



## 目录

企业文化 .....	◎ P01
企业简介 .....	◎ P02-03
发展历程 .....	◎ P04-05
圣博润全系列产品介绍 .....	◎ P06-07
安全防护系列产品 .....	◎ P08-14
安全检测与审计系列 .....	◎ P15-21
安全管理系列 .....	◎ P22-28
工业互联网安全系列 .....	◎ P29-34
云计算安全系列 .....	◎ P35-37
安全服务 .....	◎ P38
IT 认证咨询服务 .....	◎ P39
技术服务体系 .....	◎ P40-41
公司荣誉和资质 .....	◎ P42
客户名录 .....	◎ P43-44



## 企业文化

# 抱**圣贤**之思 怀**博学**之志 尽**润泽**之力

**企业宗旨:** 以持续技术创新推动中国信息安全发展

**企业愿景:** 做网络安全行业领军企业

**产品理念:** 市场导向、技术为先

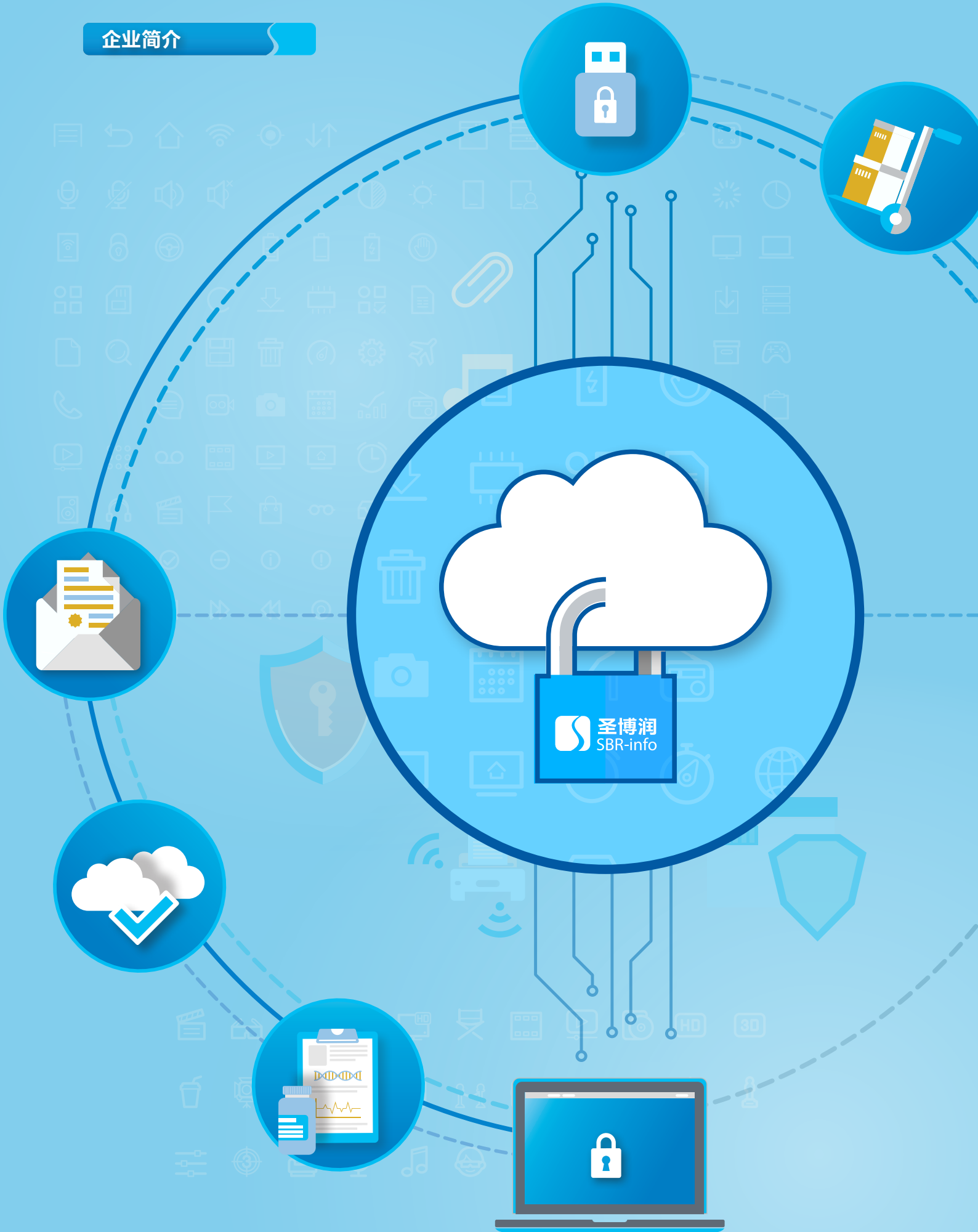
**服务理念:** 专注安全、诚信创新

**抱圣贤之思:** 格局为重、知人善用。以圣贤为榜样, 锻炼前瞻视野和格局意识, 以人为本、尊重员工, 为员工成长和个性发展创造机会和条件。

**怀博学之志:** 志存高远、博学创新。以技术创新和市场需求为导向, 树立精品意识, 勇于开拓、追求卓越, 为企业技术创新和产品持续发展搭建培育孵化平台。

**尽润泽之力:** 创造价值、服务用户。为员工、企业、合作伙伴与社会创造价值, 开放分享、合作共赢, 为用户提供最高品质的网络安全产品与服务, 为国家网络安全和社会发展贡献力量。

企业简介



# 北京圣博润高新技术股份有限公司

北京圣博润高新技术股份有限公司是一家专注于网络安全技术研究、产品研发和安全服务的高新技术企业。公司注册资金11293.402万元。自2000年成立以来，先后推出了安全防护、安全检测与审计、安全管理、工业互联网安全、云计算安全五大类30余款网络与信息安全产品，其中堡垒主机产品连续五年市场占有率第一。圣博润公司也是专业的等级保护咨询服务提供商，为数百家行业客户提供了专业的等级保护咨询服务。

圣博润于2009年在新三板挂牌，并于2017年升入创新层，是中国网络安全五十强企业、中关村新三板2018年度成长力TOP30企业、CCTV《聚焦新三板》栏目主办的2018第二届中国新三板年度风云榜十强企业、2019年北京民营科技创新百强企业、2020年中国网络安全竞争力50强企业。公司曾承担科技部、工信部、北京市科委等多项国家和地方信息安全课题研究和信息安全专项。公司是国家网络与信息安全信息通报机制技术支持单位，承担了2008年北京奥运会、2016年杭州G20峰会、2017年“一带一路”国际合作高峰论坛、2018年工业互联网安全防护演练、2018年首届工业互联网安全大赛、2019年新中国成立70周年庆祝活动等众多国家重大活动及赛事的网络安全保卫技术支持任务。

圣博润公司在政府和央企行业有着众多的客户案例。公安部、海关总署、国家发改委、国家税务总局、国家统计局、财政部等五十多个国家部委，中国人民银行、中国工商银行、中国银行等数十家金融机构，中国中车集团、航天科技集团、中航工业集团等众多中央企业都选择了圣博润的产品与服务。

近年来，公司加大了新兴网络安全领域的技术研究和研发投入，在工控安全和工业互联网安全领域推出了一系列的安全产品，包括工业防火墙、工业网闸、工控安全监测与审计、工控系统安全检查工具箱、工业互联网安全评估平台、工业互联网安全态势感知平台在内的完整产品系列。业务覆盖了产品研发、课题研究、安全服务、解决方案、安全竞赛等方面。2018年，圣博润获中国工业信息安全十大用户信赖品牌奖、中国工业信息安全工控安全监测与审计系统值得信赖品牌奖，是工业互联网安全技术试验与测评工信部重点实验室首家技术支撑单位。

“抱圣贤之思，怀博学之志，尽润泽之力”，圣博润始终以国家网络安全事业为己任，以前瞻的视野和创新的思维为用户提供专业的网络安全咨询服务和网络安全整体解决方案，圣博润愿集中智慧与力量与广大用户和合作伙伴共建网络安全的广阔未来。

### 2000

- 6月19日北京圣博润高新技术有限公司成立
- 同年通过高新技术企业认证

### 2003

- 首款自主品牌产品“LanSecS®(莱恩赛克)内网安全管理系统”发布
- 公司通过软件企业认定

### 2006

- 通过ISO9001质量管理体系认证
- 成立安全服务团队,获国家信息安全测评中心颁发的“信息安全服务资质证书”

### 2008

- 完成股份制改制,更名为“北京圣博润高新技术股份有限公司”
- 圆满完成2008年北京奥运会信息安全保障工作,获得奥组委及公安部的肯定和嘉奖

### 2009

- 第一款等级保护管理产品“LanSecS®信息安全等级保护综合管理系统”正式发布
- 获北京信息安全评测中心颁发的“北京市信息安全服务能力等级证书”二级
- 获中国信息安全认证中心颁发的“信息安全服务资质认证证书”
- 2月18日登陆新三板(股票代码:430046)

### 2010

- 自主品牌产品“LanSecS®(堡垒主机)内控管理平台”正式发布
- 公司承担的北京市经信委《北京市党政机关办公计算机终端安全管理规范》课题研究项目顺利通过验收

### 2011

- 公司承担的工信部《党政机关办公计算机终端安全管理规范》、北京市经信委《北京市党政机关办公用计算机安全配置指南》等多项国家与地方信息安全课题研究项目顺利通过验收
- “LanSecS®内网安全管理系统”获科技部科技型中小企业技术创新资金支持
- 公司承担的国家发改委信息安全专项《重要信息系统安全保护专业化服务平台》“等级保护测评和评估支撑工具研究”子课题顺利通过验收



## 2013

- 通过ISO27001信息安全管理体系认证
- “LanSecS®信息安全等级保护检查工具箱”入围公安部十一局等级保护检查产品列装目录
- 公司成为国家网络与信息安全信息通报机制32家技术支持单位之一
- 公司发起并成立了北京网络行业协会等级保护专业委员会

## 2015

- 推出LanSecS®网络安全管理工作平台、LanSecS®密级标志生成与管理产品
- 获“信息安全等级保护安全建设服务机构能力评估合格证书”

## 2016

- 成为中国网络空间安全协会首批理事单位
- 圆满完成G20峰会网络与信息安全保障任务
- 共同发起成立中国行业(私有)云安全能力者联盟,推动云安全技术的应用和推广
- 获“2016年度中国信息安全服务领军企业奖”

## 2017

- 荣获新三板“十大最具投资价值挂牌企业奖”
- 公司入选新三板创新层
- 顺利完成“一带一路”国际合作高峰论坛信息安全保障任务
- 工控安全系列产品发布,全面进军工控安全与工业互联网安全领域

## 2018

- 入选CCTV《聚焦新三板》栏目主办的2018第二届中国新三板年度风云榜十强企业
- 获得工业信息安全十大用户信赖品牌奖及监测与审计系统值得信赖产品奖
- 成为工业互联网安全技术试验与测评工信部重点实验室首家技术支持单位
- 作为协办单位参加“2018年首届工业互联网安全防护演练”活动并顺利完成技术支持与保障任务
- 作为技术支持单位参加“护网杯”2018年网络安全防护赛暨首届工业互联网安全大赛

## 2019

- 荣获公安部“新中国成立70周年庆祝活动网络安全保卫工作优秀技术支持单位”荣誉称号
- 荣获“国家信息安全漏洞库(CNNVD)三级技术支持单位”
- 入选国网网安“2019泛在电力物联网安全十佳优秀解决方案”
- 进一步补充工业互联网安全产品线,推出了:工业交换机、工控漏洞扫描系统、红军实战协同平台、圣博润网络流量安全分析系统、网络应用性能分析系统5款新产品

## 2020

- 荣获国家信息安全漏洞库“2019年度优秀技术支持单位(CNNVD)”荣誉称号
- 入围中国网络安全产业联盟“2020年中国网络安全竞争力50强”
- 加入华为安全商业联盟,正式成为华为认证服务解决方案伙伴(CSSP)



### 安全防护系列产品

LanSecS<sup>®</sup> 第二代防火墙系统 (P09)  
LanSecS<sup>®</sup> Web应用防护系统 (P10)  
LanSecS<sup>®</sup> 数据库安全防护系统 (P11)  
LanSecS<sup>®</sup> 网络终端接入控制系统 (P12)  
LanSecS<sup>®</sup> 应用交付控制与管理平台 (P13)  
圣博润恶意代码检测与防御系统 (P14)



### 安全管理系列产品

LanSecS<sup>®</sup> 网络安全管理工作平台 (P23)  
LanSecS<sup>®</sup> 内网安全管理系统 (P24)  
LanSecS<sup>®</sup> USB移动存储介质使用管理系统 (P25)  
LanSecS<sup>®</sup> 电子文件密级标志管理系统 (P26)  
圣博润主机监控与恢复系统 (P27)  
圣博润网络安全事件应急处置工具箱 (P28)



### 安全检测与审计系列产品

LanSecS<sup>®</sup> (堡垒主机)内控管理平台 (P16)  
LanSecS<sup>®</sup> 主机监控与审计系统 (P17)  
LanSecS<sup>®</sup> 网络边界完整性检查管理系统 (P18)  
LanSecS<sup>®</sup> 信息安全等级保护检查工具箱 (P19)  
LanSecS<sup>®</sup> 日志审计系统 (P20)  
LanSecS<sup>®</sup> 安全管理平台 (P21)



### 工业互联网安全系列产品

LanSecS<sup>®</sup> 工业控制防火墙系统 (P30)  
LanSecS<sup>®</sup> 工控安全隔离与信息导入系统 (P31)  
LanSecS<sup>®</sup> 工控安全监测与审计系统 (P32)  
LanSecS<sup>®</sup> 工控系统安全等级保护检查工具箱 (P33)  
圣博润工控主机安全防护系统 (P34)

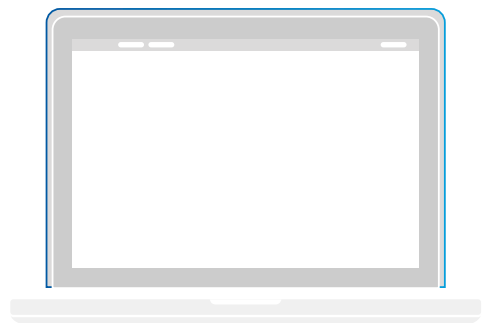
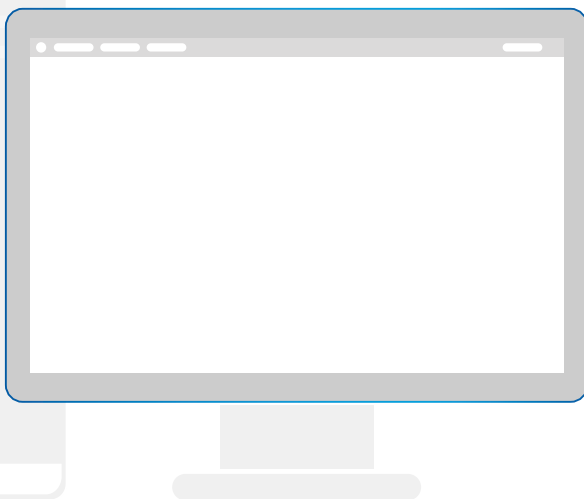
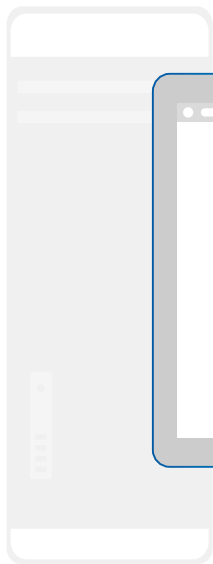




## 云计算安全系列产品

LanSecS® 云堡垒主机 (P36)

LanSecS® 云用户行为分析系统 (P37)



安全防护系列产品



# 安全防护

## 系列产品



## LanSecS<sup>®</sup> 第二代防火墙系统



LanSecS<sup>®</sup>第二代防火墙系统采用应用识别、网络可视化及带宽管理等技术, 提供网络行为管控、web安全防护和网络业务优化等安全功能, 全面应对应用层的安全威胁, 为用户提供高性能、直观有效的应用层一体化安全防护解决方案。

### 产品功能

- 全面的入侵防御
- 专业的病毒查杀
- 精细的上网行为管理
- Web应用防护
- 遏制带宽滥用
- 安全可视化

### 产品特色

- 模块化并行处理, 减少处理时间
- 高可靠性, 双机HA, Bypass
- 支持4G扩展, 外置上网卡
- 多接口模块: 支持千兆光、电模块、万兆光模块
- 支持VPN级 HA: 主备切换时, 业务不中断
- 身份认证: 支持短信和微信用户认证
- 全面的功能——支持IPSec VPN、SSL VPN、内容过滤、上网行为、应用识别、IPS、防病毒等多种功能

### 客户价值

- 全面应对应用层的安全威胁, 保证内部网络安全
- 智能化主动防御, 快速响应机制, 保障用户环境的安全性
- 完备的基础防火墙特性, 实现用户访问标准化和安全性
- 应用层数据防泄漏



## LanSecS<sup>®</sup> Web应用防护系统



LanSecS<sup>®</sup>Web应用防护系统(LWF)作为一款新型的Web应用防护产品,专注于Web应用系统的全面防护(Web防护、DDoS防护、网页防篡改),支持双向的安全检测和防护,抵御OWASP Top10等各类Web安全威胁和拒绝服务攻击。产品支持多种部署模式,为用户提供专业、灵活、高性能、高可靠的Web应用防护解决方案。

### 产品功能

- 产品内置多种防护规则库,支持防护各种常见安全风险:SQL注入、Cookie注入、命令注入、XSS跨站攻击、Webshell上传下载、DDoS攻击、cc攻击、后门、非法HTTP协议请求、Web服务器漏洞攻击、核心文件非授权访问、路径穿越、爬虫、扫描、敏感字、URL访问控制等安全防护。
- 文件权限级防篡改功能,即使黑客攻陷服务器也无法修改网站文件
- 支持HTTPS网站减压和防护
- 具有应用负载均衡功能,可以适应大规模网站架构

### 产品特点

- 支持实时在线升级防护规则库:及时更新最新安全风险库;
- 预置多级防护策略模板:网站快速上线,快速切换防护级别;
- 支持链路聚合部署:提高链路带宽;
- 支持vmware、KVM等虚拟化或云环境部署;
- 图文仪表盘:直观显示安全风险统计、流量统计等信息;
- 集成调试工具:快速处理网络故障。

### 客户价值

- 有效保护网站免遭各种网络攻击,保证业务连续性以及安全性
- 提供详细的攻击日志记录,满足合规要求,便于事后追溯



## LanSecS<sup>®</sup> 数据库安全防护系统



LanSecS<sup>®</sup>数据库安全防护系统是基于数据库协议分析与控制技术,实现对数据库操作的危险指令阻断、访问行为控制、安全态势分析、全面行为审计的数据库安全主动防御产品。

### 产品功能

- 虚拟补丁漏洞库,提前阻断针对漏洞的攻击行为
- 提供SQL注入特征库,提前预防阻断SQL注入攻击行为
- 提供行数限制功能,防止大规模的数据泄露和篡改
- 提供SQL语句黑白名单支持
- 提供自学习模式,防止由于不规则的合法语句造成业务中断
- 全面行为审计,方便事后溯源

### 产品特点

- 全面的数据库入侵阻断
- 高度应用兼容
- 全面的数据库版本类型支持
- 仪表盘实时安全态势分析
- 快速灵活的产品部署方式
- 提供自学习模式,同时可精细化自定义各种安全策略

### 客户价值

- 合规达标,符合安全规范要求;
- 抗攻击抗抵赖,提高数据库应用的访问安全能力;
- 满足数据库数据“机密性、完整性、可用性”的安全要求;
- 提高业务连续性和灾备能力。



## LanSecS<sup>®</sup> 网络终端接入控制系统



LanSecS<sup>®</sup>网络终端接入控制系统采用纯旁路部署模式,在不改变用户的网络环境前提下,对非法接入网络的终端或不满足网络健康要求的终端进行智能识别、隔离与修复,从终端准入方面做到“事前控制,事中监控,事后审计”的全生命周期管理,是软硬件一体的网络终端接入控制产品。

### 产品功能

- 网络边界识别
- 网络边界威胁感知
- 网络边界准入控制
- 全网IP地址管理
- 网络设备端口可视化及联动管理
- 设备智能识别与修复

### 产品特点

- 支持多协议混合准入技术
- 网络可视化
- IP地址可视化
- 支持无客户端部署(非控件)
- 旁路接入,对业务零影响

### 客户价值

- 确保入网设备符合安全管理规范,防止非法设备接入网络,防止不合规设备引入安全风险,提高整体网络安全性
- 自动化隐患修复,提高运维效率及降低终端运维成本
- 彻底杜绝非法内联、外联,确保满足等保合规要求
- 自动采集资产信息,提高网络故障处理能力、降低网络总体管理成本



## LanSecS<sup>®</sup> 应用交付控制与管理平台



LanSecS<sup>®</sup>应用交付控制与管理平台全面实现服务器负载均衡、链路负载均衡、全局负载均衡以及应用优化与加速、广域网优化、安全防护等功能,通过整合数据通信和网络安全两大方向的经验与技术,以数通的角度设计并研发高效硬件、数据处理机制,以安全的角度落地安全网关、数据流管理与控制,结合领先的虚拟化技术,为用户提供最优质的应用交付质量提升解决方案。

### 产品功能

- 服务器负载均衡
- 链路负载均衡
- 全局负载均衡
- 应用优化与加速
- 安全防护

### 产品特点

- 支持多种负载算法
- 基于多种协议的健康检查
- 异地数据中心的高可用性与容灾
- 提供主主、主备部署方式
- IPv6与IPv4转换
- 可虚拟多台设备同时独立使用

### 客户价值

- 链路负载,提升链路资源的利用率
- 提升用户访问应用服务器的交付效率与质量
- 有效保护用户WEB网站,抵御常见Web攻击
- 硬件加速芯片完成高性能压缩数据处理





## 圣博润恶意代码检测与防御系统

圣博润恶意代码检测与防御系统(简称LEDR),采用机器学习及大数据分析技术、高级行为分析技术和漏洞利用检测技术,结合有效的威胁情报信息,针对类似于勒索病毒等高级威胁提供及时检测和快速响应。

### 产品功能

- 检测和防御Oday攻击
- 未知恶意代码检测与防御
- 黑白名单功能
- 安全威胁追踪与取证
- 应急响应与处置

### 产品特点

- 轻量级客户端运行与维护
- 高效准确的威胁发现能力
- 有效识别和防范Oday、未知恶意威胁
- 完整的恶意代码处置——事前防御,事后补救

### 客户价值

- 主动式免疫保护,有效抵御勒索病毒等恶意软件攻击
- 获得主动防御Oday攻击和未知恶意威胁的能力



# 安全检测与审计

## 系列产品



## LanSecS® (堡垒主机) 内控管理平台



LanSecS® (堡垒主机)内控管理平台集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体,为用户提供安全可靠的运维管理与审计解决方案。

### 产品功能

- 统一身份认证
- 资源集中管理
- 统一访问授权
- 操作行为控制
- 统一审计管理

### 产品特点

- 充分考虑自身安全,采用安全加固操作系统以及完善的加密措施
- 多样化的访问控制能力,支持交叉授权、命令过滤、多级审批
- 更加便捷的易用性,支持前端双机配置、AD同步及认证
- 更强的用户生产环境适应性,支持全面国产化及IPV6,应用系统自定义接入
- 更强的用户体验度,支持用户自由选择Web方式或运维客户端方式运维

### 客户价值

- 实现集中账号管理,降低管理费用
- 实现集中身份认证和访问控制,避免冒名访问,提高访问安全性
- 实现集中授权管理,简化授权流程,减轻管理压力
- 实现实名运维审计,满足安全规范要求



## LanSecS<sup>®</sup> 主机监控与审计系统



LanSecS<sup>®</sup>主机监控与审计系统是针对涉密网络中的终端主机、安全策略配置、安全监管与审计等提供统一管理,完全满足涉密环境中对主机管控的要求,并符合分保标准要求的产品。

### 产品功能

- 终端防泄密管理
- 资产管理
- 终端安全管理
- 补丁分发管理
- 行为管理

### 产品特点

- 先进的系统架构和稳定的系统性能
- 分布负载均衡和动态性能扩展
- 分级分组的部署策略

### 客户价值

- 主机机密信息防护(机密性)
- 主机可信管理(可信性)
- 用户行为监控和审计(可控性)
- 主机加固和运行监控(可靠性)





## LanSecS® 网络边界完整性检查管理系统

LanSecS®网络边界完整性检查管理系统可快速检测、定位并阻断对于网络私自扩展的行为,包括路由器或HUB接入, AP及随身Wifi接入, BYOD接入等违规内联行为,同时也可以协助用户快速有效的完成网络IT资产梳理。

### 产品功能

- 检测非法内联行为
- 检测通过手机热点方式的非法外联行为
- 全网IP地址审计追溯, 资产识别
- 检测其他违规行为, 如系统不合规、VM虚拟机等
- 提供丰富的图形化报表

### 产品特点

- 一款软件产品, 部署无需客户端(非插件), 对于终端来讲是无感知检测
- 纯旁路部署, 无需改变用户现有的网络环境, 对产品位置无特殊要求(服务器IP地址全网可通即可)
- 可以快速检测违规设备并通过拓扑图定位, 结合SNMP协议, 通过关闭交换机端口, 可以实现对违规设备的阻断

### 客户价值

- 对非法扩大网络边界的行为发现并告警
- 对于违规接入的移动设备和无线设备发现并告警, 支持精确定位
- 快速完成网络内资产识别和梳理
- 强大界面展示和日志记录, 告警行为TOP记录



## LanSecS<sup>®</sup> 信息安全等级保护检查工具箱



LanSecS<sup>®</sup>信息安全等级保护检查工具箱是针对等级保护工作监管部门、被监管单位研发的等级保护检查、自查支撑工具,为等级保护检查、自查工作的开展提供专业化、流程化的技术支持,是提升检查工作效率,保证检查工作质量的合规性产品。

### 产品功能

- 流程化指引的工具箱管理系统
- 配套专业化等保合规检查的十款技术工具
- 融合检查工作实施经验、专家知识和分析模型的知识库管理
- 综合分析、多样化图形展示
- 自动生成权威的检查结果报告

### 产品特点

- 检查工作可视化、流程化指引
- 易用、实用的技术检查工具,自动关联检查指标
- 丰富的数据接口,便于信息共享
- 权威、全面的知识库积累
- 无缝对接监管部门的数据分析平台

### 客户价值

- 全面支持监管部门等级保护检查工作的开展
- 直观地展示被检查对象的安全保护状况
- 自动化生成权威性的检查报告
- 提高工作效率和检查质量



## LanSecS<sup>®</sup> 日志审计系统

LanSecS<sup>®</sup>日志审计系统是一款融合大数据和机器学习技术开发的,收集、处理并关联分析网络中各类软硬件资产日志,以及时发现并处置网络安全事件,满足各行各业用户安全合规审计和安全分析需求的产品。

### 产品功能

- 日志数据采集
- 日志数据存储
- 日志数据分析
- 安全事件告警管理

### 产品特点

- 采用业界最新的大数据和机器学习技术,来支撑海量日志处理
- 可视化日志范式化,更灵活、更便捷
- 基于机器学习的日志模式识别,更清晰、更高效

### 客户价值

- 提高工作效率,更加快速准确的识别安全告警,发现违规行为,进行应急响应
- 通过持续有效的安全事件分析识别安全事故、策略冲突、欺诈行为和违规操作行为
- 对设备和系统的日志及安全事件统一存储,符合企业和组织的需要,从合规合法性上满足了用户、行业及国家的要求



## LanSecS<sup>®</sup> 安全管理平台



LanSecS<sup>®</sup>安全管理平台集安全可视化、监测、预警和响应处置于一体,通过多种数据、分析方法构建动态的多层次、全天候网络安全态势感知,结合等级保护管理,为客户提供可落地的安全保障能力,构建网络安全动态深度防御体系。

### 产品功能

- 资产自动识别与管理
- 漏洞全生命周期管理
- 安全风险管控
- 智能安全分析
- 安全态势感知

### 产品特点

- 灵活的大数据技术架构
- 主被动结合的资产发现技术
- 基于机器学习的数据模式识别技术
- 内置丰富的合规报表及报告

### 客户价值

- 日常安全运维和等保管理工作的有力工具
- 全方位全天候感知网络内外的安全态势
- 资产和漏洞的全生命周期管理
- 多维度安全事件智能分析与响应

# 安全管理 系列产品





## LanSecS<sup>®</sup> 网络安全管理工作平台



LanSecS<sup>®</sup>网络安全管理工作平台是网络安全管理工作开展的综合性支撑工具,支持政府及企事业单位对安全通报、等级保护、安全检查、应急演练等工作的开展进行工作部署、工作过程监控及工作结果统计分析。

### 产品功能

- 用户日常安全工作管理
- 等级保护工作管理
- 网络安全检查工作管理
- 安全通知通报
- 安全应急工作管理
- 网络安全工作统计分析

### 产品特色

- 用户网络安全管理工作综合性平台
- 功能丰富,覆盖网络安全各层级的工作管理
- 平台简单易用、功能丰富,适用于各级安全管理人员使用
- 强大的统计分析、图形化展示、报表下载
- 可定制化强,各模块可以根据需求进行灵活组合

### 客户价值

- 支持用户开展等级保护工作
- 掌握本行业或本单位等级保护工作开展情况
- 掌握信息系统安全保护状况
- 辅助用户进行网络安全政策、行规标准、知识库等规范化管理



## LanSecS<sup>®</sup> 内网安全管理系统



LanSecS<sup>®</sup>内网安全管理系统是依照公安部终端主机管理相关标准开发,用于政府、企业及组织内网终端计算机安全加固、安全运维及安全审计管理的软件系统。

### 产品功能

- 终端安全审计
- 终端安全运维
- 终端安全加固
- 资产管理

### 产品特点

- 全方位的安全审计功能,有效地防止信息泄密
- 多层次的安全措施,保证系统运行的安全可靠
- 丰富的策略管理模式
- 灵活多样的统计报表功能

### 客户价值

- 有效地防止信息泄密
- 保证系统运行的安全可靠
- 系统维护方便、快捷



## LanSecS<sup>®</sup> USB移动存储介质使用管理系统



LanSecS<sup>®</sup>USB移动存储介质管理系统是针对USB移动存储介质进行统一的使用权限管理、使用周期管理及使用行为审计管理的软件产品。

### 产品功能

- 移动存储介质权限控制
- 移动存储介质使用审计
- 移动存储介质生命周期管理
- 资产管理

### 产品特色

- 强大的终端安全态势分析
- 先进的系统架构和稳定的系统性能
- 生命周期中的高可控性和高安全性

### 客户价值

- 规范移动存储介质管理
- 防止因移动存储介质发生的泄密
- 全程可控可审计



## LanSecS<sup>®</sup> 电子文件密级标志管理系统



LanSecS<sup>®</sup>电子文件密级标志管理系统是为满足涉密行业安全保密技术要求,将电子文件密级信息与电子文件进行绑定,实现标志信息与电子文件主体不可被非授权分离,其自身不可被非授权篡改,并能基于密级标志实现对文件细粒度权限控制,将涉密电子文件从起草、定密、解密全生命周期管理的一套系统。

### 产品功能

- 定密流程管理
- 标志管理
- 强制标密
- 文件管控
- 审计与日志

### 产品特点

- 全面的电子文件格式支持
- 良好的系统兼容性
- 完善的第三方系统集成接口
- 针对不同环境,智能选择加标算法



### 客户价值

- 有效规范定密、标密、解密工作的开展
- 涉密电子文件流转易跟踪,方便追本溯源
- 提高涉密电子文件识别与保护能力





## 圣博润主机监控与恢复系统



圣博润主机监控与恢复系统从UEFI底层开始监控主机系统的运行细节,记录系统的所有运行日志,可实现及时预警、阻断与恢复等功能,还能记录整个主机系统的运行过程及操作记录,使主机系统的运行变得更加透明、安全可控。

### 产品功能

- 全息恢复
- 文件恢复
- 系统监控
- 程序分析
- 硬盘穿越
- 全息恢复线路图

### 产品特点

- 数据恢复
- 文件溯源
- 主机系统保护

### 客户价值

- 系统快速恢复,彻底解放IT部门的运维负担
- 全息记录、逆向推导,解决文件丢失的烦恼



## 圣博润网络安全事件应急处置工具箱



圣博润网络安全事件应急处置工具箱是针对网络安全事件应急处置工作设计开发的一套专业设备,是应急处置人员进行应急取证、事件处置、数据分析工作的专业工具。

### 产品功能

- 主机日志采集分析
- WEB信息采集分析
- 系统信息采集分析
- 内核信息采集分析
- 数据库日志采集分析
- 攻击行为识别/回溯

### 产品特点

- 集成度高,分析应急处置工具一体化
- 依照应急处置工作流程智能开展工作
- 支持本地、远程及云平台采集安全事件
- 多类型操作系统、数据库、网站中间件采集分析
- 安全事件多维度自动关联分析,自动生成应急处置报告

### 客户价值

- 解决了网络安全事件应急处置工作抓手问题
- 解决了应急处置工具一体化、标准化问题
- 解决了应急处置报告自动化、科学化问题
- 解决了应急处置工作效率问题

工业互联网安全系列产品

# 工业互联网安全 系列产品



## LanSecS<sup>®</sup> 工业控制防火墙系统



LanSecS<sup>®</sup>工业控制防火墙系统旨在为工业控制网络提供基于工业控制应用层协议分析的边界访问控制解决方案。该产品通过应用基于白名单的安全策略,实现对网络边界流量的访问控制,为管理信息网与控制网的内部各区域连接提供安全保障,并且可实现对Modbus/TCP、OPC Classic、DNP3、S7、IEC60870-5-104、MMS、Ethernet/IP等协议的深度分析。

### 产品功能

- 网络安全管理
- 路由管理及地址转换
- 工控网络的白名单和黑名单
- 多种VPN功能

### 产品特点

- 基于流的状态检测技术
- 工控协议深度解析
- 多种工作模式确保网络适应性
- 工业级高可靠性

### 客户价值

- 满足工控行业等级保护合规要求
- 防范外部恶意攻击和入侵
- 杜绝内部违规访问行为





## LanSecS<sup>®</sup> 工控安全隔离与信息导入系统



LanSecS<sup>®</sup>工控安全隔离与信息导入系统(简称隔离网闸)不仅实现了对基于TCP/IP协议体系攻击的彻底阻断,也实现了对主流工业网络协议的广泛、深入支持和保证工业控制网络数据的安全传输,解决了传统安全隔离设备无法适用于工业控制网络的难题。

### 产品功能

- 工业网络隔离技术
- 双模式数据摆渡
- 测点级访问控制
- 数据断线缓存
- 分布部署和集中管理
- 日志管理

### 产品特点

- 软硬件高可靠性
- 丰富的工业协议
- 专家级数据安全

### 客户价值

- 服务器数据不被篡改或非法访问
- 生产网安全保障



## LanSecS<sup>®</sup> 工控安全监测与审计系统



LanSecS<sup>®</sup>工控安全监测与审计系统是针对工业控制网络设计的、提供网络监测、协议分析和安全审计功能的信息安全产品。该产品通过对工控网络流量的采集、分析、监测,结合特定的安全策略,快速有效识别出工业控制网络中存在的网络异常事件和网络攻击行为并进行实时告警。

### 产品功能

- 工控网络实时监测
- 工控网络安全审计
- 工控黑名单
- 工控白名单
- 流量异常监测

### 产品特点

- 精准的工控协议分析
- 专业的工控漏洞特征库
- 可靠的软硬件一体化架构
- 灵活可扩展的私有协议接口

### 客户价值

- 自主知识产权,杜绝后门隐患
- 实时网络监测,保障正常生产
- 网络安全审计,便于事件追踪
- 防御策略建议,完善防御体系



## LanSecS<sup>®</sup> 工控系统安全等级保护检查工具箱



LanSecS<sup>®</sup>工控系统安全等级保护检查工具箱通过对工控系统安全管理和技术指标的评测,以及对系统或设备的技术检测,能够对工控系统的业务对象进行全面的或针对性的安全评估,并自动生成专业的安全评估报告,是机构或企业开展工控系统安全等保检查工作的重要支撑工具。

### 产品功能

- 完善的检查计划管理
- 清晰的检查流程引导
- 可靠的等保检查措施
- 全面的工控知识库

### 产品特点

- 高效、便携
- 标准、规范
- 简单、易用
- 权威、专业

### 客户价值

- 实现常态化安全检查,提高工业控制系统安全性
- 专业、合规的检查工具,保证检查工作规范化
- 通过有效的技术检查手段,提升工业企业安全防护能力





## 圣博润工控主机安全防护系统

圣博润工控主机安全防护系统是专门为工控网络操作员站终端计算机打造的一款主机安全防护与管理软件。该产品以白名单主动防御为核心、以完整性保护为目标,通过对操作员站终端计算机提供安全加固、白名单管理、移动存储介质注册管理、主机安全审计等功能,有效抵御未知病毒、木马、恶意程序、非法入侵等针对终端的攻击手段,解决终端计算机的安全防护问题。

### 产品功能

- 工控主机的恶意代码防范
- 应用程序白名单管控
- USB存储设备管控
- 工控主机外设管控
- 日志管理、告警记录

### 产品特点

- 自动化建立工业主机安全基线
- 轻量级部署,满足实时性要求
- 无需频繁更新,更加适用工业生产环境

### 客户价值

- 有效抵御攻击,保障主机安全
- 提高系统稳定性,保障主机的高效运行
- 全面可视化监控,方便事件追踪

# 云计算安全 系列产品



LanSecS<sup>®</sup>  
云堡垒主机



LanSecS<sup>®</sup>云堡垒主机集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体,支持云端快速部署,为用户提供安全可靠的云端运维管理与审计解决方案。

### 产品功能

- 统一身份认证
- 资源集中管理
- 统一访问授权
- 操作行为控制
- 统一审计管理

### 产品特点

- 系统部署简单,快速拥有,扩容方便
- 充分考虑自身安全,采用安全加固操作系统以及完善的加密措施
- 多样化的访问控制能力,支持交叉授权、命令过滤、多级审批
- 更加便捷的易用性,支持前端双机配置、AD同步及认证
- 更强的用户生产环境适应性,支持全面国产化及IPV6,应用系统自定义接入
- 更强的用户体验度,支持用户自由选择Web方式或客户端方式运维

### 客户价值

- 实现集中账号管理,降低管理费用
- 实现集中身份认证和访问控制,避免冒名访问,提高访问安全性
- 实现集中授权管理,简化授权流程,减轻管理压力
- 实现实名运维审计,满足安全规范要求



## LanSecS<sup>®</sup> 云用户行为分析系统



LanSecS<sup>®</sup>云用户行为分析系统是一款对桌面用户操作行为进行捕捉分析与审计管理的软件。通过录屏方式记录用户完整操作过程,完整回放用户会话过程,直观反映用户操作行为。可基于操作时间、用户账号、行为进程、动作类型等进行定向审计。

### 产品功能

- 会话管理
- 在线播放
- 业务分析
- 运维管理
- 行为审计

### 产品特点

- 相关用户会话可迅速定位查看:可按照用户、服务器、应用、文件名、目录名、Windows窗口信息等检索,迅速找到审计录像
- 灵活的审计策略:可以按照用户名、应用、服务器制定审计策略,如哪些人、哪些应用、哪些服务器不审计

### 客户价值

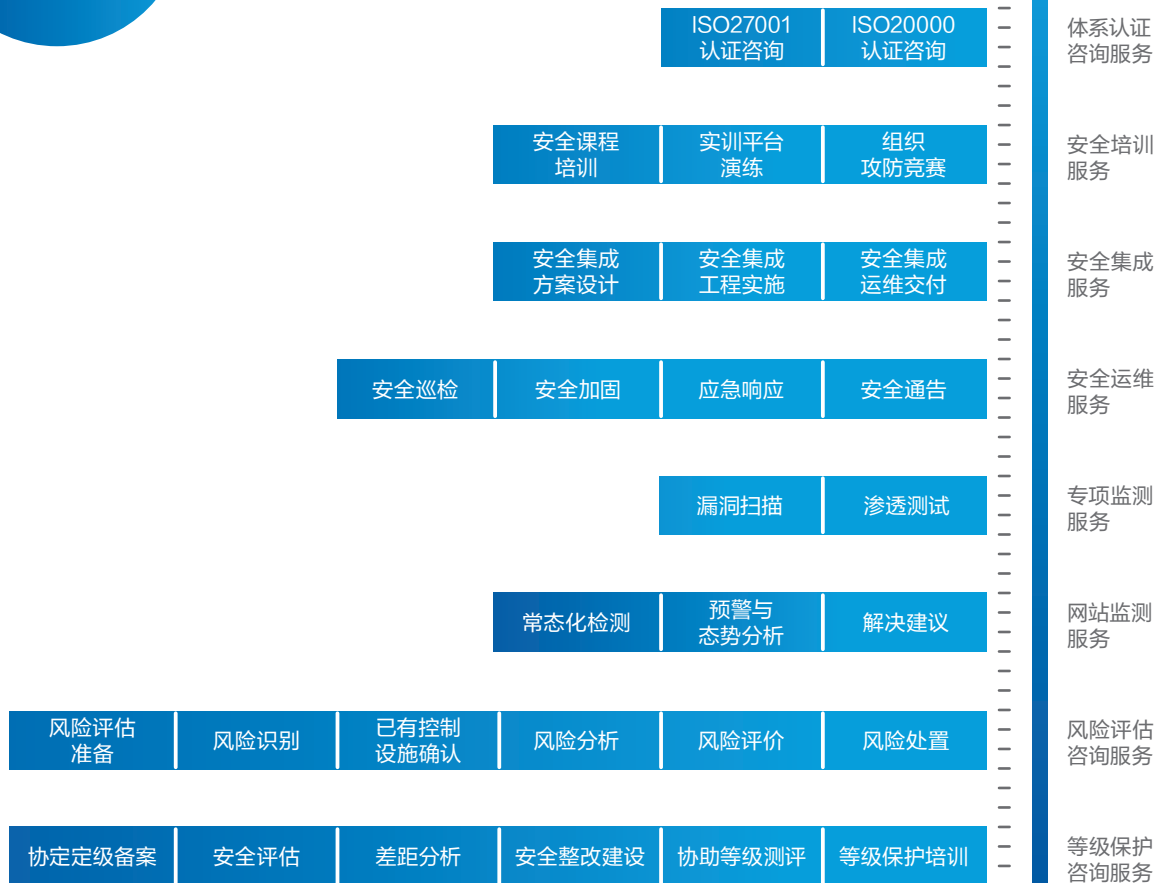
- 对用户的操作合规性、操作意图等有着直观的认识
- 对IT外包人员的工作量进行有效的统计
- 对终端用户无影响,运行无感知

## 安全服务

圣博润以用户安全为己任,以客户满意为宗旨,深耕等级保护十余年,形成了一套专业、完善的安全服务理念。围绕等保咨询、风险评估、网站监测、专项检测、安全运维、安全集成、安全培训、体系认证咨询等多维度为用户提供一体化安全保障服务,使用户信息安全不仅满足国家及行业合规性要求,更注重提高自身的信息安全保障能力和防护水平。圣博润还可为用户定制专项信息安全规划,根据实际业务特点,确定合理的信息安全需求、制定信息安全策略,形成一个覆盖管理安全、技术安全和运维安全的深度防御信息安全保障体系。

凭借专业的技术和丰富的经验,圣博润安全服务得到了广大用户的青睐,用户遍布全国,涉及政府、央企、军工、金融、公安、能源、交通、烟草、教育、医疗、电子商务等众多行业。同时,作为国家网络与信息安全信息通报中心技术支持单位,圣博润圆满完成了北京奥运会、十八大、十九大、全国“两会”、APEC会议、G20峰会、一带一路峰会、金砖会议等数十次网络安全保障任务,多次受到主管部门的通报表彰。

### 网络安全保障 服务体系





## IT认证咨询服务

圣博润拥有一支专业从事信息技术服务领域的咨询队伍,可提供IT领域的各类咨询、培训、认证服务。公司在IT服务管理领域汇集了大批具有专业IT实践和管理工作背景的专家和咨询顾问。同时公司充分利用互联网的优势资源,整合业内著名的讲师和咨询师资源,和多家咨询公司与科研院所建立良好的合作生态。

公司可提供包括系统集成资质、安全服务资质、ITSS运维服务资质、云计算服务能力评定资质、ISO20000认证、ISO27001认证的咨询服务。针对上述咨询服务项目,圣博润提供的具体服务内容如下:

01

**面对企业刚性需求,提供电话咨询与技术支持服务**  
为企业的各类标准与认证,提供专业高效的信息分享通道和专家答疑

04

**换证审核**  
**评估前的现场培训及指导服务**  
帮助企业提升效率,提供专业人士带领企业获取新的认证

02

**体系文件年度更新、管理与发布服务**  
让企业不再为各类认证资质而头疼,让工作变得轻松

05

**审核机构排期管理服务**  
提供专业人才,对企业全年各类认证维护工作进行有效规划和合理安排

03

**监督审核**  
**评估前的现场培训及指导服务**  
解决企业资质维护的痛点,减少企业的无效沟通和困扰

06

**审核/评估费用管理服务**  
帮助企业降低运营成本,帮助企业选择高性价比的服务方



## 技术服务体系

圣博润客户服务中心依托一支强大的技术服务团队,秉承“客户至上”的服务理念,努力打造“简单、专业、亲和、诚信”的客户服务品牌。经过多年的实践和积累,圣博润已经形成了一套完善、全面、高效、科学的客户服务体系。

圣博润客户服务采用一站式接入方式,为用户提供完整的产品与技术支撑服务。通过400/800呼叫中心为用户提供7\*24小时的远程问题答疑和应用建议;通过遍布全国30余个省市专业的项目实施和售后服务专家团队为用户提供本地化的“咨询、实施、交付、现场故障解决及上门巡检”等全链条技术服务。

圣博润客服人员会将您的服务请求通过“客户服务系统”第一时间提交至客户服务中心,并及时安排工程师跟进处理,尽可能缩短问题响应时间。同时将问题记录在客户档案中,持续进行追踪、回访与分析。通过定期回访及时收集客户反馈意见,这些意见也会同步反馈到相关部门的高层管理人员,以便我们能够持续改进服务和提高服务质量。

圣博润技术服务团队除了提供公司自有产品的技术支持服务外,也可随时为用户提供网络安全咨询、紧急安全援助等服务。

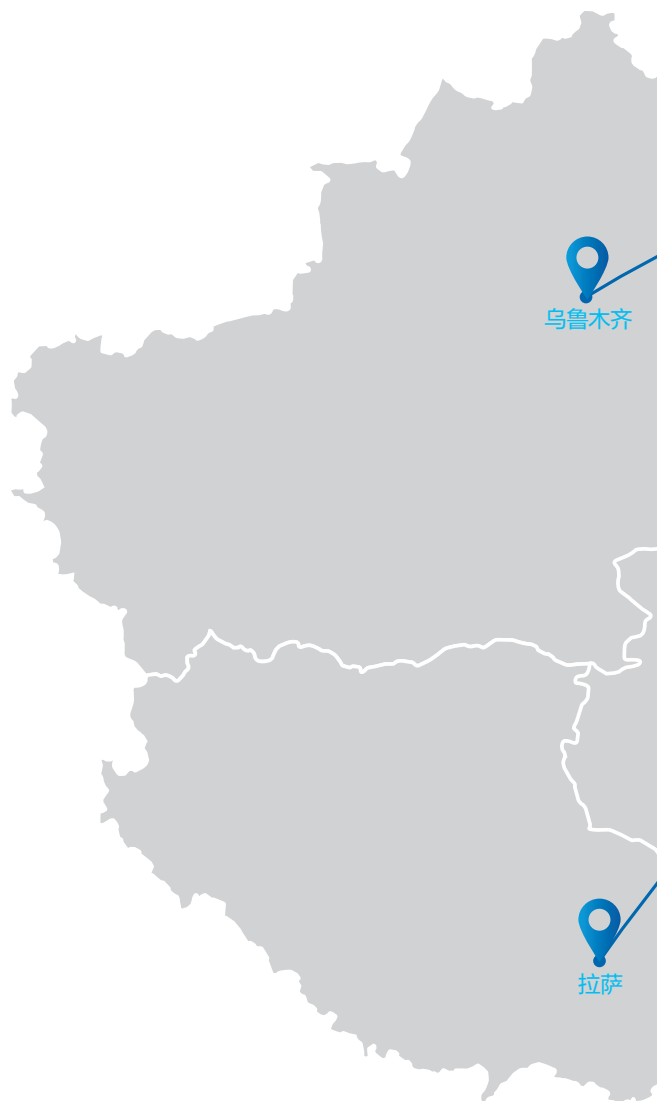
### 圣博润客户服务联系方式

400电话: 4009662332

800电话: 8008102332

QQ通信: 1423326688

Email通信: support@sbr-info.com



乌鲁木齐

拉萨



### 公司荣誉

- 国家重大活动网络安全保卫技术支持单位
- 国家信息安全漏洞库(CNNVD)三级技术支持单位
- 国家网络与信息安全信息通报机制技术支持单位
- 陕西省网络与信息安全信息通报机制技术支持单位
- 湖北省网络与信息安全信息通报中心技术支持单位
- 福建省网络与信息安全信息通报中心技术支持单位
- 广东省网络与信息安全信息通报中心技术支持单位
- 行业(私有)云安全能力者联盟副理事长单位
- 中国网络空间安全协会理事单位
- 中国保密协会会员单位
- 中国计算机学会计算机安全专业委员会会员单位
- 北京网络行业协会常务理事单位
- 北京网络信息安全技术创新产业联盟会员单位
- 工业互联网产业联盟普通会员单位
- 工业互联网安全技术试验与测评工业和信息化部重点实验室技术支持单位
- 工业控制系统信息安全技术国家工程实验室理事会成员单位
- 工业控制系统信息安全产业联盟理事单位
- 中关村可信计算产业联盟-可信工控网络安全专业委员会理事单位
- 智能制造信息安全专业委员会会员单位
- 政府网站综合防护系统(网防G01)中央企业服务站
- 政府网站综合防护系统(网防G01)北京服务站
- 连续4年入选《中国网络安全竞争力50强》

### 公司资质

- CCRC 信息安全服务资质认证证书(信息系统安全集成 一级)
- CCRC 信息安全服务资质认证证书(信息安全应急处理 一级)
- CCRC 信息安全服务资质认证证书(信息安全风险评估 一级)
- 国家信息安全测评 信息安全服务资质证书(安全工程类二级)
- 信息安全等级保护安全建设服务机构能力评估合格证书
- ISO 27001信息安全管理体系认证证书
- ISO 9001质量管理体系认证证书
- 高新技术企业证书

### 国家重大活动的网络安全保障

- 2008年北京奥运会
- 2010-2018年历年“全国人民代表大会”和“中国人民政治协商”会议
- 2012年中国共产党第十八次代表大会
- 2013年全国重要信息系统和政府网站安全专项检查技术支持
- 2015年抗战胜利70周年纪念活动
- 2015年国家级重要信息系统和重点网站安全执法检查技术支持
- 2016年二十国集团峰会(G20峰会)
- 2017年“一带一路”国际合作高峰论坛
- 2017年第十一届夏季达沃斯论坛
- 2017年金砖国家领导人厦门峰会
- 2017年中国共产党与世界政党高层对话会
- 2017年中国共产党第十九次代表大会
- 2017年全球“财富”论坛
- 2017年公安部网络安全执法检查技术支持
- 2018年数字中国建设峰会
- 2018上海合作组织青岛峰会
- 2018年改革开放40周年暨港珠澳大桥开通重大安保技术支持
- 2019年公安机关网络安全执法检查技术支持
- 2019年新中国成立70周年庆祝活动网络安全保卫工作



## 典型用户

- ◎ 中华人民共和国公安部
- ◎ 中华人民共和国海关总署
- ◎ 中华人民共和国外交部
- ◎ 中华人民共和国工业和信息化部
- ◎ 中华人民共和国财政部
- ◎ 中华人民共和国交通运输部
- ◎ 中华人民共和国自然资源部  
(原中华人民共和国国土资源部、国家测绘地理信息局、国家海洋局)
- ◎ 中华人民共和国教育部
- ◎ 中华人民共和国水利部
- ◎ 中华人民共和国国家卫生健康委员会  
(原中华人民共和国国家卫生和计划生育委员会)
- ◎ 中华人民共和国国家发展和改革委员会
- ◎ 中华人民共和国审计署
- ◎ 中华人民共和国文化和旅游部  
(原中华人民共和国文化部、国家旅游局)
- ◎ 中华人民共和国民政部
- ◎ 国家市场监督管理总局  
(原国家工商行政管理总局、国家质量监督检验检疫总局、国家食品药品监督管理总局)
- ◎ 中华人民共和国国家广播电视总局  
(原国家新闻出版广电总局)
- ◎ 中华人民共和国应急管理部(原国家安全生产监督管理总局)
- ◎ 中华人民共和国国家统计局
- ◎ 国家税务总局
- ◎ 中华人民共和国国家能源局
- ◎ 中国人民银行
- ◎ 中国地震局
- ◎ 中国气象局
- ◎ 中华人民共和国国家粮食和物资储备局(原国家粮食局)
- ◎ 中华人民共和国国家药品监督管理局
- ◎ 国家铁路局
- ◎ 中国银行保险监督管理委员会  
(原中国银行业监督管理委员会)
- ◎ 国务院国有资产监督管理委员会
- ◎ 新华通讯社
- ◎ 中国共产党中央政法委员会
- ◎ 中华人民共和国国务院参事室
- ◎ 中华人民共和国国务院新闻办公室
- ◎ 中国石油天然气集团有限公司
- ◎ 中国石油化工股份有限公司
- ◎ 中国海洋石油集团有限公司
- ◎ 中国中煤能源集团有限公司
- ◎ 中国华能集团有限公司
- ◎ 中国大唐集团有限公司
- ◎ 中国电力投资集团公司
- ◎ 中国南方电网超高压输电公司
- ◎ 中国航天科技集团有限公司
- ◎ 中国航天科工集团有限公司
- ◎ 中国航空工业集团有限公司
- ◎ 中国船舶工业集团有限公司
- ◎ 中国兵器装备集团有限公司
- ◎ 中国兵器工业集团有限公司
- ◎ 中国核工业集团有限公司
- ◎ 中国中车股份有限公司
- ◎ 中国交通建设集团有限公司
- ◎ 中国建筑股份有限公司
- ◎ 中国建设科技集团股份有限公司
- ◎ 中国一重集团有限公司
- ◎ 中国联合网络通信集团有限公司
- ◎ 中国电子信息产业集团有限公司
- ◎ 中国化工集团有限公司
- ◎ 中国中铁股份有限公司
- ◎ 中铁建设集团有限公司
- ◎ 中国铁路总公司
- ◎ 汉江水利水电(集团)有限责任公司
- ◎ 河北钢铁集团石家庄钢铁有限责任公司
- ◎ 河北金隅鼎鑫水泥有限公司
- ◎ 中国人民银行清算总中心
- ◎ 中国建设银行股份有限公司

## 典型用户

- ◎ 中国工商银行
- ◎ 中国民生银行股份有限公司
- ◎ 中国光大银行
- ◎ 华夏银行股份有限公司
- ◎ 哈尔滨银行股份有限公司
- ◎ 铁岭银行股份有限公司
- ◎ 吉林银行股份有限公司
- ◎ 辽阳银行股份有限公司
- ◎ 华商银行
- ◎ 张家口市商业银行股份有限公司
- ◎ 保定市商业银行
- ◎ 葫芦岛银行
- ◎ 衡水市商业银行
- ◎ 邢台市商业银行股份有限公司
- ◎ 潍坊银行
- ◎ 天津农村合作银行
- ◎ 交通银行云南省分行
- ◎ 乌鲁木齐市商业银行
- ◎ 中国银行股份有限公司乌海分行
- ◎ 晋中市商业银行股份有限公司
- ◎ 晋城银行股份有限公司
- ◎ 阳泉市商业银行股份有限公司
- ◎ 华夏银行南宁分行
- ◎ 济宁银行
- ◎ 上海浦东发展银行股份有限公司长春分行
- ◎ 上海证券交易所
- ◎ 民生证券有限责任公司
- ◎ 中国证券监督管理委员会宁波监管局
- ◎ 深圳市证券交易所营运服务与物业管理有限公司
- ◎ 中国人寿保险股份有限公司
- ◎ 中国人民健康保险股份有限公司
- ◎ 合众人寿保险股份有限公司
- ◎ 华泰保险集团股份有限公司
- ◎ 中国人民财产保险股份有限公司浙江省分公司
- ◎ 中原农业保险股份有限公司
- ◎ 东海基金有限责任公司
- ◎ 嘉合基金管理有限公司
- ◎ 上海银行基金管理有限公司
- ◎ 北京首创期货有限责任公司
- ◎ 山西中辉期货经纪有限公司

 政府	3000+用户
 公安	300+用户
 交通运输	200+用户
 教育	400+用户
 卫生健康	300+用户
 金融	500+用户
 能源	400+用户
 文化和旅游	300+用户
 政法	400+用户

 电信	200+用户
 军工	500+用户
 烟草	300+用户
 科研	500+用户
 财政	200+用户
 水利	200+用户
 制造业	1000+用户
 企业	3000+用户



做网络安全行业领军企业

# 专注安全 诚信创新



北京市海淀区高梁桥斜街 59 号院 2 号楼 3 层

邮编: 100044 / 电话: 010-82138088

技术支持热线: 800-810-2332、400-966-2332

Email: [support@sbr-info.com](mailto:support@sbr-info.com)

[www.sbr-info.com](http://www.sbr-info.com)