第三章　采购需求具体要求

一、采购内容一览表

序号	标项名称	数量	单位	预算金额	简要技术要求	备注
1	2019下城区综合信息系统应用模块开发与保障	1	项	1408万元	详见“第三章 采购需求具体要求”	临[2019]1113号，本项目最高限价：1408万元

重要说明：招标文件中所有带▲的内容是采购人提出的实质性条款，投标文件响应内容若不满足实质性条款要求，该投标文件将被评标委员会认定为无效。

二、采购需求

（一）项目概况

近年来，随着电子政务拓展和信息数据不断积累、开放、共享及深化利用，政务数据泄露的风险也不断加大。网络攻击行为越来越普遍，攻击手段不断翻新升级，攻击目标逐步转向政府、卫生等公共服务机构，对政府电子政务网络应用带来较大威胁，已引起国家重视。2017年6月1日，《中华人民共和国网络安全法》正式生效，其中明确规定：“国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。”

2017年底，为了加强对政务网络和数据资源的安全保障能力，浙江省政府办公厅印发《浙江省人民政府办公厅关于开展部门政务专网整合和加强政务外网安全防护工作的通知》(浙政办发〔2017〕140号)。2017年11月，杭州市智慧电子政务建设（数据资源管理）工作领导小组办公室发布《杭州市政务数据安全管理办法（暂行）》（杭电建数管办〔2017〕1号），明确要求各级政府单位应按照规范加强落实安全技术和管理措施，保障政务网络和数据安全。

为全面落实上述文件关于强化网络安全和政务数据安全保障的具体要求，深化推进“最多跑一次”改革和政府数字化转型工作，本年度拟结合文件要求、等级保护制度规范以及下城区政务网络和数据安全管理的具体需求，实施下城区政务数据安全加固及基础设施更新项目，提高下城区政务基础设施支撑能力和网络安全保障能力，为各类政务应用提供有力支撑。

同时，目前下城区企业服务相关业务系统和平台存在水平层次不齐，数据相互孤立，信息不能互通等难点堵点，急需从顶层设计角度出发，构建一体化企业信息化平台，基于微信公众号打造企业用户端，并与企业服务平台管理端打通，实现政企、企业与企业之间的互动，整合梳理企业信息资源和政务服务资源，加强政企之间的互动，增强企业办事体验，进一步优化下城区营商环境。

另外，推进基层治理“四个平台”的建设，以镇（街道）四个平台为牵引，以属地管理、全科网格、综合指挥、运行机制为支撑，重构覆盖区镇（街道）、功能集成、运行协同的基层治理体系。加快推进“四个平台”建设，是浙江省委、省政府作出的重要决策部署，对构建新基层治理体系有着极其重要的意义。结合下城区实际，配合实现杭州市市级统一地址库体系的规划建设，以地址信息作为核心关联，进一步整合资源力量，增强乡镇（街道）管理服务功能，全面提升乡镇（街道）社会管理和服务群众水平。

（二）采购清单

序号	名称	配置描述	数量
一	综合信息系统应用升级开发		
1	下城区电子档案系统二期		
1.1	超融合服务器存储一体化平台	超融合服务器存储一体化平台，新增 1 个节点，配置 2 颗英特尔至强 E5 2630 V4CPU,内存 128G，2*480GB SSD 硬盘,4*6T SATA 硬盘，≥4 个千兆网卡、≥2 个万兆网卡 ；2 个万兆多模光模块，双冗余电源；3 年原厂质保。含服务器虚拟化软件许可、网络虚拟化软件许可、存储虚拟化软件许可。	1 套
1.2	万兆交换机	≥8 个万兆口，≥20 个千兆口，配置 6 个万兆 SFP+模块。交换容量≥598Gbps，包转发率≥342Mpps，一个扩展槽，0℃～70℃温宽，支持虚拟化，三年免费质保。	2 台
1.3	一体化备份系统升级	在现有虚拟带库系统上增加 BCM-SW v3.0 灾备管理模块，实现各种故障类型的应用和数据的灾难性保护，支持 Windows，Linux，UNIX 等主流操作系统，支持对 MSSQL Server、Oracle、Sybase、Exchange Server、Lotus Domino、DB2、MySQL 等所有主流数据。包含系统和数据的实时备份许可，定时备份功能许可；应用程序感知型快照功能许可；数据压缩功能许可；数据库保护代理许可；基于 GUI 方式的图形化管理界面；支持在服务器损坏和应用不可用时，可以通过灾备管理软件的一键恢复功能快速接管应用，实现自动化的灾难恢复。三年原厂保修。	1 套
1.4	物理磁带库	2U 机架式，1 个 LTO6 SAS 驱动器，可以安装 24 盒磁带，支持槽位分区，配置 24 盒 LTO6 磁带（压缩前 2.5T，压缩后 6.25T）和 1 盒 LTO 清洗带，同时配置一套备份软件，提供 10 个客户端备份模块和 5 个数据库备份模块，三年原厂免费保修和现场技术支持服务。	1 套
1.5	数据库监控审计系统	1U 设备，支持 Oracle、MS-SQL Server、 DB2 及 Sybase 等业界主流数据库。可防止无意的危险误操作，阻止数据库软件漏洞引起的恶意攻击；有效控制越权操作、违规操作等异常操作行为；可深入到应用层协议实现细料度的安全审计。	1 套
1.6	网络入网准入系统	1U 机架结构；单电源；标准配置 6 个 1000MBASE-T 接口；每秒事务数（TPS)：≥1000（次/秒），最大吞吐量：≥500Mbps，最大并发连接数：1000（条）；最大支持 200 客户端授权。	1 套
1.7	网络版防病毒软件	一个控制中心，支持 PC 终端和 Windows 服务器病毒防护，60 客户端许可。	1 套
1.8	正版软件	Windows Server 2012 标准版 R2	3 套
1.9	等保测评	已建成系统的等级保护测评（二级）。	1 项

1.10	软件系统	共享利用平台、移交接收平台、网页信息采集、电子阅览室、系统工具、系统升级改造	1 套
2	下城区智慧基层综合信息平台升级	四个平台街道、部门个性化模块开发（支持添加各部门，支持向下科室派单，增加一体两翼相关内容建设，增加 APP 端统一标准地址库支持，增加 1CALL+1DO 工单接入，实现主动办工单的自动接入与派发，并对接实现流程的双向同步，实现手机端 H5 与 1CALL 的无缝对接，完善优化电梯监控报警，厨房监控报警接入）	1 项
3	企业服务信息化平台二期	基于微信公众号打造企业用户端，打通与企业服务管理平台，实现政企实时互动；并根据企业服务信息平台一期积累的企业数据、走访数据进行业务管理与监测建模分析，对企业的现状、遇到的问题、可能存在的需求等进行监测分析，多维度、细粒度的运行监测信息服务，为企业服务及领导决策提供数据依据。	1 项
二	政府信息化建设常规保障服务		
1	日常运维服务	全区信息化日常练合运维服务，在 2018 年智慧下城人工辅助式智能控制平台二期运维服务项目基础上整合优化方案，内容包括智慧下城综合运维服务，智慧下城数据整理服务，多部门信息化运维服务，智慧政务平台基础维护，智慧下城专业运维服务，门户网站运维服务，行政服务中心系统运维服务，专业运维服务，机房维护服务，数据库维护服务等内容。增加高级整理层服务。5×12 即时客服，总人数不少于 42 人。	1 项
2	短信服务	短信服务费（未用完部分可延续到下一年度）	1 项
三	网络与安全		
1	网络安全防护升级及存储服务器资源扩充	网络存储与服务器资源扩充。随着信息化系统项目的增加，数据的统一归集要求不断落地，服务器存储等资源目前较为紧张，云服务器为主，本地服务器为备的模式也有大量的存储等资源作为数据备份容灾，需要对现有的本地网络存储与服务器资源进行扩充，含 2 台兆交换机。 网络安全防护（安全软件、硬件）。根据《杭州市政务数据安全管理办法（暂行）》（杭电建数管办〔2017〕1 号）中第三章第一节第十六条 【经费保障】中“新建系统中政务数据安全建设经费的实际投入应当不低于系统建设总经费的 15%”的要求，进行相应的安全防护投入。根据杭州市网络安全防护检查等要求配置态势感知设备、安全设备冗余、防篡改设备、安全防护、网络监控、应用性能监控、数据脱敏等相关软件、设备、异地容灾网关、网管软件及机房运维监控。不足 15%的部分在软件开发、系统运维等项目内容中予以补足。	1 项
1.1	万兆交换机	≥24 个万兆口，≥8 个千兆口，支持虚拟化，三年免费质保。	2 台
1.2	万兆模块	DPtech SFP+万兆光模块，多模，（850nm，0.3km，LC）	16 块

1.3	存储光纤交换机	24 端口交换机，单电源（固定），含 24 个 8Gb 短波 SFP，机架套件，全光纤支持级联，三年原厂质保服务。	2 台
1.4	互联网出口防火墙	2U 机架设备，6 个千兆电口，4 个千兆光口，2 个万兆光口，整机吞吐量≥16Gbps，七层吞吐量≥4G，并发连接数≥250,0000。	1 台
1.5	Tap 镜像分流设备	配置 8 个千兆电口和 8 个 SFP 千兆口，支持镜像流量复制、汇聚功能	1 台
1.6	安全态势感知系统	安全大数据平台，含日志审计平台、DPI 流量监控平台、APT 攻击(网络战)预警平台。	1 台
1.7	数据库安全审计系统	Intel E3 及以上 CPU，主频≥3.1G；内存≥8GB；冗余热插拔双电源；硬盘可用容量≥1TB，1T*2，支持 RAID1；1 个管理口，1 个 HA 口，6 个千兆电口，2 个千兆光口，支持 12 个数据库数审计能力，峰值处理能力：20000 条/秒，审计日志检索能力：1500 万条/秒，三年原厂质保。	1 台
1.8	数据库脱敏系统	标配 4 个 10/100/1000Mbps，2 个 10000Mbps 光口； 双电源，存储容量:2TB； 脱敏速度≥2000 万条/小时; 支持 Oracle、Mysql、SQLServer、DB2、INFORMIX 数据库类型。	1 套
1.9	数据库加密系统	数据库整库透明加密系统， 6 个 GE 口，1*可扩展槽位(4SFP/2SFP+)、双电源、1T 存储，400Mbit/S 加解密速度。	1 套
1.10	数据泄露防护系统	4 个 10/100/1000Mbps，2 个 10000Mbps 光口插槽； 单电源； 存储容量:2TB； 功能：支持 smtp、ftp、http/https 协议 性能：500Mbps	1 套
1.11	服务器深度安全防护系统	服务器深度安全防护系统，包括防病毒模块、深度包检测模块，4 CPU 许可。支持服务器（Windows、Linux）病毒防护；支持利用系统漏洞的攻击行为监测和阻断，提供虚拟补丁；支持木马攻击监测和阻断；支持勒索软件监测及阻断。三年免费升级和病毒库更新。	1 套
1.12	虚拟机灾备系统	一体化备份系统，支持 VMware 平台、超融合平台虚拟机备份；支持数据库备份，双处理器；64GB 高速缓存，16 块 6TB 企业级 SATA3 磁盘，2 个千兆以太网接口，2 个多模光纤万兆以太网口。	1 套
1.13	存储扩展单元	RD500-EXP 存储扩展，2U24 盘位，配置 24 块 1.8TB 10K SAS 硬盘，冗余电源，冗余风扇，配置相应容量的容量扩展许可、存储虚拟化许可和分区许可，包含安装调试服务，三年原厂保修，三年技术支持服务。	1 台
1.14	通配符版 DV SSL 证书	Digicert+Symantec 交叉认证 PKI 体系下签发证书，保护一个带通配符域名（该*号同级别的全部明细域名）；为所有主流的浏览器和移动设备所信任；可同时保护 www. 和非 www. 网站；拥有网站安全签章。证书有效期：1 年	1 个
1.15	硬盘	1.2T SAS 10K 企业级硬盘。	16 块
1.16	服务器内存	VMware 虚拟化资源池服务器内存扩容。共 336GB，要求必须与原服务器内存兼容。	1 项

1.17	蓄电池监测系统	蓄电池监测系统，串口服务器 1 台，温湿度探测器 3 个，检测模块（测内阻）160 个，电流模块 4 个，转换模块 4 个，蓄电池系统软件接口模块 1 套，施工辅材及安装调试费用。	1 套
1.18	蓄电池更新	12V/100AH 蓄电池。	80 节
1.19	机房地插升级	将现有地插升级为工业连接器。	50 套
1.20	运维操作间装修	防静电地板敷设（无边）、强电、弱电线路改造、7 台 42U 前后网孔机柜及施工费。	1 项
2	财政系统网络安全等级保护改造		
2.1	IPS	1U 机箱 ,4 个 10/100/1000BASE-T 接口单电源, 3 年 IPS 规则特征库升级许可，整机吞吐率：2Gbps ,IPS 吞吐率：800Mbps。	1 台
2.2	数据库监控与审计系统	1U 设备，支持 Oracle、MS-SQL Server、 DB2 及 Sybase 等业界主流数据库。可防止无意的危险误操作，阻止数据库软件漏洞引起的恶意攻击；有效控制越权操作、违规操作等异常操作行为；可深入到应用层协议实现细料度的安全审计。	1 台
2.3	存储扩展单元	RD500-EXP 存储扩展，2U24 盘位，配置 24 块 1.8TB 10K SAS 硬盘，冗余电源，冗余风扇，配置相应容量的容量扩展许可、存储虚拟化许可和分区许可，包含安装调试服务，三年原厂保修，三年技术支持服务。	1 台
2.4	虚拟化服务器内存扩容	服务器内存共 1200GB，要求必须与原服务器内存兼容。	1 项
2.5	三级等保复测	金财工程一体化系统、财政业务专网系统三级等保测评复测。	1 项
3	设备维保服务	包括 2 台迪普核心交换机 2 台，31 台接入交换机，18 台服务器，9 台存储系统，4 台存储光纤交换机，1 台隔离网闸，1 台防火墙，1 台堡垒机，1 台 VPN 系统，1 台 SSL VPN 系统，1 台 Web 应用防护系统，1 台无线网控制器，130 台无线网吸顶式 AP，53 台无线网面板式 AP，POE 交换机，详见附件 2。维保服务期 1 年，提供电话技术支持、远程技术支持、现场技术支持、故障设备修复等服务。	1 项
4	网站测评、网站性能监测、网络安全测评	门户网站测评、网络安全测评、网站性能监测等保障服务	1

▲说明 1：本项目采用国产产品，不得采用进口产品。政府采购项下进口产品的界定依据为财政部颁布的文件（财库〔2007〕119 号、财办库〔2008〕248 号）。

说明 2：本项目核心产品为:【数据库加密系统、虚拟机灾备系统】。不同投标人提供的核心产品品牌应不同。如产品品牌均相同，按一家投标人计算，通过资格审查、符合性审查，评审后得分最高的同品牌投标人获得中标候选人推荐资格；评审得分相同的，商务技术部分得分最高的投标人获得中标候选人推荐资格，其他同品牌投标人不作为中标候选人。

说明 3：招标文件中所涉及的产品品牌或型号均为建议性要求或为档次选择要求或为代

替部分技术指标描述，投标人可以选择其他品牌型号的产品参加投标但投标产品须具有相当于或优于招标文件要求的指标、性能、档次。

（三）详细技术参数要求

1　综合信息系统应用升级开发

1.1 下城区电子档案系统二期

1.1.1　超融合服务器存储一体化平台

技术指标	技术指标要求
★兼容性	在现有深信服超融合基础上扩容，必须完全兼容现有平台，实现统一管理、资源统一调用。
★基本配置	超融合服务器存储一体化平台，新增 1 个节点，配置 2 颗英特尔至强 E5 2630 V4CPU,内存 128G，2*480GB SSD 硬盘,4*6T SATA 硬盘，≥4 个千兆网卡、≥2 个万兆网卡 ；2 个万兆多模光模块，双冗余电源。含服务器虚拟化软件许可、网络虚拟化软件许可、存储虚拟化软件许可。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

1.1.2　万兆交换机

技术指标	技术指标要求
配置要求	交换容量≥590Gbps，包转发率≥370Mpp
	配置：万兆光口≥8，千兆电口≥48 个，接口卡扩展槽位≥1,每个槽位均可扩展万兆接口卡
虚拟化	支持多虚一虚拟化技术，将多台物理设备虚拟化为 1 台逻辑设备。
★节能环保	为节能环保考虑，降低 UPS 电源的功率，要求设备最大功耗≤61W。
★工作环境	为保障设备环境适应能力，要求设备支持 0-60℃宽温工作。
MAC 地址用户数	要求设备单端口支持的 MAC 地址用户数≥4k。
路由特性	支持 IPv4 和 IPv6 的三层路由功能，支持静态路由、RIP、OSPF、BGP；
	支持的 OSPF 路由条目数≥12k
组播	支持 IGMP Snooping、IGMP Proxy 支持 GMRP 支持 PIM-SM、PIM-SSM、PIM-DM
MPLS	支持 MPLS L3VPN、MPLS L2VPN、MPLS-TE
网络管理	支持中文管理界面、WEB 管理接口、SNMP v1/v2/v3
▲质保与服务	三年免费质保

1.1.3　一体化备份系统升级

技术指标	技术指标要求

★兼容性	在现有柏科虚拟带库系统上增加BCM-SW v3.0灾备管理模块，必须完全兼容现有的虚拟带库系统。
基本要求	企业级多功能实时备份保护软件，基于设备底层 IP-SAN/FC-SAN 数据块级保护设计（非 TCP/IP 协议），无备份时间窗口；可实现服务器、存储等各种软、硬件故障导致的应用与数据丢失的快速恢复，以及站点级灾难性故障时的远程异地容灾。
保护方式	采用 24 小时不间断实时保护方式，RPO≈0，区别于传统备份模式，无备份窗口，无需考虑备份任务的运行时间，基于设备底层数据块的同步方式，与系统上运行的应用无关。
数据镜像	可实现服务器本地硬盘或外挂磁盘存储系统的多对一数据镜像，当服务器本地磁盘或存储出现故障时，可通过容灾系统的镜像盘快速接管，无需进行长时间的数据回滚的恢复方式，RTO≤2 分钟。
快照及代理	支持无限个数的应用软件感知型快照，单卷快照≥1000 个，当前配置 3 套 Snapshot Agent for MSSQL、3 套 Snapshot Agent for Oracle、3 套 Snapshot Agent for Domino 数据库快照代理，保证数据一致性，快照立即可用无须恢复操作，服务器可以直接对快照进行读写操作。同时支持 MSSQL、Sybase、Oralce、DB2、Domino、Exchange 等数据库，支持基于 X86 平台的 Windows、AIX、HP-UX、Solaris、Linux 和基于飞腾 CPU 平台下国产自主银河麒麟等系统。
CDP 持续数据保护	提供 CDP 持续数据保护和数据回滚功能，可以恢复最近一段时间内任意时间点(微秒级)的数据，可以准确定位到每一微秒的时间点的状态数据，采用非连续快照技术。
操作系统保护	提供操作系统保护的功能模块，要求支持 Windows、Linux 等主流操作系统的全盘保护，当操作系统出现故障，服务器可直接通过 SAN-BOOT 方式远程启动操作系统，或直接通过金属裸机 SAN-BOOT 恢复。
本机数据恢复	当数据出现故障或不可用时，只需通过应用服务器的本机操作来挂接 1 个或多个历史快照来直接接管故障的数据盘对外提供服务，无需通过灾备保护系统的控制台进行操作，以及长时间的数据恢复和回滚。也可以通过备份保护系统直接接管故障的数据盘对外提供服务。
业务接管	系统内嵌虚拟化平台，在业务服务器故障时，可一键式进行业务接管，支持 P2V、V2V 的业务接管模式，支持业务系统的完整恢复。
裸盘恢复	提供裸盘恢复功能，通过容灾系统引导光盘，将备份系统中的镜像数据直接回滚至生产服务器的硬盘，实现整机的便捷式还原。
SRM 整合	灾备系统远程数据复制技术必须与 VMware SRM(Site Recovery Manager)兼容,可接受 VMware SRM(Site Recovery Manager)的调度管理，提供 SRM 相关插件。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

1.1.4 物理磁带库

技术指标	技术指标要求
机型外观	19 寸机架
驱动器数量	1 个可扩展到 2 个
磁带盒数量	≥24 个
驱动器技术	1 个 SAS LTO6 驱动器
非压缩容量	≥60TB
压缩后容量	≥144TB
传输速率	不压缩：240MB/S、压缩：480MB/S
接口	6Gb SAS 主机通道
磁带	24 盒 LTO6 磁带
清洗带	1 盒 LTO 清洗带
备份软件	配置备份归档软件，实现将数据归档到磁带库。同时也可以直接将原有柏科 VTL 设备上的数据归档到磁带库
▲质保与服务	三年免费质保

1.1.5 数据库监控审计系统

技术指标	技术指标要求
硬件规格	1U机架式设备，配置单电源，≥6个GE接口，1×扩展槽位（可扩展4GE/4SFP）。16G内存，1T存储空间。
性能	峰值SQL语句吞吐量≥5000条/秒；并发连接数≥1000个；在线日志量2亿条以上，归档日志15亿条以上。
数据库类型	支持国际主流数据库：Oracle、SQL Server、MySQL、DB2、Postgres、sybase、informix、cacheDB、SAP HANA、Teradata等； 支持国产数据库：达梦、GBase、KingBase、Oscar等； 支持非关系型:mongoDB、Redis等； 支持Hadoop生态：Hbase、Hive、Sentry、HDFS、Impala、ES等。
审计内容	会话的终端信息：IP、MAC、Port、工具名称（程序名）、操作系统用户； 会话的主机信息、IP、Port、数据库名（实例名）、业务主机群； 会话的其它信息：登录时间、会话时长； 操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作对象（数据库实例、schema、表、字段、函数、存储过程名称）、SQL语句、SQL错误代码； 操作影响范围信息：查询、修改、删除操作的影响行数,以及返回行数； 支持数据库双向审计； 支持结果集审计、记录操作成功与失败； 支持SQL server 2005以上（含）版本，在会话登陆过程中对数据库加密用户名的审计； 针对Oracle、SQLserver等同一数据库地址下建立多个数据库实例，可区分实例的

	检索分析； 支持对超长SQL操作语句审计，单条语句长度可达2M；
审计过滤规则	审计策略的要素： where：IP地址、用户名、端口号、数据库类型； who:实例、schema； what:表、字段、视图、包； when：起始\结束时间、执行时长； how：客户端工具； Range：修改、删除或查询的行数 ResultSet：返回结果集 other：关键字、客户端工具和应用、错误码、关联表数等
应用关联审计	非时间戳的解析方式，采用应用端轻量级插件部署，以精确方式审计到应用端相关信息，支持应用用户和源IP的关联审计，支持Weblogic、tomcat、Websphere等主流的应用服务器；
数据库漏洞攻击监测	能对基于数据库漏洞进行攻击行为监测和告警，默认支持420个以上的数据库漏洞攻击规则库。
SQL注入监测	支持SQL注入、XSS攻击等外部行为监控；支持根据IP、sql特征自定义SQL注入规则。
可疑行为识别	对以下高危行为，可自动识别并进行风险处理、告警通知: 1）批量数据导出：对超过特定行数阀值的批量数据导出行为 2）高危操作：对超过特定行数阀值的批量数据修改、删除； 3）支持no where 全表Update、Delete行为监控； 4) 新型/失败语句的识别； 5) 支持耗时长、执行频繁的异常语句识别； 6) 支持活跃会话识别； 7) 支持失败登陆审计； 8) 支持口令猜测，基于频次判断失败登录风险； 9) 支持关联表个数设置； 10)支持返回错误码； 11)支持应用关联监测策略； 12)支持数据库字段级的与或逻辑设置，可建立敏感数据组进行专项监控； 13)支持周期内频次行为监控； 14)支持SQl语句模板化归类，基于语句模板关联客户端信息自定义风险语句、信任语句和不审计语句类型；
多维度分析	支持数据库分组管理，可以基于全局、分组和单库多个维度进行统计分析。采用多功能面板展现，图形化监控被审计系统风险、会话、语句分布情况。支持图形化界面深入钻取分析，直至语句、会话详情；支持对指定数据库添加关注标示。
审计查询	支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户、数据库服务（实例）名等多种丰富的查询检索条件；支持应用层关联审计查询和关联分析；支持风险、语句和会话界面的超链接钻取分

	析；
会话分析	提供全面的会话查询分析能力，包括： 1)会话统计：基于客户端IP、数据库用户、访问工具等维度统计会话量； 2)会话检索：基于客户端IP、数据库用户、MAC地址、访问工具、OS用户等条件检索会话信息； 3)失败及活跃会话分析：提供对失败登录的会话信息查询，提供对周期内的活跃会话进行统计和趋势分析；
支持敏感数据掩码	针对SQl语句中的敏感信息,可自定义规则进行数据掩码展现，防止数据二次泄密。
报表	系统提供不少于40个报表模型，分别基于多库和单库维度进行展现； 支持合规性报表：如PCI、等级保护、SOX法案等专项报表展现； 支持专项报表展现，针对风险、性能、访问源、账户、慢SQL等 信息做专项报表展现； 支持日、周、月 等综合性报表； 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表； 支持风险登陆、高危风险、客户端风险等多种类型报表展现； 支持定期推送； 支持报表数据后台定期预存，独立的预存管理体系，保障报表数据实时展现； 文档格式：WORD\ PDF\ HTML
告警策略	支持高、中、低风险告警； 支持风险登陆、风险操作、SQL注入、漏洞攻击检测、口令攻击、频次攻击等风险告警； 支持产品系统资源的监控与告警。
告警方式	告警方式包括：邮件、短信、企业微信、SYSLOG、SNMP、界面，支持以Syslog 、KA** A、CSV等方式将审计数据外送。
数据库自动发现、审计	支持基于数据流量的数据库自动发现，发现流量中的未知数据库信息，并自动添加审计需要被审计的数据库。
协议解析	支持协议自动识别数据库信息；支持Oracle无链接会话识别；支持Oracle动态端口下的审计。
备份和恢复	支持审计数据自动备份到本地和远端ftp、SFTP、NFS服务器，支持系统配置的导入导出；支持Syslog方式导出全量审计、风险审计、新型语句给第三方平台，实现审计数据的二次分析；
IP别名管理	支持客户端IP别名设置，针对不同客户端IP自定义别名展现；
业务化语言	支持sql语句自定义业务化语言翻译
旁路模式	在交换机镜像模式下，通过TAP、SPAN等技术将网络流量映射到审计设备，对数据库流量进行审计和告警；支持跨网段、跨语句、多VLAN等环境下的审计监测；
探针采集	支持服务器端安装轻量级插件，采集服务器和虚拟化环境下流量无法镜像时的数据库审计行为，产品提供agent插件状态监测功能。

▲质保与服务	三年免费质保

1.1.6 网络入网准入系统

技术指标	技术指标要求
基础要求	一体式机架结构硬件产品，不接受PC SERVER系统架构。必须为专用操作系统，非通用Linux系统或Windows系统。
硬件指标	1U 机架结构；单电源；标准配置 6 个 1000MBASE-T 接口；每秒事务数（TPS)：≥1000（次/秒），最大吞吐量：≥500Mbps，最大并发连接数：1000（条）；最大支持 200 客户端授权。
通信安全	客户端与服务端通信不超过2条常用连接。 客户端支持NAT网络环境穿越，内网NAT环境下的终端与普通终端完全一样，能够正常安装客户端程序并接受服务端的安全管理。
客户端部署	安全客户端模式部署时，客户端程序应支持功能定制，并能够实现主动安装，客户端访问 WEB 安装页面手工安装，支持 ActiveX 控件方式安装。
定向引导	支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。
资产统计	支持对软、硬件资产进行实时统计，能够灵活指定必须使用的软件资产和禁止安装的软件资产，支持对软件、硬件变动进行报警，并且能够查询变动的历史。
Windows 安全登录	可以与用户已有认证系统（UKey、LDAP 等）相结合实现 Windows 系统安全登录与身份认证（替代 Windows 本地用户/密码认证模式）。
补丁管理	系统自带补丁服务器及安全补丁安装程序，支持与微软官方同步、指定上游服务器、WSUS、离线导入等多种更新源方式。可选择严重、重要、中等和需要进行补丁自动安装。
杀毒软件	支持至少 18 种杀毒软件的检查，能够区分版本不合规、病毒库不合规，提供自动下载程序修复和网址引导修复。
系统配置安全	能够建立终端设备的安全性评估任务，支持对帐户密码安全性、屏保设置、共享安全、系统服务、进程及服务等项目进行检查、评定，对存在安全风险的终端支持实时自动修复。
软件黑白名单	支持对终端应用进行控制管理，支持建立软件黑名单和白名单，强制终端只能在管理策略允许的范围内安装应用。
软件分发	能够支持可执行程序、MSI安装包或者文档数据文件自动下发与安装。 能够支持指定组范围、指定时间进行安装并提供程序打包工具。 能够自动统计分发成功率及软件安装成功率，支持进程、注册表、安装路径等多种参数判断方式。
远程协助	远程协助即支持协助端主动连接被协助端也支持被动反向连接，同时也支持通过服务器中转方式连接协助。 远程查看、远程控制可以根据管理需要和网络状况，选择、配置适合管理员的窗口分辨率、显示比例、色彩、鼠标按键、光标等。

外联控制	能够检测出通过代理等方式产生的外联行为并进行报警阻断，在内网设备带出外网的情况下同样能够检测出上述外联行为并进行违规行为上报和阻断。
外设管理	能够禁用终端设备的USB接口、光驱、软驱、打印机、调制解调器、串并口、1394、 红外、蓝牙及PCMCIA卡等外设接口。能够单独禁用USB移动存储设备而不影响其他USB设备。
反 ARP 欺骗	支持网关、关键服务器等 IP、MAC 的静态绑定，从而免受 ARP 的欺骗攻击。 能够实时检测 ARP 欺骗的病毒源，能够对有 ARP 攻击的终端设备进行隔离。
上网访问控制	能够基于 URL 关键字设定允许或禁止终端设备访问的网站，能够对违规访问设备进行报警或阻断。
移动介质管理	能够禁止未注册USB移动存储设备的随意接入。 必须支持新USB移动存储设备用户在线申请、注册，管理员在线审核，无需上交信息中心注册。 能够对 USB 移动存储介质的插入和拔出行为进行审计。
行为审计	能够记录终端用户日常的文档操作、邮件收发、网站浏览等行为，做到有据可查、安全审计。
▲质保与服务	三年免费质保

1.1.7 网络版防病毒软件

技术指标	技术指标要求
★软件许可	1个控制中心，支持PC终端及Windows服务器病毒防护，60个客户端许可。三年免费软件升级和病毒库升级。
系统支持病毒库、处理方式与扫描运行方式	病毒处理方式必须支持智能式的处理方式。根据不同的病毒类型，采取不同的处理策略
	防病毒产品必须要支持网络病毒识别码，网络病毒识别码与传统的病毒代码不同，网络病毒识别码能够识别网络病毒攻击行为。在客户端实现网络病毒的封包过滤
	支持对USB、软驱、光驱、网络共享的使用权限进行控制
	支持对COM／LPT端口、IEEE 1394 接口、图像处理设备、红外设备、调制解调器、PCMCIA 卡、打印影屏幕键的使用权限进行控制
	防病毒管理必须提供Web管理方式；管理通讯采取加密措施
	可赋予客户端对“预设扫描”的控制权限，比如延迟扫描、跳过扫描、停止扫描等
	对于蠕虫、特洛伊木马等恶意程序的专杀工具能够随产品在线自动更新，无需手动下载
	采用智能型扫描机制，能够以文件真正格式作扫描，通过文件头的真实信息而不是简单的通过文件扩展名来识别文件的类型，以提高扫描效率
	支持客户端更新代理。
功能要求	具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击。支持当前勒索病毒、挖矿病毒等病毒防护和查杀。

	具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新
	支持与微软AD的集成，可套用AD的分组方式，方便管理，可分配AD的组和用户不同的服务器管理权限，可监视和管理AD内计算机的安全状态。
	具备远程病毒集中清除功能。可对网络中感染病毒的计算机进行远程自动清除，无需知道计算机的物理位置，无需到客户端逐一清除病毒
	管理端病毒代码及引擎升级可通过多种方式，如直接通过Internet；通过升级工具直接升级以满足大多内网用户升级的需要
	具备数据资产控制，可保护组织的数据资产免遭意外或故意泄漏。数据资产控制允许管理员执行以下操作： 1. 定义要保护的数据资产（正规表达式、关键字、文档属性）， 2. 创建用于限制或机密阻止通过网络通道（Email、FTP、HTTP、HTTPS、IM、SMB、Webmail）以及系统通道（数据记录器、对等应用程序、PGP加密、打印机、可移动储存、同步软件、剪贴板）传输数据资产的策略， 3. 按照以建立的标准强制执行合规。
	能够有效防御高级持续威胁（APT）的攻击，通过联动机制禁止客户机对命令与控制服务器的外联
	产品具备CVE弱点攻击扫描功能，能够及时防护经由网页/电子邮件下载的文档漏洞利用。
分发、安装方法	客户端软件提供多种方式的分发、安装方法。 支持WEB安装方式、SMS安装方式、MSI程序打包安装方式、共享安装等 产品安装、卸载、代码或引擎升级均无需重新启动操作系统 客户端产品防毒服务关闭和产品卸载均需提供密码保护功能，预防防毒系统漏洞的出现 可对客户端进行逻辑分组，对不同的客户端实行不同的防毒管理策略
质保服务	提供三年原厂维保服务及病毒库升级服务。

1.1.8 正版软件

技术指标	技术指标要求
基本要求	Windows Server 2012 标准版R2

1.1.9 等保测评

技术指标	技术指标要求
总体要求	依据国家信息安全等级保护相关标准及工作流程要求，结合区财政业务专网及应用系统整体需求及具体特点，对相关信息系统开展等级保护测评服务，包括协助系统定级、差距分析、协助整改、出具测评报告、完成系统备案等。
依据标准	1、GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》 2、GB/T 28448-2012 《信息安全技术信息系统安全等级保护测评要求》
测评范围	下城区电子档案系统。
系统定级	协助业主方完成其网络信息系统的等保定级工作，包括调研分析、确定系统等级、协

	助申请定级等。
差距分析	对上述系统安全保护现状与等级保护相关标准要求之间的差距进行评估分析，明确存在的安全风险，提出整改建议。
安全整改技术支持	根据差距测评发现的系统安全隐患，提供安全整改技术支持服务，帮助系统管理员、软件开发商、硬件维保公司完成安全整改与加固。
等级测评	依据 GB/T 22239-2008《信息系统安全等级保护基本要求》国家标准，对信息系统进行正式测评，评估信息系统是否符合国家标准的要求，出具等级测评报告。
协助备案	协助业主方完成系统备案工作涉及的各类材料上报工作及备案证书申请工作。
测评内容	按“安全等级保护二级”标准开展等保工作，测评内容覆盖物理环境、网络平台、主机系统、应用软件、数据安全、安全管理制度、安全管理机构、人员安全、系统建设和系统运维等层面。
项目成果	提供《信息系统等级保护测评报告》等测评结果文档。

1.1.10 软件系统

功能	**技术指标要求**
1、共享利用平台	
界面需求	系统应提供简洁有效、高友好度的系统界面和操作习惯。
全文检索	系统应提供全文检索功能，基于本功能查询对应的电子档案。 提供对部分公开的电子档案发起借阅的功能，需要借阅的用户可向电子档案所属单位提交借阅申请。
借阅管理	系统应提供借阅申请管理和借阅历史查询功能。 电子档案所属单位管理员可对借阅申请进行审核处理，确认借阅人信息、借阅天数和借阅目的等信息，完成借阅审批操作。
系统安全	系统应提供按照用户、角色、权限等三级安全架构的用户和权限管理模式。权限管理包括模块权限和数据权限。 系统应提供操作日志管理，包括登录、数据导入、删除、检索等操作日志，以及 IP、时间、用户等信息。
系统定制	系统定制应包括系统参数、辅助字典、机构管理、门类定制、字段定制、首页维护、字段配置、门类导入、门类配置和界面定制等定制功能。 系统参数：可自定义系统名称、档案馆编号的常用参数； 辅助字典：可自定义系统中常用字段值，例如性别、国家、学历等； 机构管理：可自定义管理系统中机构名称、全宗号、机构内部用户等； 门类定制：可手工创建和自定义系统中档案门类； 字段定制：可手工自定义门类中数据字段，包括中文名、英文名、字段类型、字段长度、是否主键和是否系统字段等； 首页维护：系统首页默认发布下城区档案利用制度，首页维护应提供发布内容编辑、修改和发布功能； 字段配置：提供导入数据和门类字段关联配置功能；

	门类导入：系统应提供方便的门类导入功能，新增的档案门类可通过导入功能自动定制和生成； 门类配置：对导入的门类提供门类信息和门类编码定制功能； 界面定制：提供各门类数据查看页面的自定义功能。
数据管理	系统应提供集中的按门类查看共享利用平台中已有数据的功能。 各门类电子档案可根据定制的界面，实现电子档案数据可视化。
数据导入	系统应按照电子档案组成规律，提供数据条目导入和原文批量导入挂接功能。
查档业务	系统应提供针对民生档案的查档业务功能，支持包括查档、申请、受理和办结等业务流程处理。 应支持集成高拍仪或者身份证阅读器，实现用户信息自动获取。
2、移交接收平台	
进馆管理	进馆管理模块应支持立档单位进馆需求上报、档案馆进馆计划制定和正式数据移交进馆等业务流程。 需求管理：系统中注册的立档单位，可在需求管理中上报本年度进馆时间、进馆数据情况等信息，提交给档案馆。提供进馆需求新建、修改和作废等功能。 进馆计划：档案馆可根据年度档案馆系统存储使用情况，结合各立档单位上报的年度进馆需求，制定并发布年度进馆计划。 数据进馆：立档单位可根据进馆计划，申请数据进馆，并上传数据包。数据进馆模块提供数据包上传、数据包检测、移交登记等功能。
系统安全	系统应提供按照用户、角色、权限等三级安全架构的用户和权限管理模式。权限管理包括模块权限和数据权限。 系统应提供操作日志管理，包括登录、数据导入、删除、检索等操作日志，以及 IP、时间、用户等信息。
系统定制	系统定制应包括系统参数、辅助字典、机构管理、门类定制、字段定制、首页维护、字段配置、门类导入、门类配置和界面定制等定制功能。 系统参数：可自定义系统名称、档案馆编号的常用参数； 辅助字典：可自定义系统中常用字段值，例如性别、国家、学历等； 机构管理：可自定义管理系统中机构名称、全宗号、机构内部用户等； 门类定制：可手工创建和自定义系统中档案门类； 字段定制：可手工自定义门类中数据字段，包括中文名、英文名、字段类型、字段长度、是否主键和是否系统字段等； 四性检测：根据相关规范，系统提供“准确性、完整性、可用性、安全性”的检测规则自定义功能； 首页维护：系统首页默认发布下城区档案利用制度，首页维护应提供发布内容编辑、修改和发布功能； 字段配置：提供导入数据和门类字段关联配置功能； 门类导入：系统应提供方便的门类导入功能，新增的档案门类可通过导入功能自动定制和生成； 门类配置：对导入的门类提供门类信息和门类编码定制功能；

<table>
<tr><td></td><td>界面定制：提供各门类数据查看页面的自定义功能。</td></tr>
<tr><td>业务流程要求</td><td>电子档案移交接收业务流程要求：
第一步：立档单位上报进馆需求、进馆数据量等当前电子档案移交进馆需求情况；
第二步：档案馆收集各单位上报的进馆需求、进馆数据量等情况，根据各立档单位需求和自身存储情况制定电子档案移交进馆计划，并通过系统下发给各立档单位；
第三步：各立档单位根据档案馆制定的进馆计划，在线提交电子档案进馆申请；
第四步：档案馆对各立档单位发起的进馆申请进行审核；
第五步：立档单位根据档案馆审核后反馈进馆指导意见、进馆标准、进馆流程等要求，按格式整理好数据并上报；
第六步：档案馆对移交的电子档案进行四性检测，提供定期或即时检测功能；
第七步：生成电子档案移交清单；
第八步：检测通过的数据由档案馆离线导出、并向发送数据的业务系统（或标记数据状态）反馈移交完成的消息。检测不通过，则反馈相关失败信息。</td></tr>
<tr><td>3、网页信息采集</td><td></td></tr>
<tr><td>将政府网站中有价值的原网页进行归档处理</td><td>按照国办发〔2017〕47 号文件《政府网站发展指引》中要对遇整合迁移、改版等情况的政府网站中有价值的原网页进行归档处理的要求。
系统设计支持捕获网页和网页文件元数据，并对完成对元数据的校验，将网页生成适合数字档案室归档的固化电子文件，并建立网站元数据与固化电子文件之间的关联关系。具体设计说明如下：
1、元数据捕获
元数据捕获：系统捕获指定网址时，将根据具体网址分析网页源代码，按照设定好的元数据捕获规则自动捕获网页文件的元数据信息，元数据项包括：栏目名称、栏目类别、文章标题、网页发布时间、来源、关键词、作者、摘要、网址等信息。
2、网页固化归档
网页固化按照版式电子文件长期保存格式需求（DA/T 47-2009）的要求，将网页 HTML 文件固化为 PDF 格式，保证网页内容原貌展示，并建立网站元数据与固化电子文件之间的关联关系；支持网页批量固化功能。</td></tr>
<tr><td>4、电子阅览室</td><td>电子阅览室的利用对象主要分为二类用户，一是来馆利用查询的查档者，通过接待大厅的查询电脑提供利用；二是局馆的工作人员，通过已经建成的局域网进行控制和授权。电子阅览室主要提供三个方面的信息阅览：一是馆藏的各类档案、现行文件；二是外购的人文社科类的期刊、会议文集、论文等；三是馆内的各类电子出版物和一些视频的培训教育内容。
本次项目的电子阅览室系统需作为馆藏档案管理系统的一部分进行集成。
<table>
<tr><td colspan="3">电子阅览室系统</td></tr>
<tr><td>序号</td><td>功能模块</td><td>功能描述</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td>1</td><td>数据上传</td><td>通过后台将档案条目、原文上传到电子阅览室系统。</td></tr>
<tr><td>2</td><td>数据发布</td><td>实现馆藏档案推送到电子阅览室。</td></tr>
<tr><td>3</td><td>自助查阅</td><td>提供自助查阅登录链接，用于利用大厅授权的临时用户登录浏览档案数据。</td></tr>
<tr><td>4</td><td>用户设置</td><td>电子阅览室开设维护账户，配备给档案馆专人使用。</td></tr>
</table></td></tr>
<tr><td>阅览室</td><td>电子阅览室包括以下几部分功能：
1、门户式服务：提供统一的利用服务窗口，面向查档用户提供独立的检索界面和检索方式，页面采用清新、简洁、独立的设计，能够直观显示当前公布的相关信息，用户可快速在相关分类中找到需要的信息。
2、海量资源库:以档案信息资源总库为基础，汇集了可以在内部公开的所有馆藏资料、全国期刊、馆藏照片、视频资料、音频资料、专题目录、现行文件等信息资源。以后可以根据需要自动进行扩展。
3、资源检索：利用者可以进入电子阅览室的下城档案局端，自主进行信息资源的查询检索。系统提供树状结构检索和全文检索两种方式，外部人员的利用必须受权限控制，一般通过鉴定可以开放的数据才能开放，同时可以控制是目录开放还是目录和电子文件同时开放。
4、权限赋予和收回：利用者可以提出申请，档案管理员可以进行授权，该权限将在限定时间内自动收回或人工随时收回。
5、系统管理维护:主要包括用户管理、权限管理；浏览日志记录、查询、维护。
6、在局域网中建立面向社会公众的电子阅览室，提供档案信息阅览、查询和借阅等功能。</td></tr>
<tr><td>视频分类</td><td>视频分类是对视频进行分类设置，视频上传时可以选择相应的视频分类。</td></tr>
<tr><td>视频管理</td><td>视频管理是需要上传的视频进行信息管理，包括年度、题名、档号、制作日期、分类等，档案员可以查看、修改、删除上传视频的信息。</td></tr>
<tr><td>视频挂接</td><td>视频挂接实现视频的批量上传与挂接。档案员通过档号完成视频的批量挂接。</td></tr>
<tr><td>音频分类</td><td>音频分类是对音频进行分类设置，音频上传时可以选择相应的音频分类。</td></tr>
<tr><td>音频管理</td><td>音频管理是需要上传的音频进行信息管理，包括年度、题名、档号、制作日期、分类等，档案员可以查看、修改、删除上传音频的信息。</td></tr>
<tr><td>音频挂接</td><td>音频挂接实现音频的批量上传与挂接。档案员通过档号完成音频的批量挂接。</td></tr>
<tr><td>5 系统工具</td><td></td></tr>
<tr><td>数据打包/四性检测工具</td><td>数据打包/四性检测工具提供脱离档案业务系统使用的离线电子档案数据打包及四性检测功能。
工具提供离线电子档案数据按照《基于 XML 的电子文件封装规范》（DAT 48-2009）的封装（打包）功能。
同时，工具应包含四性检测规则定制、四性检测功能、数据包下载等功能。</td></tr>
</table>

格式转换工具	格式转换工具支持脱离于档案业务系统使用的格式转换功能，提供 TIF、JPG、PNG、DOC 等多种格式向 PDF 单个和批量转换功能。
6 系统升级改造	基于下城区档案局一期项目建设成果，随着系统应用的深入和具体业务的开展，下城区档案局将在项目建设中提出部分适应性改造和升级需求，承建单位可根据实际需求评估工作量。本项目需包含 10 个工作日的定制开发服务。
7 其他	**▲二期项目要求在现有平台基础上进行融合设计开发，作为现有平台系统的扩展。**

1.2 四个平台街道、部门个性化模块开发

技术指标	技术指标要求
系统框架建设要求	展现层：通过 PC、移动终端、大屏幕进行下城区智慧基层综合信息平台(暨四个平台)综合展现。网格员、处置人员、各级领导、志愿者、公众通过移动终端与平台实现互通。
	应用层：为下城区层级提供对应的应用服务，包含区级个性化特色应用，区级民政个性化应用，同时也提供台账日志、工作签到、即时通讯、移动办公等全省标准应用。形成全身统一标准下富有下城区特色的基层治理应用体系。
	支撑层：主要指公共支撑服务，包括统一认证、数据交换、文件服务、地图服务、安全管理、组件管理、分析工具、消息服务、信息统计、搜索引擎、服务接口等支撑服务。
	数据层：建设下城区智慧基层综合信息平台(暨四个平台)本地特色数据资源池，包含区基础数据库、区专题数据库、区业务数据库。与市级平台数据库进行数据的实时交互，同时保留下城区级特色的数据资源。
	设施层：主要包括政务云基础设施、电子政务网络和互联网。
业务流程建设要求	下城区智慧基层综合信息平台的建设实现区-街道-社区-网格的纵向逐级穿透，多级联动，通过分层指挥、分类处置、逐层分流、按责转办，形成常态化的多层级的工作闭环。
	业务流转从横向上带动协同体系和公共服务体系的建立，对接区级 1Call 和 1Do 平台，实现事件的流转；纵向与市级综合治理协同平台打通业务通道，同时通过与市统一地址管理与服务平台的对接，实现地址信息的下发核查和救济上报流程。
统一地址库应用升级功能要求	
地址采集	地址采集功能将实现对新增地址的添加，可分别新增楼幢、户室地址，支持通过查询楼幢地址，在楼幢地址基础上完善添加户室地址信息功能。
地址核查	•待核查地址列表（同时根据地址数据状态需要区分有效地址、失效地址、无效地址、退回地址）； •核查有效地址（待核查列表进入后，完善地址信息，点击提交，提交后数据作为有效地址上报至地址库，可在有效地址列通过接口查看到）； •核查失效地址（待核查列表进入后，如地址已拆迁或不存在，点击失效，将数据更新后上报至地址库，可在失效地址列查看到）；

	•核查无效地址（待核查列表进入后，如地址描述不清晰无法辨识，点击无效，将数据更新上报至地址库，可在无效地址列查看到）； •退回地址（待核查列表进入后，如地址不属于管辖范围，点击退回，将数据更新后退回到街道管理员，进入退回列表）。
统一地址平台对接	与市级统一地址管理与服务平台进行对接，实现地址库数据的实时互通，可及时获取待核查地址并随时提交地址救济信息。
“系统配置”功能升级要求	
组织架构添加	对下城区基层治理平台的系统配置-组织架构进行升级。组织架构支持横向添加部门，纵向添加科室（部门下科室，暂先添加两级）（如市场监管局添加二级科室），支持事件派单功能。
权限配置	为下城区综合信息指挥中心管理云开放配置权限，实现区级中心自主权限配置功能。
“一体两翼”模块建设要求	
涉稳信息库	针对涉稳人员、涉稳场所、涉稳事件等集合形成本地涉稳信息专题库，为相关问题的分析预测提供数据支撑。
涉稳事件分析	对于事件处置中涉稳事件处置情况进行统计分析、高发热点事件专题分析，帮助下城区管理人员直观了解辖区内涉稳因素的根源。
重点对象稳控分析	对辖区内重点对象进行多角度的稳控分析，如对涉稳人员、涉稳事件等稳控情况进行统计分析。
维稳案例库	对涉稳类事件及事件处置相关信息进行提取和统一管理，形成维稳案例库，可为日后同类事件处置提供案例参考。
1call+1Do 工单平台接入功能要求	
平台对接	通过与 1call、1Do 两个平台的对接，可完成事件对接流转，事件节点信息实时同步工单平台，实现事件双向同步。
工单接入	（1）“1call”平台对接 “1call”移动办事系统是下城区自主研发的“掌上办事”与“聊天即办”相结合的新平台，已在长庆街道试点应用。可在聊天窗输入办理事项，即可知晓办理业务所需材料。将材料上传至客服，便可完成业务办理。同时，针对部分需要前往办事窗口领取证照的业务，将依托社区网格化服务和快递送达的方式，实现群众办事“跑零趟”，减少时间、人力、交通成本，提高办事效率。 本期平台升级将实现与“1call”平台的对接，连接和扩展下城区便民服务等应用场景。
	（2）1Do 平台对接 “1Do”任务处理模式是城市大脑下城平台中的应用模块，可实现了事件、信息和异常情况的实时处理，数据留痕，发挥 1Do 流转形式多样的特性，实现按需流转，精准定位，快速处理。 本期平台升级将实现与“1Do”应用的对接，为下城区提供线上服务扩展通道。
“主动办”工单自动接入与派发功能要求	
工单自动接入与派发	实现主动办工单的自动接入与派发，完成事件对接流转，使基层治理平台和“主动办”平台实现事件双向同步。

“主动办”平台对接	本期平台升级将实现与“1Do”应用的对接，为下城区提供线上服务扩展通道。
移动端升级改造	将下城区基层治理平台相对应的手机端应用进行 H5 化改造，可为日后上钉或嵌入下城区综合客户端 APP 奠定基础。
监测报警功能优化要求	
电梯监控报警优化	对市场监管局系统平台获取电梯监控报警，将已接入的报警信息呈现进行完善优化。
厨房监控报警优化	对市场监管局系统平台获取厨房监控报警，厨房监控探头及报警信息等信息，将已接入的报警信息呈现进行完善优化。
其他建设要求	
建设规范要求	以上系统建设及升级改造需考虑软件建设的一致性，均应符合下城区软件系统开发“四统一”指导规范（DB/Z HZXC0001-2018）
网络部署要求	下城区智慧基层综合信息平台(暨四个平台)网络主要依托于电子政务网，服务器虚拟托管在杭州市政务云计算中心，并由政务云负责服务器的运行环境安全，日常维护以及备份恢复。
数据存储要求	下城区智慧基层综合信息平台(暨四个平台)所需的服务器及数据存储统一部署在杭州市政务云计算中心，按具体服务器配置需求申请相应的云资源。在随着业务扩展，未来将提出扩容需求，将会根据政务云计算中心机制申请扩容。
系统对接要求	下城区信息中心交换融合了区内各个部门的政务数据，整合成效明显。依托数据整合的基础，实现全区统一的数据交换、融合、共享及服务，成为全区信息资源综合挖掘与应用的孵化平台。 依托于下城区信息中心的数据和系统对接支持， 实现“四个平台”与各业务系统之间的对接服务，目前需实现对接的系统如下： 1、对接下城区“1Call”、“1Do”平台； 2、对接“主动办”平台。
系统运维要求	（1） 日常维护 在项目实施过程中，要求现场派驻经验丰富的技术骨干开展实施工作，项目试运行完成后，根据具体情况需求继续现场派驻专业技术人员进行日常维护。 （2） 技术支持 提供 7*24 小时不间断运营，出现故障时 10 分钟响应、60 分钟到场服务。 （3） 售后服务 在系统 1 年质保期间，对于系统软件的维护、性能优化及升级，均提供最佳方案和最优惠的解决方案和技术服务支持。
安全保障要求	信息安全保障需根据下城区智慧基层综合信息平台(暨四个平台)的基本安全需求，参考国家涉密计算机系统的安全要求，从设施安全、网络安全、应用安全和管理安全等方面进行设计，云平台的防护结合市政务云的安全防护进行设计，构建全面的安全防护体系。

1.3 企业服务信息化平台二期

技术指标	技术指标要求

技术架构	该系统基于 web 采用 B/S 三层架构。
微信公众号功能要求	
用户登录	根据管理端创建的账号信息进行登录验证
在线咨询	基于下城 1call 实现在线咨询及问题上报；
资源库	（1）支持企业资源统一展示； （2）支持企业资源按照政策资源、项目申报、活动资源、其他资源的统一标准分类；
热门话题	支持话题展示、发布、回复； 支持公众号与 PC 端数据交互
消息通知	（1）支持上报问题办理进度通知； （2）支持资源推送通知；
管理端功能要求	
综合数字大屏	基于企业数据、办理单、走访日志等相关数据条件下，支持企业服务数据统计、企业服务数据分析、企业服务监测； 实现数字大屏可视化展示； 该功能 PC 端支持
办理单管理	支持办理单评价记录与公众号评价进行数据交互，对评价数据进行归集、展示； 办理单细节优化
企业标签管理	（1）支持标签类别新建、编辑、删除操作； （2）支持标签新建、删除操作； （3）支持标签权限个性化展示标签数据；
我的日志	支持对部门日志进行分类； 支持部门日志导、查询出功能； 支持日志根据权限个性化展示；
我的资源	支持资源数据同步至公众号政策库； 支持资源针对性发送至部分用户； 支持资源浏览量数据记录、展示；
用户问题反馈	支持用户上报问题的审核、分发、协办、跟踪、归类、留痕、归档流程控制，以及发送评价； 支持按负责部门、企业状态、所属楼宇以及关键字查询
企业用户管理	支持企业用户账号创建、禁用、启用、删除操作；可根据企业名称、联系人等进行数据查询；
热门话题	支持热门话题展示，回复功能；
权限管理	支持用户的数据权限、操作权限自由配置； 支持权限组新建、编辑、删除等管理操作； 支持用户多部门角色切换；
系统设置	包含用户管理，对接统一用户数据；

性能指标	系统应提供 7×24 小时的连续运行，系统应具有灾难恢复能力。
工程管理要求	本工程的项目管理与服务工作任务包括项目管理、软件集成、培训、系统运维服务等方面内容。 (1) 项目的总体工期为 9 个月。 (2) 项目全过程要求受监理方的监督管理； (3) 针对本项目建设内容制定保密措施，须提供对本项目的保密承诺。
▲售后服务要求	项目终验后提供 1 年售后服务，遵守运维管理制度，确保提供 7×24 响应服务。
技术架构	应用系统采用三层架构，支持应用集群及负载均衡部署。
客户端	B/S 浏览器支持 IE9 以上、chrome 等常用主流浏览器.
数据库	支持 Mysql、 SQLServer 数据库。
安全机制	应用系统支持统一用户接入，符合下城区《智慧下城数字化转型 “四统一”规范》要求。
其他	**▲二期项目要求在现有平台基础上进行融合设计开发，作为现有平台系统的扩展。**

2 政府信息化建设常规保障服务

2.1日常运维服务

技术指标	技术指标要求
总体要求	**▲全区信息化日常综合运维服务，在 2018 年智慧下城人工辅助式智能控制平台二期运维服务项目基础上整合优化方案，内容包括智慧下城综合运维服务，智慧下城数据整理服务，多部门信息化运维服务，智慧政务平台基础维护，智慧下城专业运维服务，门户网站运维服务，行政服务中心系统运维服务，专业运维服务，机房维护服务，数据库维护服务，高级整理层服务，5×12 即时客服，总人数不少于 42 人。**
智慧下城综合运维服务	服务目标：保障智慧下城政务工作平台的安全稳定顺畅运行。及时响应并牵头解决政务工作平台用户在使用本平台过程中遇到的各类技术问题，提供安装、配置、培训、咨询、数据备份恢复、查障、排障、记录汇总用户需求、完成用户需求初步分析等服务，通过对区政务工作平台运行情况的记录、统计和分析，为下城政务工作平台的安全稳定顺畅运行提供有力的数据支持和优化升级建议。保障“最多跑一次”工作人力成本对接。
	服务范围：含移动办公运维，智慧下城政务工作平台的 web 服务、后端接口服务、数据服务、移动端 app、流程模板等业务数据、二次开发接口及源码、文档以及其他相关中间件。“最多跑一次”系统对接人工服务及代办。
	服务内容： 1、建立智慧下城政务工作平台运维服务管理体系，根据智慧下城政务工作平台的运行使用现状提出整体优化规划报告，包括日常维护计划、缺陷修复计划、应急响应计划、重构优化计划等； 2、针对下城政务工作平台各功能模块及接入系统，提供日常巡检、定期维护、运

	行故障处理、简易缺陷修复、个性化配置调优、平台用户呼叫应答、二次开发需求跟进反馈等服务。对平台接入单位提供技术支持、回复相关电话咨询。对本平台所在设备运行状况作出定期检查，发现运行异常情况与网络故障、各类网络病毒或木马事件可能相关时应及时向网络安全负责人员报告并协助处理； 3、建立并维护智慧下城政务工作平台的安装配置手册、平台用户手册、平台管理员手册；建立并维护软件安装升级所需的安装升级包，并提供相关资料及第三方工具包； 4、提供智慧下城政务工作平台的运行状况统计、公文收发转统计、历史数据迁移汇总、平台软件升级发布、数据备份导出等平台运维服务，确保政务工作平台的安全平稳顺畅运行； 5、提供政务工作平台的推广计划及用户培训计划。协助组织开展平台推广活动及培训活动； 6、协助制定下城区智慧政务整体平台应急响应预案，并在应急事件发生时重点对政务工作平台系统及相关系统进行应急事件处理，保护平台关键业务数据免受重大故障或灾难的影响； 7、提供个性化问题的咨询服务，协助完成区党政机关各下属部门街道的权限配置、需求记录汇总、公文红头模板维护、公文栏目及流程模板的配置调试和移交工作； 8、提供智慧下城政务工作平台的相关培训； 9、完成甲方领导交办的与下城政务平台相关的其它日常工作。
智慧下城数据整理服务	服务目标：作为人工辅助式平台重要组成部分，为智慧下城政务工作安全稳定开展提供数据服务保障，利用下城区数据中心及政务工作平台，根据各级领导的具体要求，整理分析相关数据（包括各类考核评分数据的变动情况）及时上报，通过线下服务与线上分析，及时发现关键信息化建设需求，助力智慧下城建设。
	服务范围：实时关注各类客服的工作汇报，加以分类整理，对与重点项目重点工作相关的客服工作汇报数据优先处理并及时上报。
	服务内容： 收集区各电子政务应用系统数据，定时整理、分析和上报，对领导关心的系统数据重点处理，确保及时给以决策数据支持； 负责完成部门日常办公资料整理，对办公资料中的急件、要件、重点加以标识提示，并及时向领导汇报； 协助完成信息化系统需求调研及分析，为上级工作落实提供有力支持； 负责信息化相关会议的组织通知协调，完成上级交办任务； 负责信息中心对外的服务管理工作，保持线上线下信息通道顺畅，为电子政务工作创造有利环境;
多部门信息化运维服务	服务目标：根据下城区部门信息化运维服务需求，委派人员提供主场运维服务。针对办公场所终端 PC 及外设、政务信息网络、部门业务软件等 IT 相关软硬件设施，建立信息化运维规范，提供资产管理、终端 PC 软硬件维护等综合服务，保障信息网络和信息系统设施的安全与稳定运行。
	服务范围：各部门办公场所终端 PC 及外设、政务信息网络、部门业务软件等 IT 相

	关软硬件设施。
	资产管理：针对信息化设备资产（网络设备、桌面 PC 等），建立资产清单，统计资产的型号、硬件配置、序列号、参数设置等信息，并按时更新。
	终端 PC 维护：终端 PC 软硬件故障维护及终端 IP 地址管理、统一病毒库升级、访问控制管理，以及其他终端合规性管理等。
	安全管理：配合省市区政务安全管理工作，落实必要的安全措施，例如终端病毒软件升级，安全加固等。
	应用系统维护：配合软件开发商和集成商，完成部门业务系统的日常管理维护工作，解决软件日常使用和操作问题。
	其他：用户交办的其他事项。
	服务时间：工作日 5*8 小时。
智慧政务平台基础维护	服务目标：为下城区智慧政务整体平台的安全与稳定运行提供有力的保障，通过对平台运行情况的记录、统计和分析，为下城区 IT 基础设施的安全运行提供有力的数据支持和加固建议，为视联网会议的安全平稳运行提供有力保障。
	服务范围：下城区智慧政务整体平台的网络设备、服务器、系统平台、安全设备、存储、PC 机和打印机及其他相关设备，视联网系统软件、硬件设备、会议场地设施。
	视联网运维：非会议期间，每日巡检下城区视联网系统软件、硬件设备及会议场地设施的安装保养情况，发现可能造成无法进行正常视频会议的异常情况时，及时处理并汇报。负责接通调试视联网系统，完成会前准备。负责向参会人员培训系统使用方法，确保主要参会人员顺利完成视联网会议。会议期间，对软硬件问题引起的会议干扰、暂停的情况给以及时处理，无法单独处理的及时联系相关技术保障人员及单位协助紧急处理。完成区领导交办的其它视联网会议相关工作。
	故障维护：提供网络设备、安全设备、服务器、系统平台、存储、机关大楼内部的 PC 机、打印机及其他设备的日常运行维护、故障处理。对接入单位提供技术支持、各类电话咨询。对机房和设备运行状况检查，处理各类网络病毒或木马事件。
	资产管理：针对信息化设备资产建立资产清单，统计资产的型号、硬件配置、序列号、参数设置等信息；建立软件和升级包配置档案。
	安全运维：提供下城区智慧政务整体平台的安全状况监测、漏洞扫描、安全加固等安全运维服务，每月一次对下城区智慧政务整体平台进行漏洞扫描和安全加固、安全审计和日志分析、病毒日志分析、病毒和漏洞公告，确保智慧政务整体平台的安全平稳运行。
	配合风险评估：配合安全服务公司，每半年作一次风险评估，对可能存在的安全风险进行综合分析评估，制定对应措施。
	应急演练：负责制定下城区智慧政务整体平台应急响应预案，并在应急事件发生时进行事件处理，保护关键业务免受重大故障或灾难的影响，每年举行不少于一次应急演练。
	咨询服务：提供安全咨询服务，系统集成咨询服务；

	培训服务：提供智慧政务整体平台相关培训。
智慧下城专业运维服务	下城区智慧政务支撑平台的网络设备、服务器、系统平台、安全设备、存储等。
	7*24 小时响应和技术咨询：中标人应设立值班响应电话，并安排有经验的工程师接收报障。当设备出现故障时，采购单位通过中标人指定的值班响应电话进行报障，保证采购单位关于设备和软件的技术性问题得到及时、有效的解答。
	远程支持服务：对于通过电话指导不能解决的故障，如果设备具备提供远程技术支援的能力，中标人在征得采购单位同意后，通过远程接入手段，登录到故障设备，进行故障诊断，查找故障出现的原因，指导现场维护人员处理故障。
	故障响应服务：对于通过电话支持和远程支持都不能解决的故障，中标人应迅速提供现场支持服务，安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案，并最终排除故障。
	定期巡检与优化：中标人为采购单位维护保修服务范围内的设备和软件进行定期的现场检查，及时发现运行中存在的隐患，通过系统调整等手段，减少系统发生故障的概率，保证系统稳定、高效的运行。
	重点保障服务：采购单位根据需要向中标人提出重点保障服务请求（包括但不限于机房搬迁服务、设备应用功能调整），中标人收到请求后与采购单位共同指定重点保障期间的设备和软件保障方案。
	应急响应与预演服务：中标人需与采购单位一起了解其业务需求及服务质量需求的前提下，确定应急恢复计划的范围与目标，设计提供应急恢复方案，以保证采购单位业务的持续性和可用性。双方需共同讨论以完成应急恢复方案计划。应急恢复方案设计完成后，双方应共同参与，完成应急方案的测试预演，以确定其是否满足业务需要和达成设定的恢复目标。
	安全评估服务：提供每年不少于两次安全评估及安全咨询服务。
	平台建设服务：建立信息系统安全知识库、安全服务数据库以及信息化设备数据库，为网络系统及信息化设备的安全、稳定运行和信息化平台的建设发展提供支撑
	分析报告服务：定期提交每个设备的配置和存储应用情况报告、网络拓扑报告、IP 分配报告；定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； 对核心服务器进行工作压力监控，针对业务的增长定期生成主服务器的工作压力报表，并且预估业务增长对服务器压力的影响提出合理化建议
	备份服务：对关键的网络设备服务配置文件进行定期离线备份；制定系统数据备份计划，确定合理的系统备份策略。定期备份重要业务信息、系统数据及软件系统等；根据数据的重要性和数据对系统运行的影响，执行数据的备份，每月提交数据备份报告，必要时实施数据恢复；
	资源资产管理：信息中心固定资产统计与整理，现有资产清点，资产信息变更登记、统计，现有软件服务统计，硬件资源情况分析与改建建议。
	网络结构优化：研究优化网络结构，提供优化方案与建议。
	运维管理与协调服务：针对下城信息化建设现状与机房运维管理现状，结合现有管理制度与运维手段，系统地建立起运维服务管理体系。如各类机房、设备管理制度，运

	维管理制度，人员分工与职责，各类应急预案，服务响应机制。
	管理与培训服务：根据制定优化的制度对全体运维人员开展每月不少于 1 次的培训与业务指导。
	虚拟化服务：中标人需为采购单位提供虚拟化搭建及迁移的技术咨询服务，指导现场维护人员对虚机进行扩容、迁移等工作。
门户网站运维服务	服务目标： 通过技术更新和完善“杭州·下城”门户网站功能体系，配合采购人理顺门户网站服务管理体系，明确指出门户网站发展方向，配合完成国家、省、市对门户网站的考核。 通过技术更新和完善门户网站功能体系，功能上符合国家、省、市等相关考核要求，性能上保证门户网站安全、稳定、可靠运行。 配合理顺门户网站服务管理体系，提高门户网站内容可用性、正确性及信息更新及时性。 对门户网站未来发展方面，提出明确意见，特别是各级考核标准变更。 配合完成国家、省、市对门户网站的考核，特别是各级整改意见，积极对门户网站进行整改和更新。
	日常维护服务：系统本身的缺陷的修正（程序 bug 修正，界面调整、文字错误），各种专题制作，不涉及系统功能更改的应用调整（模块、菜单结构的调整、界面结构的调整、表单界面的调整和修改、如表格顺序的调整、添加字段），需根据用户方提出的合理需求，对系统进行改进和完善。
	门户网站定期优化服务：在服务期内，为了确保门户网站的安全、稳定、健康运行和及时解决系统运行过程中出现的实际问题，项目经理将每月到用户现场，解决系统进一步调试优化和系统维护工作。
	制定备份和巡检：在系统维护期内，中标单位根据用户实际情况制定切实可行的备份方案，免费提供备份工具软件。并每月定期安排工程是对备份数据进行检查，确保备份数据安全有效。
	重大技术问题解决服务：在系统维护期内，如遇到重大的技术问题（如系统崩溃，无法运行等），项目经理立刻通过远程方式对问题进行诊断和解决，如无法通过远程方式解决，中标单位将派工程师现场上门解决，服务响应时间为 2 小时，并承诺 2 小时内恢复运行。
	技术支持要求：提供 7*24 小时的电话咨询、远程连接支持等各类技术支持服务，技术工程师常驻用户现场进行门户网站的日常维护、调整优化、故障受理等工作，协助用户制订日常运行管理规范和运行应急预案；其它各种技术问题等。当派驻工程师及其他支持方式无法解决问题时或技术力量不足时，中标方应及时提供后援技术支持和补充。
行政服务中心系统运维服务	保障下城区行政服务中心网络设备及线路、服务器和应用系统平台、桌面 PC 终端、叫号系统、大屏幕等外设正常稳定运行。
	建立运维服务管理体系和日常运维管理制度。
	对下城区行政服务中心网络设备及线路、服务器和应用系统平台、叫号系统、大屏幕等外设实行每日定时巡查和记录。

	实时监控下城区行政服务中心网络设备及线路、服务器和应用系统平台、叫号系统、大屏幕等外设运行情况。
	针对下城区行政服务中心网络设备及线路、服务器和应用系统平台、桌面 PC 终端、叫号系统、大屏幕等外设的日常维护和故障处理。提供服务台电话技术支持、技术咨询、故障排除、软件安装服务等。
	建立资产清单库和配置档案库等信息资料。
	终端定期杀毒、病毒库更新。
	提供定期运维分析总结报告，包括资产变化、事件故障、更新发布、安全态势、总体运行健康度等。
	提供相关培训服务。
	负责下城区行政服务中心交办的其它日常工作。
	人员常驻现场，5*8 小时服务。
机房维护服务	机房保养：每月一次，检查测试工作环境：包括环境温度、湿度、照明、地线和接地电阻等；机房地板清洁、机房天棚清洁、机房隔墙隔断清洁、机房抗静电活动地板下清洁；清洁机架内外、设备面板和监视器、显示器屏幕、设备除尘、设备保养；清洁各监视器和计算机内部；清洁各设备的电路板和接插件
	机房配电柜、强电线路、插座维护：每季度一次，检查测量机房市电电压、电流、功率计算负载；检查、清理，包括：锁紧母线及开关接线端螺母；清理开关、插座等设备的卫生、清扫积碳、检查开关触头扣合情况，绝缘老化程度
	机房防雷器、接地网系统维护：每季度一次，检查防雷器状态，是否有失效情况，部件及时更换；测量机房零地电压、接地电阻是否正常，是否在合理范围，并根据防雷检测报告做出处理。
	机房网络线路整理、维护：每季度一次，检查网络线路、模块、面板通讯是否正常，及时更换损坏部件。对部分调整线路进行整理、确认、标识。
	机房空调维护（艾默生 DME3000 系列空调 3 台）： 一、空气处理机的维护（每季度一次） 1.表面清洁，风机转动部件无灰尘、油污、皮带转动无异常摩擦；2.过滤器清洁，滤料无破损、透气孔无阻塞、无变形；3.蒸发器翅片应明亮无阻塞、无污痕；4.翅片水槽和冷凝水盘应干净无沉积物，冷凝水管应畅通；5.送、回风道及静压箱无跑、冒、漏风现象。 二、风冷冷凝器的维护（每季度一次） 1.风扇支座紧固，基墩不松动，无风化现象。电机和风叶应无灰尘、油污、扇叶转动正常，无抖动和摩擦；2.定期用钳形电流表测试风机的工作电流，检查风扇的调速机构，看是否正常；3.经常检查、清洁冷凝器的翅片，应无灰尘、油污。接线盒和风机内无进水；4.电机的轴承应为紧配合，发现扇叶摆动或转动不正常时应进行维修或更换。 三、压缩机部分的维护（每季度一次） 1.用高、低压氟利昂表测试高低压保护装置，发现问题及时排除；2.经常用手触摸压

	缩机表面温度，有无过冷过热现象，发现有较大温差时，应查明原因；3.定期观察镜内氟利昂的流动情况，判断有无水份，是否缺液；4.检查冷媒管固定位置有无松动或震动情况；5.检查冷媒管道保温层，发现破损应及时修补；6.制冷管道应畅通，发现堵塞及时排除。 四、电气控制部分的维护（每季度一次） 1.定期检查报警器声、光报警是否正常，接触器、熔断器有无松动或损坏，发现问题及时排除；2.检查电加热器的螺丝有无松动，热管有无尘埃，如有松动和尘埃应及时紧固和清洁；3.用钳形电流表测试所有电机的负载电流，测量数据与原始记录不符时，应查出原因，进行排除；4.检查继电器和电子元件有无损坏和变质，发现问题及时更换；5.用干湿球温度计测量回风温度和相对湿度，偏差超出标准时，应进行调正；6.测量设备的保护接地线，如果引线接触不良，应及时紧固；7.测量设备绝缘，检查导线有无老化现象。
	机房 UPS 系统运行维护：每季度一次，检查测量 UPS 电压、电流、功率计算负载；检查、清理，包括：锁紧母线及开关接线端螺母；清理开关、插座等设备的卫生、清扫积碳、检查开关触头扣合情况，绝缘老化程度; 定期检查 UPS 三相负载均衡情况，对较大三相不平衡，作出调整，使之恢复三相基本均衡。对设备故障予以修复解决。
	机房门禁系统运行维护：每季度一次，调用近一个月的数据，看是否记录正确门禁系统维护维护内容：系统运行检测（每月进行一次）：一人刷卡，一人观察门禁软件，是否记录正确；采用不同的授权卡，对不同的门进行检测，看是否授权正确；设备维护电磁锁：用不同的力度推拉门，观测大门是否严实按钮及读感器：拆掉读感器的外壳，用电笔测试电压是否正常；门禁控制器（每三个月一次）：打开门禁控制器的门，观测控制器各指示灯的状态。
	机房 KVM 系统运行维护：每季度一次，检查 KVM 状态，是否有失效情况，部件及时更换；软硬件运行是否正常。
	机房动力环境监测系统：每季度一次，检查、监测设备的运行是否正常，软件系统是否运行正常，失效及时更换调试。
	其他设备服务：其它机房相关设备的巡检；机房相关标识标牌制作等。
数据库维护服务	服务目标：结合下城区财政系统 Oracle 的实际情况，提供切实可行的运维建设机制，提供 7×24 小时全天技术支持服务，内容覆盖 Oracle 数据库的日常维护、紧急故障处理，软件升级等。
	对数据库的基本状况进行检查，包含 Oracle 实例状态、Oracle 服务进程、Oracle 监听进程
	检查相关的日志文件，包含：检查操作系统的日志文件，检查 Oracle 日志文件，检查 Oracle 核心转储目录，检查 Root 用户和 Oracle 用户的 email。
	检查相关 Oracle 对象的状态，包含：检查 Oracle 控制文件状态，检查 Oracle 在线日志状态，检查 Oracle 表空间的状态，检查 Oracle 所有数据文件状态，检查 Oracle 所有表、索引、存储过程、触发器、包等对象的状态，检查 Oracle 所有回滚段的状态。
	检查 Oracle 相关资源的使用情况，包含：检查 Oracle 初始化文件中相关的参数值，检查数据库连接情况，检查系统磁盘空间，检查 Oracle 各个表空间使用情况，检查

	一些扩展异常的对象，检查 system 表空间内的内容，检查对象的下一扩展与表空间的最大扩展值。
	检查 Oracle 数据库的安全性，包含：检查系统安全信息，定期修改密码。
	检查当前 crontab 任务是否正常，检查 Oracle Job 是否有失败，监控数据量的增长情况，检查失效的索引，检查不起作用的约束，检查无效的 trigger。
	定期对数据库进行性能优化。
	利用工具采集系统运行时的各项监控数据。
	分析系统主要的性能瓶颈。
	分析系统、网络、应用软件及数据库等各方面资源的使用情况。
	确定系统性能现状及性能调整的目标。
	定位系统中出现的性能瓶颈。
	测试验证改进方案，提供数据库性能优化方案报告。
	为了保证数据库系统的数据安全性，降低各种故障、灾难给客户带来的数据丢失，根据客户系统实际情况，协助客户规划实施符合客户工作要求的完善的备份恢复方案，以确保客户数据库系统的安全可靠运行。
	运维服务过程中，由于硬件的原因或其它一些外在因素需要对数据进行迁移，包括迁移到更加高级的主机上、迁移到远程的机房上、迁移到不同的平台下，提供相应的数据库迁移服务。
高级整理层服务	针对下城区各业务系统开发项目提供定量、定性分析等高级整理层服务。
	分析项目业务特点和业务流程，辅助驻场部门完成需求分析和整理，以及与区数据资源局、应用开发商、集成服务商等单位的协调与沟通，反馈问题与意。
	根据政府“最多跑一次”、“数字化转型”等业务需要，完成全区各类信息化相关信息采集，形成详细的工作日志及时整理和上报。
	针对各类采集汇总的信息数据进行定量定性分析，输出日/周/月/季度/年度分析结果报告。
	结合下城区信息化项目管理办法，通过项目群工作日报与工作交流内容等多方面途径，采集、跟踪、监管重要信息化项目的工作进展，根据需要定期通报项目进展情况。
	完成省市下达的“政务服务网”相关实施推广工作，包括与省市区相关职能部门协调对接、业务学习、信息更新、部门问题咨询解答、问题处置、数据对比统计分析等。
	区数据资源管理局业务培训、会议组织、工作分配、日常管理与制度编纂等工作。
	区数据资源管理局交办的其他工作。
5×12 即时客服	承担全区“最多跑一次”线上服务平台“1CALL”平台用户在线咨询回复的值守工作（线上）。
	承担下城区重点项目如“城市大脑”、“数据安全”等即时咨询和解答服务，针对部门、街道等相关办事人员提出的问题给与及时答复。
	承担全区信息化问题求助中心 Helpdesk 问题接报和处置，分别通过来电接听和在线

	咨询承接各类信息化软硬件故障、问题、咨询请求，及时指派软硬件维护人员进行解答和处置，并做好记录与反馈。
	工作时间：工作日 5×12 小时，早晨九点至下午九点。
服务期限	一年。后续年度经采购人考核合格后另行续签合同。

2.2 短信服务

提供 100 万条可发送移动、联通、电信手机的短信发送量，发送成功率需高于 90%，未发送完的短信量可延续到下一年度。

3 网络与安全

3.1 网络安全防护升级及存储服务器资源扩充

3.1.1 万兆交换机

技术指标	技术指标要求
接口要求	≥24 个 1/10G SFP+端口，≥8 个千兆电口
性能要求	交换容量≥2.5Tbps,转发性能≥370Mpps
MAC 地址表项	≥128K
VLAN	≥4k
功耗	整机功率≤130W
电源	双交流电源
二层协议	支持 STP/RSTP/MSTP，支持 IEEE 802.3x、802.3ad、802.1P、802.1q ，支持 MAC 地址黑洞
VLAN	支持 port-based VLAN (4k VLANs) ，支持 MAC-based VLAN ，支持 QinQ, Selective QinQ ，支持 VLAN Mapping ，支持 GVRP
IPv4 路由协议	支持静态路由、RIP v1/v2、OSPF v1/v2、BGP，支持策略路由，支持 VRRP
IPv6 路由协议	支持静态路由、RIPng、OSPFv3、BGP4+，支持策略路由
组播	支持 IGMP Snooping v1/v2/v3, MLD Snooping v1/v2 ，支持 IGMP v1/v2/v3, MLD v1/v2 ，支持 PIM-DM, PIM-SM
ACL	支持 L2 ~ L4 包过滤，支持基于五元组的流分类
QoS	支持 CAR (Committed Access Rate) ，支持每端口 8 个队列，支持 Weighted Fair Queuing ，支持 Strict Priority (SP), Weighted Round Robin (WRR)， SP+WRR ，支持 packet redirection
安全	支持 Portal, MAC address-based ,AAA, Radius 802.1X 认证，支持 port isolation 和 PVLAN，支持 IP+MAC+port 绑定，支持 ARP detection
高可靠性	支持 FRRP 快速环网恢复协议、FLRP 快速链路恢复协议，支持 VRRP
▲质保与服务	三年免费质保

3.1.2 万兆模块

技术指标	技术指标要求
基本要求	SFP+万兆光模块，多模，（850nm，0.3km，LC）
▲质保与服务	三年免费质保

3.1.3 存储光纤交换机

技术指标	技术指标要求
★基本要求	24 端口光纤交换机，开通 24 端口，8Gb/s 速率，含 Web tools、Zoning、EGM 软件授权；支持级联，机架套件。
光纤模块	配置 24 个 8GB 光纤短波模块
管理软件	配置高级 Zone 管理软件，支持 web 界面管理
▲质保与服务	三年免费质保

3.1.4 互联网出口防火墙

技术指标	技术指标要求
★兼容性	必须完全兼容现有的互联网出口深信服万兆防火墙，实现 HA 热备和数据同步，并支持故障自动切换。
性能配置	网络层吞吐量 16G，应用层吞吐量 4G ，并发连接数 250W，新建连接数（CPS）25W，SSL VPN 接入数（最大）1000 个，SSL 最大加密流量 400M，IPSec VPN 隧道数（最大）1000 个，IPSec VPN 加密速度 600M； 2U 尺寸，1T SATA 硬盘，冗余电源，6 个千兆电口，4 个千兆光口，2 个万兆光口。
部署及网络特性	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式，支持链路聚合功能，支持端口联动。
基础功能	能够识别应用类型超过 1200 种，应用识别规则总数超过 3000 条。
	支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。
	支持基于应用类型，网站类型，文件类型进行流量控制，支持基于 IP 段、时间、国家/地区、认证用户、子接口和 VLAN 进行流量控制。
	访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。
	支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施。
DoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测。
	支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为。

内容安全	内置病毒样本数量超过 200 万； 支持应用协议命令级控制，如 FTP 可细化到 rmdir、get、put 等命令级控制； 支持压缩文件查杀。
	支持从多维度聚合分析主机的中毒情况，并根据主机的夜间外联次数，恶意访问 IP 分布，云鉴情报等多个维度。
	支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告。
入侵防护	为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在 7400 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号，参考信息和建议的解决方案。
	为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。
Web 应用安全防护	具备独立的 Web 应用防护规则库，Web 应用防护规则总数在 3500 条以上。
	支持对 web 页面黑链进行检测。
	支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等。
	支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护。
	支持对已经植入 webshell 后门的服务器持续检测，对后续非法的通信动作进行识别和阻断。
	设备具备 web 业务自学习能力，可自行判断与标记业务特征，确认业务模型学习趋势。
僵尸主机检测	设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在 60 万条以上。
	支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址。
	支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。
	支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址。
安全可视化	支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别。
	支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息。
	支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险。

	支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证。
安全管理中心	为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。
	支持与 EDR 产品实现联动，当防火墙发现僵尸网络或者勒索病毒违规向主控端连接时，可实现防火墙联动 EDR 对终端进行扫描和取证，对威胁进行隔离、处置。
	支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置。
	支持 SD-WAN 智能选路功能。
	支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.5 Tap镜像分流设备

技术指标	技术指标要求
★基本配置	标准机架式结构；
	提供 8 个固定千兆电口，支持 4 路串接 GE/FE 电口接入；提供 8 个 SFP 千兆接口，SFP 接口可支持 1000BASE-LX/1000BASE-SX/1000BASE-T 等多种介质 SFP 模块，可支持分光采集器输出后的链路接入；
	提供 10/100/1000M 自适应带外管理端口及一个串口 CONSOLE 管理接口；
	设备支持交流 220V 或直流-48V 供电，配置双电源冗余供电；
基本功能	接收交换机镜像端口或分光采集器的 GE 接口输出的克隆数据，对接收的数据进行复制、汇聚、过滤、处理并从自定义端口输出给后端分析设备；
	设备的所有端口均可以灵活配置为输入输出，可以设置为 1:N、M:N、N:1 等模式；
	可根据数据报文特征，对采集流量进行有效过滤，只将满足条件的流量分发给后端分析工具，过滤条件支持 L2-L4；
	设备基本管理功能。支持本地管理功能；支持通过远程登录方式进行管理；必须支持 HTTP WEB 界面完成系统支持的所有功能配置，同时支持基于 SSH 或 TELNET 命令行方式的远程管理功能；
	设备 GE 端口线速流量不丢包（64 字节到 1518 字节）， 设备支持 7*24 小时的稳定运行，交换背板处理性能不低于 16Gbps；
特性功能	可通过 WEB 图形方式查询系统时间、运行时间、软件版本信息；
	支持端口曲线图流量统计，以流量曲线方式实时展现端口的收发性能状态；
	支持端口表格流量统计，至少包含当前发送报文数、当前接收报文数、当前发送字节数、当前接收字节数、接口当前发送/接收速率等统计指标，并支持一键清空统计流量；
	支持端口面板图形化显示，当鼠标移至任一端口上，可直观展现前面板所有接口

	的 LinkUP/LinkDOWN 状态、接口字符串描述、接口当前速率、SFP 模块插入/拔出状态，接口当前发送/接收报文计数信息；
	设备在配置任意输入输出策略及规则时均可达到 64 字节小包线速不丢包性能；
	系统支持基于 WEB 的配置文件的导入和导出功能；
	系统支持基于 web 方式的远程在线升级功能；
	设备基本管理功能：系统支持本地日志记录和 syslog 服务配置，系统支持 SNMP V1/V2/V3 协议管理；
	接口流量溢出告警提示--即该端口的峰值发送或接收速率接近于接口线速（接口物理带宽值 95%以上）速率时，则在接口状态统计当前行标记用以提示用户。在用户点示清除所有时，则清除掉该标记显示；
★重要功能	支持单纤输入输出及复用功能。即光接口在仅插入接收方向单纤时能够成功 Link 并采集流量，在端口通过单纤输入采集流量时同时能够通过同一端口单纤输出流量；
	数据类型。支持 VLAN 封装及 MPLS 封装的数据转发。支持透明转发以太网控制帧及 BPDU 流量；
	基本流量复制汇聚功能，可将采集的一路或多路网络流量进行复制并分发给不同的工具处理，可将通过不同网络端口采集的网络流量进行汇聚，并分发给单台工具处理，可将采集的多路网络流量进行汇聚之后同时复制成多份输出给不同的工具处理；
	流量过滤输出。可根据数据报文特征，对采集流量进行有效过滤，只将满足条件的流量分发给后端分析工具，其过滤条件应支持以下维度： 1）支持基于报文采集来源端口、五元组标准协议域、源/目的 MAC 地址、IP 碎片标记、传输层端口、TCP 标志位、以太网类型字段、VLANID 等对流量进行分类过滤转发； 2）过滤条件支持一个或多个条件灵活搭配组合的配置模式； 3）单台设备需支持不少于 2000 条过滤规则； 4）在配置基于规则的过滤采集输出时，规则条数不影响系统性能，均能达到 64 字节小包线速处理能力；
	输出处理功能：支持对分类流量进行各种策略的负载均衡分发，需至少支持以下两种： 1）支持哈希分流负载均衡方式输出； 2）支持基于过滤规则的报文分类输出；
	IPV6 规则支持。设备应支持 IPV6 地址、协议号、IPV6 流标签等 IPV6 报文的规则进行分类过滤；
	动态负载均衡在执行分流负载均衡输出时，在同一端口组内的任一端口失效（DOWN）后支持将流量自动分配至组内其它正常（UP）端口，不需要人工干预重配置；
	Span 镜像端口隔离功能。在端口被配置为镜像输入采集模式时，各镜像输入端口之间应互相隔离，避免产生环路；

	应支持 link-reflect 功能，即网络侧一端 down 后会反射状态到另一侧；
▲质保与服务	三年免费质保

3.1.6 安全态势感知系统

技术指标	技术指标要求
硬件指标	1、系统：产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时； 2、系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改。 3、处理器：采用当前 Intel E3 或 E3 以上 CPU，至少 4 核 4 线程，主频至少 3.1G； 4、内存：≥8GB DDR3 1600Mhz； 5、电源模块：具备冗余热插拔双电源； 6、硬盘可用容量：≥1TB，1T*2，支持 RAID1，最大支持扩展到 4T*2 硬盘。 7、网络端口：支持监听接口扩展；配备至少 2 个千兆电口管理口 支持千兆网络环境下的监听能力，标配至少 2 个千兆电口和 2 个千兆光口 支持最大扩展至 4 电 4 光或 8 电或 8 光共 8 个千兆以太网口。
处理能力	1、审计性能：能够稳定、流畅地同时支持 8 数据库数审计能力，不会产生漏审； 2、峰值处理能力：≥20000 条/秒； 3、审计日志检索能力：≥1500 万条/秒；
部署方式	为适应各种复杂的部署环境，产品部署模式上应满足以下的要求： 1、旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计； ★2、支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；提供国家权威检测机构检测报告。 3、支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询； 4、管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展； 5、管理中心和探测器直接的数据传输速率、时间、端口都可自定义； 6、支持与大数据平台部署和对接，支持审计数据外送至大数据平台。
协议支持	为审计和防护不同类型、不同版本的数据库，产品支持以下： 1、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 六种主流数据库审计； 2、支持 PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计； 3、支持 MongoDB、Hbase 非关系型数据库审计； 4、支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM； 5、支持对 SQLserver（2005 及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护； 6、支持对各种协议自动识别编码及在 web 界面手工配置特定编码
审计功能	为满足对数据库操作行为审计，满足业务、安全等方面的需求，产品满足以下的要求： 1、支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；

	2、支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小； 3、支持跨语句、跨多包的绑定变量名及绑定变量值的审计。
智能发现	为更加便捷使用数据库审计，数据库审计需具备以下功能： 1、自动识别流量中存在的数据库 2、支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告；
应用关联	为了更好的完成追踪溯源，数据库审计产品需要具体三层关联功能，要求如下： 1、支持 B/S 业务系统三层关联审计； 2、支持通过部署 agent 实现 java web 环境 100%准确关联 3、支持旁路自动学习三层审计关联功能
安全审计	为发现数据库中不安全访问行为及审计数据二次泄露等问题，数据库审计需满足以下功能： 1、支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义； 2、内置安全特征库不少于 300 条，如 SQL 注入、缓冲区溢出、弱口令等； 3、可自定义审计规则，审计规则至少支持 18 个条件； 4、规则各条件之间支持与或非逻辑关系； 5、告警数量需支持最大告警数量限制，超过告警阈值之后便不告警； 6、告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理；
审计查询	为满足审计追踪溯源、分析安全问题等需求，数据库审计应满足以下的查询需求： 1、具有高效的查询性能，后台采用 SPHINX 全文检索引擎检索； 2、查询条件易于使用，审计查询条件均为非正则表达式形式进行 3、支持采用部分匹配模糊查询方式检索审计日志 4、支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询；
统计报表	为满足事后分析需求，数据库审计满足以下的需求： 1、系统提供内置多种报表模板库，内置的报表不少于 35 种； 2、报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告； 3、支持按照数据库访问行为生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为； 4、支持按照时间曲线统计流量、在线用户数、并发会话、DDL 操作数、DML 操作数、执行量最多的 SQL 语句等报表； 5、支持性能分析，准确提炼出 SQL 语句执行频率和执行时间异常的报表； 6、支持 Word、PDF、ppt 等格式的报表导出； 7、支持报表自定义，自定义的条件不少于 20 个；
模型分析	为了更加智能发现数据库安全问题，产品具备以下功能： 1、支持对数据库自动建模及智能对异常行为告警功能； 2、可通过行为轨迹图方式展示数据库访问行为；

	3、可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警； 4、可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况；
数据管理	为满足数据备份保留的需求，产品需要具备以下功能： 1、支持根据保留天数和占用百分比自动清理最早的数据； 2、提供审计策略和系统配置信息的单独导入、导出功能；
系统管理	为增加系统管理的安全性、适应性、可维护性，产品需要具备以下的功能： 1、支持用户界面告警、Syslog、SNMP、邮件、短信、ftp 六种方式告警； 2、采用 B/S 架构管理，支持中英文两种管理界面 3、支持系统安全配置（会话锁定、超时退出、IP 地址访问控制、密码复杂性管理、验证码登陆等措施） 4、支持 NTP 时间同步、SNMP(v1、V2、V3)网络管理协议
故障排错	系统内置独立的故障排错系统，支持一键导出系统调试日志，一键检测服务、许可证、流量等常见故障；支持流量分析功能，包括抓包、包内容查看、自动探测 sql 语句等；
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.7 数据库安全审计系统

技术指标	技术指标要求
硬件指标	1、系统：产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时； 2、系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改。 3、处理器：采用当前 Intel E3 或 E3 以上 CPU，至少 4 核 4 线程，主频至少 3.1G； 4、内存：≥8GB DDR3 1600Mhz； 5、电源模块：具备冗余热插拔双电源； 6、硬盘可用容量：≥1TB，1T*2，支持 RAID1，最大支持扩展到 4T*2 硬盘。 7、网络端口：支持监听接口扩展；配备至少 2 个千兆电口管理口 支持千兆网络环境下的监听能力，标配至少 2 个千兆电口和 2 个千兆光口 支持最大扩展至 4 电 4 光或 8 电或 8 光共 8 个千兆以太网口。
处理能力	1、审计性能：能够稳定、流畅地同时支持 8 数据库数审计能力，不会产生漏审； 2、峰值处理能力：≥20000 条/秒； 3、审计日志检索能力：≥1500 万条/秒；
部署方式	为适应各种复杂的部署环境，产品部署模式上应满足以下的要求： 1、旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计； 2、支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；

	3、支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询； 4、管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展； 5、管理中心和探测器直接的数据传输速率、时间、端口都可自定义； 6、支持与大数据平台部署和对接，支持审计数据外送至大数据平台。
协议支持	为审计和防护不同类型、不同版本的数据库，产品支持以下： 1、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 六种主流数据库审计； 2、支持 PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计； 3、支持 MongoDB、Hbase 非关系型数据库审计； 4、支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM； 5、支持对 SQLserver（2005 及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护； 6、支持对各种协议自动识别编码及在 web 界面手工配置特定编码
审计功能	为满足对数据库操作行为审计，满足业务、安全等方面的需求，产品满足以下的要求： 1、支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计； 2、支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小； 3、支持跨语句、跨多包的绑定变量名及绑定变量值的审计。
智能发现	为更加便捷使用数据库审计，数据库审计需具备以下功能： 1、自动识别流量中存在的数据库 2、支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告；
应用关联	为了更好的完成追踪溯源，数据库审计产品需要具体三层关联功能，要求如下： 1、支持 B/S 业务系统三层关联审计； 2、支持通过部署 agent 实现 java web 环境 100%准确关联； 3、支持旁路自动学习三层审计关联功能。
安全审计	为发现数据库中不安全访问行为及审计数据二次泄露等问题，数据库审计需满足以下功能： 1、支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义； 2、内置安全特征库不少于 300 条，如 SQL 注入、缓冲区溢出、弱口令等； 3、可自定义审计规则，审计规则至少支持 18 个条件； 4、规则各条件之间支持与或非逻辑关系； 5、告警数量需支持最大告警数量限制，超过告警阈值之后便不告警； 6、告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理；
审计查询	为满足审计追踪溯源、分析安全问题等需求，数据库审计应满足以下的查询需求：

	1、具有高效的查询性能，后台采用 SPHINX 全文检索引擎检索； 2、查询条件易于使用，审计查询条件均为非正则表达式形式进行 3、支持采用部分匹配模糊查询方式检索审计日志 4、支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询；
统计报表	为满足事后分析需求，数据库审计满足以下的需求： 1、系统提供内置多种报表模板库，内置的报表不少于 35 种； 2、报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告； 3、支持按照数据库访问行为生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为； 4、支持按照时间曲线统计流量、在线用户数、并发会话、DDL 操作数、DML 操作数、执行量最多的 SQL 语句等报表； 5、支持性能分析，准确提炼出 SQL 语句执行频率和执行时间异常的报表； 6、支持 Word、PDF、ppt 等格式的报表导出； 7、支持报表自定义，自定义的条件不少于 20 个；
模型分析	为了更加智能发现数据库安全问题，产品具备以下功能： 1、支持对数据库自动建模及智能对异常行为告警功能； 2、可通过行为轨迹图方式展示数据库访问行为； 3、可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警； 4、可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况；
数据管理	为满足数据备份保留的需求，产品需要具备以下功能： 1、支持根据保留天数和占用百分比自动清理最早的数据； 2、提供审计策略和系统配置信息的单独导入、导出功能；
系统管理	为增加系统管理的安全性、适应性、可维护性，产品需要具备以下的功能： 1、支持用户界面告警、Syslog、SNMP、邮件、短信、ftp 六种方式告警； 2、采用 B/S 架构管理，支持中英文两种管理界面 3、支持系统安全配置（会话锁定、超时退出、IP 地址访问控制、密码复杂性管理、验证码登陆等措施） 4、支持 NTP 时间同步、SNMP(v1、V2、V3)网络管理协议
故障排错	系统内置独立的故障排错系统，支持一键导出系统调试日志，一键检测服务、许可证、流量等常见故障；支持流量分析功能，包括抓包、包内容查看、自动探测 sql 语句等；
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.8 数据库脱敏系统

技术参数	技术指标
系统架构	软硬件一体设备，标配 4 个 10/100/1000Mbps，2 个 10000Mbps 光口； 双电源，存储容量:2TB； 脱敏速度≥2000 万条/小时。
数据库类型	支持多种数据源，包括：Oracle、Mysql、Informix、DB2、MySQL 等多种数据库。
管理方式	系统基于 B/S 方式，采用 HTTPS 方式远程 WEB 安全管理，无需安装管理客户端，中文操作界面。
脱敏方式	系统支持自定义、图形化操作的脱敏规则和脱敏方式，支持 UNICODE 标准、GBK、UTF-8 等字符编码。 支持数据库到数据库、数据库到文件、文件到文件、文件到数据库等多种方式。
敏感数据自动发现	支持特定隐私敏感数据类型的自动发现功能：数据脱敏软件能够根据数据本身的特征，包括类型、长度、数据本身的编码特征、校验算法特征、语义特征等等进行数据分析、分类判断，能够分辨包含但不限于以下种类的隐私数据类型。包括：中文姓名、身份证号码、电话号码、地址、卡号、社保卡号、电子邮件、邮政编码、企业名称、工商注册号、组织机构代码、纳税人识别号。
	系统能读取数据库或 txt、csv、exce1 等文件内容，根据内容和脱敏系统内置敏感数据特征规则自动发现敏感数据。
	应支持一个单元格是由多段敏感数据组合的数据发现规则。
脱敏方案	支持自定义脱敏方案，用户可将若干脱敏策略组合成为适用于该场景的脱敏方案，脱敏方案制定后，可被重复利用。
脱敏模板	脱敏策略可以进行下拉菜单式的参数化配置，便于理解和操作。
数据子集管理	支持对源数据库中一部分数据进行脱敏，用户可指定过滤条件，对数据来源进行过滤筛选，形成数据子集。
脱敏任务管理	支持对脱敏任务进行停止、启动、重启、暂停、继续，并且支持设置计划任务、任务顺序并发，充分利用系统资源，提高脱敏效率。脱敏任务可兼容执行过程中遇到的异常情况，支持跳过异常数据继续执行任务。
脱敏资源管理	支持对脱敏设备本身的 CPU、内存进行监控,了解作业并发情况。
DDL 抽取	支持对源数据库的 DDL 进行抽取，包括源数据环境的主外键约束关系、表空间定义、触发器、过程、链接等，自动加载到目标端环境。
支持跨用户脱敏	对于 oracle、DB2 数据库，支持拥有 DBA 权限的用户，可以进行单任务多用户数据脱敏，也可实现数据库连接用户和脱敏用户不同脱敏迁移。
异常处理	对脱敏中出现的异常数据,需要有详细报告。
脱敏算法	同义替换：使用相同含义的数据替换原有的敏感数据，如姓名脱敏后仍然为有意义的姓名，住址脱敏后仍然为住址。
	部分数据遮蔽：可自定义脱敏算法，将原数据中部分或全部内容，用“*”或“#”等字符进行替换，遮盖部分或全部原文。
	数据关联脱敏：脱敏算法保持数据关联性,能够保持同一数值在不同表字段之间的数据关联性,如身份证日期部分与出生日期字段的关联脱敏。
	保留均值和方差：实现金额数据脱敏的同时均值和方差不变。

	仿真脱敏：确保脱敏后的数据可保留部分数据特征，便于将脱敏后的数据用于第三方分析机构和内部经分团队进行数据分析。
静态脱敏部署模式	无代理旁路部署：数据库脱敏设备无需在数据源安装任何代理程序，针对数据库环境仅通过 JDBC 数据接口配置、针对结构化文件脱敏,即可实现全部脱敏任务。
三权分立	为了满足脱敏平台多用户的需求,并保证各用户间的隔离性,可以针对不同用户、不同角色、不同业务系统实现任务级的权限控制，并提供系统管理员、安全管理员和审计管理员来管理脱敏设备。
自身审计	系统针对脱敏产品操作人员的操作行为进行审计记录，可以由审计管理员进行查询，具有自身安全审计功能。
用户管理权限	为了满足脱敏平台多租户的需求,并保证各租户间的隔离性,数据脱敏系统具备完善、统一的权限管理体系,可以针对不同用户、不同角色、不同业务系统实现数据行级的权限控制,完成用户建立、用户分配、用户身份验证等管理功能,满足系统用户所有资源信息具备最小颗粒度的可配置、可分配的能力,能够保证用户间的信息隔离，保证针对具体的使用用户进行分配，每个用户仅能使用其分配的资源。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.9 数据库加密系统

指标项	指标要求
规格要求	双电源，板载 6 电口，16 内存，1T 存储空间。1×扩展槽位（支持扩展：2 个万兆光/4 个千兆光/4 个千兆电/8 千兆电/8 千兆光）。
	支持对 Oracle，MySQL、sqlserver、达梦等数据库加密,支持 Windows、Linux、AIX、Solaris、Unix 操作系统，支持单表千万（记录条数)级数据规模的加密。
质量要求	产品质量管理体系符合 GB/T 19001-2016/ISO 9001:2015 标准和 ISO27001 标准，其质量管理体系产品范围为数据库安全系统的设计开发和服务。
存储加密能力	支持以表空间/数据表为单位进行数据加密，加密后的数据在数据库中以密文格式存储。密文表支持明文、密文同时存储密钥独立管理，提供对密钥的备份恢复机制；提供图形化的数据加密配置和快速恢复策略。
权限控制增强	被保护数据表的权限控制应独立于数据库的权限控制，防止数据库用户的权限提升引起的数据泄密。 实现基于密文的增强访问权限控制，防止 DBA 及高权限用户对敏感数据进行访问。 对于授权用户对受保护数据的访问能够限定到指定的 IP、应用程序，更加精确的授权和访问控制；
应用用户关联防护	能够实现应用系统和应用系统用户对数据库用户的绑定，仅允许合法的应用或应用用户使用授权的数据库用户对密文进行加解密操作。防止授权数据库用户口令泄露后，绕开业务系统，直接访问密文数据。
三权分立	实现系统管理员、安全管理员和审计管理员的三权分立。其中安全管理员通过使用安全管理工具，完成日常的加密数据配置、数据库用户的密文权限控制等安全维护

	和管理操作。 审计管理员进行审计开关的控制，检索、分析密文访问操作的审计信息工作。 系统管理员则负责进行系统配置，如 IP，端口等的配置。
性能	表空间级加密，数据库平均吞吐量相比加密前损失不超过 7%；加密后单表千万级数据规模下的全表扫描和统计分析操作的性能损失相比明文表不超过 17%。
透明性	支持 SQL、PL/SQL、JDBC、ODBC 的透明性，不需要改造； 加密后，原有主外键约束无影响，原有 check 约束无影响。 加密后，对 CDC 数据同步透明，无影响。 支持现有数据库维护工具的透明性，数据库管理员依然可以使用现有工具实现备份恢复和数据库维护。 不影响原有索引技术； 支持基于密文数据的等值和范围查询；
容灾能力	支持主、从互备，及异地灾备等多级容灾能力，支持 cdc 远程备份加密，防止主机故障、网络故障、程序故障引起的业务损失。同时各种容灾手段应能快速启用、自动切换，且切换期间能保证数据一致性，业务不受损。 主、从服务之间的切换应能在 3 秒之内完成； 提供离线解密工具，当数据库不能正常启动时，通过离线工具对密文数据文件执行解密操作，还原数据，防止数据丢失。
▲质保与服务	三年免费质保

3.1.10 数据泄露防护系统

技术指标	技术指标要求
架构要求	产品为软硬件一体化设备，内部系统采用定制 Linux 操作系统，不接受纯软件产品
性能要求	标准 2U 机架型： 标配 4*10/100/1000Mbps,1 个插槽； 存储容量:1TB； 性能：400Mbps
用户认证	支持用户名、口令本地认证方式；
数据解析	为了确保数据安全，系统需支持中文分词、正则表达式、中文编码、中文语言库等；
	为了确保数据检测更全面，系统需支持 1100 种以上文档类型识别，250 种以上文档内容解析。包含但不限于：30 种以上文字处理格式、20 种以上演示文件格式、10 种以上电子表格文件格式、10 种以上归档文件格式和 30 种以上源代码文件格式、文档标记格式、电子邮件格式、CAD、图形、OFD、ceb、cebx 等，共计达 250 类以上文件内容解析；
匹配技术	支持关键字匹配；支持关键字组匹配（按逻辑关系及出现频度）；支持正则表达式匹配；支持模式脚本匹配；
	支持点滴式泄露防护，防止多次发送少量敏感信息导致信息泄露。
	支持 OCR 图片相似度匹配，防止敏感图片通过变形后外泄

	支持文件指纹匹配；
	拥有基于用户行为和数据状态的识别技术；
	支持二维智能学习算法，帮助用户更好的梳理企业所拥有的数据，进而对数据进行分级分类；
管理功能	支持组织资源配置与管理功能；
	支持业务资源配置与管理功能、业务资源与组织资源关联管理与配置功能；
	支持中文 WEB 管理界面，无需安装任何客户端进行管理与配置；
	支持加密 HTTPS 协议管理界面，防止管理配置信息通过网络被窃取；
	支持配置受信任的管理主机，配置信任主机后管理界面将仅可以从信任主机进行访问；
	支持系统管理员、安全管理员及审计员三权分立功能，三权相互独立防止越权操作；
预置脚本	内置中国身份证识别判断脚本；
	内置银行卡号识别判断脚本；
	内置计算机信息识别判断脚本；
	内置源代码识别判断脚本；
	内置一般密码识别判断脚本；
	内置机动车驾驶证识别判断脚本；
	内置常用姓氏判断识别脚本；
	内置中文地址判断识别脚本；
地理映射功能	支持将 IP 地址（地址段）与地理位置信息进行关联，便于统一展示模块以地理位置信息展示与统计相关联事件信息；
配置信息管理功能	支持将系统资源配置、规则、策略等配置信息进行归档备份功能，方便进行快速系统恢复；
	支持利用归档的配置信息快速恢复系统，无须进行初始化，一键快速恢复系统配置至可用状态；
协议解析	系统需支持 smtp/smtps、pop3、imap、ftp、http/https、telnet 协议解析；
地址解析	对带有敏感数据的数据包解析其源地址和目的地址；
数据流向动态展示	支持对敏感数据流向以地图形式实时动态展示，不同事件严重性以五种颜色标识；
	支持网络传输敏感数据按部门和业务进行统计；
	支持网络传输敏感数据按协议类型统计；
事件审核流程	支持根据事件严重性级别，支持人工审核流程；
	支持根据审核流程，通过邮件方式通知到相应用户；
仪表盘展现	支持数据安全状态、系统维护状态的仪表盘展现；
	支持展现风格、方式定制；
事件统计和分	支持基于组织角色、业务类型、严重性、服务端 IP、客户端 IP、策略、规则组、规

析	则、状态等事件的跟踪和统计；
	支持基于角色的系统维护事件和系统事件分析；
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.11 服务器深度安全防护系统

技术指标	技术指标要求
虚拟化平台支持	产品无代理防病毒、入侵防御功能支持如下虚拟化平台： - VMware - 华为 FusionSphere（Xen，KVM） - 华三 CAS （3.0, 5.0） - 品高云（7.x） - Citrix Xen Server （6.x，7.1） - 微软 Hyper-v 产品支持以上虚拟化平台的统一平台管理。
公有云平台支持	产品可以支持公有云环境部署；
病毒防护	产品防恶意软件功能要求和虚拟化环境以无代理方式集成，不需要在每台虚拟机上安装客户端，以便减少对物理机的资源占用；主机整体资源与搭载虚拟机数量无直接关系；虚拟资源消耗不会随虚拟机数量成长。
Web 信誉	提供 WEB 信誉功能，通过阻止对恶意 URL 的访问来保护用户和应用程序。
防火墙功能	产品具有防火墙功能，不依赖分布式交换机可以无代理运行,并且可集中控管防火墙策略，策略定制可以针对 IP,Mac 地址或通讯端口，可保护所有基于 IP 通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等）。
入侵防御功能	产品具有 DPI(深度内容检测)功能，不依赖分布式交换机可以无代理运行,可以同时保护操作系统和应用服务（数据库，Web，DHCP 等）。
完整性监控	产品支持无代理完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改。
日志审计	产品支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件，为组织提供审计证据；日志审计提供将事件转发给 SIEM 的能力，如 Splunk，Qradar, ArcSight 以及 AWS SNS。
应用程序控制	产品具备应用程序控制模块监控计算机软件变化，一旦启用应用程序控制，将会记录所有软件更改，并创建事件。检测到应用程序更改时，管理员可以允许或阻止该软件，并锁定计算机。
添加被保护的计算机	1. 添加本地网络计算机； 2. 从 Microsoft Active Directory 添加计算机组，可以从任何基于 LDAP 的目录服务导入计算机组； 3. 添加 Virtual Center； 4. 添加在 VMware vCloud 上托管的虚拟机；

	5. 添加 AWS 云账户； 6. 添加 Microsoft Azure 云账户； 7. 将客户端程序安装到 Amazon Machine Image（AMI）基于的实例上； 8. 使用部署脚本来保护大量的计算机，进行自动安装和激活客户端。
Docker 容器防护	支持各种 Docker 容器的防恶意程序和入侵防护，包括：Amazon ECS，Docker Datacenter, Kubernetes, Docker Swarm, Rancher 等。
预测性机器学习	产品的恶意软件防护功能要求支持通过预测性机器学习为未知威胁和零日攻击提供增强的恶意软件防护。使用先进的机器学习技术关联威胁信息并执行深入的文件分析，以通过数字 DNA 指纹识别，API 映射和其他文件功能检测新出现的安全风险。
实时压缩扫描	病毒制造者经常试图通过实时压缩算法来避开病毒过滤，要求产品可以阻止实时压缩的可执行文件并将它们与其他恶意软件特征进行匹配，以帮助减少此类病毒进入网络的风险。
扫描嵌入式 Microsoft Office 对象	某些 Microsoft Office 版本使用对象链接和嵌入（OLE）将文件和其他对象插入到 Office 文件中。这些嵌入的对象可能包含恶意代码，要求产品能够具备扫描嵌入式 Microsoft Office 对象的功能。
NSX 安全标签	一旦检测到恶意威胁，产品可将 NSX 安全标记应用于受保护的 VM，NSX 安全标记可与 NSX Service Composer 一起使用，以自动执行某些任务，例如隔离受感染的 VM。
入侵防御规则条目	产品要求支持6000条以上入侵防御规则，同时支持自定义入侵防护规则。
IPS 引擎	要求产品 IPS 功能使用独立的扫描引擎来处理所有规则。
SSL 支持	入侵防御支持 SSL 配置，对于入侵防御功能能够识别 https 流量，从而对计算机进行防护。
推荐扫描	产品支持推荐扫描，根据不同计算机的扫描结果自动下发对应的入侵防御规则。
数据库支持	产品自身使用的数据库应该支持外挂企业级数据库，例如：SQL Server，Oracle。
病毒库更新	1. 产品支持更新的多级部署，分流冗余节省带宽，更新速度快； 2. 产品安全升级支持 Pattern 回退； 3. 产品支持设置定时任务检查软件升级和安全升级； 4. 产品支持自定义升级某一个或者某一些客户端的病毒码，而不是只能一次升级所有客户端的病毒码。
多租户支持	1. 管理中心支持多租户； 2. 支持不同租户 widget、事件、安全策略、管理、日志文件相互隔离； 3. 支持不同租户计算机、终端、安全配置相互隔离。
异常监控与告警	产品支持不少于100种异常监控和告警规则。
系统事件	1. 产品支持不少于7000种系统事件，记录包括管理员、审计员、系统等所有审计日志； 2. 系统事件支持标记功能，根据条件自动标记事件，并可以根据标记展示和过滤时间，标记条件包括事件、事件 ID 和级别、目标、操作者、管理中心和事件起源。

报表/报告	1. 产品提供至少19个报表模板，覆盖所有功能，包括数量排名、图形展示； 2. 可指定任意虚拟机/终端、计算机组、策略、时间段和标记进行报表生成，支持定义报表保密级别，支持生成报表加密。
和 VMware Operation Manager 集成	产品支持通过 API 方式与 VMwareOperationManager 进行集成，可以提供各种事件日志在 VMwareOperation Manger 里呈现，包括： ➢ Computers Total event count ➢ ESXI total event count ➢ AM ➢ LI ➢ IM ➢ FW ➢ IPS ➢ WRS 等 TOP 10排序。
升级服务	三年免费升级和病毒库更新

3.1.12 虚拟机灾备系统

技术指标	技术指标要求
设备基础要求	3U 机架式；800W（1+1）冗余电源；两颗 64 位六核处理器；64GB 高速缓存；16 个热插拔位；硬盘容量（配备 16 块 6TB 企业级 SATA3 磁盘，7200 转，裸容量 96TB）；2 个千兆以太网接口；2 个多模光纤万兆以太网口。
	中转保护设备，用于高性能环境下快速中转保护虚拟化环境的数据。2U 机架式，550W（1+1）冗余电源（80PLUS 金牌认证），64 位四核处理器，内存 32GB；2 个企业级固态缓存；提供 2 个千兆以太网接口。8Gb 目标模式双端口光纤通道卡；2 个多模光纤万兆以太网口。
	设备系统基于存储专用的 64 位 UNIX 嵌入式系统，存储系统及软件功能预装在独立的存储介质中，不占用 RAID 硬盘组的存储空间。
	支持通用 RAID 0、1、5、6、50、60 等多种 RAID 方式，同时具备三重数据校验技术，即三块硬盘同时损坏数据不丢。
	备份容灾一体化设备，应支持备份、持续数据保护、存储、NAS、虚拟带库、虚拟主机等功能。
	支持的数据本地复制，以及到任一台备份设备的远程复制；支持接收 NAS 设备远程复制过来的数据。
	支持目标端在线重复数据删除功能，在数据存储时实时完成重复数据删除处理，不占用额外硬盘空间，不增加后期处理操作。不占用数据源端服务器处理资源，开启重删后，对设备本身的 CPU 资源占用要小于 10%，可随时开启或关闭重删功能。为保证数据源端的资源安全，不接受数据源端、服务器端的的重删方式。
	提供本地快照保护功能,保留历史数据副本，当发生蓝屏、病毒入侵、误删除数据等逻辑错误时，通过调取历史快照副本快速恢复业务。快照时间间隔可通过界面由用户设定，分钟级快照颗粒度；快照数量针对每个卷/分区授权许可不低于 4000 个。

备份功能支持	支持 Windows、Linux 及 Unix 操作系统下的文件或数据库在线备份。
	支持不同平台下 Oracle、Oracle RAC、Sybase ASE、Sybase IQ、SQL Server、DB2、Exchange Server、Lotus、MySQL 等国外数据库备份及恢复。
	支持人大金仓、武汉达梦、南大通用、神州通用等国产数据库备份及恢复功能。
	支持 HP 安腾平台下的文件及数据库备份与恢复。
	支持打包备份功能、备份任务自动拆分处理功能，可针对细碎文件进行有效的备份处理，并支持对各种数据库进行脚本备份功能；
	支持 Oracle、Oracle RAC 的备份，在数据库服务器上无需安装任何客户端程序，即可实现数据备份。支持采用多通道备份方式，实现单一备份任务可并行多条备份通道进行数据备份，最大发挥高速网络（如万兆）和存储性能。备份工作支持完全、增量、差异等策略，最短备份间隔可缩短到每分钟进行一次数据备份。备份脚本可自动生成，支持按照实际需求手动编写备份脚本功能。
	支持对 VMware 的备份恢复，通过 vSphere API 进行 VMware 虚拟机的完全和增量备份恢复，无需在 Vcenter 服务器或中转服务器上安装任何代理，即可实现数据备份工作。支持多种级别的备份，包括：数据中心、ESXI/Cluster、vApp、虚拟机、虚拟磁盘等方式，能够支持数据并发备份，并发方式按照 ESXI 与虚拟主机的数量进行并发，支持备份完成后自动删除快照功能。
	能够灵活定制备份策略，如具有定时备份功能，能够自主地设定数据库、文件备份的策略，具有完全备份、增量备份、差分备份功能；提供时间和多种计划触发机制，实现任务计划的灵活性；
	支持远程备份，采用多主控模式，各主控能独立工作；支持断点续传、脱机备份、双向缓冲、流量控制等有效的广域网数据备份技术，减少网络通信流量，提高数据传输的稳定性和高效性；并可实现一对一、一对多、多对一、多对多的备份方式；
	能够提供操作系统的裸机恢复功能，能够对业务系统的操作系统进行手动备份和计划性在线增量备份，备份时不需要关机或重起，当操作系统意外损坏时，能够通过将 Window/linux 操作系统迅速恢复到之前备份的状态，而不需要重新安装操作系统；
	支持 FC SAN 网络中异构平台下的多台服务器 LAN-Free 备份功能，支持以虚拟磁带库（VTL）或者物理磁带库作为 LAN-Free 的备份目标，不接受采用基于磁盘预先划分固定分区方式实现。支持同一存储空间（虚拟/物理磁带介质）被 Windows、Linux 和 Unix 主机共享使用。
虚拟带库功能	可将内部磁盘空间仿真为磁带设备，通过 FC-SAN 或 IP-SAN 连接到网络，可供自身备份功能或者第三方备份/归档应用程序使用。
	设备支持虚拟磁带库功能。
	可虚拟出多种品牌的磁带库。包括：Oracle/SUN/STK、IBM、Quantum、Spectra Logic 等主流磁带库。
	可虚拟磁带库数量≥128、虚拟磁带机数量≥1024、虚拟磁带数量≥65536。支持 HP LTO-4 LTO-5 磁带机、支持 IBM LTO-4 LTO-5 磁带机。最大连接备份主机数:无限制;
持续数据保护要求	基于块存储级别的持续数据保护（CDP）技术，产品采用旁路接入架构设计，在原有服务器到存储的数据路径中不需要加入设备，彻底避免设备本身故障造成生产存储

	访问中断的风险可能性。设备在部署时不应改变现有系统环境架构，不会导致生产停顿或业务数据丢失，无需迁移数据。
	持续数据保护的目标设备为块设备，链路必须支持 iSCSI 和 FC 方式，不接受 P2V 文件的方式进行持续数据保护工作，支持 Windows、Linux 等 X86 环境下的持续数据保护工作，支持 AIX、HP-UX、Oracle（sun）solaris 等 Unix 环境下的持续数据保护。
	可对业务系统的每个写 I/O 操作（精确到毫秒）进行记录，同时产生连续的无限数量恢复点，当系统出现故障后可恢复至任意选定时间点，不接受精确度在分钟级别或秒级别的保护方式。支持数据写入生产存储和 CDP 设备保持完全同步，在故障时两端数据差异不超过 1 个 I/O。
	支持生成无限数量的 Oracle、SQL Server 等应用数据的一致性恢复点，最小间隔可达 1 秒，不接受限定数量的快照。
	支持存储设备的灾难接管功能，当被保护的存储设备（包含服务器内置存储以及外接存储）发生故障损坏后，可将 CDP 设备的目标磁盘直接挂载前端服务器，接替故障存储使用。 在 AIX、HP-UX、Oracle（sun）solaris 等 Unix 环境下，需实现主存储故障时的本机零中断无缝接管（RPO=0，RTO≈0）。支持挂载到本机或者另外的物理/虚拟服务器用于存储接管。
	设备能提供对虚拟化环境的持续保护，包括：VMWare、CAS、FusionSphere、Microsoft Hyper-V、KVM 等，保护方式须为基于块设备的持续数据保护。
	配置远程数据复制功能，可将本地 CDP 数据以数据块级别的增量方式复制到灾备中心；复制对象可自定义选择块设备，数据传输支持断点续传、加密、压缩、限时传输、重删后数据复制等策略。远程复制过程中，可实现自动同步或按策略同步方式。
	支持在持续数据保护正常运行的情况下，将对目标磁盘的多个历史数据状态的快照挂载到其他物理主机上，挂载方式同样为 iSCSI 和 FC 方式，不接受 NFS、CIFS 方式，其他主机可针对快照进行读写操作，能够在不影响数据保护正常运行的情况下，用于灾备演练、数据分析和测试等用途。
	支持在持续数据保护正常运行的情况下，能够对目标磁盘的多个历史数据状态的快照，可直接生成虚拟化文件，直接将被保护主机快照转换为 VMware、Hyper-V、VirtualBox 等虚拟机磁盘镜像格式，可将磁盘镜像文件映射到虚拟主机上， 虚拟主机可针对虚拟机映像文件进行读写操作，能够在不影响数据保护正常运行的情况下，用于灾备演练、数据分析和测试等用途。
	复制到远程目标设备的数据，必须与本地设备一样为块设备，应包含快照、历史 I/O 记录和一致性恢复点，可用于回滚、挂载。异地灾备设备的块设备属性与本地设备的块设备属性需完全一致。
	支持保护大于 2TB 的 GPT 磁盘，CDP 最大可保护 900TB 以上的单个 LUN。
	支持保护 Windows、Linux 操作系统，并在系统盘损坏时直接从容灾设备历史点数据启动，支持 FC 光纤、iSCSI 等多种 SAN Boot 方式。
虚拟化保护	支持华为、华三云平台实现无代理备份，支持深信服云平台、超融合平台实现容灾备份。
	支持 Vmware vSphere ESX/ESXi、Microsoft Hyper-V、KVM、CAS、FusionSphere

	等主流虚拟化应用保护。
	支持对 Vmware vSphere ESX/ESXi 虚拟化的保护，且在保护过程中，无需在任意虚拟机中安装任何客户端代理
	在对 VMWare 的保护过程中，支持 CBT、SDK、CDP 等多种备份方式。
	支持 SAN/vSAN 环境下的 Lan-Free 备份，减少备份过程中对于业务网的占用。
	支持备份任务并发，能够同时备份多个 ESXI 上的各自的虚拟机，或单台 ESXi 上的多个虚拟机，在单个任务下实现多个 ESXI 或多个虚拟机同时发起备份。
	支持永久增量备份，只需要进行一次初始化的全备份，其余备份全部采用增量备份方式；并且要求，在进行了多次备份作业后，VMWare 的性能不降低。
	支持备份集的自动合并功能，要求在一份完整备份基础之上，将后续每次的增量数据与完整数据自动合并，合并成一份最新的完整数据，节省存储空间占用。在备份集合并之后，要求保留历史时间点的数据。
	为保证 VMware 虚拟机的性能稳定，在 VMware 虚拟机快照记录中最多保留 2 个快照点。
	能够从备份设备的备份文件快速启动虚拟机用于生产，而无需将备份文件先恢复到生产存储。
	支持 VMware 虚拟机的挂载功能，在原有虚拟机故障后，无需数据恢复过程，可将任意备份快照点挂载启动。支持单虚拟机粒度挂载，并支持虚拟机挂载后是否自动开机和联网。
	支持瘦模式和厚模式磁盘分配的虚拟机。
	根据不同的网络环境(SAN, LAN, WAN)可自定义数据去重的块大小。
	提供无限数量的历史恢复点，可供 ESXi 进行恢复选择。
	支持以数据中心模式、VMware 集群模式、vAPP 模式、/虚拟机模式以及虚拟磁盘模式提供 VMware 数据备份，实现针对 VMware 环境更加准确的保护。
	支持多种备份介质，包括磁盘阵列、虚拟磁带库、NAS、物理磁带库等。
	管理控制台的可完全独立于备份服务器之外，用于在笔记本电脑和台式机上，而无需与备份服务器之间建立远程桌面协议 (RDP) 会话。
	支持备份集的自动合并功能，要求在一份完整备份基础之上，将后续每次的增量数据与完整数据自动合并，合并成一份最新的完整数据，节省存储空间占用。在备份集合并之后，要求保留历史时间点的数据。
	支持 CAS 虚拟机的挂载功能，在原有虚拟机故障后，无需数据恢复过程，可将任意备份快照点挂载启动。
	提供无限数量的历史恢复点，可供 ESXi 进行恢复选择。
	支持备份任务并发，能够同时备份多个物理主机上的各自的虚拟机，在单个任务下实现多个物理主机同时发起备份。
数据保护 CDM 备份方式	支持 Oracle、Oracle-rac、SQLserver、MySQL、Sybase8T、PostgreSQL、恒辉等数据库的定时备份。
	支持采用多通道备份方式，实现单一备份任务可并行多条备份通道进行数据备份，最

	大发挥高速网络（如万兆）和存储性能。
	针对 Oracle RAC 的备份，支持多节点、多通道并发备份方式，不接受单一节点备份方式，最大发挥高速网络（如万兆）和存储性能。
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台的永久增量备份。
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台任意备份时刻的 5 分钟内快速挂载恢复，且挂载恢复的虚拟机文件应为完整的不含历史快照的文件集。
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台同一备份时刻可生成无限制数量的快照副本，且所有快照副本可同时挂载给不同或相同的生产系统满足使用需求。
	支持 VMware 多种级别的备份，包括：数据中心、ESXi/Cluster、vApp、文件夹、虚拟机、虚拟磁盘等方式，能够支持数据并发备份。
	支持 Oracle、Oracle-rac、SQLserver、MySQL 等主流数据库同一备份时刻可生成无限制数量的快照副本，且所有快照副本可同时挂载给不同或相同的生产系统满足使用需求。
	支持文件及操作系统的永久增量备份。
	支持文件备份的过滤功能，提高备份效率，节省备份空间。
	支持 Oracle 数据库 BCT （Block Change Tracking）数据保护模式，且支持用户自定义快照合并周期。
	支持 1 对多，多对 1，多对多的远程灾备功能，且所有节点的远程灾备计划任务在同一界面即可配置完成。
权限管理	设备支持三权分立管理，可分为系统管理员、安全保密管理员和安全审计员，系统管理员负责创建和删除用户，进行系统维护；安全保密管理员负责设置所有用户的密码保存周期，重置用户密码，对普通用户进行授权，能够查看系统日志、用户日志和安全审计员日志；安全审计员用户名负责对系统管理员日志和安全保密管理员日志进行审计。
授权许可	内嵌备份功能主模块；含 96TB 备份授权； 配置相应数量的磁带驱动器使用授权；配置无限数量的数据迁移器使用授权； 配置远程备份代理模块；配置备份对象复制选件； 配置场地授权的 Windows、Linux 版本的文件代理模块，操作系统代理模块和数据库代理模块； 含 FC 磁盘阵列功能，iSCSI 磁盘阵列功能，NAS 功能，虚拟主机功能。 内嵌 Windows、Linux 环境下 CDM 高级备份模块。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.13 存储扩展单元

技术指标	技术指标要求
★灾备系统升级要求	对当前在用的柏科数据 Rorke RD580 存储系统进行升级扩容：包括 EXP 扩展单元，硬盘，容量扩展、分区许可、存储虚拟化管理许可等，必须完全兼容现有存

	储。
扩展单元	存储扩展单元，内部无线缆连接，冗余电源，冗余风扇，机架套件
硬盘	配置 24 个 1.8TB 10K SAS 硬盘，含硬盘托架及适配器
许可	配置磁盘存储系统 43.2TB 的容量扩展许可、虚拟化管理许可 48TB，实现存储的虚拟化和统一管理。
SAN 存储加速	可通过 SAN 存储加速功能监控磁盘的访问模式，然后自动将频繁访问的热点数据提取到 SSD 等高性能磁盘组成的缓存中以加快读取速度,从而加速随机访问及整体 I/O 的读取速度，提供热点数据资源策略和访问统计信息的功能截图。
卷共享	配置六个节点的 ImageSAN 卷共享 Volume Share 功能。
存储管理和异地容灾	须兼容现有柏科 VRD 系列存储虚拟化设备和存储设备，支持现有的存储虚拟化平台统一管理和调度，无须额外的协议转换设备和第三方软硬件设备，无需二次开发，可在本地或异地进行集中灾备和统一管理。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.1.14 通配符版DV SSL证书

技术指标	技术指标要求
基本要求	Digicert+Symantec 交叉认证 PKI 体系下签发证书，保护一个带通配符域名（该*号同级别的全部明细域名）;为所有主流的浏览器和移动设备所信任;可同时保护 www. 和非 www. 网站；拥有网站安全签章。
证书有效期	1年

3.1.15 硬盘

技术指标	技术指标要求
规格	1.2T SAS 10K企业级硬盘，含硬盘托架及适配器。数量：12个
兼容性	必须兼容现有柏科RD6810F存储阵列。
▲质保与服务	三年免费质保

3.1.16 服务器内存

技术指标	技术指标要求
规格	VMware虚拟化资源池服务器内存扩容。共336GB，要求必须与原服务器内存兼容。
▲质保与服务	三年免费质保

3.1.17 蓄电池监测系统

技术指标	技术指标要求
串口服务器	数量 1 台，IU 机架型

温湿度探测器	数量 3 个
检测模块（测内阻）	数量 160 套
电流模块	数量 4 套
转换模块	数量 4 套
蓄电池系统软件接口模块	数量 1 套
数据中心监控管理软件扩容	数量 1 套
管线材等辅料	数量 1 批，国产
▲质保与服务	三年免费质保

3.1.18 蓄电池更新

技术指标	技术指标要求
规格	12V/100AH电池
▲质保与服务	三年免费质保

3.1.19 机房地插升级

技术指标	技术指标要求
规格	32A工业连接器
▲质保与服务	三年免费质保

3.1.20 运维操作间装修

序号	名称	配置描述	单位	数量
1	网络设备迁移理线	3 汇聚柜网络设备迁移理线	项	1
2	防静电地板敷设（无边）	600*600*35mm	㎡	33
3	踢脚线	密度板基础板、不锈钢饰面	m	24
4	市电国标插座安装	10A/86 型	套	11
5	电线穿管线	ZR-BVR4mm2	卷	3
6	KBG25 管安装	KBG25 管安装	m	150
7	金属软管安装	直径 25 金属软管安装	m	30
8	机柜	42U 标准机柜，前后网孔门	台	7
9	机柜专用 PDU	12 孔，输入 16A，输出为 10A	条	6
10	机柜插座电缆	ZR-RVV3*4mm2	米	150

11	工业连接器	3P/16A	套	6
12	曹氏桥架	200*100	米	20
13	六类双绞线缆	全铜六类双绞线缆	箱	5
14	六类面板模块	每个工位 3 个信息点、RJ45	个	33
15	桌面面板	单/双孔	个	22
16	24 口配线架（含模块）	24 口配线架（含模块）	只	1
17	理线架	1U 理线架	只	1
18	PVC 线槽	白色方形 PVC 线槽	m	30
19	86 型接线、分线盒安装	86 型	个	50
20	标签制作	标签制作	项	1
	▲质保与服务	三年免费质保		

3.2 财政系统网络安全等级保护改造

3.2.1 IPS

指示项	指示要求
基本要求	要求采用先进的多核网络专用架构多核硬件平台，x86 多核处理器，非 MIPS 的多核架构或 ASIC 架构；
	为保证日志记录与攻击证据保留存储于读写速度，磁盘有碎片不会影响系统的性能，采用专业 SSD 固态硬盘存储日志等其他数据，非 SATA 普通硬盘；
	采用 19 英寸标准 1U 机架机箱；含 3 年攻击特征库升级许可，1 年网站知识库升级许可，≥10 个 10/100/1000BASE-T 接口,其中≥3 对支持 Bypass; 单电源；
性能要求	IPS 吞吐率：≥1Gbps
系统要求	设备符合中华人民共和国网络安全法，自身操作系统必须具有完全自主知识产品，且采用专用的安全操作系统，使用多核平台，实现并行处理技术；
	支持备份操作系统与主操作系统软件并存，防止设备或配置出现问题造成的网络中断，充分保证系统的稳定性；为适应安全形势的发展，在网页配置界面不能设置系统切换，要在设备启动时进行多系统选择；
	为适应现代网络发展的需求，提高病毒防御的防御性能，可以支持后续能够扩展支持病毒防御功能；
	能够通过将多个处理器内核并行区分，从而提高设备处理性能；
接入模式	支持直连模式、路由模式、虚拟局域网模式、旁路监听模式等多种接入模式。支持源地址和目的地址、接口的策略路由；
	支持链路聚合技术，链路负载不少于十种算法，可动态探测链路响应速度并选择最优链路进行转发；
部署环境	支持 VLAN、MPLS、PPPoE 网络，能够在该网络环境中检测出攻击事件；

	支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络，能够在该网络环境中检测出攻击事件。提供产品通过 IPv6 测试认证证书；
流量采集	支持流量采集功能，支持在设备界面对服务器地址、端口、以及采样百分比进行设置；
	支持流量采集策略设置，对流量采集的方向、时间、源 IP 地址、目的 IP 地址、源端口、目的端口进行设置；
规则库	攻击规则库单独分开，可支持手动、自动、以及离线升级。 应用识别规则库单独分开，可支持手动、自动、以及离线升级。 URL 过滤库单独分开，可支持手动、自动、以及离线升级。 支持病毒库，单独分开，可支持手动、自动、以及离线升级。
防火墙功能	系统可以设置访问控制规则，实现对网络层到应用成的访问控制功能。
	支持连接数控制，并且可以选择源目的区域及源目的地址、协议类型进行控制；
	系统支持源、目的地址转换以及双向地址转换；
	系统支持 IP/MAC 地址绑定，支持设置协议与非常用端口的绑定策略；
入侵防御能力	入侵防御引擎系统具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御；
	入侵防御引擎系统支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作；
	入侵防御引擎系统支持自定义攻击检测规则；
	入侵防御引擎系统支持黑名单，将攻击源加入黑名单，一段时间内禁止访问；
	入侵防御引擎系统支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据；
	涵盖广泛的攻击特征库、能够针对 4100 种以上攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御；
	能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等攻击事件；
	支持自定义规则，并且自定义规则库可以导入导出；
URL 过滤	系统应具备独立的 URL 检测过滤引擎。 支持黑白名单，精确匹配和模糊匹配。 支持阻断、URL 重定向、返回默认页面、返回自定义页面等多种动作。
	支持包括恶意网站、违反国家政策法规、潜在不安全、浪费带宽、大众兴趣、多种论坛、行业、计算机技术、等多种分类的 URL 过滤。 支持 URL 地址分类库，超过 1000 万种。
流量异常检测	支持对设备接口流量的阀值进行设置及报警；
	支持对网络内的 TCP、UDP、其他流量协议占比进行设置及报警；
	支持对协议组的流量阀值和连接数进行设置及报警，协议组类型包括 P2P 类、即时通讯类、标准协议类、移动应用类、http 应用类、工控互联网类等；
DDOS 防御	系统支持 DNS 异常包及 DNS Flood 攻击防御；系统支持 DHCP 异常包及 DHCP

功能	Flood 攻击防御；系统支持 ARP 异常包及 ARP Flood 攻击防御；系统支持 CC 攻击防御，且能够对 Web 服务器上的指定 URI 页面进行防护设置；系统支持主机并发连接数和半连接数的限制；系统支持 DDOS 机器人自学习功能，学习时间可设置。
应用管控功能	系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的 23 大类超过 2100 种应用。
	应用管理系统应支持灵活的应用管理策略配置功能，实现基于主机地址、时间、应用等多维度的全面、细致监控。
	应用管理支持对应用协议的阻断和流量管控以及记录应用日志。
	自定义应用：支持协议自定义功能。
日志管理	产品为响应网络安全法要求，系统支持日志本地存储和日志发送至单独的日志服务器，并且支持以上两种方式双存储，自动判断日志服务器的状态后自动选择日志的存储方式。
	系统应提供基于告警级别、时间、IP 地址、事件类型、等条件的日志检索功能，具备日志导出备份、清除功能。
	系统支持攻击检测日志中可以直观的展示攻击事件中的攻击特征编码。
	支持外发日志服务器时，自定义字符编码格式 GBK/UTF8。
	系统应具备日志归并功能，避免日志风暴。
统计	支持对应用协议的连接数和流量的报警信息进行展示，红色表示有报警，绿色表示没报警。
	支持在应用排名中，展示该应用的主机的 IP 地址所对应的的主机所属国家，以及连接数、上行流量、下行流量，并且可以对其进行排序。
	支持查看任意接口接受和发送报文字节大小分布图。
	支持查看近 24 小时、一周、一个月内历史系统性能件事情况、连接数变化情况及新建会话速率情况。
管理	系统支持 web 页面和命令行等多形式灵活安全策略配置。
	支持多级部署，且设备也可采用 B/S 管理模式或 C/S 管理模式。
	支持登陆界面图形验证码功能，防止管理员账号被暴力破解。
监控	应系统界面支持资源监视和攻击事件实时显示。 支持实时基于主机、区域的攻击与被攻击的统计显示，在监控信息中直观显示 IP 地址所处国家。并支持自定义地址薄导入功能。
	保障设备已正常设备运行，设备界面支持设备温度监控功能，且达到阀值时可以报警，为用户方便，设备温度阀值可自定义。
	支持查看当前连接信息，如当前连接正在建立，正在握手还是已经拆除、当前连接所使用的协议、连接的源/目的地址和端口号、该连接是否应用源 NAT/目的 NAT 策略、 该连接建立过程中源地址发送的数据报文个数、目的地址发送的数据报文的个数等信息； 支持查看连接排名，可以查看当前（用户访问此菜单时刻）通过入侵防御系统建立的连接排名信息。每一条连接信息包括如下内容：根据连接数排名方式的不同显示 排

	名、源 IP 地址、目的 IP 地址、协议、端口号、连接数量等信息。
▲质保与服务	三年硬件免费质保，3 年攻击特征库升级许可，1 年网站知识库升级许可。

3.2.2 数据库监控与审计系统

技术指标	技术指标要求
硬件规格	1U机架式设备，配置单电源，≥6个GE接口，1×扩展槽位（可扩展4GE/4SFP）。16G内存，1T存储空间。
性能	峰值SQL语句吞吐量≥5000条/秒；并发连接数≥1000个；在线日志量2亿条以上，归档日志15亿条以上。
数据库类型	支持国际主流数据库：Oracle、SQL Server、MySQL、DB2、Postgres、sybase、informix、cacheDB、SAP HANA、Teradata等； 支持国产数据库：达梦、GBase、KingBase、Oscar等； 支持非关系型:mongoDB、Redis等； 支持Hadoop生态：Hbase、Hive、Sentry、HDFS、Impala、ES等。
审计内容	会话的终端信息：IP、MAC、Port、工具名称（程序名）、操作系统用户； 会话的主机信息、IP、Port、数据库名（实例名）、业务主机群； 会话的其它信息：登录时间、会话时长； 操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作对象（数据库实例、schema、表、字段、函数、存储过程名称）、SQL语句、SQL错误代码； 操作影响范围信息：查询、修改、删除操作的影响行数,以及返回行数； 支持数据库双向审计； 支持结果集审计、记录操作成功与失败； 支持SQL server 2005以上（含）版本，在会话登陆过程中对数据库加密用户名的审计； 针对Oracle、SQLserver等同一数据库地址下建立多个数据库实例，可区分实例的检索分析。 支持对超长SQL操作语句审计，单条语句长度可达2M；
审计过滤规则	审计策略的要素： where：IP地址、用户名、端口号、数据库类型； who:实例、schema； what:表、字段、视图、包； when：起始\结束时间、执行时长； how：客户端工具； Range：修改、删除或查询的行数 ResultSet：返回结果集 other：关键字、客户端工具和应用、错误码、关联表数等
应用关联审	非时间戳的解析方式，采用应用端轻量级插件部署，以精确方式审计到应用端相关信

计	息，支持应用用户和源IP的关联审计，支持Weblogic、tomcat、Websphere等主流的应用服务器；
数据库漏洞攻击监测	能对基于数据库漏洞进行攻击行为监测和告警，默认支持420个以上的数据库漏洞攻击规则库。
SQL注入监测	支持SQL注入、XSS攻击等外部行为监控；支持根据IP、sql特征自定义SQL注入规则。
可疑行为识别	对以下高危行为，可自动识别并进行风险处理、告警通知: 1）批量数据导出：对超过特定行数阀值的批量数据导出行为 2）高危操作：对超过特定行数阀值的批量数据修改、删除； 3）支持no where 全表Update、Delete行为监控； 4) 新型/失败语句的识别； 5) 支持耗时长、执行频繁的异常语句识别； 6) 支持活跃会话识别； 7) 支持失败登陆审计； 8) 支持口令猜测，基于频次判断失败登录风险； 9) 支持关联表个数设置； 10)支持返回错误码； 11)支持应用关联监测策略； 12)支持数据库字段级的与或逻辑设置，可建立敏感数据组进行专项监控； 13)支持周期内频次行为监控； 14)支持SQl语句模板化归类，基于语句模板关联客户端信息自定义风险语句、信任语句和不审计语句类型；
多维度分析	支持数据库分组管理，可以基于全局、分组和单库多个维度进行统计分析。采用多功能面板展现，图形化监控被审计系统风险、会话、语句分布情况。支持图形化界面深入钻取分析，直至语句、会话详情；支持对指定数据库添加关注标示。
审计查询	支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户、数据库服务（实例）名等多种丰富的查询检索条件； 支持应用层关联审计查询和关联分析；支持风险、语句和会话界面的超链接钻取分析；
会话分析	提供全面的会话查询分析能力，包括： 1)会话统计：基于客户端IP、数据库用户、访问工具等维度统计会话量； 2)会话检索：基于客户端IP、数据库用户、MAC地址、访问工具、OS用户等条件检索会话信息； 3)失败及活跃会话分析：提供对失败登录的会话信息查询，提供对周期内的活跃会话进行统计和趋势分析；
支持敏感数据掩码	针对SQl语句中的敏感信息,可自定义规则进行数据掩码展现，防止数据二次泄密。
报表	系统提供不少于40个报表模型，分别基于多库和单库维度进行展现； 支持合规性报表：如PCI、等级保护、SOX法案等专项报表展现； 支持专项报表展现，针对风险、性能、访问源、账户、慢SQL等

	信息做专项报表展现； 支持日、周、月 等综合性报表； 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表； 支持风险登陆、高危风险、客户端风险等多种类型报表展现； 支持定期推送； 支持报表数据后台定期预存，独立的预存管理体系，保障报表数据实时展现； 文档格式：WORD\ PDF\ HTML
告警策略	支持高、中、低风险告警； 支持风险登陆、风险操作、SQL注入、漏洞攻击检测、口令攻击、频次攻击等风险告警； 支持产品系统资源的监控与告警。
告警方式	告警方式包括：邮件、短信、企业微信、SYSLOG、SNMP、界面，支持以Syslog 、KA** A、CSV等方式将审计数据外送。
数据库自动发现、审计	支持基于数据流量的数据库自动发现，发现流量中的未知数据库信息，并自动添加审计需要被审计的数据库。
协议解析	支持协议自动识别数据库信息；支持Oracle无链接会话识别；支持Oracle动态端口下的审计。
备份和恢复	支持审计数据自动备份到本地和远端ftp、SFTP、NFS服务器，支持系统配置的导入导出；支持Syslog方式导出全量审计、风险审计、新型语句给第三方平台，实现审计数据的二次分析；
IP别名管理	支持客户端IP别名设置，针对不同客户端IP自定义别名展现；
业务化语言	支持sql语句自定义业务化语言翻译
旁路模式	在交换机镜像模式下，通过TAP、SPAN等技术将网络流量映射到审计设备，对数据库流量进行审计和告警；支持跨网段、跨语句、多VLAN等环境下的审计监测；
探针采集	支持服务器端安装轻量级插件，采集服务器和虚拟化环境下流量无法镜像时的数据库审计行为，产品提供agent插件状态监测功能。
▲质保与服务	三年免费质保

3.2.3 存储扩展单元

技术指标	技术指标要求
★灾备系统升级要求	对当前在用的柏科数据 Rorke RD580 存储系统进行升级扩容：包括 EXP 扩展单元，硬盘，容量扩展、分区许可、存储虚拟化管理许可等，必须完全兼容现有存储。
扩展单元	存储扩展单元，内部无线缆连接，冗余电源，冗余风扇，机架套件
硬盘	配置 24 个 1.8TB 10K SAS 硬盘，含硬盘托架及适配器
许可	配置磁盘存储系统 43.2TB 的容量扩展许可、虚拟化管理许可 48TB，实现存储的虚拟化和统一管理。

SAN 存储加速	可通过 SAN 存储加速功能监控磁盘的访问模式，然后自动将频繁访问的热点数据提取到 SSD 等高性能磁盘组成的缓存中以加快读取速度，从而加速随机访问及整体 I/O 的读取速度，提供热点数据资源策略和访问统计信息的功能截图。
卷共享	配置六个节点的 ImageSAN 卷共享 Volume Share 功能。
存储管理和异地容灾	须兼容现有柏科 VRD 系列存储虚拟化设备和存储设备，支持现有的存储虚拟化平台统一管理和调度，无须额外的协议转换设备和第三方软硬件设备，无需二次开发，可在本地或异地进行集中灾备和统一管理。
▲质保与服务	三年免费质保
厂商承诺	投标文件中提供产品制造商针对本项目的授权书和服务承诺函原件。

3.2.4 虚拟化服务器内存扩容

技术指标	技术指标要求
规格	VMware虚拟化资源池服务器内存扩容。共1200GB，要求必须与原服务器内存兼容。
▲质保与服务	三年免费质保

3.2.5 三级等保复测

技术指标	技术指标要求
总体要求	依据国家信息安全等级保护相关标准及工作流程要求，结合区财政业务专网及应用系统整体需求及具体特点，对相关信息系统开展等级保护测评服务，包括协助系统定级、差距分析、协助整改、出具测评报告、完成系统备案等。
依据标准	1、GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》 2、GB/T 28448-2012 《信息安全技术信息系统安全等级保护测评要求》
测评范围	金财工程一体化系统、财政业务专网系统。
系统定级	协助业主方完成其网络信息系统的等保定级工作，包括调研分析、确定系统等级、协助申请定级等。
差距分析	对上述系统安全保护现状与等级保护相关标准要求之间的差距进行评估分析，明确存在的安全风险，提出整改建议。
安全整改技术支持	根据差距测评发现的系统安全隐患，提供安全整改技术支持服务，帮助系统管理员、软件开发商、硬件维保公司完成安全整改与加固。
等级测评	依据 GB/T 22239-2008《信息系统安全等级保护基本要求》国家标准，对信息系统进行正式测评，评估信息系统是否符合国家标准的要求，出具等级测评报告。
协助备案	协助业主方完成系统备案工作涉及的各类材料上报工作及备案证书申请工作。
测评内容	按“安全等级保护三级”标准开展等保工作，测评内容覆盖物理环境、网络平台、主机系统、应用软件、数据安全、安全管理制度、安全管理机构、人员安全、系统建设和系统运维等层面。
项目成果	提供《信息系统等级保护测评报告》等测评结果文档。

3.3 设备维保服务

技术指标	技术指标要求
服务内容	针对维保清单内的软硬件设备，提供技术咨询、故障响应、定期巡检、补丁（知识库）升级、技术培训等服务内容。
▲维保期限	1 年
故障响应速度	维保方提供 7*24 小时热线电话技术支持，安排有经验的技术人员接受报障，对于用户提出的故障申告后 2 小时内给予实质性响应。如电话不能解决，应安排工程师在 4 小时内抵达现场，24 小时内排除故障。规定时限内不能解决的，无偿提供备机备件。

设备维保服务清单

序号	设备名称	型号	数量	维保期限
1	核心交换机	迪普 DPX8000-A12	2 台	1 年
2	接入交换机	迪普 LSW3600-24GT4GP	18 台	1 年
3	接入交换机	迪普 LSW3600-48GT4GP	13 台	1 年
4	PC 服务器	DELL R910	5 台	1 年
5	PC 服务器	DELL R720	4 台	1 年
6	PC 服务器	HP 580G7	3 台	1 年
7	PC 服务器	华为 RH5885	4 台	1 年
8	PC 服务器	DELL R910	2 台	1 年
9	存储系统	柏科 RD6810F	1 台	1 年
10	存储系统	柏科 RD6810F	2 台	1 年
11	存储系统	Dell SC40	2 台	1 年
12	存储系统	DELL SC220	2 台	1 年
13	存储系统	柏科 RD6810	2 台	1 年
14	存储光纤交换机	柏科（Rorke）RD300	4 台	1 年
15	隔离网闸	启明星辰天清 GAP-6000-620BD	1 台	1 年
16	防火墙	天融信 NGFW4000-UF TG-61040（猎豹）	1 台	1 年
17	堡垒机	思福迪 LogbaseB3600	1 台	1 年
18	VPN 系统	深信服 VPN-3050	1 台	1 年
19	SSL VPN 系统	深信服 VPN-2050	1 台	1 年
20	Web 应用防护系统	深信服 AF-2020	1 台	1 年
21	无线网控制器	信锐 NAC-6300	2 台	1 年
22	无线网 AP	信锐 NAP-2600	120	1 年

23	无线网 AP	信锐 NAP-2400-P	53	1 年
24	POE 交换机	信锐 SW-5024	1 台	1 年

3.4 网站测评、网站性能监测、网络安全测评

3.4.1 24 小时网站监测服务

24 小时网站监测防护：对门户网站安全实施监测，主要监测内容：网站 24 小时告警监测服务、网站错别字检测等。主要内容：

网站 24 小时告警监测服务：

人工 7×24 小时(节假日不休)接受告警信息并进行人工确认，全部告警均经过值班人员审核，告警属实则以短信和电话通知客户技术人员。

网站错别字检测服务：

对客户网站进行定期的错别字检测，如果发现有错别字并经过人工核实后，以邮件、短信、报告等方式通知用户，并协助用户对错别字进行定位及修改。

3.4.2 政府网站及政务服务网考核指标监测

按照《国务院办公厅关于开展第一次全国政府网站普查的通知》(国办发〔2015〕15 号）和《国务院办公厅秘书局关于印发政府网站与政务新媒体检查指标、监管工作年度考核指标的通知》的要求，对政府网站及政务服务网监测，及时发现问题并协助整改。主要内容：

（1）网站日常监测系统服务

搭建系统对“杭州·下城”政府门户网站进行技术监测，系统技术监测的指标包含：首页错链（日常监测）、首页栏目内容更新监测（两周监测）、网站错误链接（日常监测）、网站错别字（需人工审核，每两周监测一次）、敏感字词监测（两周监测一次，需人工审核）无法下载附件（日常监测）、

在线申报错误（日常监测）、长时间未更新栏目（人工审核，每月监测一次）、空白栏目（需要人工审核，每月监测一次）、网站总更新量（日常监测）、栏目更新汇总(日常监测)、网站首页更新量、（日常监测）、首页可用性（日常监测）、站点可用性（日常监测）；人工评测报告：专按照国务院办公厅、浙江省政府及杭州市政府要求对“杭州·下城”政府门户网站进行人工评测报告服务，具体指标见附件，并且网站每季度出具两份报告，每年 12 份，每季度提供一次网站域名名称规范性、网站标识添加情况、已公开留言规范性抽查，站内搜索功能实效性检测、网站主流浏览器兼容性测试，共计 4 次。

（2）“杭州·下城”门户网站普查服务

按照《国务院办公厅关于开展第一次全国政府网站普查的通知》(国办发〔2015〕15 号）的要求，采用人工监测和技术监测相结合的方式对被查网站进行常态化核查。

（3）浙江政务服务网下城分厅监测

按照事项类型检测“个人办事”和“法人办事”服务指南所含事项要素是否存在空白或信息明显不实、不准确问题（含具体事项中人工可查范围内的错链、断链）进行监测，提供 1 次政务服务网全查监测报告服务。完整报告以后每月提供五家部门窗口（按事项类型）检测“个人办事”和“法人办事”服务指南所含事项要素是否存在空白或信息明显不实、不准确的问题出具报告。

（4）服务期：一年

（四）服务培训具体要求

1、新建内容售后服务与培训

1.1 投标人应达到以下标准：

（1）在质保期内，投标人应提供现场维护保障和技术支持服务，提供第二个工作日上门服务（24 小时内上门响应），承诺尽力在最短时间内恢复系统正常运行，如果故障不能在 72 小时内排除，如果投标人在接到通知后的 48 个小时内未作出响应，则由于故障所造成的全部损失由投标人承担；

（2）质保期内系统停止运行的时间应从其质保期内扣除；

（3）投标人必须为维护和技术支持所未能解决的问题和故障提供正式的升级方案；

1.2 在质保期内，投标人有责任解决所提供的系统产品的任何问题，在质保期满后，当需要时，投标人仍须对因投标系统产品本身的固有缺陷和瑕疵承担责任；

1.3 对系统产品服务要求的有效响应将被视为投标人对其所投标的物服务承诺，如果中标，须将服务承诺列入合同的服务条款。

1.4 投标人应提供此次投标的服务策略和服务计划（售后服务内容、等级、相关服务指标、售后服务组织机构及人员安排情况及其联络信息）。

1.5 投标人负责培训的人员应具有同类产品的维护经验，投标人应提供相应的培训计划，详细说明培训的方式、地点、人数、时间等实质性内容。技术培训费用应包含在投标总价中。

（1）现场培训，要求投标人在整个项目实施过程中对用户进行现场培训，培训内容包括项目所涉及软件系统的日常操作及注意事项。此培训主要目的是解决日常维护工作中可能会出现的问题。

（2）集中培训，要求投标人在项目实施完毕后，安排一次集中的培训，培训课程的主要内容包括所有软件产品技术性能特点、使用方法、注意事项等内容，通过现场实验使用户掌握相关产品的使用和解决故障。需根据项目情况提供具体的培训课程。

（3）对相关用户培训，使相关用户掌握相关产品的使用和故障解决。

三、商务要求

（一）报价要求

▲报价应包括完成本项目工作所需的人力物力成本、管理费、其他费用、利润、税金等完成本项目的所有费用。本次投标报价为人民币价。

（二）签订合同

▲1、本项目合同甲方为杭州市下城区数据资源管理局，乙方为中标人，合同款支付给乙方。甲乙双方应当在中标通知书发出之日起 30 日按招标文件确定的事项及投标文件响应内容签订本合同。

主体、关键性工作不得分包，其他工作如拟在中标后进行分包，应当在投标文件中载明分包承担主体，分包承担主体不得再次分包。

（三）履约保证金交纳

▲详见《第四章 采购合同》

（四）付款条件

▲详见《第四章 采购合同》

（五）其他内容

详见招标文件的“第四章 采购合同”，投标人应对合同内容进行审核，如有偏离，请在投标文件的“偏离表”中反映。

四、落实政府采购政策要求

1. 本项目对符合财政扶持政策的中小企业（小型、微型）、监狱企业、残疾人福利性单位给予价格优惠扶持，价格优惠扶持见《第五章 评标办法》。

满足转发财政部 工业和信息化部关于印发《政府采购促进中小企业发展暂行办法》的通知（浙财采监〔2012〕11 号）的规定的中小企业可享受优惠扶持。

满足关于政府采购支持监狱企业发展有关问题的通知（财库〔2014〕68 号）的规定的供应商可享受优惠扶持。

满足关于促进残疾人就业政府采购政策的通知（财库〔2017〕141 号）的规定的供应商可享受优惠扶持。

2. 节能产品的强制采购政策

▲根据财政部、国家发展改革委、生态环境部、国家市场监管总局《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9 号文件规定，对政府采购节能产品实施品目清单管理，依据品目清单和认证证书实施政府强制采购。采购人拟采购的产品属于品目清单范围内的政府强制采购产品（清单中以★标注）的，投标人提供的产品应具有国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，并在投标文件中提供该产品节能产品认证证书或“政府强制采购的节能产品用于本项目的承诺书”，否则无效。

【注：本项目执行财政部、国家发展和改革委员会关于印发节能产品政府采购品目清单的通知（财库〔2019〕19 号）、市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019 年第 16 号）】

3. 节能产品、环境标志产品的优先采购政策

根据财政部、国家发展改革委、生态环境部、国家市场监管总局《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9 号文件规定，对政府采购节能产品、环境标志产品实施品目清单管理，依据品目清单和认证证书实施政府优先采购。采购人拟采购的产品属于品目清单范围内的优先采购品目的，投标人提供的产品应具有国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，并在投标文件中提供该产品的节能产品认证证书或环境标志产品认证证书、产品所属节能环保品目清单中对应产品名称。

【注：本项目执行财政部、国家发展和改革委员会关于印发节能产品政府采购品目清单的通知（财库〔2019〕19 号）、财政部、生态环境部关于印发环境标志产品政府采购品目清单的通知（财库〔2019〕18 号）、市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019 年第 16 号）】

五、投标现场演示要求

◇演示下城区基层四平台统一地址采集、核查、上报的操作流程（2 分），实现对有效地址、失效地址、无效地址、退回地址的核查操作和信息查询（2 分）。（4 分）

◇演示组织架构的设置功能，在原有组织结构设计的基础上实现横向添加部门、纵向添加二级科室（2 分），并对添加的新结构实现事件派单功能（2 分）。（4 分）

◇展示街道基层治理风险防范中对有安全隐患的重点对象、重点事件等的关注和多角度

分析。（2 分）

说明：现场可提供投影机（VGA 接口）、无线网络，其他演示条件需由投标人自备。演示时间约 20 分，投标人事先准备。