附件一华为云产品及安全服务报价总表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序 号 | 产品名称 | 计费模式 | 购买量 | 单 位 | 购买个数 | 规 格 | 原价 | 参 选优惠价 |
| 1 | 弹性云服务器 | 包年 | 1 | 年 | 1 | X86计算 | 通用计算增强型 | c7.xlarge.2 | 4核 | 8GiB; CentOS | CentOS 7.9 64bit; 通用型SSD | 500GB;  |  |  |
| 2 | 弹性云服务器 | 包年 | 1 | 年 | 1 | X86计算 | 通用计算增强型 | c7.xlarge.4 | 4核 | 16GiB; CentOS | CentOS 7.9 64bit; 通用型SSD | 500GB;  |  |  |
| 3 | 弹性云服务器 | 包年 | 1 | 年 | 2 | X86计算 | 通用计算增强型 | c7.xlarge.4 | 4核 | 16GiB; CentOS | CentOS 7.9 64bit; 通用型SSD | 500GB;  |  |  |
| 4 | 弹性云服务器 | 包年 | 1 | 年 | 1 | X86计算 | 通用计算增强型 | c7.xlarge.2 | 4核 | 8GiB; Windows | Windows Server 2016 数据中心版 64位简体中文; 通用型SSD | 500GB;  |  |  |
| 5 | 云数据库 | 包年 | 1 | 年 | 1 | 通用可用区 | MySQL | 8.0 | 主备 | 独享型 | 4核16GB; 极速型SSD | 500GB; |  |  |
| 6 | 弹性公网IP | 按需计费 | 1 | 小时 | 1 | 独享 | 全动态BGP | 按流量计费 | 1GB x4; 4个; |  |  |
| 7 | 共享流量包 | 包年 | 1 | 年 | 2 | 共享流量包 | 全动态BGP | 按流量计费 | 一年 | 16TB |  |  |
| 8 | 企业主机安全 | 包年 | 1 | 年 | 5 | 旗舰版;  |  |  |
| 9 | 虚拟专用网络 | 包年 | 1 | 年 | 1 | 专业型1-非固定IP | 10个连接组数; | HA模式：双活 EIP1带宽 20Mbit/s； EIP2带宽 20Mbit/s； |  |  |
| 10 | DDoS防护 | 包年 | 1 | 年 | 1 | 保底防护带宽：10Gbit/s； 业务带宽：100Mbit/s； 防护域名数：50个 |  |  |
| 11 |  |  |  |  |  | 合 计 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序 号 | 服务名称 | 服务内容描述 | 原 价 | 参选优惠价 |
| 1 | 等保安全咨询服务 | 1. 差距分析服务：针对新部署的系统功能模块，结合原有系统定级情况。根据《信息系统安全保护等级基本要求》将定级信息系统等级保护的各项基本要求与信息安全现状进行比较分析，从技术方面找出存在的问题并进行差距分析，提供《网络安全等级保护差距评估报告》。
2. 漏洞扫描服务：安全专家通过专业的漏洞扫描设备对指定信息资产进行漏洞扫描，扫描检测对象包括：网络设备、操作系统、数据库、中间件等。扫描完成后形成漏洞扫描报告，提出整改建议。（季度/次）；
3. 漏洞跟踪复查跟踪服务：对发现的网络层、主机层以及应用层的高危漏洞提供漏洞跟踪复查服务，定期根据客户反馈的漏洞修复情况进行复查，并制定漏洞跟踪表，定期督促客户及时对漏洞进行修复。（季度/次）；
4. 安全加固服务：依据三级等保对新系统的安全配置标准要求，对操作系统、网络设备、安全产品、应用系统、中间件、数据库等对象进行全面的安全策略加固。（季度/次）；
5. 渗透测试服务：在客户授权许可的情况下，通过模拟黑客的攻击方法，对信息系统的现状进行安全评估。渗透测试过程包括对系统的弱点、技术缺陷进行分析和利用,将入侵的过程和发现的漏洞详情形成报告反馈给客户，并提出解决方案，配合客户修复漏洞。（年/2次）；
6. 安全管理制度完善服务：对现有安全管理制度进行调研，针对不足进行整改，完善管理制度。（年/次）；
 |  |  |
| 2 | 混合云基础安全服务 | 1. 云上架构优化服务：定期为应用提供成本和架构优化建议。（季度/次）；
2. 网络通道部署服务：提供华为云VPN部署及安全策略配置服务，实现华为云上资源与线下机房资源加密互联。（单次）；
3. 网络链路调优服务：定期评估混合云网络链路指标，如带宽、延迟、丢包率等；根据评估结果进行配置及参数调优。（季度/次）；
4. 风险评估服务：安全专家依据《信息安全风险评估规范》等技术标准，从风险管理的角度，运用科学的方法和手段，全面的分析信息系统所面临的威胁及其存在的脆弱性。安全专家将评估安全事件发生后可能造成的危害程度，为客户提出针对性的防护对策和整改措施。（年/次）；
5. 安全巡检服务：安全工程师对信息系统定期现场或远程巡检，及时发现信息系统（网络架构、网络设备、主机、数据库、安全设备等对象）存在的各种安全隐患。并输出《安全巡检报告》。（季度/次）；
6. 基线核查服务：针对操作系统、数据库、网络设备、安全产品、应用系统等对象基于信息安全风险的角度进行配置核查，核查内容包含安全策略设置、审计策略、口令策略、漏洞修复情况、防病毒措施等。（季度/次）；
7. 网站安全监控服务：对网站的安全状态进行全方位监测，包括网站可用性、网站漏洞、网页挂马、暗链、敏感关键字、变更等，并定期出具网站监控报告。（季度/次）；
8. 应急演练服务：制定各类应急预案，对相关人员进行应急预案的教育和培训。举行应急预案的演练，保证当发生安全事件时，能够按照应急预案对系统进行应急处置，并且在应急演练结束后形成详细的应急演练报告。（年/次）；
9. 应急响应服务：参照国家信息安全事件响应处理相关标准，帮助客户在发生安全事件后，按照预防、情报信息收集、遏制、根除、恢复流程，提供专业的7\*24的紧急响应处理服务，帮助客户快速响应和处理信息安全事件。（全年）；
10. 安全通告服务：根据目前的信息安全形势，提供最新的安全态势以及根据客户的资产对象定制漏洞通告以及对应的解决方案，协助客户修复漏洞。（全年）；
11. 安全培训服务：提供安全基础知识、安全政策标准、安全防护意识等内容的培训，采用讲授、讨论、实践相结合的方式，提升客户安全意识和安全实践能力。（年/次）；
12. 安全咨询与远程支持服务：当遇到网络异常缓慢、发现病毒现象、发现黑客入侵等安全现象时，及时启动安全咨询和应急预案，我司工程师提供7\*24小时的网络与信息安全问题电话咨询服务。（全年）；
 |  |  |