圣博润
SBR-info

工控安全解决方案

智慧·智能·安全

为工业系统安全保驾护航

公司能力

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
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
北京网络行业协会会员单位
北京网络信息安全技术创新产业联盟会员单位

公司资质

信息系统安全集成服务资质（一级）
信息安全应急处理服务资质（二级）
信息安全风险评估服务资质（二级）
信息安全服务资质（安全工程类一级）
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

公司简介

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。公司自2000年成立以来，累计 推出了四大类20余款网络安全产品，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。

圣博润是中国网络安全五十强企业，是2017年新三板创新层企业和 2016年新三板十大最具投资价值企业。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”国际合作高峰论坛等众多国家重大活动的 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。海关总署、国家 发改委、国家税务总局、国家统计局、公安部、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、华能集团等三十多 家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、移动安全和云计算安全领域推出了一系列安全产品，在新兴 网络安全领域处于技术领先地位。

工控安全解决方案

工控网络安全挑战

系统故障
网络威胁
人为误操作
蓄意攻击

现场技术陈旧

两化融合，工业网络互连趋势

设备分散，不易管理

设备供应商，通讯协议多

缺乏资产可视化管理

工控网络安全威胁

SCADA自身不安全

不恰当的操作

不安全的通信接入

缺乏异常检测手段

缺乏监视及日志

缺乏专业安全人员

应急预案不完善

补丁更新不及时

工控安全解决方案

网络边界准入管理

- 网络边界识别和资产识别，自动识别在线终端，捕捉终端指纹信息特征，智能识别终端类型
- 入网终端身份鉴别和合规验证，展示与交换机端口的映射关系，未达标终端的安全修复
- IP实名制登记和入网终端网络信息生命周期管理，准确识别违规接入和修改IP、MAC等行为

网络安全监测与审计

- 工控网络资产管理，设备运行状态监测，异常行为监测和工控协议细粒度审计
- 基于机器学习和深度协议分析技术，自动收集数据行为并提取特征，生成白名单规则
- 内置安全黑名单，有效识别恶意入侵和安全威胁

操作终端安全管理

- 创建操作员站终端计算机的可信运行环境，有效抵御病毒、木马和非法主机入侵
- 通过进程与应用程序白名单管理、移动存储介质注册与使用管理、计算外设管理，有效防范用户违规操作和误操作
- 实现主机非法入侵和违规操作的监测、报警与审计记录

网络边界隔离与防护

- 通过白名单策略和协议分析实现工控网络之间、工控网络与管理信息网络之间的边界访问控制
- 为工控网络安全接入管理信息网络提供逻辑安全隔离手段，实现通讯的单向传输
- 快速识别网络上的非法操作、外部攻击和异常事件，实时告警和阻断非法数据包

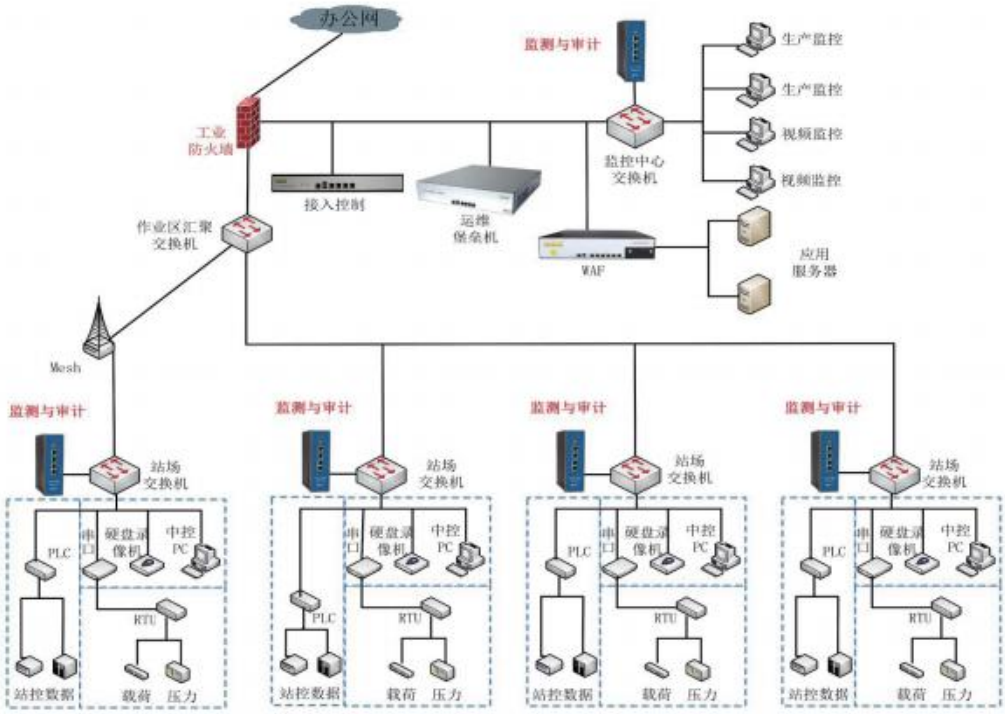
设备运维操作审计

- 建立设备运维操作黑白名单机制，实现操作人员实名制管理，对操作人员进行全方位的运维操作审计
- 支持字符和图形操作两种管理方式，完整记录和回放操作人员的运维操作会话
- 实时切入用户运维操作会话，对用户运维操作行为进行现场检查

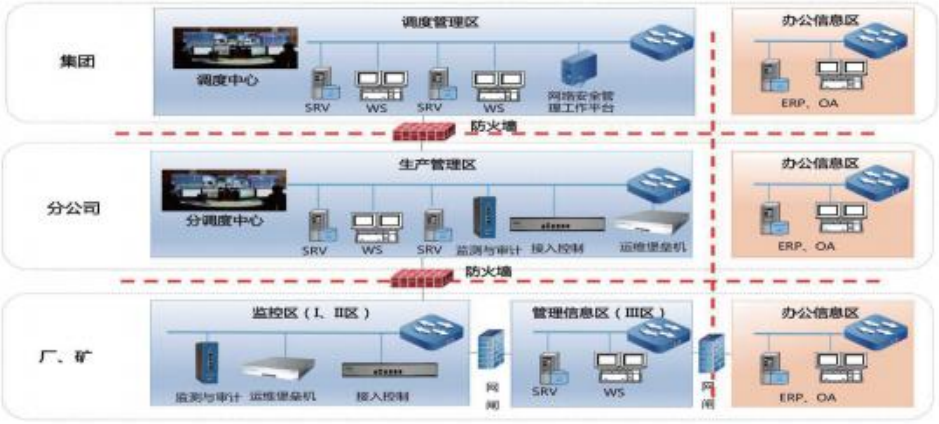
安全合规与应急管理

- 建立体系化的等级保护工作管理、信息通报工作管理机制和相应的工作平台，促进安全管理工作落地
- 实现工控网络和应用系统的定级、备案、安全整改、安全自评估、安全检查管理
- 实现网络与信息安全信息通报工作的任务部署、过程跟踪、结果反馈、应急支持管理

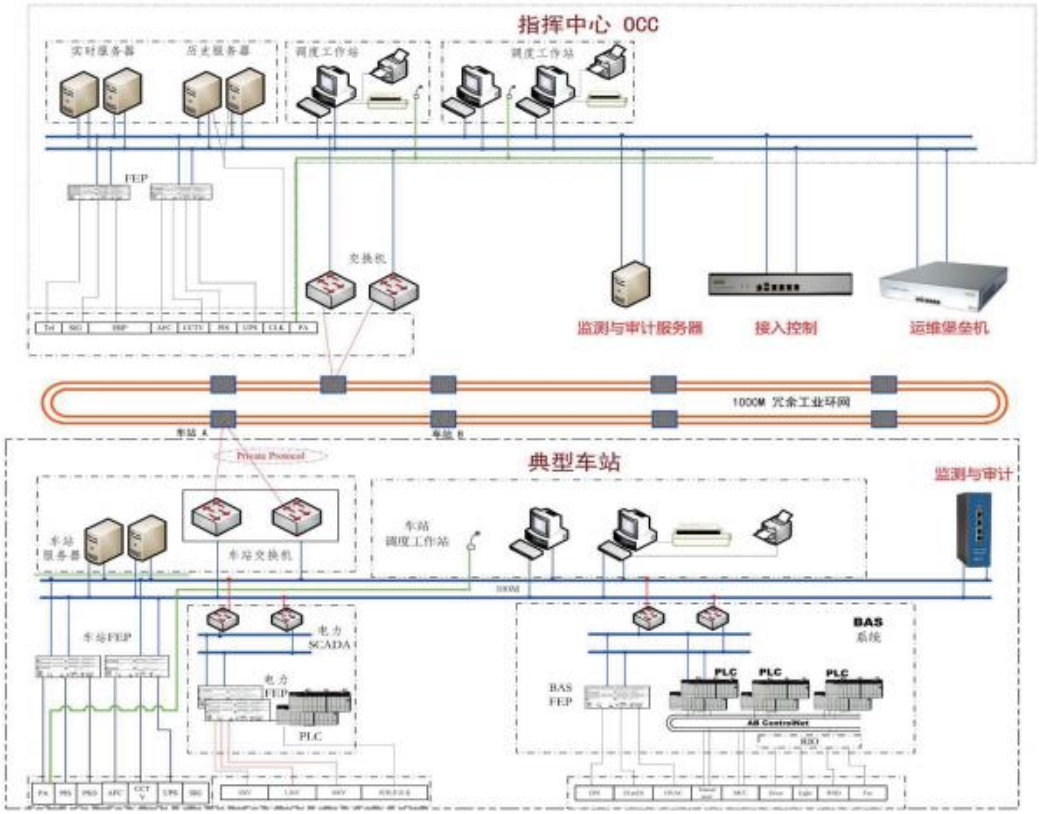
■ 采油行业解决方案



■ 煤炭行业解决方案



■ 轨道交通行业解决方案


指挥中心 OCC
实时服务器
历史服务器
调度工作站
调度工作站
FEP
交换机
监测与审计服务器
接入控制
运维堡垒机
1000M 冗余工业环网
车站 A
车站 B
Private Protocol
典型车站
监测与审计
车站
服务器
车站交换机
车站
调度工作站
100M
车站FEP
电力
SCADA
电力
FEP
PLC
BAS
系统
BAS
FEP
PLC
PLC
PLC
AB ControlNet

方案特色

合规性

满足《网络安全法》框架下的关键信息基础设施安全保护制度要求、网络安全等级保护制度要求、网络与信息安全信息通报制度要求。

全面防护

从网络、终端、通信、数据、管理多个层面提供完整的安全防护与管理手段，实现工控网络全面的安全保护。

可视化

实现工控网络资产可视化管理，动态识别非法接入设备，直观展示工控网络安全威胁。

最小干扰

所有安全组件均采用非侵入式安全监测与防护工作方式，确保将设备对工控网络的干扰降低到最低。

多协议支持

支持常见工控协议，如 Modbus TCP/R-TU/+、OPC、IEC101/102/103/104、CDT、DLT645、BacNet、IEC61850、MDLC/MDLC over IP、DNP3、ProfiNet、EIP等。

工控安全产品

- LanSecS®工控安全监测与审计系统
- LanSecS®工业控制防火墙系统
- LanSecS®工控安全隔离与信息导入系统
- LanSecS®网络终端接入控制系统
- LanSecS®（堡垒主机）内控管理平台
- LanSecS®终端安全卫士
- LanSecS®网络安全管理工作平台

■ LanSecS®工控安全监测与审计系统

产品概述

LanSecS®工控安全监测与审计系统（LSDA）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。系统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

协议监测与告警

通过对工控网络流量的采集以及工控协议的深度分析，实现实时监测及实时告警，帮助用户实时掌握工控网络运行状况。

流量监测与告警

对流量的流入流出的异常情况进行监测，以仪表盘的形式实时展现，直观显示数控流量情况。对于超过预定值的情况进行告警。

状态监测

提供工控网络设备状态监测功能，可对设备的资源状况、端口工作状况等进行监测。

日志与报表

LSDA提供统计与分析功能，可输出结果日志，并提供多种格式的报表输出。

工控网络审计

对工控网络中的所有活动提供协议审计、流量审计，生成完整记录便于事后审计追溯。

策略管理

LSDA支持审计与告警策略定制，策略以黑白名单的形式来体现：

- 工控黑名单：黑名单指工控专业漏洞库，包括工控设备漏洞、工控协议漏洞、工业以太网漏洞、工控系统漏洞等；
- 工控白名单：通过智能学习技术，自动学习生成白名单库，管理员可定义白名单规则，通过白名单规则匹配判断工控协议数据包是否异常，白名单包括多种工控协议和传统协议白名单。

产品特色

真正的工控网络异常检测

- 异常行为检测和深度分析；
- 提供现场设备故障报警；
- 提供恶意入侵活动报警。

可视化展示

- 提供独立的工控网络概览图，直观展示工控网络设备节点以及节点之间的连接情况；
- 自动创建网络通讯安全基线；
- 提供可视化的网络故障展示与告警。

易安装、易使用

- 一体化设计，旁路接入，不影响工控网络运行；
- 提供成熟的多点部署方案；
- 提供用户友好的违规事件调查分析界面；
- 集中监控多个网段（依赖于具体的网络架构）。

完整、兼容性强

- 可记录发送到 / 来源于现场设备的所有的指令和指令执行结果；
- 支持众多的工控协议，包括但不限于：Modbus TCP/R-TU/+IEC60870-5-101/104、IEC60870-5-101 over TCP/IP、MDLC / MDLC over IP、DNP3 / DNPi、Siemens Profinet/Profibus、Siemens Teleperm XP、Siemens TIM、GE UDH、Rockwell Automation DF1；
- 通过定制开发可提供更多的工控协议支持。

■ LanSecS®工业控制防火墙系统

产品概述

LanSecS®工业控制防火墙系统（简称FCFM）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，为控制网与管理信息网的连接、控制网内部各区域的连接提供安全保障，并且可实现对MBTP、EIP、OPC、Modbus、DNP3.0、IEC104、IEC61850、Profinet、BacNet等协议的深度分析。

产品功能

工业协议深度过滤

深度分析、细粒度解析,支持各种主流ICS 标准通讯协议和厂商自定义协议。

策略实现访问控制

基于白名单的访问控制策略,支持工业协议深度扫描和病毒扫描。

读写控制

对数据进行读写安全控制，且支持安全数据采集、存储和转发功能。

病毒检测

提供防病毒检测模块，识别病毒、木马和恶意代码。

日志与审计

提供完整的访问控制日志。

简单易用

界面友好，易于操作

IPsecVPN

支持IPsecVPN功能，实现加密通信传输。

产品特色

安全性

- 业务端口和管理端口分离设计；
- 识别工业控制协议的每个字节和每个位；
- 支持细粒度读写权限控制；
- 提供严格的身份认证来管理系统配置权限；
- 支持国密IPsecVPN加密传输，更加充分保障数据安全；
- 提供防病毒和防恶意代码功能；
- 支持通过内网服务器自动或手工进行系统升级和日志备份。

数据完整性

- 具有自动判断网络连接状态，异常时自动启动断线缓存功能；
- 日志服务器可以记录系统产生的所有行为，确保信息完整；
- 支持各种主流ICS标准通讯协议和厂商自定义协议，如OPC、Modbus、DNP3.0、Profinet、 IEC101/102/103/104、CDT、IEC61850、EIP等。

可靠性

- 实时检测系统状态，对关键模块进行诊断、异常自动报警；
- 具备完善的故障自动恢复功能；
- 适合多种工业应用场合，具有强大的环境适应性；
- 硬件产品达到工业三级B以上指标；
- 无风扇全封闭设计；
- 设备支持主从备份、双机热备功能；
- 支持硬件故障自动旁路转换（Bypass）功能；
- 电源采用1+1冗余供电。

易用性

- 多种灵活的安装方式，包括导轨安装、机柜安装等；
- 方便对网关的配置，支持配置文件的导入导出；
- 可远程监视网关的运行状态、运行参数、通讯报文等；
- 可通过网络接口实现对网关状态的诊断。

客户价值

通过部署LanSecS工业控制防火墙系统设备用户可获得如下收益：

- 对违规操作及时报警或阻断；
- 对网络攻击等事件进行实时阻断；
- 记录和分析 RS-232/422/485 通信过程；
- 关注控制网与监控网间的传输安全；
- 整合信息网的安全防护经验；
- 防护设备与生产管理运维措施同步；
- 逐层防护，统一管理对上行下行数据进行严格的数据级别的访问控制。

■ LanSecS®工控安全隔离与信息导入系统

产品概述

LanSecS®工控安全隔离与信息导入系统（简称LGAP）是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。该设备连接在两个独立主机系统之间，主机系统之间不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据的无协议"摆渡"，有效避免了安全等级较低的信息管理网络对安全等级较高工业控制系统和设备的攻击和破坏。

产品功能

丰富的应用模块

- 按需量身定制多种功能模块。

高安全的文件交换

- 对文件进行病毒扫描、签名校验、文件类型校验、文件内容过滤；
- 不开放任何连通两侧的网络通道，绝对安全地实现数据“摆渡”。

高可用设计

- 支持网络口、HA多种高可用实现模式；
- 最多支持32台设备进行负载均衡。

传输方向控制

- 采用双通道通信机制，支持各通道传输方向可控；
- 特殊应用环境中支持数据的单向传送，避免信息的泄漏。

完善的安全审计

- 根据需要进行日志审计；
- 支持本地日志缓存；
- 支持Syslog日志存储；
- 支持日志的分级发送。

产品特色

高速隔离交换

- 协议隔离：内、外网单元主机分别独立完成网络协议的终止，无法直接建立任何的协议会话，从而阻断风险传递；

- 应用隔离：采用模块化的应用解码，各单元分别独立完成与用户会话交互、提取安全数据等待数据交换；
- 访问控制：采用严格的白名单机制，只有配置允许的数据才能访问，否则默认禁止传输；
- 内容隔离：对内容检查与病毒查杀，不合规的数据被直接删除，合规的数据才被安全传输；
- 通讯加密：内外网之间数据传输采用加密方式；
- 风险隔离：基于白名单机制运行，仅许可正常的、用户许可的网络应用，防范未知的安全风险，并且系统集成防病毒并可扩展多种常规安全防护引擎，如入侵检测等，可检测60000多种病毒、4000多种网络入侵，双重安全机制最大程度上实现了风险隔离。

客户端精细识别

- 多网隔离：满足多种网络形式接入，比如“一对一、一对多、多对一”的网络隔离；
- 多样化的身份认证：支持多样灵活的身份认证方式；
- 地址绑定：提供IP与MAC地址绑定功能，可对指定接口所连接的网络中的主机的IP和MAC 地址进行绑定，防止内部用户盗用IP和内网地址资源分配的混乱，方便网络IP资源管理；
- 内容检查：提供多种内容安全过滤与内容访问控制功能，能有效的防止外部恶意代码进入内网。

专家级数据安全

- 数据安全专家：高效的病毒扫描和细粒度的内容过滤技术；
- 严格白名单：严格的白名单任务策略，精确到对每一个数据的控制，拦截各种非法数据报文，保证数据的安全；
- 安全访问控制：通过访问用户身份识别，保证数据不被非法访问和传递。

业内领先高可靠性

- 冗余设计：可选电源冗余、双机热备、端口冗余、链路聚合等；
- 可靠性设计：如宽温、低功耗、无风扇、自诊断、自恢复、双看门狗；
- 模块高稳定结合：外网模块可与安全监控预警平台SSMC相连，内网模块一般不进行日志和数据传输到外网。

支持广泛的工业协议

支持常见工业协议如： Modbus/TCP、OPC、IEC101/102/103/104、DNP、CDT、DLT645、BacNet、IEC61850、ProfiNet、EIP等。

■ LanSecS®网络终端接入控制系统

产品概述

LanSecS ® 网络终端接入控制系统（LAC）为新一代网络准入产品，采用硬件纯旁路部署方式接入工业控制网络，准确识别入网终端身份，提供终端健康检查与隔离修复，实现对工业控制网络终端设备的全面接入控制。

产品功能

网络边界识别

- 通过网络分析自动识别全网在线终端；
- 捕捉终端网络信息特征，智能识别终端类型；
- 通过流量分析，完成网络资产识别及统计；
- 智能生成网络拓扑。

网络边界威胁感知

- 智能发现并记录网络中的私建网中网、BYOD设备接入、双网互连、IP地址冲突等违规事件；
- 提供终端入网网络信息生命周期管理，准确识别违规修改IP、MAC等违规行为。

网络边界准入控制

- 提供入网终端的合法性与合规性验证；
- 可针对未合法登记终端提供入网引导；
- 根据管理策略智能划分终端归属，并可针对不同归属终端提供不同网络访问权限；
- 可识别伪造、仿冒合法终端行为并进行阻断与告警。

全网IP地址管理

- 提供对全网IP地址管理功能，图形化展现并统计IP使用情况；
- 实施DHCP方式准入时，可实现IP地址自动下发与回收；
- 提供IP资源历史回溯、IP实名制登记等功能，以实现IP地址资源生命周期管理。

设备智能识别与修复

- 对于不符合企业安全规范的终端，提供智能修复功能，在用户无感知的情况下完成修复，消除安全隐患；
- 智能修复方式包括：主机和用户身份信息自动绑定、软件自动安装、补丁自动安装、安全配置修复、软件自动卸载等。

网络设备端口可视化及联动管理

- 交换机性能、端口状态、流量展示、端口管理；
- 提供终端实名网络定位，实时定位终端的接入位置；
- 可提供IP/MAC/端口自动绑定功能、可根据MAC分配指定IP；
- 可对交换机配置自动备份，并提供配置变动告警；
- 支持识别接入终端类型进行IP分配。

产品特色

- 准入技术适应性强：支持多种准入控制技术，包括 DHCP准入、802.1X 准入、ARP准入、SNMP准入、无线Portal准入，支持准入控制技术的单独和混合部署。
- 资产管理可视化：通过直观图示的方式对全网设备及其IP地址情况做可视化展示，包括但不限于VLAN、IP总数、可用IP、离线IP、在线IP、绑定IP、保留IP等信息，并可对详细信息进行统计。
- 管理界面友好：管理界面提供触屏大图标式管理模式，直观易用；终端入网管理提供友好引导界面，可快速完成入网配置。
- 无客户端工作模式：传统的网络准入需要安装客户端才能实现，包括代理程序或浏览器插件两类。LAC可提供无客户端的工作模式，以支持打印机、视频摄像头等类型的终端准入。

■ LanSecS®（堡垒主机）内控管理平台

产品概述

LanSecS ®（堡垒主机）内控管理平台是一款定位于对工业控制网内的设备运维人员远程执行服务器和网络设备运维操作的全过程管理的产品。主要实现了远程运维操作过程中的集中帐号管理、集中登录认证、集中用户授权和集中操作审计。

产品功能

账号管理

- 账号全生命周期管理：对所有可远程管理的服务器、网络设备的账号以及所有使用堡垒主机开展运维管理活动的自然人的账号实行集中管理。实现主账号和从账号的增、删、改、查、注销、锁定等操作；
- 从账号口令变更管理：自动定时批量修改从账号口令，用户可自定义口令变更时间、周期、复杂程度等内容，减轻设备运维人员的工作压力。

认证管理

- 用户身份认证：系统支持静态口令认证、动态口令认证、USB-KEY、数字证书、动态令牌、生物特征等多种组合认证方式，并且传输过程加密；
- 单点登录（SSO）：系统提供单点登录功能，设备运维人员仅需一次登录堡垒主机，就可以访问被授权的多个设备资源，无需再次输入设备账号和密码信息，提高了运维的效率，改善用户体验。

授权管理

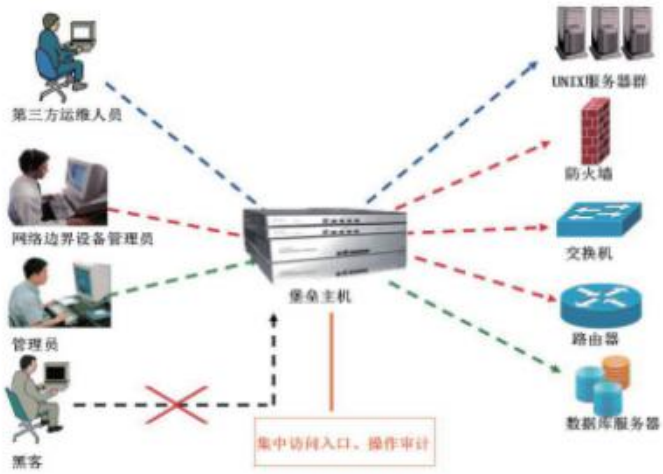
- 权限管理：堡垒主机提供统一的管理界面，对用户、角色、行为、资源进行关联授权，以达到对运维权限的细粒度分配和管控；
- 访问控制：提供基于访问时间、访问地点、资源、系统账号、操作命令、自定义命令的强访问控制。通过对访问内容的监控记录和危险命令的过滤，实现安全可靠的运维操作。

审计管理

- 运维监控与阻断：提供实时的运维会话监控功能，随时可切入用户操作会话当中进行运维过程监视和指导，对违规操作实时阻断；
- 运维操作审计：支持对如下协议进行审计：Telnet、SSH、RDP、FTP/SFTP、VNC、X-window等，提供高保真、流畅的行为审计录像及文本审计日志；

- 审计报表：堡垒主机管理员可以按照用户定义条件，以及系统自定义的报表模板定制审计报表。

产品部署



产品特色

- 安全可控的设备运维：针对工业控制网络中的服务器、网络设备提供了安全可控的远程运维管理手段，通过细粒度的访问控制避免运维权限滥用的风险；
- 丰富的运维协议支持：支持工业控制网络中常用的远程运维协议：包括Telnet、SSH、RDP、FTP/SFTP、VNC、X-window等；
- 独有的会话保持能力：当运维操作意外中断时，运维人员再次登录系统时可自动切入原来的会话，保证运维工作不受影响；
- 分布式部署和集中式管理：系统支持分布式部署和集中管理，为全网施行统一的运维管理策略和统一的审计日志管理提供解决方案。

■ LanSecS®终端安全卫士

产品概述

LanSecS®终端安全卫士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。LanSecS®终端安全卫士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

进程与应用程序白名单管理

对操作员站终端计算机上运行的进程和应用程序设置白名单，只有白名单中的进程和应用程序才允许运行。防止非法程序对终端的访问和恶意破坏。

移动存储介质管理

对移动存储介质进行全生命周期管理，跟踪移动存储介质的行为，实现对移动存储的可信管理。

防病毒管理

通过实时检测防病毒软件安装状态、病毒特征库版本和防病毒软件运行状态，全面保证内网计算机不受病毒侵扰。

补丁管理

提供全网统一的补丁管理中心，自动检测终端补丁的缺失情况，自动或手动进行补丁更新，维护全网补丁更新统计信息。

安全审计

提供内网计算机安全事件审计及用户行为审计。包括文件操作、服务与进程活动、系统日志、注册表操作、系统帐户变更、信息泄密、资源滥用等。

产品特色

- 终端运行环境保护：LanSecS®终端安全卫士通过其白名单机制为终端计算机创建了一个安全的运行环境，非法进程和应用程序无法通过安全检验，确保将病毒、木马以及恶意软件阻挡在终端运行环境之外。
- 全面管控外设端口：对USB端口、蓝牙、无线接口进行前面管控，U盘等未授权设备无法接入终端计算机，有效防范通过USB接口发起的高级攻击。
- 完整审计违规操作：对终端用户的进程访问、软件运行、安全策略变更、移动介质使用、文件操作、注册表访问等行为进行全面审计和日志记录，及时发现违规行为并予以告警和处置。

■ LanSecS®网络安全管理工作平台

产品概述

LanSecS ® 网络安全管理工作平台依据国家在信息安全等级保护、安全通报、安全检查等方面的标准及行业标准设计和开发，并融入了我司多年来在信息安全领域积累的咨询服务经验和信息安全工具开发经验，可为各单位在网络与信息安全管理工作提供专业化的技术支撑，指导并协助用户开展各项日常管理工作，提升工作效率，提高检查质量。

利用本平台，政府及企事业行业单位可以对安全通报、信息系统等级保护、安全检查、应急演练等工作的开展进行全面部署、工作过程监控及工作成果统计分析等。使得网络安全管理工作沟通渠道通畅、沟通效率提升，快速部署、快速反馈、快速响应，相关信息完备准确、数据更新及时、管理量化、规范化，同时为管理层在安全管理工作决策提供有力依据。

产品功能

等级保护管理

信息系统等级保护管理模块可实现信息系统的定级、备案、建设整改、等级测评、监督检查等工作的全过程管理与指导，为落实系统信息安全等级保护工作提供信息化数据支撑。

安全通报管理

安全通报管理模块为建立健全网络安全信息通报与报送机制，提供全方位的工作管理流程，包括信息安全通报的下发、上报、接收、审阅、查询、分析等功能。

安全检查管理

安全检查管理模块提供对信息安全检查工作的计划制定、检查执行和结果处理等功能。本平台可与信息安全检查工具箱相结合，共同完成信息安全检查的整个检查管理流程。前者负责信息安全检查计划的制定、日常工作任务下发以及检查数据的集中管理；后者提供现场检查的技术支持，采集和检查结果数据录入，并将检查结果数据上报到本平台。

应急工作管理

应急工作管理模块是为应对信息安全突发性事件的发生，提高安全事件的应急处理能力，保证网络与信息安全指挥协调等工作。主要功能包括应急演练工作的任务下发、接收、上报和查询功能。

基础库管理

基础库管理模块完成对网络安全管理工作当中各环节所需的基础数据进行综合管理。主要包括上传资料、测评机构、行政区划、信息联络员和专家库等管理功能。

产品特色

网络安全管理工作流程化

实现信息安全等级保护审核路径定制功能，满足用户业务动态变化和扩展的需要。系统以信息系统等级保护定级、备案、整改、测评和自查为主线，将流程化管理与等级保护管理进行结合，实现用户等级保护工作的信息化和流程化。

信息系统安全性评价标准化

提供重要信息系统的安全性评价功能，通过建立重要信息系统安全性评价专家体系，对重要信息系统的安全性进行评价。以等级测评、风险评估、专家评审、执法检查、行业检查和自查的结果为评价指标，通过评价详细反映重要信息系统等级保护工作的计划、实施、检查和改进的情况，为管理层的工作安排提供指导。

丰富的报表和数据展现能力

系统具备完善的查询、报表和统计功能，可为用户提供丰富的数据展现，满足管理层、执行层人员对安全工作全面掌控的需求。

完备的数据接口

系统具有完备的数据接口规范，可对重要信息系统的信息进行收集和管理，为信息系统的安全状态评估提供基础数据；也可与公安部的重要系统基础数据库平台结合进行数据上报，将行业系统的备案信息上报到基础数据库平台中。

北京圣博润高新技术股份有限公司
BEIJING SBR HIGH-TECH CO.,LTD

地址：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：
8008102332/4009662332 / 技术支持邮箱：support@sbr-info.com / 网址：www.sbr-info.com