服务内容：

1. 本次项目服务需按照等保2.0三级要求开展。设备维保升级或软件升级后，供应商需保证升级后的设备及软件满足等保2.0三级要求，针对不符合要求的高中风险项目，应及时协助完成整改（费用包含在成交价中）。

2.设备维保升级后，供应商需保证升级后的设备及软件仍支持标准协议的日志外发（如：syslog等）。

3.服务内容

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **类别** | **服务项目** | **服务频率** | **服务成果** | **具体要求** |
| 1 | 亚信安全云主机深度安全防护系统软件DeepSecurity V20.0维保服务 | 远程支持 | 不限次数 | 原厂授权许可、续保升级license | **详见4.具体服务要求** |
| 现场支持 | 不限次数 |
| 同代系统版本升级服务 | 不限次数 |
| 产品特征库升级服务 | 不限次数 |
| 产品保修 | 不限次数 |
| 2 | 亚信安全防毒墙网络版软件 V16.0维保服务 | 远程支持 | 不限次数 | 原厂授权许可、续保升级license |
| 现场支持 | 不限次数 |
| 同代系统版本升级服务 | 不限次数 |
| 产品特征库升级服务 | 不限次数 |
| 产品保修 | 不限次数 |
| 3 | 亚信安全信桅高级威胁监测系统（TDA） V6.5维保服务 | 远程支持 | 不限次数 | 原厂授权许可、续保升级license |
| 现场支持 | 不限次数 |
| 同代系统版本升级服务 | 不限次数 |
| 产品特征库升级服务 | 不限次数 |
| 产品保修 | 不限次数 |
| 备机服务 | 不限次数 |
| 4 | 亚信安全运维管理平台维保服务 | 远程支持 | 不限次数 | 原厂授权许可、续保升级license |
| 现场支持 | 不限次数 |
| 同代系统版本升级服务 | 不限次数 |
| 产品特征库升级服务 | 不限次数 |
| 产品保修 | 不限次数 |
| 5 | 安全服务 | 安全策略优化服务 | 每周一次 | 《巡检记录表》及《安全巡检月度总结报告》12份； |
| 产品日志分析服务 | 每周一次 |
| 产品巡检服务 | 每周一次 |

1. 具体服务要求：

**序号1 终端防病毒维保服务（**亚信安全云主机深度安全防护系统软件DeepSecurity V20.0维保服务**）**

1、须与现已部署的防病毒客户端（系统厂商为亚信科技（成都）有限公司、亚信安全防毒墙网络版软件V16.0）兼容，提供不低于2200个客户端1年升级维保服务，并且提供与现有防病毒客户端环境相兼容的防病毒客户端版本升级、病毒库升级服务、现场巡检服务等，配合医院做好等保测评、攻防演练、相关安全督查等工作**。**

2、对于提供的防病毒服务中所使用的服务工具，针对文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类。

**序号2 服务器端防病毒软件及入侵防护系统维保服务（**亚信安全防毒墙网络版软件 V16.0维保服务**）**

1、须与现已部署的服务器端防病毒软件及入侵防护系统（系统厂商为亚信科技（成都）有限公司、亚信安全云主机深度安全防护系统用软件DeepSecurityV20.0）兼容，提供不低于455个服务器端防护能力包括但不限于防病毒及防恶意软件能力、服务器端防火墙能力、url安全检测、入侵防护能力、日志审计能力等；并且提供与现有防病毒客户端环境相兼容的防病毒客户端版本升级、病毒库升级服务、现场巡检服务等，配合采购人做好等保测评、攻防演练、相关安全督查等工作。

2、提供的服务器端防病毒服务，支持本地扫描和云扫描，支持实时扫描、预设扫描、手动扫描和快速扫描；如发现特殊情况（如业务高峰期），可支持终止操作。

**序号3 亚信安全信桅高级威胁监测系统（TDA） V6.5维保服务**

1、提供的威胁检测服务中所使用的服务工具具有虚拟化沙盒系统，并且支持高度定制化，可以支持高度模拟真实环境的操作系统平台与应用。

2、信桅高级威胁监测系统（TDA）（产品厂商为亚信科技（成都）有限公司，设备型号为TDA2300）维保服务，维保服务内容包括但不限于：

（1）提供现场巡检服务，配合采购人做好等保测评、攻防演练、相关安全督查等工作；

（2）为保证防病毒客户端及监测服务工具处于高效、准确工作，供应商需提供定期上门，检查防病毒客户端、深度威胁发现设备版本等版本升级等，降低误报率；

（3）当设备故障时提供备机服务，能够保证故障期间正常检测。

**序号4 防病毒安全运维平台维保服务**

1、提供防病毒安全运维平台续保服务（产品厂商为亚信科技（成都）有限公司，产品型号为亚信安全信池统一安全管理平台UAP V5.0），防病毒安全运维平台支持现有终端防病毒、现有深度威胁发现设备和主机防病毒及入侵防护系统的防病毒运维工作，提供可视化界面，统一分析病毒风险、威胁告警等能力；并提供现场巡检服务等，配合采购人做好等保测评、攻防演练、相关安全督查等工作。

2、提供威胁可视服务，在一个页面上从威胁的生命周期（至少包含侦测、分析、响应）角度进行监控。

3、提供威胁日志的二次分析服务，所使用的服务工具必须具备能够展示攻击关系的线性放射图，实现以攻击源头为中心，展示在一定时间范围内的被攻击目标、手段的场景。

**序号5 安全服务**

**1.产品续保服务要求**

（一）远程支持服务

在服务期内，产品使用过程中，因某种原因出现问题，成交人需提供电话方式远程支持服务，派工程师对问题进行诊断解决；如不能通过电话解决，需通过远程联机管理解决故障。

（二）现场服务

在服务期内，通过电话交流或者远程调试无法解决的，成交人需派工程师在2小时内响应并到现场维护。

（三）系统版本升级服务

在服务期内，续保产品（上述维保设备清单）系统版本出现可升级的新版本时，成交人需根据产品性能为采购人提供同代版本升级服，并派工程师现场为系统进行配置备份。在不影响业务系统正常运行的情况下，对系统版本进行升级，并完成新系统的配置恢复。新系统上线后，成交人需对网络连通性和业务可用性进行测试，保证业务的正常运行。

（四）产品特征库升级服务

在服务期内，日常运维的过程中，对需要升级特征库版本的防病毒软件及信桅高级威胁监测系统（TDA）等安全产品，续保产品（上述维保设备清单）需根据产品的性能对安全产品的特征库进行定期升级，保证特征库版本最新有效。

（五）产品保修服务

在服务期内，若续保产品（上述维保设备清单）出现软硬件故障，成交人需提供维修服务（维修费用包含在成交价中，采购人不另外付费），保障设备及业务系统的持续可用性。

对于购买日期超过6年的设备，如在硬件市场上找不到相应的配件进行维修，且设备故障48小时内无法修复的情况下，成交人需提供不低于故障设备型号的备机直至服务期结束。

（六）备机服务

成交人需具备完善、充足的备机配件库。当设备发生故障且48小时内无法修复时，成交人需提供备机服务，将备机或备件送至现场进行更换，确保业务系统的正常运行。

**2.安全产品现场巡检服务要求**

（一）安全策略优化服务

在服务期内，成交人需派工程师对安全产品的安全策略进行梳理，定期对安全产品和信息系统现有状况进行分析评估。在系统状况评估基础上，分析策略是否有效、冲突、冗余，统计安全策略的命中率，依据“最小化”原则，给出安全策略梳理建议，进行安全策略的配置调整和优化。

（二）产品日志分析服务

在服务期内，成交人需派工程师对网络安全设备进行安全日志分析，在大量日志信息中找到与系统安全相关的数据。分析系统运行情况，检查系统中有无危害安全性的活动，及时发现潜在威胁和挖掘异常行为。帮助采购人快速识别病毒攻击、异常流量以及非法行为等重要的安全信息，从而运用合理的安全策略，保证网络的安全。

（三）产品巡检服务

在服务期内，成交人需针对防病毒软件及信桅高级威胁监测系统（TDA）等，定期对设备和系统的运行状况、安全配置、运行日志等进行全方位的安全检查，提供巡检分析报告并提供合理的安全整改建议，协助采购人及时对各类安全问题进行修复、处理，确保采购人信息安全。