政府采购项目采购需求

采购单位：广元市昭化区卫生健康局

所属年度：2023年

编制单位：广元市昭化区卫生健康局

编制时间：2023年12月27日

一、项目总体情况

（一）项目名称： 广元市昭化区卫生健康局“医疗云”服务采购项目

（二）项目所属年度： 2023年

（三）项目所属分类： 服务

（四）预算金额（元）：500,000.00元 ，大写（人民币）：伍拾万元整

（五）项目概况：根据医疗机构需求，整合昭化区卫健系统三家机房承担的业务服务需求，拟采购一家服务商提供云储存、云计算、云安全、卫生专网等服务，满足等保2.0安全、业务空间资源需求，网络专线、数据迁移、运营服务等要求。

（六）本项目是否有为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商：否

二、项目需求调查情况

依据《政府采购需求管理办法》的规定，本项目不需要需求调查，具体情况如下：

·本项目属于以下应当展开需求的情形

·本项目属于以下可以不再重复开展需求调查的情形

（一）需求调查方式

（二）需求调查对象

（三）需求调查结果

1.相关产业发展情况

2.市场供给情况

3.同类采购项目历史成交信息情况

4.可能涉及的运行维护、升级更新、备品备件、耗材等后续采购情况

5.其他相关情况

三、项目采购实施计划

（一）采购组织形式：政府集中采购

（二）预算采购方式：非公开招标

采购方式：竞争性磋商

（三）本项目是否单位自行组织采购：否

（四）采购包划分：不分包采购

（五）执行政府采购促进中小企业发展的相关政策

本项目不专门面向中小企业采购

注：监狱企业和残疾人福利单位视同小微企业。

（六）是否采购环境标识产品：否

（七）是否采购节能产品：否

（八）项目的采购标的是否包含进口产品：否

（九）采购标的是否属于政府购买服务：否

（十）是否属于政务信息系统项目：否

（十一）是否省属高校、科研院所科研设备采购：否

（十二）是否属于PPP项目：否

（十三）是否属于一签多年项目：是

一签多年服务期限：三年

四、项目需求及分包情况、采购标的

（一）分包名称：合同包一

1、执行政府采购促进中小企业发展的相关政策

1) 不专门面向中小企业采购

2、预算金额（元）：500,000.00，大写（人民币）： 伍拾万元整

最高限价（元）： 500,000.00，大写（人民币）： 伍拾万元整

3、评审方法：综合评分法

4、定价方式：固定总价

5、是否支持联合体投标：否

6、是否允许合同分包选项：否

7、拟采购标的的技术要求

1	**采购品目**	云计算服务	**标的名称**	广元市昭化区卫生健康局“医疗云”服务采购项目
	数量	1.00	**单位**	项
	合计金额（元）	500,000.00	**单价（元）**	500,000.00
	是否采购节能产品	否	**未采购节能产品原因**	无
	是否采购环保产品	否	**未采购环保产品原因**	无
	是否采购进口产品	否	**标的物所属行业**	软件和信息技术服务业

标的名称：广元市昭化区卫生健康局“医疗云”服务采购项目

参数性质	序号	技术参数与性能指标
	1	（一）资源需求： 数量：1套 ▲1.VCPU数量≥800，内存≥1200GB；单物理处理器主频≥2.1GHz，物理核心≥26-Core；单节点存储≥48T，总节点≥3。

	2	（二）虚拟化软件及分布式存储软件：数量：1套 1.虚拟化主机服务，即利用虚拟化技术或容器技术实现一台物理服务器分割成多个虚拟专享服务器，使每个虚拟机都可分配独立IP地址、独立操作系统、实现不同虚拟机间磁盘空间、内存、CPU资源、进程和系统配置的隔离，为应用程序模拟出“独占”使用计算资源的服务。 2.虚拟机定制化服务。根据业务系统需要的资源能力，利用弹性计算能力对虚拟机模板进行动态资源调整。当虚拟机无法满足应用系统的计算处理能力时，可动态为虚拟机增配CPU及内存资源；当虚拟机无法满足应用系统的存储空间需求时，可动态为虚拟机增配磁盘存储空间。 3.支持在线扩展，升级扩容过程不需要停机，且不影响原始生产数据，单集群最大可扩展至≧250节点；提供证明材料。 4.支持2副本/3副本、EC的数据保护模式，且支持+2/+3/+4灵活EC 配比。 ▲5.支持数据快速重构，当磁盘或存储节点故障时，系统能自动进行数据重建，在无人工干预条件下，数据重建速度能满足每TB≤15分钟。提供证明材料。 6.支持配置存储故障后是HA虚拟机，以保障业务的高可用； 7.系统具有高可靠的特点，配合VM之间的高可用系统，实现计算平台和应用平台的多种高可用，业务系统可以根据业务负载灵活的在不同的物理机之间移动。 8.支持用户自定义性能图表并指定对象，对 CPU利用率、内存利用率、带宽、IOPS、时延、磁盘利用率、存储池利用率等进行统计。支持通过 SNMP V2/V3 协议向第三方平台上报告警，方便统一运维管理。 9.存储节点采用分布式集群存储架构，提供标准iSCSI协议。 10.支持磁盘亚健康管理功能：定期检查硬盘的 SMART 信息，判断磁盘亚健康情况(硬盘扇区重映射数超过门限、读错误率统计超标)，主动隔离并告警。支持慢盘检测，并在磁盘损坏前进行隔离并告警。支持 SSD 磨损寿命识别，提前告警及隔离处理。
	3	（三）光模块 1.光模块-SFP+-10G-，满足组网需求。
	4	（四）核心数据交换机，数量：1台 1.端口≥24个万兆SFP+,≥6个100GE QSFP28,含一个≥600W交流电源，交换容量≥2.56Tbps/25.6Tbps，包转发率≥1260Mpps，支持双电源，支持扩Vxlan。
	5	（五）汇聚数据交换机；数量：1台 1.端口≥48个10/100/1000BASE-T以太网端口，≥4个万兆SFP+,单子卡槽位，交换容量≥1.28Tbps/12.8Tbps，包转发率≥252/402Mpps，支持双电源，自带一个≥150W交流电源。
	6	（六）板卡；数量：1个 1.端口≥8端口10GE SFP+接口板。

	7	（七）核心出口网关；数量：1套 1.内存≥4G，闪存≥32G，≥端口6个10/100/1000Mbps 自适应电口，≥2个万兆 SFP+光口。 2.吞吐量≥4000Mbps，包转发率≥800kpps，最大并发连接数≥400W。 3.数据分流：可依据来源 IP、目的 IP、来源端口、目的端口、域名、应用协议进行线路分配或依据上网用户数量自动分配走向，并支持上下行分离分流，提供证明材料。 ▲4.一键智能流控：只需要选择流控场景并设置广域网带宽,设备依据带宽使用状况，实时优化带宽资源，保证关键应用，同时提升带宽利用率；另外，支持手动流控模式，支持客户个性化定制特定流控策略，提供证明材料。 5.流控模块：可精确识别≥3200 多种应用协议，对各种应用协议指定优先级和线路走向，数据库支持实时在线更新，实现基于应用协议的精准流控，提供证明材料。 6.线路备份技术：一条为主线路,一条为备用线路。当主线路掉线后,备用线路顶替工作,保证网络畅通。 7.支持 DDOS 防御和流量攻击防御，支持内外网禁 Ping，禁止内网客户端Tracert。
	8	（八）运维服务系统；数量：1套 1.运维管理软件+裸金属服务器 2.配置单颗CPU频率≥2.20 GHz，CPU≥10-Core*1,内存≥16G*1,硬盘≥2*600G。
	9	（九）云专线要求；数量：4条 ▲1.提供不少于2条300M以上专线，2条不少于100M以上灾难性备份专线互为冗余（专线和灾难性备份专线需走不同的方向主线，保障业务可靠性）。 ▲2.对现有卫生专线、党政外网专线等业务线路进行迁移。
	10	（十）防火墙服务；数量：1项 ▲1.≥17个电口,≥8个SFP,≥6个SFP+,≥2个扩展插槽,配置≥15个SSL VPN用户授权，配置≥3年应用识别、防病毒和URL特征库升级服务，配置≥3年硬件质保服务。 2.整机吞吐量≥10G,最大并发连接数≥500W,新建连接数≥10W。 3.实现静态路由、策略路由、RIP、OSPF、BGP等路由协议。 4.实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 5.支持高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 6.支持基于对包括但不限于对操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于对服务器、客户端的防护策略。在筛选特征缺省动作支持丢弃、允许、重置和黑名单。 7.支持基于文件协议、邮件协议（SMTP/POP3/imap)、共享协议（NFS/SMB）的病毒功能。 ▲8.支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配，提供功能截图； 9.支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。 10.支持≥2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性，提供功能截图。 11.支持国密SM2/3/4算法。 ▲12.支持多用户共享上网行为管理，提供功能截图； ▲13.产品具有公安部（国家认可机构）颁发的计算机信息系统安全专用产品销售许可证或网络关键设备和网络安全专用产品安全认证和安全监测结果，提供有效证书证明。

	11	（十一）终端安全服务；数量：1项 ▲1.配置≥30 Windows服务器授权许可,20≥个Linux服务器授权许可，配置功能包括病毒防护、漏洞管理、边界管理、软件管理、IP/MAC管控、网络管控、流量管控等功能，三年升级服务。 2.采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。 3.与系统控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。 ▲4.支持虚拟分级管理，可以实现全省或全市终端都部署在一台服务器上，但不同地市或县市管理员分别管理所属客户端，且不影响同一台服务器上的其他终端，需提供功能截图； 5.支持自主授权分割功能，管理员可以从主系统中心分割授权客户机数量给下级系统中心，限制下级系统中心对客户机的注册数量，阻止非法客户机注册。 ▲6.支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件，需提供功能截图。 7.支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；默认支持32层压缩扫描，且用户可以自定义设置扫描层数。 8.对勒索者病毒提供防护机制，采用虚拟钓饵方式有效拦截勒索者病毒。 9.支持根据设定好的固定区域对未知威胁文件及黑文件进行定向追溯，实现对所有可疑威胁文件进行全周期追踪。 10.服务器客户端具备资产管理及运维管理的功能，包括软件资产管理，网络管控、流量管理、密码管控功能。

	12	（十二）网络入侵防护服务；数量：1项 ▲1.≥2U,双电源,≥6个GE电口(3路Bypass),≥4个GE光口,≥2个扩展槽位,≥2个千兆管理口，配置入侵检测、Ddos、数据防泄漏、流量管理、应用管理模块，三年硬件质保服务；网络层吞吐量≥10G,应用层吞吐量≥1G；系统攻击特征库数量为≥1万+。 2.系统需提供入侵规则分类，帮助更便捷的制定防护策略。如勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等。 3.支持基于SCADA、IEC 61850、IEC 60870-104等工控协议的相关漏洞攻击检测与防护。 4.支持DoS/DDoS攻击防护能力，支持PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持TCP Port Scan/UDP Port Scan, 支持 PING Sweep，支持ARP Spoof以及HTTP GET/HTTP POST FLood等常见的DoS/DDoS的攻击。 ▲5.能够有效识别某IP上登录的用户并将用户名关联在该IP触发的安全事件上。用户信息来源于：网站登录用户、数据库用户、远程登录用户、即时通讯用户、文件传输、邮件用户等，提供功能截图； 6.提供≥10种以上内置规则模板，帮助用户快速上线。如DMZ区服务器、内网客户端、Web服务器、Windows服务器、UNIX服务器防护等规则模板，并可根据内置规则模板直接派生模板。 7.支持至少七种弱口令配置，支持导入自定义弱口令字典。支持强密码复杂度限制，如同时包含大小写字母、特殊字符、数字、不能包含用户名等组合方式限制。 8.支持HTTP、FTP、SMTP、POP3、IMAP、NFS、SMB2、工控（IEC-61850、IEC 60870）等协议，需提供功能截图； 9.提供积累的恶意IP黑名单库，≥4万。 ▲10.支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP入侵事件、TOP入侵事件目的IP、TOP入侵事件源IP、TOP源IP地理分布等威胁事件的下钻分析，点击对应的威胁事件可下钻到对应日志分类查看威胁事件的详细信息，提供功能截图； 11.能够有效抵御SQL注入、XSS注入、webshell等多种常见的应用层安全威胁，并可配置SQL注入白名单。 ▲12.支持能够与本地、云沙箱的联动,防御勒索病毒、0day 漏洞、APT攻击等各种未知威胁沙箱检测到的威胁数据可联动入侵防御系统完成防御工作，沙箱返回结果可以是高级恶意样本详情，未知恶意软件传播的 URL地址、恶意IP等，提供国家认可检测机构出具的带有“CNAS和CMA”标识的检测报告。 ▲13.支持基于SCADA等工控协议的相关漏洞攻击检测与防护，提供国家认可检测机构出具的带有“CNAS和CMA”标识的检测报告。

	13	（十三）远程安全评估系统服务；数量：1项 ▲1.软件形态部署，配置≥1000的IP地址或域名授权，≥3年系统漏洞规则库升级服务；最大并发主机数≥60个,最大并发任务数≥10个。 ▲2.支持检测的漏洞数≥250000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书，提供功能截图。 3.同时支持远程扫描和采用SMB、SSH、Telnet、RDP、HTTP、HTTPS、WinRM等协议对Windows、Linux等系统进行登录扫描。 4.支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息，提供功能截图。 ▲5.支持扫描国产操作系统、应用及软件的安全漏洞，如华为欧拉、open欧拉、统信、麒麟、bclinux、达梦、南大通用、人大金仓、神通、金蝶、东方通等，要求能够扫描≥40000条相关漏洞，提供功能截图。 ▲6.支持扫描容器镜像存在的漏洞，支持扫描互联网上公开仓库中的镜像以及私有仓库中的镜像，提供功能截图。 7.支持对C/C++/Python/Java/Php/go等语言的代码解析，语言的词法、语法分析。内置缺陷模板和缺陷规则，并支持自定义。 8.支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。 9.支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。 10.支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情。 11.支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。 ▲12.支持认证信息管理，可将系统登录信息、配置检查模板进行统一管理和配置，提供登录信息导入功能，无须每次下任务时进行配置。可跟堡垒机联动获取账户的密码，支持登录信息的批量更新和全部更新。 13.支持对扫描出的漏洞提供取证性质的验证并输出报告，直观展示漏洞利用过程和危害性。支持漏洞验证扫描任务，包括系统漏洞验证扫描、Web漏洞验证扫描。

	14	（十四）运维安全管理系统服务；数量：1项 ▲1.软件形态部署，配置≥200的IP资产授权，≥3年软件升级服务。 2.支持基于SDP技术的远程接入，无需额外部署VPN设备。支持服务隐藏功能，开启后，攻击者无法扫描到对应服务端口。支持服务端口代理功能，支持可将多个服务端口代理成一个，支持客户端在开启VPN的情况下，通过SDP技术和该端口建立安全隧道。 3.能够划分多级组织架构（≥10个层级），不同层级有独立的用户管理，用户角色管理，资产管理，密码管理、策略管理、审计管理的权限角色，支持不同角色相互组合。 4.堡垒机专用客户端和堡垒机建立加密隧道，隧道加密算法可按需选择是国密或者标密。 ▲5.用户登录堡垒机实现多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、USBKEY认证、PIN+软件OTP、短信认证、企微认证、钉钉认证、OAuth2.0等身份认证方式，提供功能截图。 ▲6.能够从LADP、AD域、企业微信、钉钉等手动或自动同步账号，提供功能截图。 ▲7.提供静态PIN+动态OTP口令认证方式，并支持配置PIN码的有效期、到期提醒、PIN码强度及弱PIN码字典，提供功能截图。 8.能够通过RDP、X11、VNC、SSH、TELNET、RLOGIN、SFTP、FTP、SAMBA协议的HTML5运维，无需本地运维客户端；支持通过H5文件运维的方式上传和下载文件。 9.支持终端合规检查策略，包含针对Windows补丁检测、操作系统版本检测、端口检测、进程检测和安装应用检测；支持可由管理员自定义配置合规策略，自定义范围包括但不限于检查项、告警等级、执行操作等，提供功能截图。 10.支持基于网络、位置、时间的动态授权，并支持仅告警、二次认证、授权审批和阻断的授权管理动作。 11.通过参数配置开启或关闭字符、图形、文件等协议运维行为审计，但不影响对应协议的会话审计，以便满足客户防范涉密运维行为泄露。 12.通过自动化运维，支持自定义自动化脚本，可在线编辑和本地导入；支持设定任务为手动、定时和周期执行方式；支持登录后自动执行脚本，执行完后堡垒机保存运维记录。 13.配置运维审计，审计日志包括认证日志、授权日志、网页审计、图形审计、字符审计、文件审计、数据库审计、隧道日志、系统日志。

	15	（十五）日志审计系统服务；数量：1项 ▲1.软件形态部署，支持鲲鹏、飞腾和海光等国产硬件平台，操作系统支持银河麒麟、openEuler和统信等国产操作系统，虚拟化支持KVM、vmware和HVM方式安装部署，支持华为云、阿里云平台部署；系统默认支持≥100以上日志源接入。 2.系统应基于大数据平台架构，具备海量数据收集与快速检索能力。 3.系统应支持内置采集器，不依赖其他设备即可进行日志采集。 4.系统应提供前端界面自定义能力，应支持用户自定义文字标题、主题色、LOGO等多种元素。 5.系统支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、KAFKA、WMI、二进制数据、专用Agent等方式采集日志。 6.系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind等。 7.系统支持采集国产化数据库数据接入，包括但不限于：人大金仓、南大通用、达梦数据库，神州通用。 8.系统应支持界面配置即可完成未识别日志接入，无需编写xml，提供功能截图。 9.系统应支持规则自适应日志接入，仅输入IP范围及端口即可自动匹配相应规则，完成日志自动接入。 10.系统应支持基于SM2非对称加密算法、SM3密码杂凑算法等国密算法对日志进行签名验签操作，以满足日志完整性校验要求。 ▲11.系统应支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式，提供功能截图。 12.系统应支持资产标签，≥6种标签，根据标签可快速查询资产。 13.系统应能够按照多种维度统计日志信息，包括但不限于攻击日志、审计过滤、恶意程序、防火墙、主机报表、应用服务器、网络设备、Windows审计、Linux审计、绿盟终端审计、SOX合规、PCI合规、ISO 27001合规、VPN账号异常等多种场景。 14.系统应支持自身日志记录并可查询、自身CPU、内存和磁盘使用率可监控并以图形化方式动态显示，且支持状态监控和主动告警。 ▲15.支持各种安全设备、网络设备、数据库、Windows主机、Linux主机、Web 服务器、虚拟化平台、网络流量设备、中间件、业务系统、文件等日志的接入，同时支持规则自适应日志接入，仅输入 IP范围及端口即可自动匹配相应规则，完成日志自动接入，提供国家认可检测机构出具带有“CNAS和CMA”标识的检测报告。 ▲16.支持利用JDBC的方式对数据库表日志进行综合管理与分析，提供国家认可检测机构出具带有“CNAS和CMA”标识的检测报告。

	16	（十六）数据库审计系统服务；数量：1项 ▲1.软件形态部署，配置≥10个数据库实例授权，≥3年软件升级服务。 2.支持旁路镜像部署，Agent引流部署、混合部署。部署模式可通过界面快速选择与切换。 3.Agent配置数据传输加密，可通过界面快速开启或关闭加密传输，保证待审计数据安全传输。 4.支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、MariaDB、Cache、Teradata、Impala、Greeplum等国际主流数据库审计。 5.支持HBase、MongoDB、Hive、Redis、ElasticSearch、Hana、Spark、Flink、HDFS等大数据环境审计。 6.支持数据库结构扫描，包含但不限与：数据库、数据表、表空间、视图等。 7.支持数据资产的风险评估，包括漏洞扫描、配置检查等。自定义数据资产扫描任务，支持自定义扫描基线规则。且支持敏感数据扫描和扫描结果手工梳理。 ▲8.支持对数据库访问行为建模，维度至少应包含：数据库对象、账号、客户端IP、客户端工具以及操作类型，提供功能截图； ▲9.同时支持高级查询，需包括：SQL关键字、结果集关键字查询，提供：与、或、非三种查询依赖条件，提供功能截图； 10.报表内容基于总体概况、性能、会话、语句、风险等多层面进行展现。内容提供图表结合展现，图表形式包含但不限于：柱形图、饼状图、条形图，双轴折线图等多种统计图展现。 11.支持手动导出与定时自动推动功能。自动推送支持自定义定义推送周期以邮件形式推送报表文档。手动导出报表格式至少包括：WORD、PDF、HTML、PNG等常用办公格式； ▲12.支持镜像旁路部署下，对风险IP、风险账号、风险工具、风险时间段、风险语句进行阻断，且支持自定义阻断时长，提供功能截图； 13.支持利用访问行为模型建立审计基线，对超出基线模型的操作可自动识别和告警。

	17	（十七）WEB应用防护系统服务；数量;1项 ▲1.软件形态部署，≥500Mbps，≥3年软件升级服务。 2.支持对HTTP协议合法性进行验证，支持对HTTP协议的URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他在内字段类型和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。 3.支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等插件应覆盖:dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress等。 4.支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。支持对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT。 5.支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。 6.支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。 7.支持XML防护，包括XML基础校验、Schema校验以及SOAP校验，需提供功能截图并加盖投标人公章。 ▲8.支持API攻击防护，可查看基于OWASP TOP 10的API安全事件统计，并可查看API安全事件详情，提供功能截图。 9.支持人机识别，可通过JS脚本识别自动化工具，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测，识别攻击工具，主要包括：市面上主流扫描器，如burpsuite、nessus等，市面上主流自动化工具selenium、phantomjs等，脚本攻击识别。 10.支持TCP Flood防护；支持基于阈值及算法配置的HTTP Flood防护。 11.支持多达七种的防护动作，包括放过、阻断、接受、重定向、伪装、清除和替换。 12.支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。 13.支持SSL卸载及加载，支持对SSL（HTTPS）加密会话进行分析，SSLv2, SSLv2/v3, SSLv3、TLS1.0\1.1\1.2\1.3。 ▲14.支持紧急模式:支持配置并发连接数阈值，当并发连接数超过设置阀值时，WAF自动进入紧急模式，已经代理的连接正常代理，对新增的请求直接转发；当连接数恢复正常时，自动退出紧急模式。 15.支持XML防护策略，支持导入Schema文件和WSDL文件对上传的XML文件进行格式校验，提供国家认可检测机构出具带有“CNAS和CMA”标识的检测报告。 ▲16.支持可开启API学习，当API学习未启用时在影子列表中查看影子API和资产详情，API列表中对API进行导入导出，支持API攻击防护，包括注入类攻击、滥用事件、敏感信息泄露、协议违背和安全配置错误等，提供国家认可检测机构出具带有“CNAS和CMA”标识的检测报告。
	18	（十八）灾备裸金属服务器；数量：1台 1.配置≥2U 12盘位机箱；配置≥2颗10核处理器；配置≥128GB内存；配置≥2块240GB 系统盘；配置≥6块8TB 存储盘；配置≥2个千兆电口；配置≥1GB阵列卡；配置冗余风扇；配置冗余电源。

	19	（十九）软件性能要求； 1.配置≥48TB硬盘授权容量许可；配置≥40TB软件备份容量许可；配置≥889个Intel、AMD平台下客户端备份许可；配置≥222个Intel、AMD平台下数据库备份许可；配置≥88台Intel、AMD平台下虚拟机备份授权；配置≥213个海光、兆芯、飞腾、鲲鹏、龙芯、申威平台下客户端备份许可；配置≥99个海光、兆芯、飞腾、鲲鹏、龙芯、申威平台下数据库备份许可；配置≥55台海光、兆芯、飞腾、鲲鹏、龙芯、申威平台下虚拟机备份授权；配置≥11台设备非结构化数据实时同步功能授权；配置≥33个Oracle、MySQL、IBM DB2、PostgreSQL、Redis、达梦数据库事务级实时同步节点授权；配置≥3个容灾模块：提供业务系统容灾所需的计算、存储、网络资源，以及相关的定时/实时数据同步功能模块，并通过统一界面管理，实现在一套设备内能同时能接管多个业务系统的运行。 2.支持源端压缩及重复数据删除、目标端压缩及重复数据删除两种数据备份优化模式。 3.支持NAT穿透技术，支持将备份系统部署在内网中，也可以同时备份外网的数据，同时也支持备份系统部署在外网中，备份内网的数据。（提供备份系统支持NAT穿透的功能截图） ▲4.支持模拟备份功能，可在不执行实际备份的前提下，获取到备份目标的文件数量、数据大小等信息，以便更合理地规划配置备份任务。（提供文件模拟备份和数据库模拟备份的功能截图） 5.支持CDP在Windows系统和Linux系统上文件、视频等数据的实时保护。 6.实时监控数据变化并备份至目标端，为保障业务系统稳定运行，不能采用植入系统内核驱动捕获IO的方式实现实时备份。 7.支持CDP连续数据保护功能支持实时复制到对象存储，支持文件和数据库的自动恢复演练。可建议自动恢复演练任务，定时将已备份的数据恢复到指定位置，以便管理员检查备份数据的有效性。 ▲8.备份过程中支持通过安全传输协议（TLS）进行加密，保证数据传输的全过程安全，可自定义加密证书，支持CA证书加密。（提供备份客户端、备份任务和备份空间自定义密钥和CA证书的功能截图） 9.备份系统支持数据加密，至少支持AES 256和SM4加密算法，以便适应不同的数据类型和保密要求。
	20	（二十）灾备服务要求；数量：1项 1.备份系统支持离线备份D2T功能，可将数据流直接备份到磁带库中，不可使用备份到本地磁盘，再打包到一体机的方式（提供备份系统磁带库配置界面及识别磁带库的功能截图）。 ▲2.为避免病毒及勒索软件对备份数据的破坏，备份系统支持将磁盘介质虚拟成磁带格式（支持LTO4-LTO8磁带格式），并提供相关端口映射配置，可将虚拟带库任意机械臂、驱动器映射到指定端口。（提供备份系统创建虚拟带库，以及映射机械臂、驱动器的功能截图） 3.备份系统支持对磁带的导入导出管理。（提供备份系统对磁带导入导出管理的功能界面） 4.支持Windows 2003-2019、Linux Kernel 2.4及以上所有操作系统版本下目标端的备份与恢复功能。 ▲5.支持以租户为单位无代理备份和恢复OpenStack的实例、卷、快照及镜像。（提供OpenStack的实例、卷、快照及镜像无代理备份的功能截图） 6.支持无代理备份Docker的镜像与容器实例。（提供无代理备份Docker的镜像与容器实例的功能截图） ▲7.支持数据库离线恢复，即备份数据可直接恢复至数据库，也支持将备份数据恢复成文件，恢复的文件可以以离线的方式在异地直接恢复至异地数据库，完全不依赖备份系统，同时也不需要在异地搭建备份系统。（提供主流数据库Oracle、SQL Server、MySQL支持直接恢复至数据库及恢复至文件的功能截图） 8.支持数据库事务级实时同步复制，实时将数据库备份到目标端，目标端数据库实时可读，RPO指标达到秒级，RTO分钟级，数据库实时备份支持主流商业及开源数据库，包括Oracle、MySQL、IBM DB2、PostgreSQL、Redis、达梦。（提供Oracle、MySQL、IBM DB2、PostgreSQL、Redis、达梦实时复制配置界面及实时复制状态的功能截图） 9.支持SAP HANA、SAP MaxDB数据库的的备份与恢复功能。（提供SAP HANA、MaxDB数据库备份的功能截图）

8、供应商一般资格要求

序号	资格要求名称	资格要求详细说明
1	具有独立承担民事责任的能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
3	具有健全的财务会计制度。	供应商可提供2021年以来任意一个年度经审计的财务报告，或内部财务报表，或其基本开户银行出具的资信证明，其他组织或自然人，提供银行资信证明；（提供其中一种相关证明材料复印件，供应商注册时间截止响应文件递交截止日不足一年的，也可提供加盖工商备案主管部门印章的公司章程。）
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。

9、供应商特殊资格要求

序号	资格要求名称	资格要求详细说明
1	无	无

10、分包的评审条款

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
1	详细评审	报价	1.满足招标文件要求且投标价格最低的投标报价为评标基准价,其价格分为满分。其他供应商的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×30×100%。 2.根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）、《国务院关于印发扎实稳住经济一揽子政策措施的通知》（国发〔2022〕12号）、《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022)19 号）的规定，对小型和微型企业(含监狱企业、残疾人福利企业）产品的价格给予20%的价格扣除，用扣除后的价格参与评审。	30.0	是

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
2	详细评审	技术指标及配置	根据本项目技术参数要求按照逐条累计得分的方法进行评审，所投软、硬件应完全满足技术参数要求；其中： 1.带“▲”技术要求得分=（条款数-负偏离条数）×1分。（注：“▲”条款数：共计43条） 2.非“▲”技术要求得分=（条款数-负偏离条数）×0.1分。（注：非“▲”条款数：共计109条） 3.该项总得分=带“▲”技术要求得分+非“▲”技术要求得分。 注：▲项参数中有要求的按要求提供，其他非▲需提供相应的证明材料，包括彩页或官网截图以及其他类似能够证明投标产品符合招标要求的证明材料复印件，否则一律按负偏离作扣分处理。	54.0	是
3	详细评审	类似业绩	2019年以来，1个类似项目业绩得1分，最多得3分。	3.0	是
4	详细评审	履约保障能力要求	1、要求防火墙服务厂商应同时具有国家信息安全测评信息安全服务资质证书-安全开发类和工业信息安全产业发展联盟颁发的工业信息安全测试评估机构能力认定证书。同时提供两项等级为二级及以上的有效证书复印件并加盖原厂公章，满足两项得2分，满足一项得1分，两项皆不满足不得分。 2、要求网络入侵防护服务厂商应具有中国网络安全审查技术与认证中心颁发的《CCRC数据安全管理认证证书》，提供有效证书复印件并加盖公章，提供证明材料得2分，其余不得分。 3、为保证软件开发能力，WEB应用防护系统服务厂商应具备CMMI软件为5级的有效证书复印件并加盖原厂公章。提供证明材料得2分，其余不得分。 4、要求日志审计系统服务厂商具备ITSS信息技术服务标准符合性证书SaaS服务资质，提供等级为二级及以上的证书复印件并加盖厂商公章。提供证明材料得1分，其余不得分。 5、要求远程安全评估系统服务厂商为微软MAPP计划成员单位，提供微软安全响应中心官网截图证明并加盖厂商公章. 提供证明材料得1分，其余不得分。	8.0	是
5	详细评审	服务要求	投标人完全满足本项目（售后服务及其他要求）的得5分；每有一项不满足扣1分，直至该项分值扣完为止。（按要求响应或提供证明材料）	5.0	是

11、合同管理安排

1）合同类型：买卖合同

2）合同定价方式：固定总价

3）合同履行期限：自合同签订之日起90日

4）合同履约地点：广元市昭化区卫生健康局（昭化区益昌大道107号）

5）支付方式：分期付款

6）履约保证金及缴纳形式：

中标/成交供应商是否需要缴纳履约保证金：否

7）质量保证金及缴纳形式：

中标/成交供应商是否需要缴纳质量保证金：否

8）合同支付约定：

1、 付款条件说明： 双方签订合同后，付预付款， ，达到付款条件起 7 日内，支付合同总金额的 30.00 %；

2、 付款条件说明： 项目完成建设，服务期满半年， ，达到付款条件起 7 日内，支付合同总金额的 50.00 %；

3、 付款条件说明： 待服务期满1年后 ，达到付款条件起 7 日内，支付合同总金额的 20.00 %；

9）验收交付标准和方法：1.验收：由采购人组织，成交人配合进行： 2.验收标准：按国家有关规定以及本磋商文件的服务内容及要求、成交人的响应文件及承诺与本合同约定标准进行验收，其他未尽事宜应严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的通知要求以及行业部门的技术要求统一验收。

10）质量保修范围和保修期：同项目履约服务期

11）知识产权归属和处理方式：1.供应商在本项目使用任何产品和服务(包括部分使用)时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。 2.采购人享有本项目实施过程中产生的知识成果及知识产权，并依据实际情况对采购标的涉及的知识产权的进行处理。 3.供应商如欲在项目实施过程中采用自有知识成果，需在投标文件中声明，并提供相关知识产权证明文件。使用该知识成果后，供应商需提供相关技术文档，并承诺提供无限期技术支持，采购人享有永久使用权。 如采用供应商所不拥有的知识产权，则在投标报价中必须包括合法获取该知识产权的相关费用。

12）成本补偿和风险分担约定：按国家、行业标准执行

13）违约责任与解决争议的方法：1.供应商必须遵守采购合同并执行合同中的各项规定，保证采购合同的正常履行；2.如因供应商工作人员在履行职务过程中的的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任。

14）合同其他条款：5. 售后服务 5.1供应商应有完善的技术支持与服务体系，提供完善实施方案；专门固定的售后服务电话、专业工程师和售后服务机构。 5.2针对本项目需要提供7*24小时热线电话，远程服务，现场服务等方式，一般性问题5分钟响应，2小时内到场，4小时内解决；重大问题5分钟响应，1小时内到场，4小时内解决。 6.其他要求 供应商应采用高效、安全的云机房提供云服务。具备完善的网络安全防护能力以及服务存储扩展能力，以应对高速发展的信息化时代，充分保证信息安全和服务质量。当采购人有紧急扩容需求时，供应商可提供快速扩容服务能力，包括但不限于提供私有云、混合云等服务方式。

12、履约验收方案

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起3日内组织验收

8）验收组织的其他事项：无

9）技术履约验收内容：按国家有关规定以及磋商文件的服务内容及要求、成交人的响应文件及承诺与本合同约定标准进行验收；

10）商务履约验收内容：按国家有关规定以及磋商文件的服务内容及要求、成交人的响应文件及承诺与本合同约定标准进行验收；

11）履约验收标准：其他未尽事宜应严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的通知要求以及行业部门的技术要求统一验收。

12）履约验收其他事项：无

五、风险控制措施和替代方案

该采购项目按照《政府采购需求管理办法》第二十五条规定，本项目是否需要组织风险判断、提出处置措施和替代方案：否