圣博润
SBR-info

抗击疫情，携手共行

圣博润助力远程安全运维


王霄

日期：2020.02


北京圣博润高新技术股份有限公司

圣博润基本情况

2000年成立于中关村科技园区，20年专注网络安全；

在全国29个重要城市设有办事机构；

约500名员工，其中研发和技术人员300+；

产品涉及安全防护、安全监测与审计、安全管理、工业互联网安全、云计算安全、大数据安全；

最专业的安全服务团队；

用户数超10000家。

专 业

- 工业互联网安全专家
- 等级保护咨询专家

创 新

- 工业互联网安全
- 云计算安全
- 大数据安全

责 任

- “十九大”网络安保
- G20 杭州峰会安保
- “一带一路”安保
- 2008北京奥运安保

价 值

- 网络安全50强企业
- 新三板创新层企业
- 新三板十大最具投资价值企业

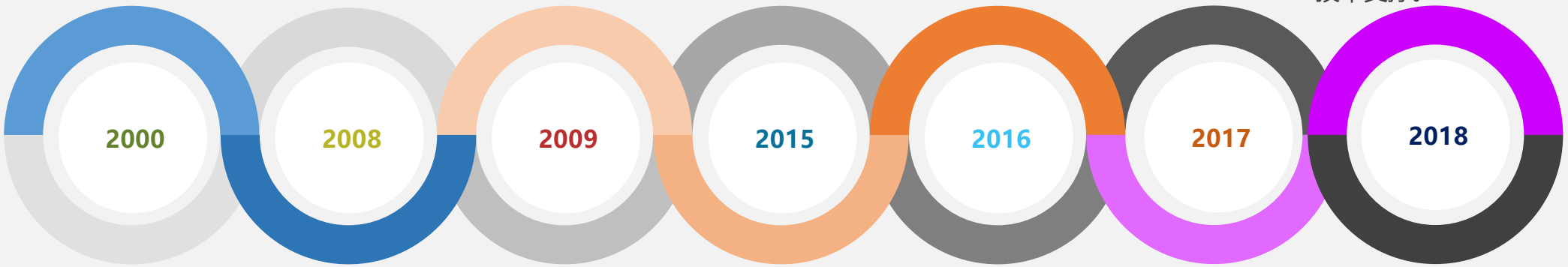
圣博润-发展历程

2000年公司成立，同年通过高新技术企业认证，2003年建立LanSecS®自有产品品牌并推出终端安全相关产品。

2009年新三板挂牌，企业规模迅速扩大，业务覆盖全国二十多个省市范围。

2016年快速发展，推出工业互联网安全、大数据安全、云计算安全产品，开启新一轮的高增长。

工业互联网安全业务大突破，获工业信息安全十大用户信赖品牌奖，成为工信部工业互联网安全技术试验与测评重点实验室首家技术支持单位；为2018年首届工业互联网安全防护演练和2018年首届工信部护网杯安全大赛提供技术支撑。



2008年推出等级保护咨询服务业务，并圆满完成2008年奥运政务专网网络安全保卫工作。

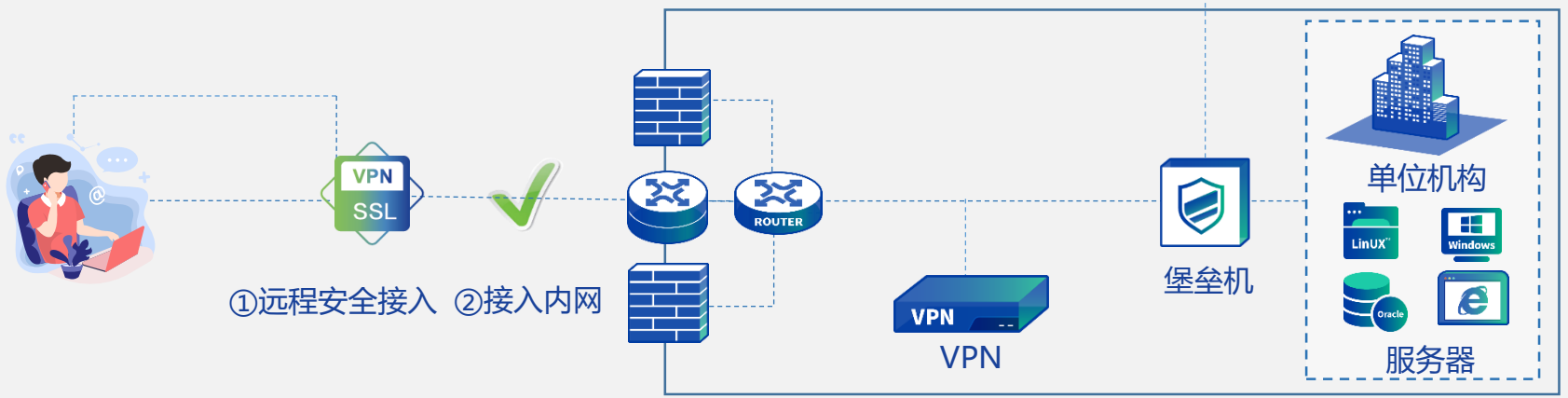
2015年首批获信息安全等级保护安全建设服务机构能力评估合格证书，启动做市交易，累计融资8600万元。

2017年入选新三板创新层，累计融资2亿元；发布工业互联网安全系列产品；获三项最高等级安全服务资质。

疫情期间远程运维方式1：VPN+堡垒机+终端安全

③堡垒机实时保证运维安全

- 权限最小化策略，运维人员只能访问权限内服务器
- 安全运维策略，敏感命令直接阻断或审批后才可执行
- 完善运维手段，提供友好、全面的运维工具方便运维工作
- 实时监控和记录运维操作，责任精准定位



可搭配内网/准入/EDR等产品，增强访问内网的客户端安全性

- 禁止接入U盘、移动硬盘、智能手机等外接设备
- 操作系统、补丁、防病毒软件安装、可疑文件、注册表检查

运维流程设计：

1)在 网关设备上对外映射相关端口，供运维人员、第三方运维人员通过客户端登陆 SSL VPN， 与部署于企业或单位数据中心的的 SSL VPN 建立远程 VPN 接隧道

2)登录成功后，VPN 向终端推送准入规则

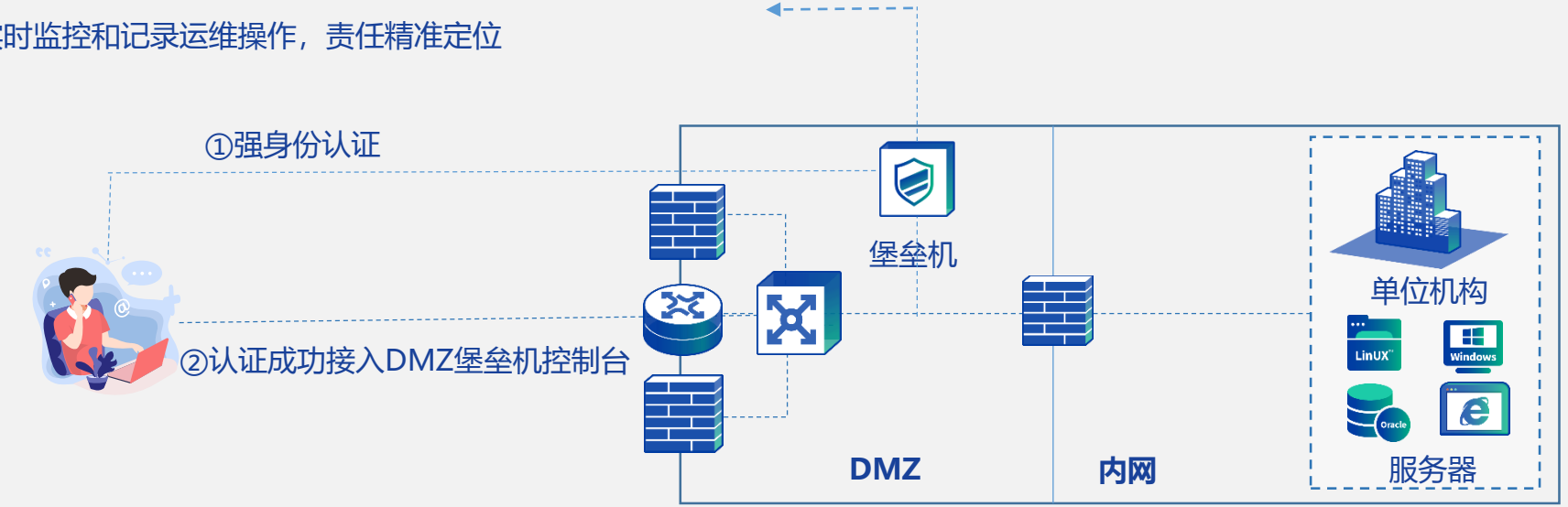
3)运维操作过程中堡垒机实时保证运维安全

4)断开连接

疫情期间远程运维方式2：DMZ+堡垒机+终端安全

③堡垒机实时保证运维安全

- 权限最小化策略，运维人员只能访问权限内服务器
- 安全运维策略，敏感命令直接阻断或审批后才可执行
- 完善运维手段，提供友好、全面的运维工具方便运维工作
- 实时监控和记录运维操作，责任精准定位



可搭配内网/准入/EDR等产品，增强访问内网的客户端安全性

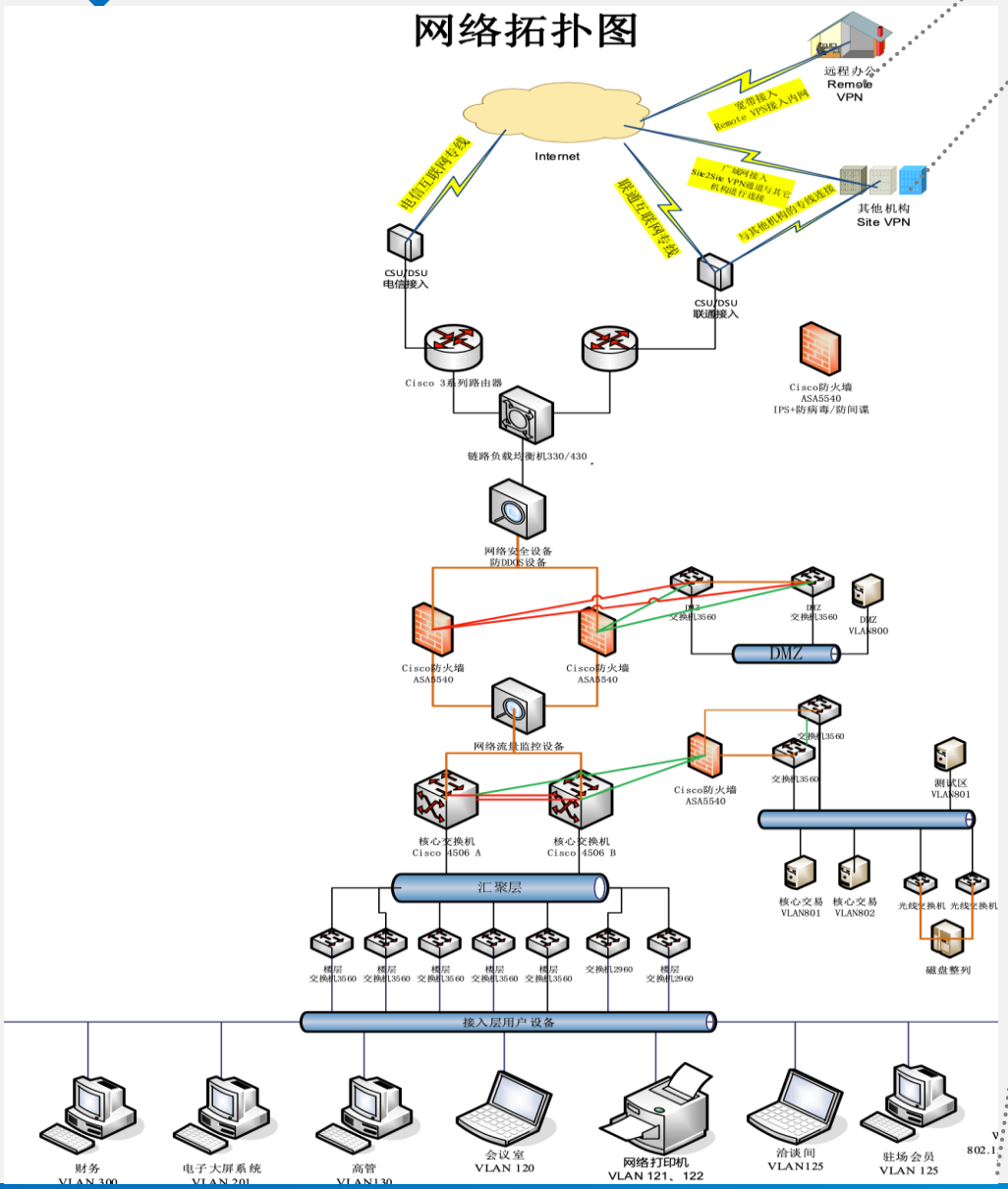
- 禁止接入U盘、移动硬盘、智能手机等外接设备
- 操作系统、补丁、防病毒软件安装、可疑文件、注册表检查

运维流程设计：

1）在DMZ映射堡垒机web访问与固定协议代理端口；
2）堡垒机挑战用户强身份认证（短信、LDAP、AD、数字证书、动态令牌等）
3）设定端口访问规则，只允许堡垒机访问内网服务的特定运维端口
4）运维操作过程中堡垒机实时保证运维安全
5）断开连接

疫情期间远程运维-案例

- 特殊时期远程设备运维需求
- 第三方厂商人员运维需求
- 同时存在内外网访问路径



该机构其他工作要求

1、提供双路保障：一路是通过VPN至DMZ区并通过堡垒机访问设备，另一路是对于部分现场人员仍需提供内网堡垒机访问路径

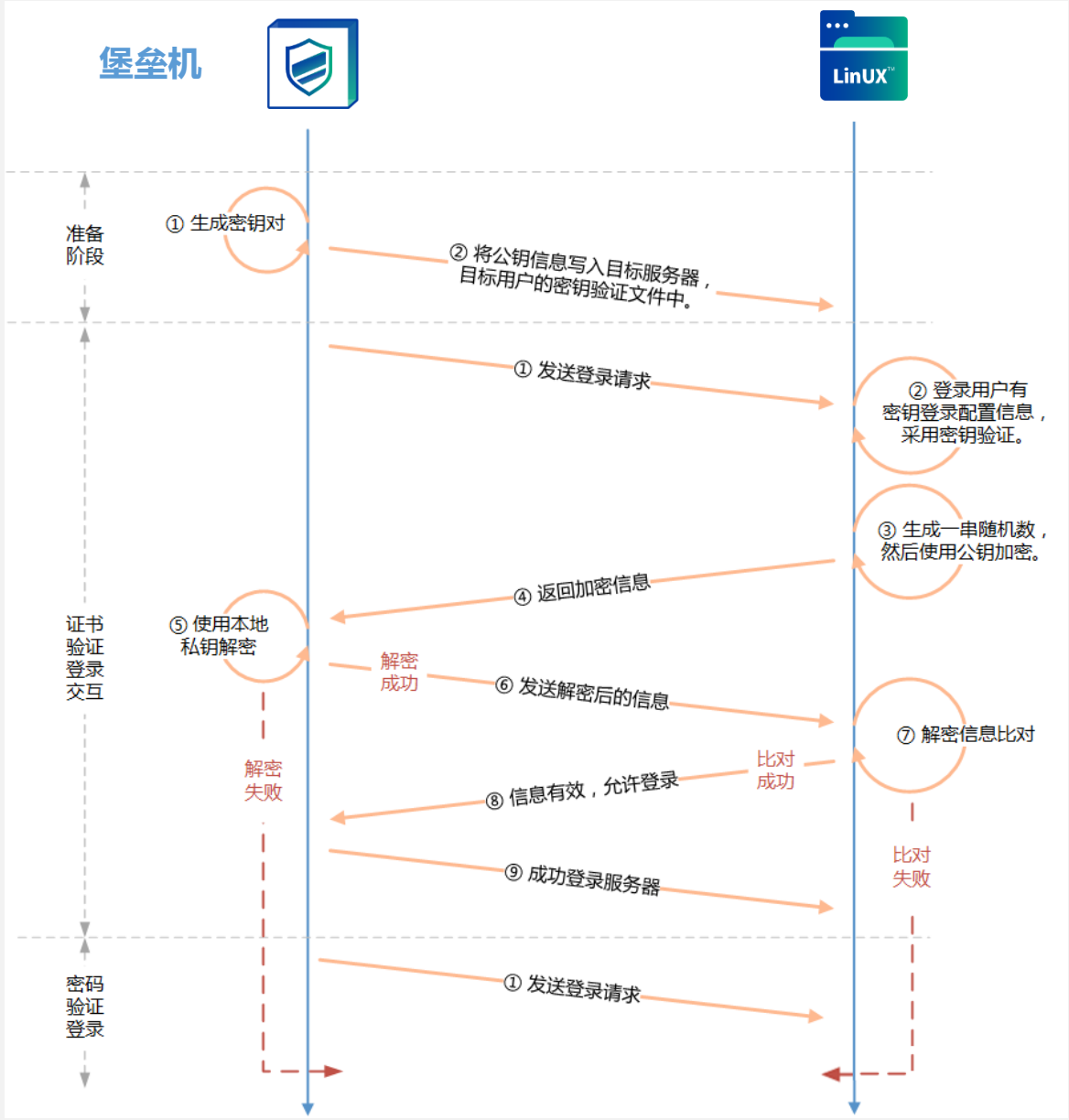
2、DMZ及内网均部署统一身份认证系统（IAM）要求堡垒机访问必须通过统一身份认证，并启用强身份认证F2A（基于动态口令 手机APP）

3、所有设备访问所产生的命令、操作痕迹录像均需保留3个月

4、支持审计的协议包括SSH、TELNET、RDP、 X11、VNC 、FTP、SFTP以及数据库访问行为

5、堡垒机上每位运维人员所能运维的资产列表均以最小化原则授予。

强身份认证-公私钥-1次1密



圣博润堡垒主机发展历程

2007

圣博润堡垒机起步

2010

市场化

圣博润堡垒主机逐步进入市场，开启市场化脚步

2014

100,000点

在设备超过100,000台的环境中成功部署，国内最大部署案例

2015

30分支

在全国范围超过30个分支节点的环境中成功部署

2016

8000并发

在超过8000个字符并发的环境中成功部署

2017

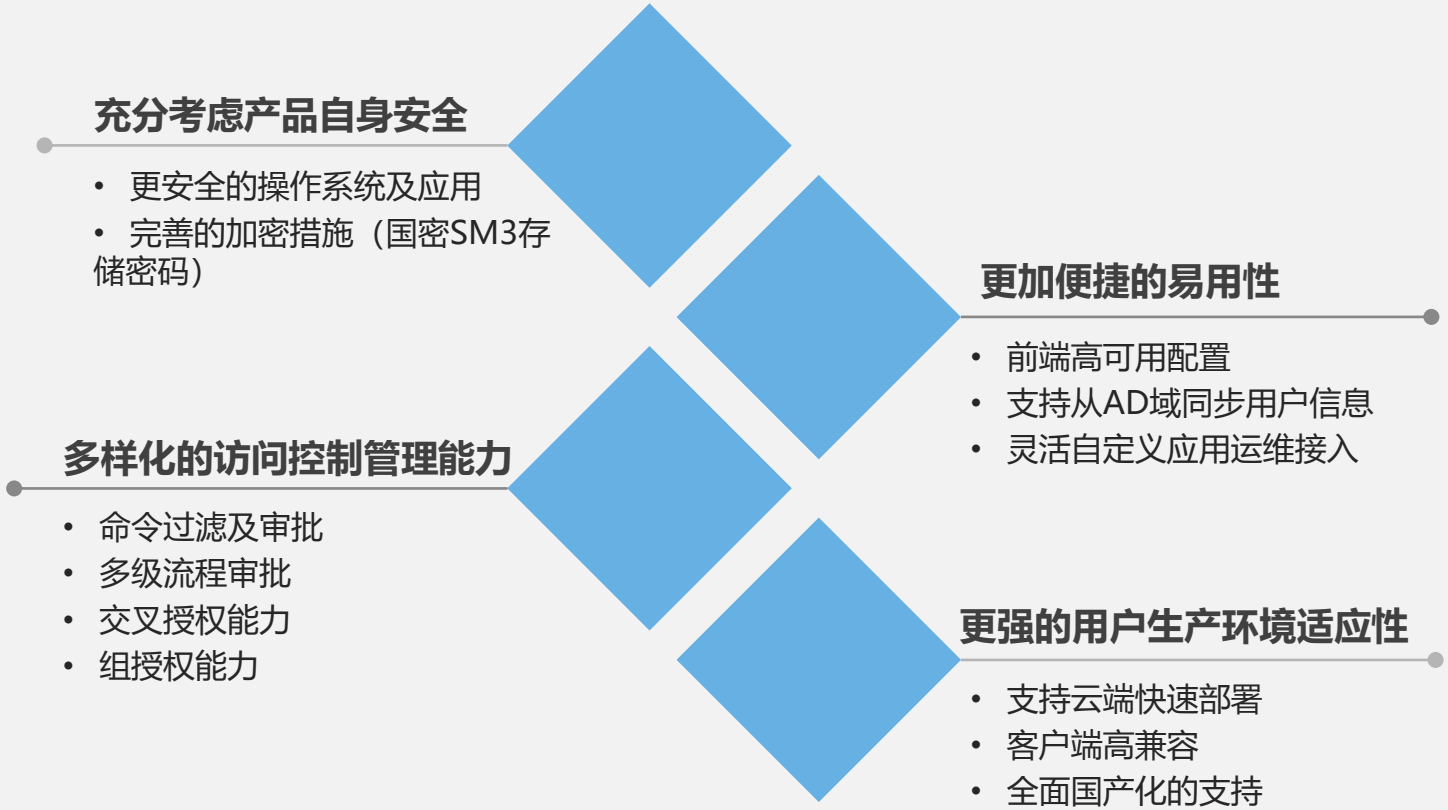
市场占有率第一

连续5年市场占有率第一

2019

云堡垒步入市场

优势分析-全面应对疫情期远程运维



充分考虑产品自身安全

- 更安全的操作系统及应用
- 完善的加密措施（国密SM3存储密码）

更加便捷的易用性

- 前端高可用配置
- 支持从AD域同步用户信息
- 灵活自定义应用运维接入

多样化的访问控制管理能力

- 命令过滤及审批
- 多级流程审批
- 交叉授权能力
- 组授权能力

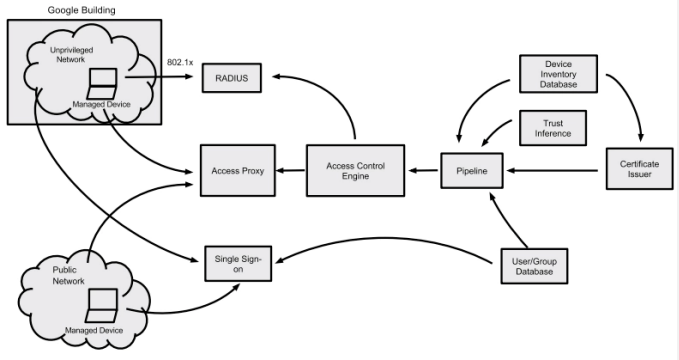
更强的用户生产环境适应性

- 支持云端快速部署
- 客户端高兼容
- 全面国产化的支持
- 自由选择Web/客户端运维
- 全面支持IPV6

趋势1-零信任的初衷思想

边界防御

传统的边界防御模型，构建一个由私有地址构成的企业“内网”，在内网边界架设防火墙、入侵防护等各种防护设备，配合VPN接入、网络准入、内部路由策略、对外上网行为管理等构成一个内外有别的环境



边界不再清晰。如果企业所有员工都只在办公楼内工作，传统模型仍然简单有效。但随着移动办公的出现，有很多需要在物理边界之外办公的需求，加上访客、供应商等需要进入企业并访问网络，包括内部员工可能携带个人设备（尤其是手机）进入企业内部

边界模糊

一方面，由于前述原因，内网必然存在一些无法完全信任的危险设备
另外一方面，传统模型带来的可靠性错觉使得很多企业忽视了内网的安全防护，包括基本的补丁更新、安全配置等。过度依赖于边界的防护，一旦这个边界被突破，内网存在严重隐患

内网隐患

趋势1-基于零信任的堡垒机模型

发动机-数据库 → **堡垒机用户、资源管理**

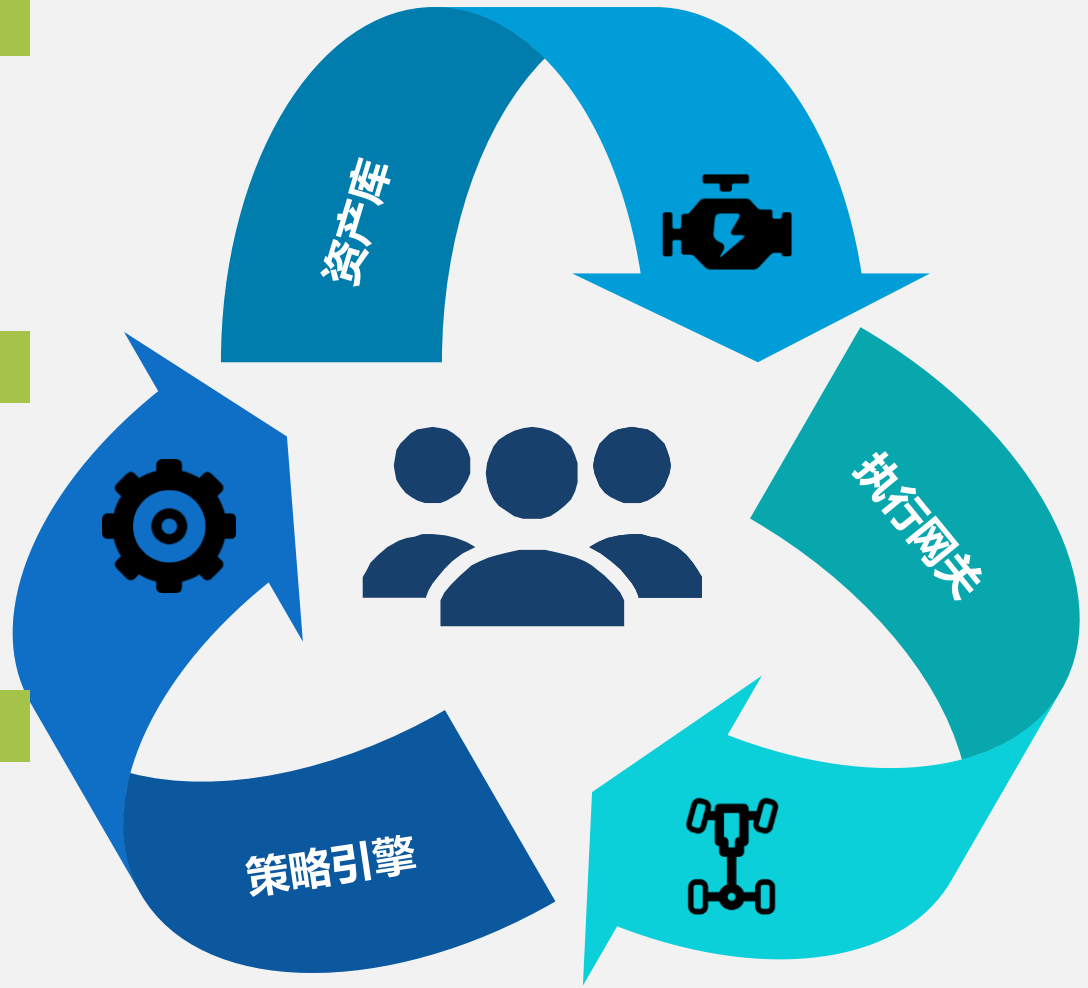
用户信息、受管设备
非对称信息资产关联

变速箱-策略引擎 → **堡垒机策略访问授权**

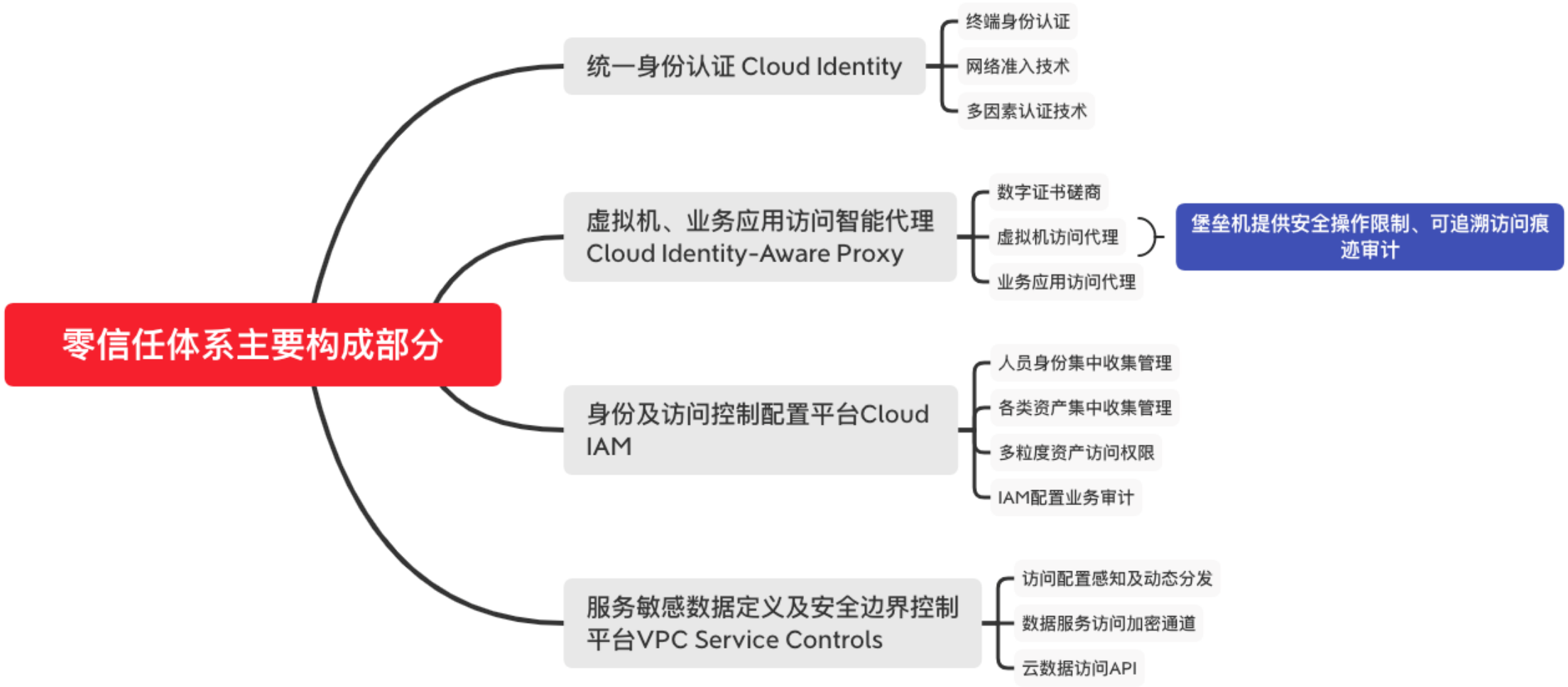
信任等级评估
用户生命周期动态策略变更
信任证书管理

底盘-执行网关 → **堡垒机协议代理**

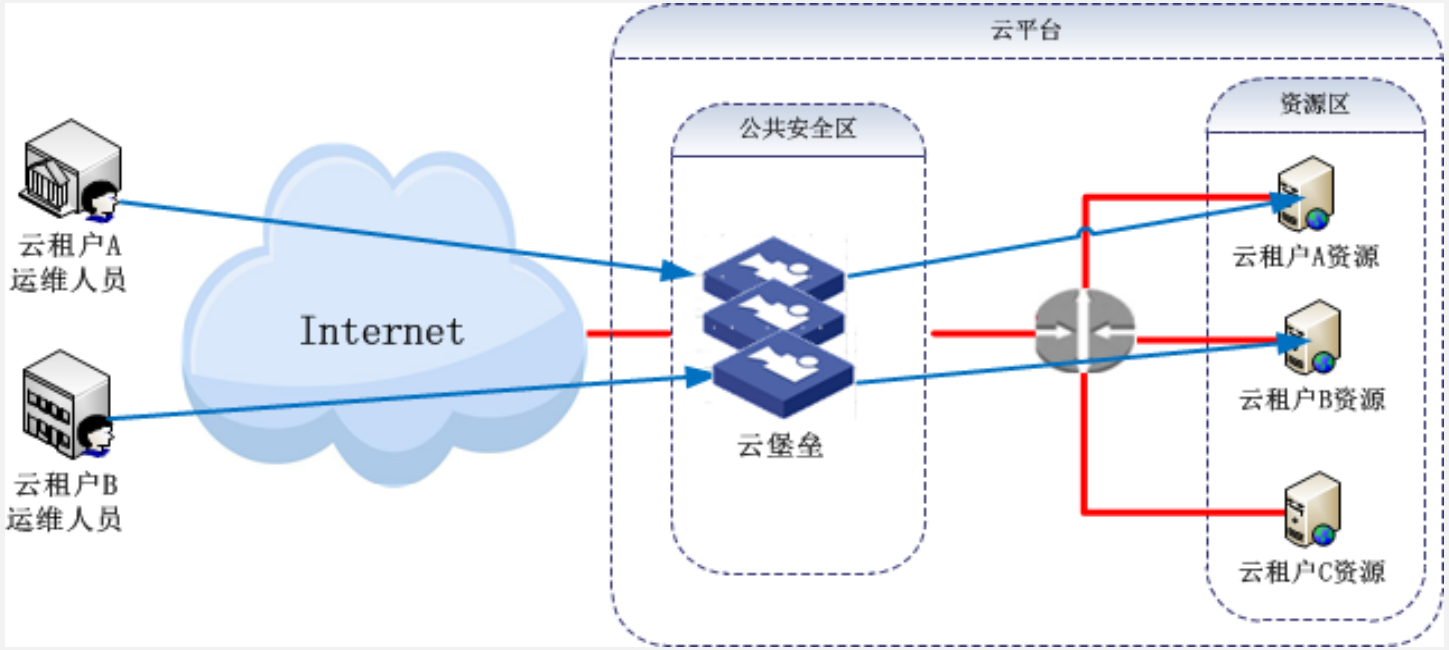
网络访问控制（802.1X，radius）
HTTP/S应用由访问代理AP
加密服务器（TUN设备）



趋势1-堡垒机在零信任体系中的作用



趋势2-云堡垒（私有云或公有云）



云堡垒关键点

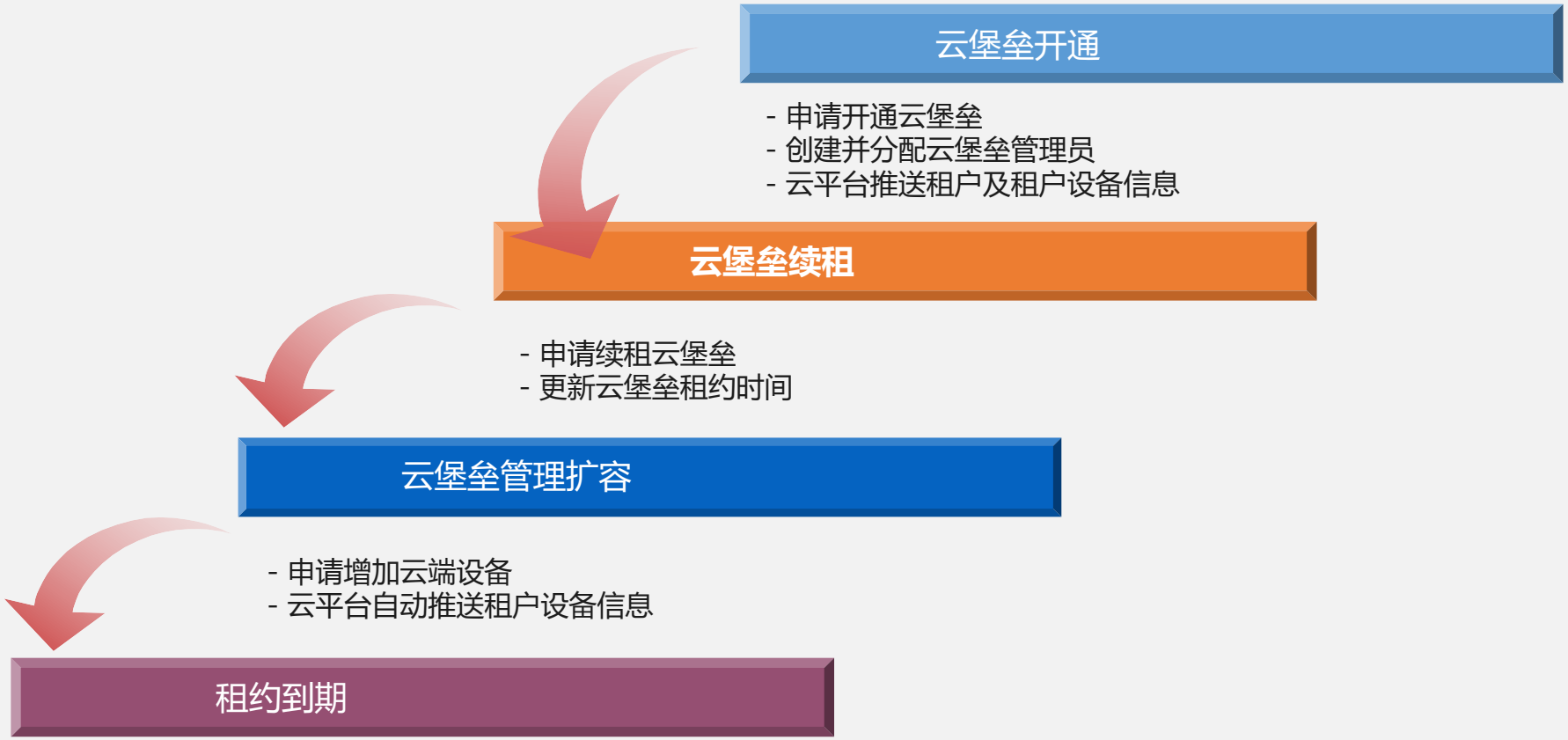
1、顺应数据集中的趋势，在资源及访问用户进行逻辑切割，每个云租户拥有自己独立的资源范围以及自我管理的运维人员

2、将堡垒作为平台允许租户对服务的开通、续租、扩容进行

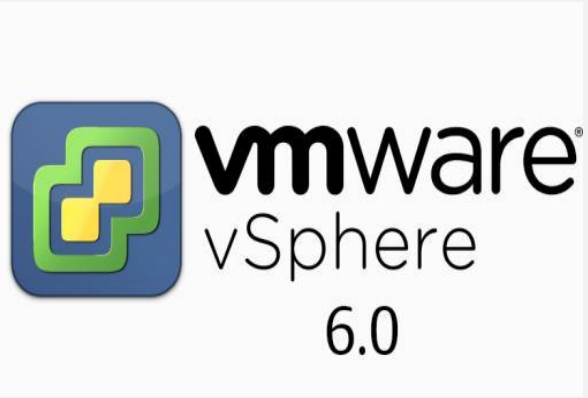
3、为支撑高访问量需支持可水平扩展的集群结构

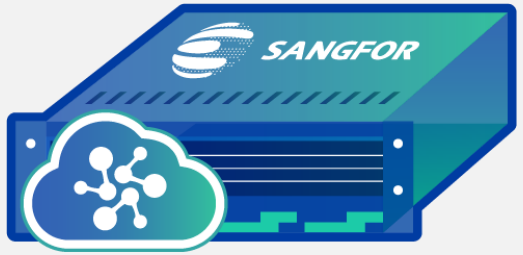
4、为云计算运营机构提供所有租户及租户资源的全面视角（访问量、运行状态、高危操作统计）

趋势2-云堡垒（私有云或公有云）



疫情期间快速部署-全格式镜像





疫情期间安全保障服务-互联网网站远程安全监测预警服务

服务介绍

需要具备的条件	服务方式	服务内容

本项服务针对于互联网网站。
仅需要提供网站域名、IP地址、授权文件和紧急联系方式，可对重点网站开展安全检测。

本项服务采用莱恩赛克网站安全监测平台，对互联网网站实现7×24小时的实时性监测。

本项目服务可对互联网网站的可用性、安全漏洞、挂马暗链、网页篡改、关键字、域名劫持、后门进行7×24小时实时监测，发现安全风险，及时通过邮件、短信或电话等方式发出告警。***实现网站安全“体温监测”。***

疫情期间安全保障服务-远程安全评估服务

服务介绍

需要具备的条件	服务方式	服务内容

本项服务针对于系统运行所涉及的网络设备、安全设备、主机系统及中间件。用户需要提供授权文件、远程接入环境（网络层对相关的监测设备放开限制）、访问权限（如堡垒主机）并安排相关人员进行我方操作监控等。

本服务通过安全服务人员和“圣博润网络脆弱性扫描与管理系统”相结合的发方式提供服务。

本项目服务可对网络设备、安全设备、主机系统及中间件的安全配置、安全策略、安全漏洞进行评估，对重要日志进行分析，发现潜在安全风险和隐患。***提升系统自身“基础免疫力”。***

疫情期间安全保障服务-互联网网站渗透测试服务

服务介绍

需要具备的条件	服务方式	服务内容

本项服务针对于互联网网站。
仅需要提供网站域名、IP地址、授权文件和紧急联系方式，并做好重要数据的备份等工作，可对重点网站开展渗透测试工作。

本项服务通过远程渗透测试工具扫描及安全漏洞人工验证（人工评估）两种方式配合开展。能够根据使用者的实际要求进行有针对性的测试。

本项服务尽可能完整的模拟黑客使用的漏洞发现技术和攻击手段，对网站进行全面检查。，发现应用系统中最薄弱环节。***杜绝应用系统“带病运行”。***

疫情期间安全保障服务-远程应急处置服务

服务介绍

需要具备的条件	服务方式	服务内容

本项服务面向用户针对网络安全事件的管理。
仅需要提供授权文件、紧急联系方式和远程接入环境，即可开展远程应急处置工作。

本项服务通过7×24小时电话响应。帮助用户在第一时间遏制网络安全事件的进一步蔓延。

本服务对安全事件进行分析研判，溯源网络安全事件发生的原因，并提供详细的修复建议，协助用户快速恢复网络服务。**做到“快速响应，全力救治，减少伤亡”。**

圣博润
SBR-info

祝大家身体健康，共克疫情！

圣博润疫情期间快速服务电话：
400-966-2332
周经理 18588659288

www.sbr-info.com

地址：北京市海淀区高梁桥斜街59号院2号楼3层

电话：010-82138088

技术支持热线：800-810-2332 / 400-966-2332

技术支持邮箱：support@sbr-info.com