网络准入和数据防泄漏系统招标公告

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

网络准入和数据防泄漏系统一套

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。
5. 应证人在最近三年内未因自身任何违约、违法行为及违反商业道德的行为而导致取消参选资格、合同解除或败诉。
6. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
7. 法律、行政法规规定的其他条件。
8. 应证人需提供厂商对本项目的授权书。
9. 售后服务要求
10. 应证人应为征集人提供及时周到的系统技术支持。
11. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
12. 应证人所提供设备保质期均为三年（具有特殊要求的除外），集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
13. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
14. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
15. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
16. 验收
17. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
18. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
19. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
20. 报名方式

有意者请于2019年9月13日之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号 顾晓磊收

联系人：顾晓磊

联系方式：021-66988356 guxl@aaic.com.cn

1. 举报邮箱：[kehufuwu@aaic.com.cn](mailto:kehufuwu@aaic.com.cn)
2. 招标参数要求

|  |  |  |
| --- | --- | --- |
| 规模：全国范围500台终端 | | |
| 基本要求 | 公司资质 | 通过ISO9001认证，注册资本5000万以上 原厂具有CMMI\国家高新技术企业证书、重点软件企业认定证书 |
| 产品资质 | 提供著作权登记证书、公安部针对安全产品销售许可证书 |
| 产品有效案例 | 投标人提供5份所投产品在保险行业使用案例，具备太平洋保险集团内案例优先。 |
| 全国服务能力 | 在全国具有服务能力，提供超过30个主要城市的办公地址及办公室租赁合 |
| 系统参数 | 客户端支持操作系统类型 | Windows、Mac OS、Linux、Android、Linux |
| 策略定义与下发 | 通过Web登录统一的管控中心，进行所有策略的定义和下发 |
| 审计附件查询 | 在管控中心的的web页面上点击链接，即可解密存储在安全审计服务器上的文件 |
| 审计信息接收与查询 | 负责接收客户端采集的数据，并通过web页面进行自定义查询； |
| 安全模式 | 安全模式下，策略依然生效； |
| 组织架构管理 | 组织架构管理 | 支持自动同步企业AD/LDAP上的组织架构部门信息、用户账号信息、设备信息； |
| 支持手工维护组织架构部门和成员信息，允许通过导入导出操作进行批量维护； |
| 支持设置多级部门，子部门关系级数无限制； |
| 部门用户信息应包含但不限于工号、全名、备注、所属部门、联系方式（电话、手机号、邮件地址、Windows Message）； |
| 网络安全管理 | 拓扑发现 | 支持对接入网络的终端进行发现和定位，发现信息包含：设备名、设备IP、设备MAC、设备接入端口和使用设备的用户 |
| 支持对接入设备的设备类型进行识别，如windows主机，linux服务器，打印机，网络摄像头等主流终端的识别； |
| 入网权限控制 | 系统能够根据用户、部门和设备设置接入网络访问权限； |
| 能够根据哑终端的类型分配网络访问权限； |
| 系统能够自动判断打印机、网络摄像头、IP电话，并对这些设备进行自动入网授权，入网权限按照设备类型分配，实现权限最小化控制，网络权限控制支持TCP/UDP和端口级别。（需要提供系统配置截图） |
| 能够区分同一用户使用客户端和使用Web认证的网络访问权限。以免权限释放过大 |
| 支持终端安全检查失败本地ACL隔离机制，可基于协议、特定地址、IP范围来控制终端访问权限，从而无需操作交换机达到终端网络控制目的，实现细粒度的访问控制管理，支持不同终端修复区域定义。 |
| 访客及外协管理 | 支持访客接入，提供页面填写申请单方式。支持系统匹配受访人信息自助接入、受访人审核和系统管理员审核接入模式，以满足不同的管理需要，以满足不同的管理需要。 |
| 支持通过HTTP、POP3、短信方式提醒访客输入访客码，或提醒未安装Agent的终端安装Agent |
| 准入方式 | 有线环境，基于802.1x的网络准入方式。 |
| 无线环境，基于802.1x的网络准入方式。 |
| LAN/WAN/VPN/HUB等环境下的网络准入控制。 |
| 端口镜像方式准入。 |
| 策略路由方式准入。 |
| cisco eou方式准入。 |
| protal方式准入。 |
| 认证方式 | 能自动同步AD/LDAP上的组织架构信息和用户帐号信息，组织架构信息用于设置用户的资源访问权限。 |
| 内置帐号认证、兼容微软AD域帐号验证、LDAP帐号验证、证书帐号验证 |
| 支持手机、电脑通过微信方式入网 |
| 双因子认证 |
| 安全检查 | 接入帐号的合法性，接入的硬件信息，包括MAC地址、主机硬件标识等； |
| 接入设备的安全设置，防病毒软件的安装与更新信息，必须要支持现有防病毒客户端的准入检查； |
| Guest来宾账户检查、弱口令账户检查、AD域用户检查、共享目录检查； |
| 系统补丁检查、注册表项检查、文件要求检查、软件配置检查、软件组配置检查、准入客户端的软标签 |
| 对未安客户端软件的终端通过Web与邮件重定向方式的提醒 |
| 对未通过身份检查的终端通过Web与邮件重定向方式的提醒； |
| 对未通过终端安全检查的终端通过Web与邮件重定向方式的提醒； |
| 提醒内容需要包括接入失败的准确原因。 |
| IP/MAC绑定检查 |
| 基于设备行为特征的仿冒检查 |
| 基于指纹特征的仿冒检查 |
| 终端安全管理 | 资产管理 | 硬件信息：对设备当前的CPU、主板、BIOS、硬盘、显卡、声卡、网卡、PCI、磁盘、显示器、内存等信息进行采集； |
| 软件信息：可获取终端上软件的名称、版本、类型（Office、浏览器、补丁、驱动等）、类别（商业、免费）、安装时间、安装目录。 |
| 远程协助 | 支持远程确认模式，终端用户和远程管理员都可发起远程请求，此模式下，远程管理员发起的远程请求必须由终端用户进行确认，才能建立远程连接，连接建立后，终端用户桌面必须有明确提醒管理员正在远程； |
| 支持远程监控模式，远程管理员可直接对权限范围内的终端建立远程连接，在终端用户无感知的情况下，远程查看终端实时画面； |
| 支持一对多模式，一个管理员可同时对多个终端进行远程协助； |
| 支持在远程过程中进行双向文本消息沟通； |
| 支持在远程端向被远程端发送文件，支持在远程端从被远程端获取文件； |
| 支持对NAT网络内的终端发起远程； |
| 支持远程Windows、MAC OS、Linux终端； |
| 软件分发 | 支持将PC作为下载中继服务器，以节省带宽 |
| 支持自定义安装时间范围，避免软件影响用户正常使用； |
| 支持远程卸载软件； |
| 在任务开始前和安装成功后对终端的注册表、文件、操作系统版本、进程、服务、软件进行检查，可对满足检查条件的终端设定安装和不安装的触发条件； |
| 软件商城 | 支持在Web页面上传软件安装文件，并自动获取软件名称、版本等信息； |
| 支持从软件仓库中选取软件进行分发范围（同策略应用范围）设定； |
| 普通用户可通过客户端的软件管理入口卸载已安装软件； |
| 补丁管理 | 支持微软WSUS补丁服务器，同时也支持独立的补丁服务器，能够自动从微软网站下载补丁，或者通过拷贝方式将补丁导入到补丁服务器； |
| 支持补丁分发对带宽、对业务终端性能的影响;要求补丁分发时，可以指定分发的开始时间、结束时间； |
| 通过对PC进行中继处理从而对补丁分发带宽占用进行优化：对于分支当地没有服务器的情况； |
| 支持蓝屏修复； |
| 能自动统计终端补丁程序安装率，并提供补丁分发报表，分别从补丁，或终端角度查看、统计补丁安装情况； |
| 移动存储介质管理 | 支持移动存储设备注册管理，终端用户可在本机自行注册、申请移动存储设备，并可进一步控制注册移动存储设备只能在指定的终端或指定的部门使用，防止外来移动存储设备在本单位使用； |
| 移动存储设备读写审计与控制，管理员可定义是否允许读、写移动存储设备上的文件，并可定义能读、写哪些类型文件、以及定义写到移动存储设备上的文件是否自动加密； |
| 对移动存储设备的读、写操作进行审计，包括文件创建、复制、删除、修改、改名等操作。移动存储介质的插入和拔出动作的详细记录，包括事件类型，移动存储介质的名称、用户、计算机IP地址和事件时间。 |
| 非法外联控制 | 提供终端设备的外联接口进行安全管控，包括但不限于红外、蓝牙、软盘、光盘、串口、并口、网络接口、USB接口以及其他外联设备； |
| 支持禁用终端电脑共享WiFi热点（含windows和MAC OS) |
| 支持对未注册U盘进行禁用、只读、审计； |
| 主机进程管理 | 支持通过进程名称、进程文件属性（产品名称、公司名称、描述、源文件名、内部名称）、进程文件CRC值、进程文件MD5值、软件名称、目录名称、进程签名等方式对进程黑白名单管理； |
| windows本地安全策略 | 支持禁止修改注册表、禁止修改网络属性、禁止设置TCP/IP属性、禁止设置固定IP等 |
| 防火墙 | 防火墙为双向防火墙，能对终端向外访问与对外提供的服务分别控制； |
| 防火墙提供自定义协议与服务端口，支持TCP、UDP、RDP、HTTP、FTP、共享； |
| 防病毒检查 | 提供主流防病毒软件检查，包括软件版本、杀毒引擎版本、病毒库更新； |
| 可以控制终端用户防病毒软件病毒库的更新日期； |
| 数据安全管理 | 文件操作管控 | 支持管控终端上的文件操作，对通过剪切版（复制剪切）、导入导出、读写（文件资源管理器）等行为，文件源或目的为本地硬盘、移动存储介质（U盘、移动硬盘、SD卡）、网络共享、mstsc远程桌面或其他存储设备，可以进行禁止、审计、备份等管控操作 |
| 打印管控 | 对文件的打印行为进行安全管控，可基于打印机的访问IP、端口、型号特征进行黑白名单管理 |
| 对打印文件进行禁止、审计、备份等管控操作 |
| 审计打印文件时，可针对打印的页数、份数做针对性处理 |
| 水印方案 | 允许在终端访问敏感信息时自动加载数字水印以规避拍照、截图等外泄手段； |
| 支持多种形式的数字水印（文字、二维码、图片、矢量水印），水印信息应可包括登录用户、设备、时间等信息； |
| 支持自定义水印的内容形式，包括但不限于水印内容、水印大小、字体类型、颜色、透明度、行间距等； |