# 云服务器及安全防护参数要求

# 1、询价内容一览表

|  |  |  |  |
| --- | --- | --- | --- |
| **合同包** | **品目号** | **货物名称规格** | **数量** |
| 1 | 1 | 云服务器及安全防护服务 | 1套 |

# 技术参数要求

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **详细技术指标要求** |
| 1 | 安全管理中心 | 为用户提供统一的安全管理与运营平台，满足用户服务监控、服务报表、威胁展示、服务管理等需求，帮助用户实现用户细粒度的安全自主可控、可管理的安全目标。  **主要功能：**  1、综合概览：提供租户所购买的安全服务在使用过程中所产生的事件监控，展示租户的整体情况，展示最近一小时的时间风险分布、攻击类型统计图等；  2、个人中心：提供账号信息管理、资产管理、审计日志和权限管理等功能； |
| 2 | 下一代防火墙（100M） | 立足于用户网络边界，实现边界防护与访问控制。  **主要功能：**  1、防护概览：包括源地址全部事件、目的地址全部事件、源地址阻断事件、目的地址阻断事件。  2、防护配置：提供基于源/目的IP地址的精细粒度的安全访问控制，支持对已设置的防护策略的增、删、改、查；  3、防护日志：支持查看已设定的策略的防护日志  4、统计报表：云租户设置报表生成条件后，用户管理平台即可按照设置的条件从运营平台上获取统计报表数据。租户可以对报表进行添加、查看、删除等操作。  5、服务管理：云租户可以对已购买的服务订单进行扩容、续约操作。 |
| 3 | WEB应用防火墙（100M） | 抵御OWASP Top 10等各类Web安全威胁和拒绝服务，保卫Web应用免遭当前和未来的安全威胁攻击  **主要功能：**  1、防护概览：事件风险分布图、攻击类型统计等  2、协议支持：支持针对HTTP和HTTPS两类协议的检测，当协议选择HTTPS时，可配置协议使用的证书。  3、Web通用防护：支持SQL注入、XSS注入、命令注入、远程文件包含、路径遍历、XPATH防护、HTTP协议检查、下载限制、上传限制、HTTP访问控制、WEB服务器插件、扫描攻击等  4、防护日志：云租户在购买web应用防火墙服务，并对指定防护IP配置并下发防护策略后，即可查询web应用防火墙服务的防护生效后所产生的事件日志  5、统计报表：云租户设置报表生成条件后，用户管理平台即可按照设置的条件从运营平台上获取统计报表数据。云租户可以对报表进行添加、查看、删除等操作。 |
| 4 | 防病毒（1台） | 提供终端查杀病毒、软件管理、漏洞补丁、统一升级管理等功能；  **主要功能：**  1、主机防火墙：通过配置主机防火墙(网络管控)策略，能有效防护全网终端免受网络安全攻击。支持对IP、端口协议及访问方向等维度过滤，能智能识别网络协议，严格的端口管理减少端口暴露而带来的病毒传播、安全攻击等机率；  2、漏洞加固：实时扫描记录终端的操作系统及常用应用软件漏洞，快速掌握全网终端漏洞情况及风险状况，包括补丁安装情况、补丁风险占比、漏洞未修复情况。可按补丁查看修复终端，以及按终端查看修复情况。  3、勒索病毒防御：系统内置了已申请专利基于HIPS的勒索者主动防御机制，蠕虫病毒、勒索病毒、宏病毒等已知未知威胁防范无忧。 |
| **5** | 漏洞扫描/WEB漏洞扫描服务 | 安全工程师利用专业的系统漏洞扫描工具，发现云主机系统存在的安全隐患，方便管理员对主机的安全进行检查和分析，及时修复漏洞、提高系统安全防护能力。 |
| **6** | 网站漏洞扫描服务 | 安全工程师利用专业的Web漏洞扫描工具，发现网站应用存在的安全隐患，方便管理员对网站的安全进行检查和分析，及时修复漏洞、提高系统安全防护能力。 |
| **7** | 7\*24小时值守 | 提供7\*24小时技术支持，由专业的安全工程师值守，确保随时为云安全提供服务，解决问题。 |
| **8** | 应急响应服务 | 当云主机出现黑客入侵事件后，由专业安全工程师远程提供应急响应服务，查找事件原因，提供事件处理分析报告。 |
| **9** | 入网评估服务 | 安全工程师在开通云安全服务后，会对已上线的业务系统进行全面地评估，评估内容为系统安全、Web应用安全、数据库安全和日志安全等，输出检查结果及整改建议。 |
| **10** | 病毒清除服务 | 安全工程师对云主机出现的顽固病毒进行全面分析，制定针对性的清除方案，实施病毒清除操作。 |
| **11** | 安全报告服务 | 根据安全能力防护情况、每月系统漏洞评估及Web应用漏洞评估情况，提供针对性的整改建议，并输出月度报告发送至用户指定邮箱。 |
| **12** | SSL 证书 | 数量1，企业型（OV），SHECA 国际标准、通配符型。 |
| **13** | 云备份 | 500G主机容量+1T备份容量  以上安全防护服务期限：3年 |
| **14** | 其它 | 本项目云主机需符合《信息安全技术网络安全等级保护基本要求》GB/T22239-2019（三级）要求，并在二级等保评审中协助医院完成官网系统评审工作。  提供最大 5Gbps DDoS 攻击防护能力 |

# 3、服务器要求

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **详细技术指标要求** |
| **1** | 云主机配置要求 | CPU：16核  内存：32G  系统盘：100G  数据盘：1T  带宽：50M  期限：3年 |

# 4、云专线要求

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **详细技术指标要求** |
| **1** | 云专线 | 30M，运营商机房至门诊部机房链路。  期限：3年 |