是中国深受欢迎的教育信息化综合服务提供商。

经过近十年在教育SaaS领域的深耕，校宝在线已经帮助超过90000个教育品牌实现信息化管理，帮助超过180000个校区实现互联网+教育的业务升级，服务教育从业者超100万，年经办交易流水400亿元。基于多年的行业沉淀以及阿里巴巴、蚂蚁金服等优质战略资源的整合，校宝在线以“双轮驱动+增值服务”战略全面布局教育服务产业。即，校宝在线除了为教育培训机构与K12全日制学校提供SaaS信息化服务，更进一步用金融服务、内容服务和营销服务等增值服务全面赋能机构，真正助力学校成长与发展。

目前，校宝在线的产品已经全面覆盖教育培训机构及K12全日制学校领域，解决招生、教学、教务、财务等全方位运营及管理难题，持续从不同的层面为用户提供优质体验，现产品体系包含校宝学校管理系统、校宝家、校宝学院、校宝智慧校园、校园宝、校宝收银宝、校宝安心保、校宝招生宝、校宝1Course。

校宝在线在成就客户的同时，也获得了各领域的肯定。自2014年以来，校宝在线陆续获得了好未来、蚂蚁金服等多家机构的投资，目前，已获得了由蚂蚁金服领投的超2亿元C轮投资。校宝在线将通过更多的创新增值服务更好地达成“推动教育服务加速进步”的使命。

从校宝的第一个产品诞生，校宝人就将客户的数据视作生命，并以最高的标准打造校宝的信息安全体系。随着成千上万的学校将校宝系统作为办学的核心管理工具，校宝人更是时刻感受到重担在肩，承载着千万学校的核心数据，势必走得更好、更稳。

在外，我们首先与阿里云、微软云这些全球最领先的底层服务商合作，站在巨人的肩膀上；其次，我们拥有超强的百人技术团队，他们中很多来自浙江大学、中国科技大学等中国最高学府，技术带头人校宝CTO孙琳更是英国剑桥大学计算机博士，人工智能专家。多年来，校宝技术团队打造的网络安全、数据安全双重堡垒曾经先后多次抵御住包括勒索病毒、DDOS攻击等多次外来攻击。

在内，我们有严格的制度管理，不仅设置了入职前的尽职调查，入职后更是将包括工程师在内的员工在工作时有机地与客户数据隔离；最重要的是，校宝一直以来保持独立经营权，做到客户数据对高管、股东、董事的有效保密。

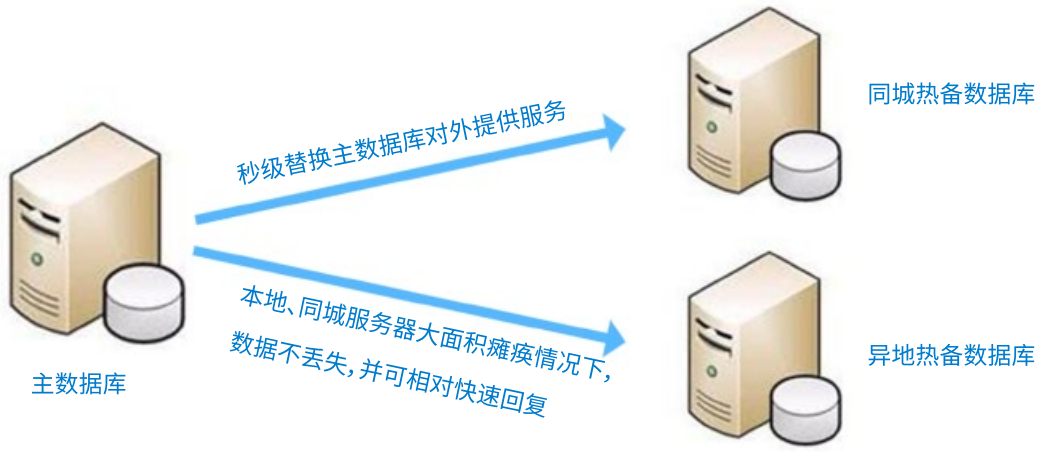
二、数据安全为底线

- *我的账号密码会泄露吗?*
- *我校的学生信息会被盗取吗?*
- *数据误删了可以恢复吗?*

2.1数据分级

校宝在线对所有用户提供数据存储安全保护;按照数据价值和敏感度对数据进行等级划分。根据数据安全分级,制定相对应的保护策略和要求。其中,校宝在线的产品系统账号安全体系依托口令策略和访问控制策略,系统将检测弱口令,对非法登录尝试进行实时监控。

2.2数据防泄漏

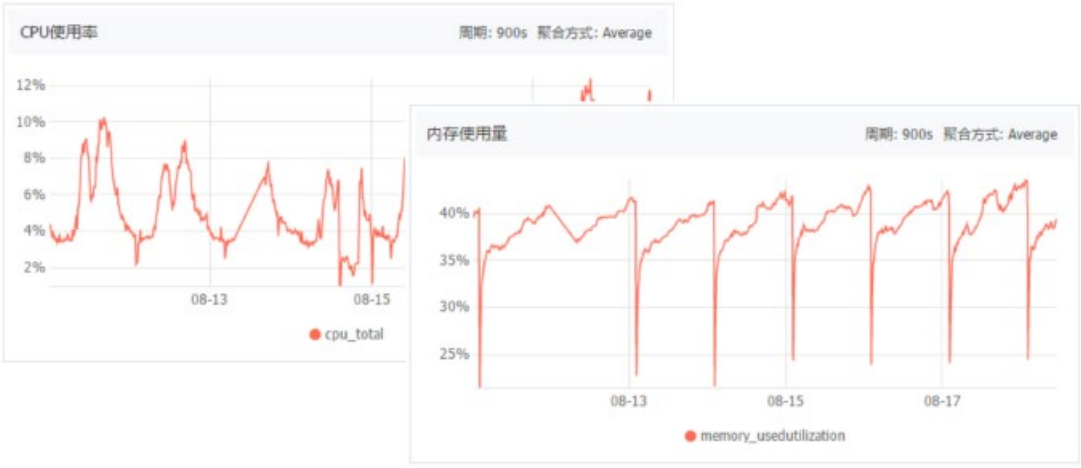


图表一 数据防泄漏

校宝在线对用户和机构数据进行了分等级保护,对用户使用和应用展示进行了严格控制——禁止展示机密信息;同时在需要展示信息的场景使用了防爬技术,阻断对敏感信息的爬取,从而防止用户数据被窃取。另外,校宝在线将服务器架设在阿里云上使得客户的数据安全得到双重维护和保障。

对于数据的可靠性,校宝深知“不能将所有鸡蛋放在一个篮子里”,通过异地多热备的方式,有效保障数据可用性。而目前校宝系统的数据存储持久性已达到99.9999%,这意味着理论上已不存在物理数据异常丢失的可能性。

2.3可用性监控



图表二 可用性监控

2.3.1系统可用性监控

校宝系统通过对各个关键业务点的智能模拟访问，保证系统实时可用；且当系统出现异常时，运维团队先于所有人掌握情况，以便快速反应，有效抢救。

2.3.2服务可用性监控

校宝系统依靠底层一个个健壮的服务引擎，通过对服务的监控，保障底层服务的稳定性。

2.3.3硬件可用性监控

校宝在线提供的所有系统和服务，最终都依靠硬件提供最底层的支持。因此，校宝在线硬件工程师实时监控、观察硬件运行情况，并设立“预警”和“告警”两套警告通知机制，所有的警告信息保证100%处理。不仅如此，通过优化预警处理的机制，校宝系统还能逐步减少告警通知出现的几率，为上层提供坚实可靠又高效的支撑。

2.4可用性保障

2.4.1动态调整

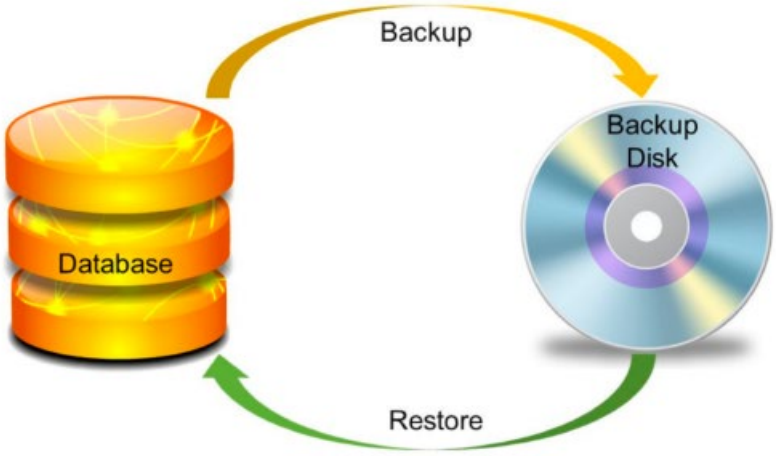
图表三 动态调整

校宝系统依据运行状态数据的分析，会动态调整云端环境的配置和数量，保障业务高峰期的运行稳定性。

2.4.2大事件预测

基于校宝的行业大数据和热点事件的预判，校宝系统会进行早期的主动调整，避免系统服务出现波动。

2.5数据恢复



图表四 数据恢复

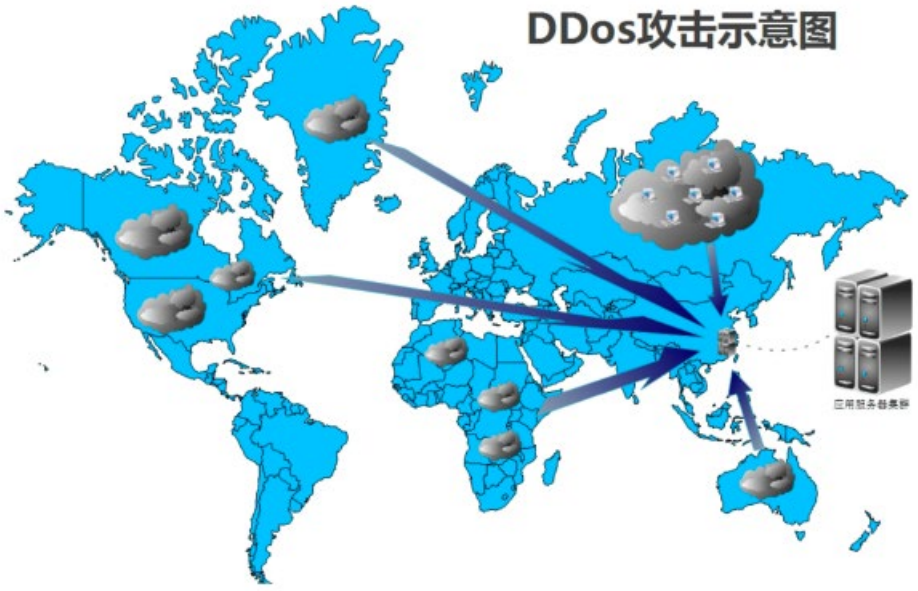
校宝在线通过严格的数据等级保护制度和周密的数据储存方案，为用户和机构的使用数据搭建了稳固的安全屏障。即使是用户本身产生的信息安全隐患，校宝在线也充分应对、制定了完备的应急预案。例如机构核心信息被机构内部人员有意或者无意删除，校宝系统在通过客户授权后，可通过技术手段（或安全机制）提供过去一年任何一天的数据快照，最大限度地帮助用户做好数据备份恢复。

三、网络安全作堡垒

- *我们受到过网络攻击吗?*

3.1攻击与防御

3.1.1DDOS攻击



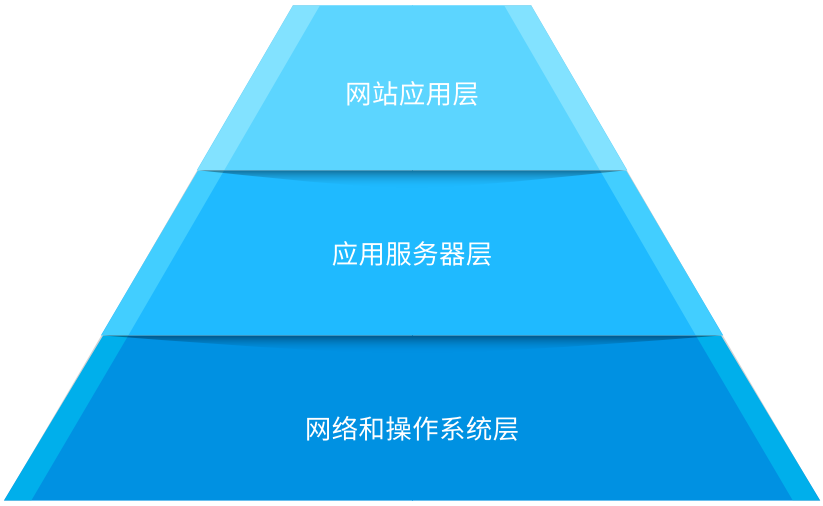
图表五 DDos攻击示意图

DDOS攻击包括CC、SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood、HTTP Get Flood等。

危害程度：中，会导致系统短时间内无法服务正常用户。

校宝防范等级：中，已成功抵御瞬时达几十G的流量攻击。

3.1.2漏洞扫描



图表六 漏洞扫描

漏掉扫描包括网络和操作系统的漏洞扫描、应用服务器的漏洞扫描、网站自身的漏洞扫描。常见的sql注入攻击就是扫描出网站对数据库访问的代码漏洞进行的攻击。

危害程度：高，严重情况会导致用户数据的泄露。

校宝防范等级：高，对所有漏洞做最高级别的防范，并通过隔离手段进一步避免遭受该种攻击。

3.1.3暴力破解

暴力破解通过对输入参数的穷举实现暴力破解登录等信息的攻击行为。

危害程度：中高，严重情况会导致部分用户数据的泄露。

校宝防范等级：高，拒绝使用简单密码，发现暴力破解迹象立刻启动识别机制。

3.2安全加固

3.2.1服务器隐身

校宝系统的服务器不直接对公网提供服务，由带负载均衡的前端机进行转发，这就好像给服务器加了一层隐身衣，让攻击者无法找到真身在哪，攻击自然无从下手。

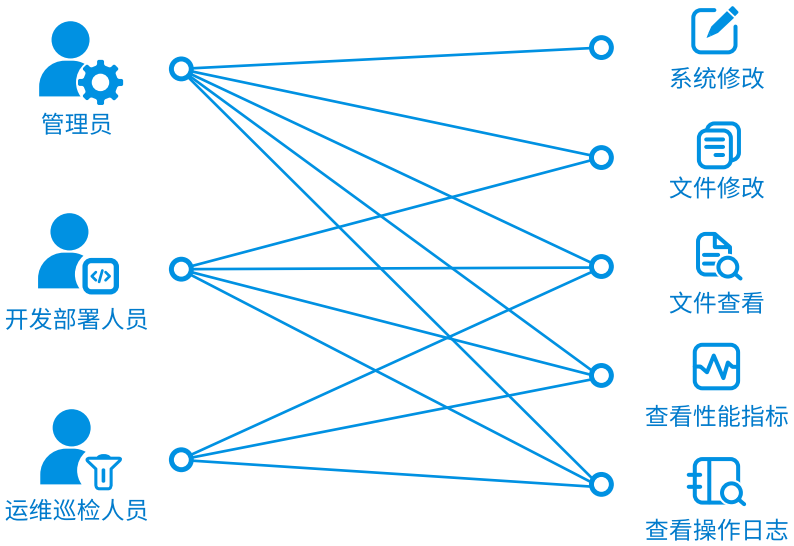
3.2.2指定信任网络

校宝将搭建完善的防御体系，划分安全使用区域，防止外界侵入。也就是说，校宝系统服务器的登录被限制在指定的办公网络范围内，其他网络环境无法访问。

四、基础安全为生命

- *校宝系统的服务器安全吗?*
- *是否每个校宝工作人员都可以登录服务器?*

4.1操作系统安全



图表七 操作系统安全

4.1.1系统软件安全配置标准

校宝在线的服务运行在可信的操作系统版本上，及时安装基础软件的漏洞修复。

4.1.2系统登录授权访问

校宝的服务器上除了线上运维人员可拥有较高权限外，其他人员的账号会对功能权限进行最大限制。

4.2物理安全

数据中心包含以下标准的物理安全控制要求：

4.2.1数据中心各线上设备区域系统、各核心骨干区域系统、各动力区域系统、各仓储系统、各报警监控系统的访问均需使用定制的电子卡，且电子卡由数据中心专门物业保管，特定授权需求方按需求领取归还，并配备紧急电子卡以备不时之需（如常规电子卡遗失），一旦发生遗失情况立即申请电子卡管理系统进行权限注销。

4.2.2数据中心的物理设备（包括其对应的各种组件），配件耗材的安置或存放区域必须要与所有办公区域和公共区域隔离（如办公室或大堂）。

4.2.3数据中心所有专属物理设备、设备配件、网络耗材，以及设备厂商的维修设备、配件、耗材等进出数据中心，必须由内部授权人员发送盖有专人保管印章的设备进出单传真，数据中心现场核实无误后方可允许设备、配件、耗材等进出。

4.2.4仓储系统中的重要配件，如核心网络设备的网络模块，精密存储介质等，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关。

4.2.5仓储系统中的任何配件，必须由授权工单和授权人员方能领取，且领取必须在仓储管理系统中进行登记记录，数据中心管理有专人定期对所有仓储系统物资进行综合盘点追踪。

4.2.6数据中心内部的每个区域，或外部走廊区域，或仓库门口区域，都使用了摄像机，物业保安7x24小时分段巡逻，并对所有基础设施进行7x24小时集中视频监控。

4.2.7采用全方位电子摄像机对数据中心的基础设施内外部区域进行视频监控，对设施区域中的其他系统进行检测和监控跟踪访问人员情况。

4.2.8所有人员活动记录电子保存（长期），所有视频记录被保存（3个月），以备后期审计，同时提供额外的安全控制措施，如：特定区域采用隔离或生物识别技术认证。

4.2.9只允许具备长期授权名单内的内部人员（实时更新），或审批通过的其他人员，以及授权认可的第三方固定人员名单内的人员（每月更新）进入数据中心，且非长期授权人员再以核实需求工单真实性的形式进行二次审核，准确无误后方可进入。

4.2.10非长期授权，非固定人员授权名单内的人员访问，必须要求数据中心内部管理需求方在流程系统上提交需求，由各层级主管提前审批通过后，方可同意其访问想要访问的内部特殊区域，并由对应数据中心的专人全程指导陪同。数据中心管理不定期对访问数据中心的人员登记情况进行审计，严格控制非授权人员访问数据中心。

4.3 环境控制

数据中心采用一系列措施来保障运行环境：

4.3.1电力

为保障数据业务7x24小时持续运行，数据中心采用冗余的电力系统（交流高压直流），主电源和备用电源具备相同的供电能力，且主电源发生故障后（如电压不足、断电、过压、或电压抖动），会由备用发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力，这是数据中心一个关键的组成部分。

4.3.2气候和温度

均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在一个恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。并且，设备冷风区域进行了冷风通道密闭，充分高制冷效率，绿色节能。空调机组均采用N+1的热备冗余模式（部分数据中心采用N+2的冷、热双重冗余模式），空调配电柜采用不同的双路电源模式，以应对其中一路市电电源发生故障后空调能正常接收供电。且在双路市电电源发生故障后，由柴油发电系统提供紧急电源，减少服务中断性的可能，以防止设备过热。

4.3.3火灾监测及消防

自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在火灾或烟雾事件触发时，在着火区提供声光报警。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火器。

五、制度安全作防护

- *我们的数据会被校宝的工程师看见吗？*
- *我们的数据会被校宝的大股东或者董事、高管看到吗？*

5.1尽职调查

在国家法律法规允许的情况下，校宝在线将通过一系列背景调查手段来确保每位入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策，背景调查手段涉及刑事、职业履历和信息安全等方面，背景调查的程度取决于岗位需求。

5.2安全保密

5.2.1 员工保密

在入职后，所有的员工必须签署保密协议，确认收到并遵守公司的安全政策和保密要求，尤其关于客户信息和数据的机密性要求在入职培训过程中重点强调。此外，公司依据员工的工作角色进行额外信息安全培训，确保员工接触的用户数 据必须按照安全策略执行。

5.2.2董事会、股东会、高管保密

公司因为强大的技术实力和行业领先的客户服务数量，受到了专业投资机构的青睐，获得多轮融资。依据《中华人民共和国公司法》、《中华人民共和国合同法》、《中华人民共和国侵权责任法》、《非上市公众公司监督管理办法》以及包括但不限于《校宝在线（杭州）科技股份有限公司章程》（已在全国中小企业股份转让系统公告）、《股东大会议事规则》、《董事会议事规则》等在内的公司制度，任何股东均不会对公司的业务独立、机构独立、人员独立、资产完整、财务独立、经营独立产生不利影响，公司在采购、研发、销售等方面与所有股东保持独立，且客户信息对于任何股东均予以保密。

5.2.3 用户知识产权保障

校宝在线高度重视用户知识产权保障。凡与校宝在线达成合作并签订合同的用户，其录入校宝软件或利用校宝软件形成的数据信息不仅受到知识产权相关法律的保护，亦受到与校宝在线之间的合同条款的保护。在每一份校宝软件的合同中，校宝在线均与用户约定，用户录入校宝软件的数据信息的使用权及所有权均仅归属于用户，用户有权在使用校宝软件期间随时免费导出其录入校宝软件的数据信息；并且，校宝在线进一步书面承诺保护用户信息安全，用户于校宝软件项下的数据库，除校宝在线指定人员可以维护外，不被任何他方获取或利用。

5.3开发流程安全

5.3.1 需求安全

校宝技术工程师团队在开发流程的各个阶段中都引入了安全保障手段：

图表八 开发流程

5.3.2开发安全

校宝技术开发团队制定了完整的使用安全规范和代码检查等方案，避免开发人员写出不安全的代码。

5.3.3测试安全

校宝测试团队使用安全扫描工具进行系统检测，避免对外暴露接口，保证系统安全性。

5.3.4项目发布安全

校宝技术团队负责人，将依据上述环节评价结果决定项目是否发布。进行层层把关，严谨地进行评审项目各环节。

5.3.5安全隐患应对

校宝运维工程师进行安全运营及事件应急响应方案设计。面对安全隐患，进行实时监测并提供及时有效的应对方案。

六、安全认证与合作

· *除了校宝本身的防护措施，我们是否还能得到别的安全支持？*

6.1国际最高标准信息安全管理体系认证及质量管理体系认证


CCCI

信息安全管理体系认证证书

注册号：02117I10125R0M

兹证明

校宝在线（杭州）科技股份有限公司

统一社会信用代码：91330108552697774F

注册地址：中国·浙江省·杭州市滨江区六和路368号一幢（北）三层D3020室

办公地址：中国·浙江省·杭州市西湖区文三路华星时代广场A座2005-2007

信息安全管理体系符合

ISO/IEC 27001:2013

本证书覆盖范围如下：

与计算机应用软件开发相关的信息安全管理活动。

（适用性声明版本：V1.0）

本证书有效期自2017年5月15日至2020年5月14日

认证范围涉及法律法规要求的行政许可、资质许可、强制性认证的，证书与资质共同使用有效。

在正常接受年度审核的情况下，与年度监督保持通知一并使用有效。

本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询。

华夏认证中心有限公司

总经理：

http://www.ccci.com.cn

颁证日期：2017年5月15日

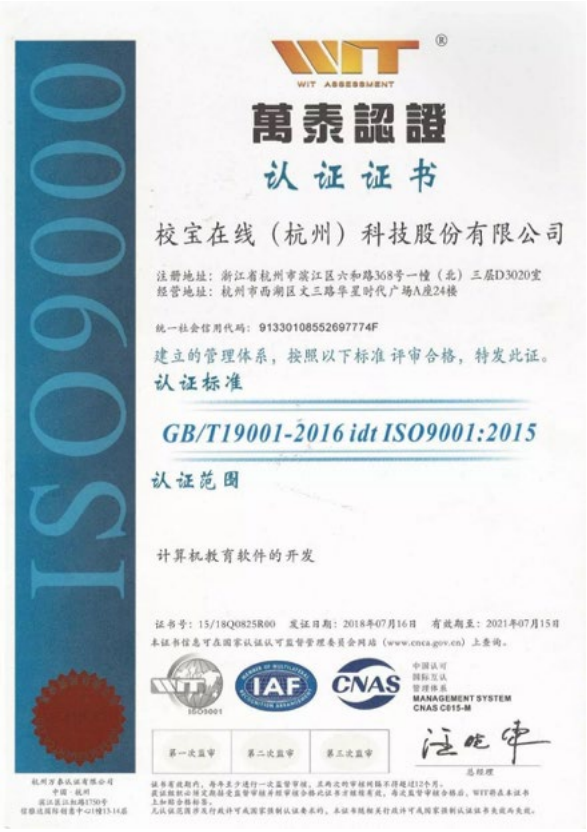
IAF

CNAS

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C021-M

图表九 信息安全管理体系认证证书

校宝在线的信息安全防护成果是受到第三方权威机构认证的。目前，校宝在线已经获批“信息安全管理体系认证证书”。此前阿里云、钉钉等企业服务领域的行业标杆都曾先后获得这张证书，并将此视为对客户信息安全的承诺。获得这张证书，意味着受认证企业的信息安全管理体系符合“ISO/IEC 27001: 2013”这个行业标准。该标准是国际上最权威、最严格、也是最被广泛接受和应用的信息安全管理标准，由知名的ISO 9000系列管理标准制定者BSI所倡导制定。



图表十 质量管理体系认证证书

2018年，校宝在线正式获得ISO 9001:2015质量管理体系认证，是行业内少数获得此类认证的服务商。获得该认证的企业，被证明具有稳定的提供满足顾客要求和法规要求的产品能力，各项管理满足标准要求，达到国际水平。产品和服务在国际市场中也能畅通无阻。通过认证的企业每年至少需要接受监督审核一次。企业必须以该标准严格要求自身，否则不能通过认证和审核。获得认证表明，校宝在各个环节都达到国际水平，产品和服务不仅让客户满意，也在行业里具有标杆作用。

6.2国家非银行机构最高级别信息安全认证


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，校宝在线（杭州）科技股份有限公司 单位的：

第 三 级 学校管理 系统

予以备案。

证书编号： 330118-99056-00001

中华人民共和国公安部监制

杭州市公安局 专用章

备案公安机关公章

2018 年 11 月 08 日

图表十一 国家信息系统安全等级保护三级备案证明

2018年，校宝在线获得国家信息系统安全等级保护三级备案。国家信息系统安全等级保护三级是对非银行机构的最高级别信息安全认证，属于国家监管级别，由公安机关进行评定，主要应用于地市级以上国家机关、重要企事业单位。例如铁路网站、医疗、社保等重要政府涉密系统。该备案审核极为严格，机构的安全体系需要通过5道审核流程，涵盖安全技术、安全管理两大类别共10个维度，测评分类73类，包含近300项要求。这是互联网行业内获得该证书较少的重要原因之一，在教育信息化行业，通过该项认证的企业屈指可数。

6.3国家级安全防护机构保障

校宝在线和国内著名的安全社区以及提供安全产品和服务的公司合作，通过更深入的方式，进一步加固系统的安全性。

值得一提的是，校宝在线于2017年1月17日与中国领先的信息安全产品提供商安恒信息签署安全战略合作协议，双方将充分发挥各自优势，产业协同，战略携手“教育机构SaaS领域数据安全”，合力共筑教育信息领域“安全生态圈”。双方还将建立新兴的互联网教育行业的威胁情报共享机制，对教育行业SaaS的数据架构、安全态势进行深入研究和讨论，分享信息安全领域的最新动态与研究成果，打造互联网教育行业的安全社区，共同推动教育机构SaaS形成更深层次的安防服务与解决方案。

6.4全球顶尖技术厂商支持

校宝在线积极与全球顶尖的服务商，如微软、阿里云、钉钉等企业合作，期间也因为优秀的企业资质接到了大牌服务商主动伸出的橄榄枝。2017年1月，校宝在线入选微软加速器计划，并成为首家中国地区入选的教育培训SaaS服务提供商。作为人工智能、大数据领域的创新型公司，校宝获得了微软认知服务(Microsoft Cognitive Services)API和工具包(CNTK)的技术支持，并且能够借助微软自身的生态资源，例如用微软Azure云服务平台，给予团队聚力探索创新很大助力。

此外，微软集团还对校宝在线开放了一些宝贵的原生资源，例如校宝的后端开发框架即为微软出品。这些技术支持加速提升了校宝系列产品的稳定性和安全性，为广大教育培训机构提供了更好的用户体验。

七、校宝安全大事纪

2010年10月 校宝信息安全体系初步构架完成。

2012年12月 校宝与阿里云达成战略合作，接入阿里云服务。

2013年5月 校宝信息安全体系完成第三次重要升级。

2015年6月 校宝完成双机热备负载均衡架构升级，数据实现远端备份。

2015年8月 校宝学校管理系统全面迁移云平台，完成前端负载均衡＋服务集群架构升级，数据实现实时多地三备份，比如数据敏感度区分处理。

2016年6月 系统遭受峰值流量为21.15G的DDoS攻击，系统未出现停服故障。同月，系统架构再做升级，当承受更极限流量攻击出现系统抖动时，可快速切换集群提供服务。

2017年1月 校宝在线与安恒信息签署安全战略合作协议。(见注1)
校宝在线成为微软加速器中国地区首家入选的教育培训SaaS服务提供商。(见注2)

2017年5月 校宝在线获批“信息安全管理体系认证证书”。

2018年7月 校宝在线正式获得“ISO 9001:2015质量管理体系认证”，是行业内少数获得此类认证的服务商。

2018年11月 校宝在线获得“国家信息系统安全等级保护三级”备案。

2019年11月 校宝在线官网上线“安全中心”，更好的公示系统和业务的安全维护工作以接受社会监督。

图表十二 校宝安全大事纪

注释1:安恒信息为北京奥运会，国庆60周年庆典，G20峰会，上海世博会等大型活动全方位网络信息安全保障方。
注释2:微软加速器·上海于2016年10月14日开启首期招募后，加速器收到了数千份项目的正式申请书，最终仅有14家创新创业企业入选，录取率低于2%，校宝有幸入选并为中国地区入选的首家教育机构SaaS服务提供商。

【结　　语】

推动教育服务加速进步，是近千名校宝人不懈努力、坚守的使命。

而保障信息安全，是校宝在线实现该使命的核心准则。

近十年来，校宝在线以同行业无法比拟的人力与资源、资金投入，打造出校宝安全体系为核心的信息安全堡垒，经过实践检验，合作伙伴、国际第三方机构等的认证，铸就了行业高标准。

我们许诺，在更加坚固的信息安全堡垒下，校宝在线的整体解决方案将让更多的教育者更轻松、更期待，作为行业领军者，校宝在线将为教育培训及K12教育行业赋予更多新可能！

【版权声明】

【服务声明】

本文档仅供参考。对于本文档中的信息，校宝在线不作明示、默示的保证。本文档基于现状编写。在本文档中的信息和意见，包括网址和其他互联网网站参考，均可能会改变，恕不另行通知。您将承担使用它的风险。

本文件未授予您任何校宝在线产品的任何知识产权的法律权利。您可以复制和使用本文档内容作为您内部以参考为目的的使用。


校宝在线
管理学校 就用校宝