**采购需求**

**一、采购标的**

1. 采购标的

主要工作内容是依托北京市政务云资源，采购政务云基础服务、其他云上拓展服务和云上系统安全保障服务等工作。

本项目所需服务如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务类、服务项** | **服务描述或规格型号** | **计价单位** | **报价单位** | **数量** | **服务期（月）** |
| **一** | **政务云基础服务** | | | | | |
| （一） | 计算服务 | | | | | |
| 1 | X86平台云主机服务-vCPU | 主频不低于2.4GHz | CPU | 元/月 | 1515 | 12 |
| 2 | X86平台云主机服务-内存 | 内存 | GB | 元/月 | 7263 | 12 |
| （二） | 存储服务 | | | | |  |
| 1 | 普通性能存储 | 单盘技术指标：单盘IOPS 1000-3000） | GB | 元/月 | 124550 | 12 |
| 2 | 高性能存储 | 单盘技术指标：单盘IOPS 3000-20000 | GB | 元/月 | 120482 | 12 |
| 3 | 本地备份服务 | 本地备份服务 | GB | 元/月 | 131264 | 12 |
| 4 | 静态存储（NAS） | 大容量、高可靠的数据存储服务，具备PB级线性扩展能力 | TB | 元/月 | 25 | 12 |
| （三） | 网络服务 | | | | |  |
| 1 | 互联网链路服务1 | 互联网链路带宽 | Mb | 元/月 | 320 | 12 |
| 2 | 互联网链路服务2 | 互联网IP地址租用服务、并提供备案服务 | IP | 元/月 | 65 | 12 |
| 3 | 主机负载均衡服务 | 主机负载均衡服务 | IP | 元/月 | 57 | 12 |
| 4 | 远程接入服务 | 远程接入运维，每个账号结合身份验证，通过VPN远程接入堡垒机进行维护（免费提供1个账号） | 账号 | 元/月 | 34 | 12 |
| 5 | VPN服务 | SSL VPN 接入（每套10个并发用户，所需带宽参照“互联网链路带宽”购买） | 套 | 元/月 | 7 | 12 |
| 6 | WAF防护 | web应用防火墙服务 | IP | 元/月 | 12 | 12 |
| （四） | 云主机深度监控服务 | | | | |  |
| 1 | 特定云主机深度监控及运维保障服务（7×24小时值守） | 7×24小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容。 | 台 | 元/月 | 237 | 12 |
| **二** | **其他云上拓展服务** | | | | |  |
| （一） | 云上物理服务器租用服务 | | | | |  |
| 1 | 流数据节点服务器 | 服务器租用，提供计算资源。 | 台 | 元/月 | 4 | 12 |
| 2 | 元数据节点服务器 | 服务器租用，提供计算资源。 | 台 | 元/月 | 2 | 12 |
| 3 | 计算与存储节点服务器 | 服务器租用，提供计算资源。 | 台 | 元/月 | 4 | 12 |
| （二） | 平台资源2-基础软件支撑服务 | | | | |  |
| 1 | 国产数据库和应用中间件维护服务 | 1、日常维护;2、故障处理;3、备份与恢复;4、升级服务;5、系统巡检;6、性能评估及调优;7、中间件基础优化及日常监控;8、数据库和中间件的安装部署、架构规划与管理;9、重点时期运维保障;10、安全演练技术保障 | 套 | 元/月 | 1 | 12 |
| 2 | 数据库一体机服务 | 数据库一体机租用服务 | 月 | 元/月 | 12 | 12 |
| 3 | SQL Server 数据库 | SQL Server 2014 单机版数据库租用服务，单节点。 | 月 | 元/月 | 12 | 12 |
| 4 | 商用操作系统套餐1 | Windows Server套餐：Windows Server租用、安装及维护，根据漏洞扫描结果或等级测试要求对操作系统进行安全加固。 | 套 | 元/月 | 4 | 12 |
| （三） | 通信接入服务 | | | | |  |
| 1 | 民政部数据数据专线 | 用于市民政局与国家民政部数据交换 | 条 | 元/月 | 1 | 12 |
| 2 | 市金融监管局专线、市政交通一卡通公司专线 | 用于市民政局与市金融监管局、市政交通一卡通公司数据交换 | 条 | 元/月 | 1 | 12 |
| **三** | **云上系统安全保障服务** | | | | | |
| 1 | 主机漏洞扫描 | 为用户提供针对主机层面的安全扫描服务，并反馈相关结果。 | 台 | 元/月 | 237 | 12 |
| 2 | 网页防篡改服务 | 提供网页防篡改服务。通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性。 | 套 | 元/月 | 21 | 12 |
| 3 | 主机日志分析 | 对主机系统日志进行采集分析处理，发现各种安全威胁、异常行为事件。并定期为用户提供分析报告，协助用户进行整改工作。 | 台 | 元/月 | 237 | 12 |
| 4 | 数据库审计服务 | 支持Oracle、SQL-Server、DB2、MySQL等数据库审计。 | 套 | 元/月 | 21 | 12 |
| 5 | 主机杀毒服务 | 对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。 | 台 | 元/月 | 237 | 12 |
| 6 | WEB应用安全云防护服务 | 对WEB应用提供安全防护服务，服务内容：1. 智能DNS；2. 防火墙 3. 防火墙策略集控制；4.智能攻击防御；5.WebShell防护；6.协同防御；7.精准访问控制；8.站锁与防篡改；9.可视化、数据下载、安全报告；10. 抗DDoS、抗CC攻击。 | 项 | 元/月 | 1 | 12 |
| 7 | 全流量数据分析服务 | 对网络进行信息资产调查，对流量数据进行回溯分析、健康分析、安全评估，提供应急响应。本项目进行12期为定期分析服务，按需提供不定期服务（应急服务），时间由双方协商制定，首期从合同签订第一个月初开始，然后每个月进行一期分析，输出服务报告，截止到一年后月末结束。 | 项 | 元/月 | 1 | 12 |
| 8 | 数据库安全防护服务 | 通过数据库安全防护系统，能够对数据库访问的行为进行限制，高危操作进行拦截，；虚拟补丁通过协议解析技术，捕捉外部系统利用数据库漏洞进行的网络攻击行为并对其进行管控，从而防止通过已知漏洞对数据库的攻击。1、优化防护业务系统种类及数量；2、优化学习期及行为建模；3、防护安全策略如会话、结果集、长语句的配置及测试策略运行状态；4、数据库补丁填补、防护；5、安全策略细化；6、结果集监控及阻断；7、持续更新安全漏洞。 | 项 | 元/月 | 1 | 12 |
| 9 | 数据水印云服务 | 数据水印服务是将标记信息嵌入原始实现数据溯源的服务，具有高隐蔽性、高易用性、高管理融合性等特点，通过标记信息追溯该泄露数据流转全流程，并精准定位泄露单位及责任人，实现数据泄露精准追责定责解决数据在分发后的风险追责。 | 项 | 元/月 | 1 | 12 |
| 10 | 态势感知 | 针对部署在政务云环境的237台云主机、10台物理主机及oracle数据库一体机开展态势感知服务，提供业务可视化、威胁可视化、攻击与可疑流量可视化服务，在系统受到高级威胁入侵之后，损失发生之前及时发现威胁。服务部署在政务云互联网区域及政务外网区域，提供监控演示账号，可以直观看到网络攻击情况，服务按月度产出态势感知报告。 | 项 | 元/月 | 1 | 12 |
| 11 | 网站安全监测服务 | 包括Web漏洞监测、SSL安全监测、安全事件监测、资产变动监测、内容合规监测、可用性监测、可视化数据报表、安全报告及多种扫描方式等。可以持续的去监测网站暗链、坏链、挖矿、挂马、风险外链等安全事件；可持续监测网站web安全漏洞，发现漏洞后可以快速定位漏洞，及时协助快速修补漏洞，防止web攻击事件发生；对网页敏感词进行持续监控涉及暴恐、涉黄、涉政、反动、博彩、民生、政治、其他等8类词库，可以及时掌握网站的内容安全风险；7x24小时不断监测业务系统、服务器的可用性，访问异常时，第一时间告警通知到管理人员，及时解决问题。 | 项 | 元/月 | 1 | 12 |
| 12 | 威胁情报服务 | 提供威胁情报查询，重点时期推送威胁情报信息。 3万次/年，单日上限500次，每秒最大连接数50，提供云端账号IP情报查询服务，订阅IP自动推送情报；与黑客IP库联动，针对攻击IP进行扩展性信息查询，可查询攻击IP的其他信息，经纬度、运营商等信息，查看攻击IP过往是否是类似攻击行为，有效识别已知风险和潜在威胁，并提供对应的处理方案。HVV期间可以针对攻击队的IP进行查询 | 项 | 元/月 | 1 | 12 |
| 13 | 蜜罐服务 | 部署诱饵和陷阱在关键网络入口，诱导攻击者攻击伪装目标，保护真实资产。包括威胁告警、黑客画像、攻击特征识别、安全报表、威胁态势指挥大屏、协同防御、攻击溯源及预警通知等。SaaS部署的方式，实现云蜜场和业务系统隔离，通过部署诱饵诱导攻击者攻击伪装目标，在通过观察黑客的攻击路径、手段，让黑客帮助提前发现系统漏洞；通过孪生蜜罐作为陷阱，让黑客无法快速辨别真实资产； | 项 | 元/月 | 1 | 12 |
| 14 | 数据加密应用无感知云服务 | 透明加密（TDE）是高级安全选件的功能，实现对存储在数据库里的数据、使用数据泵导出的数据以及使用 RMAN 的备份数据进行加密，避免了存 储介质被拿走或维修替换，或是 DBA 窥视所导致的数据泄露，保护业务数据的存储安全。透明数据加密对应用透明，不需要修改应用。 支持国密算法，与TDE配合完成数据存储加密和数据备份加密，满足等保与密评的合规要求。 | 项 | 元/月 | 1 | 12 |

2. 项目背景/项目概述

依据《关于印发〈关于推进我市政务信息系统整合共享的实施方案〉的通知》（京经信委发〔2017〕89号）《关于印发〈北京市政务信息资源管理办法（试行）〉的通知》（京政发〔2017〕39号）《关于印发〈北京市市级政务云管理办法〉的通知》（京经信函〔2019〕150号）等文件要求，落实北京市电子政务总体要求，推进北京市民政局政务信息化统筹集约发展，实现政务信息系统统一入云部署，充分合理利用市级政务云服务资源，确保信息系统和数据资源安全、稳定运行。

**二、商务要求**

1. 交付（实施）的时间（期限）和地点（范围）

**（1）实施的时间(期限)**

自合同签订之日起一年。

**（2）实施的地点(范围)**

北京市民政局、市级政务云机房。

2. 付款条件（进度和方式）

**（1）付款进度**

合同生效后10个工作日内支付合同金额的50%，中标人向采购人按中标金额的5%提供履约保函；该项目通过阶段性验收后10个工作日内支付合同金额的20%；该项目包含的所有内容均通过最终验收后10个工作日内支付尾款30%。

**（2）付款方式**

采购人每次付款前，中标人应提供等额、合法发票，否则，采购人有权拒绝付款且无需承担违约责任。采购人付款如遇到国库财政预算支付的限制，可以顺延付款期限，采购人不承担违约责任，但采购人应当将延迟付款理由通知到投标人，且在支付限制解除后立即完成对中标人的付款。中标人不得因此暂停、终止、拒绝、延迟义务的履行。

**三、技术要求**

**（一）服务要求**

1、政务云基础服务

充分依托云服务商已有的成果和基础，为入云系统提供基础环境支撑。租用x86 平台云主机服务、普通性能存储、高性能存储、本地备份服务、静态存储服务、互联网链路服务、主机负载均衡服务、远程接入服务、VPN服务、WAF防护和云主机深度监控等政务云基础服务。

中标人需提供对基于云计算架构的硬件基础资源和云平台的监控及维护，并对监控与维护情况及时与采购人和对应系统的应用开发厂商做好协调沟通工作，中标人应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，能满足安全三级等保要求，并积极配合采购人根据各信息系统具体等保需求，开展相应等保评估、检查、整改等工作。中标人管辖范围内的硬件、软件及支撑环境资源，至少达到信息系统的最高安全等级要求。

2、其他云上拓展服务

租用政务云服务商提供的流数据节点服务器、元数据节点服务器、计算与存储节点服务器、国产数据库和应用中间件维护服务、数据库一体机服务、SQL Server 数据库、商用操作系统套餐、民政部数据数据专线、市金融监管局专线、市政交通一卡通公司专线等各类服务，完成信息系统的日常运维和安全运维服务工作（包括但不限于：日常技术支持、系统日常维护、系统状态运行监控、系统事故处理，安全运维服务相关的工作以及其他运维工作），确保入云系统安全、稳定地运行。

3、云上系统安全保障服务

提供主机漏洞扫描、网页防篡改服务、主机日志分析、数据库审计服务、主机杀毒服务、WEB应用安全云防护服务、全流量数据分析服务、数据库安全防护服务、数据水印云服务、态势感知、网站安全监测服务、威胁情报服务、蜜罐服务、数据加密应用无感知云服务等云上系统安全保障服务，全方位保障入云信息系统的安全。

（1）主机漏洞扫描

为用户提供针对主机层面的安全扫描服务，并反馈相关结果。

（2）网页防篡改服务

提供网页防篡改服务。通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性。

（3）主机日志分析

对主机系统日志进行采集分析处理，发现各种安全威胁、异常行为事件。并定期为用户提供分析报告，协助用户进行整改工作。

（4）数据库审计服务

支持Oracle、SQL-Server、DB2、MySQL等数据库审计。

（5）主机杀毒服务

对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。

（6）WEB应用安全云防护服务

开展WEB应用安全云防护服务，服务内容包括：1. 智能DNS；2. 防火墙3. 防火墙策略集控制；4.智能攻击防御；5.WebShell防护；6.协同防御；7.精准访问控制；8.站锁与防篡改；9.可视化、数据下载、安全报告；10. 抗DDoS、抗CC攻击。

（7）全流量数据分析服务

开展全流量数据分析服务，对网络进行信息资产调查，对流量数据进行回溯分析、健康分析、安全评估，提供应急响应。

（8）数据库安全防护服务

开展数据库安全防护服务，能够对数据库访问的行为进行限制，高危操作进行拦截；虚拟补丁通过协议解析技术，捕捉外部系统利用数据库漏洞进行的网络攻击行为并对其进行管控，从而防止通过已知漏洞对数据库的攻击。1、优化防护业务系统种类及数量；2、优化学习期及行为建模；3、防护安全策略如会话、结果集、长语句的配置及测试策略运行状态；4、数据库补丁填补、防护；5、安全策略细化；6、结果集监控及阻断；7、持续更新安全漏洞。

（9）态势感知

针对部署在政务云环境的237台云主机、10台物理主机及oracle数据库一体机开展态势感知服务，提供业务可视化、威胁可视化、攻击与可疑流量可视化服务，在系统受到高级威胁入侵之后，损失发生之前及时发现威胁。服务部署在政务云互联网区域及政务外网区域，提供监控演示账号，可以直观看到网络攻击情况，服务按月度产出态势感知报告。

（10）网站安全监测服务

开展网站安全监测服务，包括Web漏洞监测、SSL安全监测、安全事件监测、资产变动监测、内容合规监测、可用性监测、可视化数据报表、安全报告及多种扫描方式等。持续监测网站暗链、坏链、挖矿、挂马、风险外链等安全事件；可持续监测网站web安全漏洞，发现漏洞后可以快速定位漏洞，及时协助快速修补漏洞，防止web攻击事件发生；对网页敏感词进行持续监控涉及暴恐、涉黄、涉政、反动、博彩、民生、政治、其他等8类词库，可以及时掌握网站的内容安全风险；7x24小时不断监测业务系统、服务器的可用性，访问异常时，第一时间告警通知到管理人员，及时解决问题。

（11）威胁情报服务

提供威胁情报查询，重点时期推送威胁情报信息，供云端账号IP情报查询服务，订阅IP自动推送情报；与黑客IP库联动，针对攻击IP进行扩展性信息查询，可查询攻击IP的其他信息，经纬度、运营商等信息，查看攻击IP过往是否是类似攻击行为，有效识别已知风险和潜在威胁，并提供对应的处理方案。HVV期间可以针对攻击队的IP进行查询。

（12）蜜罐服务

部署诱饵和陷阱在关键网络入口，诱导攻击者攻击伪装目标，保护真实资产。包括威胁告警、黑客画像、攻击特征识别、安全报表、威胁态势指挥大屏、协同防御、攻击溯源及预警通知等。SaaS部署的方式，实现云蜜场和业务系统隔离，通过部署诱饵诱导攻击者攻击伪装目标，在通过观察黑客的攻击路径、手段，让黑客帮助提前发现系统漏洞；通过孪生蜜罐作为陷阱，让黑客无法快速辨别真实资产。

（13）数据水印云服务

数据水印服务是将标记信息嵌入原始实现数据溯源的服务，具有高隐蔽性、高易用性、高管理融合性等特点，通过标记信息追溯该泄露数据流转全流程，并精准定位泄露单位及责任人，实现数据泄露精准追责定责解决数据在分发后的风险追责。

（14）数据加密应用无感知云服务

透明加密（TDE）是高级安全选件的功能，实现对存储在数据库里的数据、使用数据泵导出的数据以及使用 RMAN 的备份数据进行加密，避免了存储介质被拿走或维修替换，或是 DBA 窥视所导致的数据泄露，保护业务数据的存储安全。透明数据加密对应用透明，不需要修改应用。支持国密算法，与TDE配合完成数据存储加密和数据备份加密，满足等保与密评的合规要求。

**（二）实施要求**

1、总体要求

投标人提供的服务在性能、规格、安全等方面须满足北京市民政局云上信息系统正常运行的基本要求，实施过程中应提出规范、完整的项目管理方案，包括但不限于质量管理、进度管理和风险控制措施。

投标人在项目实施中必须做到：

（1）实施过程从严要求服务工作的质量。

（2）提供详细、全面的服务过程文档。

（3）投标人须同意让北京市民政局有关工作人员参与实施工作，接受北京市民政局的监督。

2、团队要求

为使项目建设按质、按量、按时及有序实施，投标人应以类似案例成果和相关专业团队为基础，配备完善和稳定的组织机构。

投标人应负责提出本项目实施的人员配置方案，主要要求如下：

（1）投标人应提供主要项目人员的名单、学历、项目履历、在本项目中的职责分工；提供所有主要项目人员的个人简历、资质证书复印件，以上资料应加盖投标人公章。

（2）项目经理具备本科及以上学历；满足10年（含）以上工作经验；具备信息系统项目管理师（高级）资质证书。

（3）技术负责人，具备本科及以上学历；满足8年（含）以上工作经验；具备有效的注册信息安全专业人员CISP证书。

（4）服务团队人员至少8人以上；所有人员拥有本科及以上学历且具备5年（含）以上的工作经验。

（5）投标人应承诺项目经理、技术负责人固定服务本项目，未经采购人同意，不得随意更换。

3、部署要求

本项目涉及的所有信息系统目前已在北京市政务云平台平稳运行，此次招标预算包括信息系统的云租用及安全费用，投标人如需要迁移部署，须自行考虑应用系统迁移部署及此项工作产生的相关费用并提供详细、具备可行性的迁移部署方案，投标人应承诺中标后3个工作日内，以最低风险完成所有应用迁移部署工作，无法完成采购人有权解除合同。

**（三）运维服务要求**

1、运维服务

中标人须利用监控系统或人工对硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，应第一时间向采购人报告，并通知相关人员及时处理，最终成监控报告。

中标人负责设立技术支持热线，并安排专人值守，提供7\*24小时热线支持服务。中标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

2、故障响应服务

中标人应当提供高效的系统维护服务，有效防范系统风险，中标人需保持7\*24小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在2小时内到达运维现场提供服务。系统发生宕机问题时，中标人应在15分钟内响应，故障处理完毕后提供相关系统宕机报告。

中标人须具备故障快速定位和恢复能力，故障定位排除时限不超过30分钟，重要信息系统故障定位排除时限不超过10分钟 。

3、重点保障要求

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求中标人提供运维服务，保证在业务高峰期内系统平稳运行。

4、安全及保密要求

中标人须严格遵守采购人的相关信息安全规定，本项目涉及人员须与中标人签订保密协议，项目中标后本项目服务人员须与我局签订针对本项目的保密协议，中标人应选派具有良好职业道德的人员参与和从事本项目工作，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏，中标人须承担相关保密责任。

**（四）验收标准**

中标人所提供资源应满足招标文件规定的要求。保证合同期内系统安全稳定运行，不因硬件故障导致服务中断12小时。在2025年11月底前对合同项目进行阶段性验收，服务期届满，对合同项目进行最终验收。中标人应当在采购人指定的验收日前向采购人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

项目完成后，由采购人组织验收，并作为支付尾款的参考。