附件一：招标主要设备与服务需求

注：如招标工程量清单中的“招标主要技术/功能参数”与本章节需求不一致，产品选型依据请以本章节需求为准。

1.1 省市际卡口及交通枢纽感知前端

1.1.1 省市际卡口系统

- **900 万一体化抓拍单元**

图像传感器：采用 1 英寸 GMOS 支持视频帧率在 1～25fps 可调
视频压缩标准：H.264/H.265/MJPEG
输出图片格式：JPEG
主码流 4096*2160@25fps
支持识别：民用车牌，警用车牌，2012 式新军用车牌，2012 式武警车牌，新能源车牌。
最大图像尺寸≥4096×2160 像素，字符叠加时最大可支持 4096×2800
支持机动车、二轮车（摩托车、自行车、电动二轮车）、三轮车和行人分类检测
支持车前窗挂坠、年检标识、抽烟、驾驶员人脸识别、驾驶室人脸抠图、遮阳板识别等检测功能 支持车辆捕获抓拍功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的捕获率均≥95%支持车牌识别功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的识别准确率均≥95%使用闪光灯补光时，抓拍图片可看清司乘人员人脸 支持主副驾驶人脸抠图功能 外壳防护等级应不低于 IP66
工作环境温度支持：-30℃～+60℃
工作环境湿度：5%~95%@40℃，无凝结

- **1 英寸 50mm 镜头**

定焦，50mm

- **红外白光一体式闪光灯**

进口 LED 灯珠，支持 LED 频闪，白光气体爆闪，红外气体爆闪。
可覆盖 1 个车道。
采用进口高亮度 LED 芯片，寿命长，稳定性好，发光效率高
采用步进电机功能，实现红外滤片的切换
气体光源回电时间小于 67ms，支持超速连拍，
气体补光控制具有峰值抑制功能
支持 LED 灯频闪、白光气体爆闪，红外气体爆闪
支持相机误触发保护功能，触发信号输入异常时自动保护、且自动恢复
结构采用 IP66 设计

- **终端管理设备**

嵌入式操作系统；
内置 1 块 3.5 寸 2T 硬盘；支持 12 路 IPC 接入；双网卡，内置 8 个 100M 以太网接口及 2 个 1000M 网络接口；
支持 VGA 输出；1 个 RS485、2 个 RS232、2 个 USB、4 路报警输入\报警输出、1 个 eSATA 接口；电源:DC12V；
支持对通行车辆的信息（记录和图片）存储；
支持录像存储功能；
可配置多种字符叠加、图片合成模式；

支持区间测速功能；
支持配置增加 GPS 校时模块；

- **态势监控高清球机**

800 万像素红外网络高清高速智能球机
4K 星光球机，1/1.2＂靶面传感器
具备人脸、人体抓拍并关联输出功能，支持指哪抓哪、多场景轮巡抓拍、远距离卡口抓拍模式
支持人脸人体车辆同时抓拍，人脸人体关联输出，并实现对人脸、人体、车辆结构化属性特征信息提取
前端建模比对：前端存储 15 万张人脸图片进行建模后，对场景中抓拍的人脸进行比对并输出结果
支持 GB35114 安全加密
支持防破坏预警功能
人员布控：支持前端实时建模比对，对人脸和人体进行布控跟踪，跟踪过程中目标经纬度信息实时上传，构建时空域场景
车辆布控：支持前端实时建模比对，对黑白名单车辆进行布控跟踪，跟踪过程中目标经纬度信息实时上传，构建时空域场景
最低照度: 0 Lux with IR,彩色：0.0005Lux @ (F1.6，AGC ON),黑白：0.0001Lux @ (F1.6，AGC ON)
宽动态: 支持
光学变倍: 40 倍
焦距: 7.5- 300mm，40 倍光学变倍
水平范围: 360°
垂直范围: -20°-90°(自动翻转)
水平速度: 水平键控速度：0.1°-210°/s,速度可设;水平预置点速度：280°/s
垂直速度: 垂直键控速度：0.1°-150°/s,速度可设;垂直预置点速度：250°/s
主码流帧率分辨率: 50Hz:25fps(3840×2160)；60Hz:30fps(3840×2160)
视频压缩标准: H.265,H.264,MJPEG
网络存储: NAS (NFS，SMB/ CIFS)
网络接口: RJ45 网口,自适应 10M/100M 网络数据
SD 卡扩展: 支持 Micro SD(即 TF 卡)/Micro SDHC/Micro SDXC 卡,最大支持 256G
报警输入: 7 路报警输入
报警输出: 2 路报警输出
音频输入: 1 路音频输入
音频输出: 1 路音频输出
具有 RS485 接口
红外照射距离: 250m
防补光过曝: 支持
电流及功耗: AC24V±25%，62W max（其中加热 5Wmax，红外灯 12W max）
工作温湿度: -40℃-70℃；湿度小于 95%
尺寸: Φ267×430mm
重量: 9.6Kg
防护: IP67

1.1.2 交通枢纽感知前端

- **交通枢纽人脸相机**

传感器类型 1/1.8 英寸 CMOS；像素 800 万；最大分辨率 3840×2160；最低照度 0.01Lux（彩色模式）；0.001Lux（黑白模式）；最大补光距离 300m；镜头类型电动变焦；镜头焦距 6.7mm~134mm；通用行为分析物品遗留；支持区域入侵、越界入侵、徘徊、物品移除、物品遗留、人员聚集、停车，并联动报警；徘徊检测；人员聚集；停车检测；视频压缩标准 H.265；H.264；电子防抖支持；透雾功能支持；报警事件支持无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；动态检测；视频遮挡；区域入侵；绊线入侵；物品遗留/消失；场景变更；音频异常侦测；虚焦侦测；接入标准 ONVIF；GB/T28181；最大 Micro SD 卡 256G；音频输入 1 路；音频输出 1 路；报警输入 2 路，报警输出 1 路；供电方式 AC24V；防护等级 IP66

含抓拍单元、防护罩、镜头、电源等所有设备。

- **广场人脸相机**

传感器类型 1/1.8 英寸 CMOS；像素 800 万；最大分辨率 3840×2160；最低照度 0.01Lux（彩色模式）；0.001Lux（黑白模式）；最大补光距离 300m；镜头类型电动变焦；镜头焦距 6.7mm~134mm；通用行为分析物品遗留；支持区域入侵、越界入侵、徘徊、物品移除、物品遗留、人员聚集、停车，并联动报警；徘徊检测；人员聚集；停车检测；视频压缩标准 H.265；H.264；电子防抖支持；透雾功能支持；报警事件支持无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；动态检测；视频遮挡；区域入侵；绊线入侵；物品遗留/消失；场景变更；音频异常侦测；虚焦侦测；接入标准 ONVIF；GB/T28181；最大 Micro SD 卡 256G；音频输入 1 路；音频输出 1 路；报警输入 2 路，报警输出 1 路；供电方式 AC24V；防护等级 IP66

含抓拍单元、防护罩、镜头、电源等所有设备。

- **广场枪球联动相机**

具有 1 个 RJ45 接口，1 个音频输入接口、1 个音频输出接口、2 1 个报警输入接口、1 个报警输出接口、1 个 SD 卡插槽，可输出两路视屏图像：通道 1、通道 2。

采用 DC36V

设备水平旋转范围为 0~256°，垂直旋转范围为 -35°~90°

支持最低照度可达彩色 0.00021x，黑白 0.00011x

支持视屏图像存储至 SD 卡或客户端，支持 SD 卡热插拔，SD 卡支持最大 256G

支持电源电压在电压在 DC36V±25%范围内变化能正常工作

云台定位精度 0.1°

支持快速聚焦功能，设备对监控区域内的移动目标进行跟踪录像，录像通过单帧回放时应能保证每帧画面清晰稳定。

支持检出两眼瞳距 20 像素点以上的人脸图片，人脸检出率不小于 99%，支持单场景同时检出不少于 40 张人脸图片，并支持面部跟踪。

在距离设备 40 米处，人脸抓拍准确率不小于 99%，人体抓拍准确率不小于 99%。

设备可对 30 米处的行人进行人脸抓拍，并可生成分辨率不小于 110×120 的人脸图片,图片中人脸两眼瞳距应≥40 像素。

支持车辆检测功能

可通过客户端软件在监视画面中，绘制规则线并设置联动录像时长

镜头从最小倍变到最大倍数所需时间小于等于 1.8s

支持全局配置：支持在绊线入侵、区域入侵 、进入/离开区域、越界入侵、穿越围栏、快速移动、物品搬移、物品遗留、停车检测则下灵敏度调节和标定区域可对两路（全局摄像机和细节摄像机）监控画面中的机动车、非机动车、人员中的一种或者多种同时进行抓图及属性检测。

- **高空全景监控相机**

- 800 万全景相机

传感器类型 1/1.8 英寸 CMOS;全景由 4 个 200 万镜头拼接成 800 万 180° 视场角，集成 200 万 40 倍云台球一体；最大红外距离：大于等于 400 米；宽动态 120dB；镜头焦距全景： 2.8mm；球机： 5.7mm～220mm；音频输入 1 路音频输入；音频输出 1 路音频输出；报警输入 7 路；报警输出 2 路；支持超星光；防护等级 IP66；标配光模块。

- 1600 万全景相机

传感器类型 1/1.8 英寸 CMOS；全景由 8 个 200 万镜头拼接成 1600 万 360° 视场角,集成 200 万 40 倍云台球一体;最大红外距离:大于等于 400 米;宽动态 120dB;镜头焦距全景：5mm；球机 6.6mm～220mm；音频输入 1 路音频输入；音频输出 1 路音频输出；报警输入 7 路；报警输出 2 路；防护等级 IP66；标配光模块。

1.1.3 停车场出入口标准卡口

- **900 万一体化抓拍单元**

图像传感器：采用 1 英寸 GMOS 支持视频帧率在 1～25fps 可调
视频压缩标准：H.264/H.265/MJPEG
输出图片格式：JPEG
主码流 4096*2160@25fps
支持识别：民用车牌，警用车牌，2012 式新军用车牌，2012 式武警车牌，新能源车牌。
最大图像尺寸≥4096×2160 像素，字符叠加时最大可支持 4096×2800
支持机动车、二轮车（摩托车、自行车、电动二轮车）、三轮车和行人分类检测 支持车前窗挂坠、年检标识、抽烟、驾驶员人脸识别、驾驶室人脸抠图、遮阳板识别等检测功能 支持车辆捕获抓拍功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的捕获率均≥95% 支持车牌识别功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的识别准确率均≥95% 使用闪光灯补光时，抓拍图片可看清司乘人员人脸 支持主副驾驶人脸抠图功能 外壳防护等级应不低于 IP66
工作环境温度支持：-30℃～+60℃
工作环境湿度：5%~95%@40℃，无凝结

- **1 英寸 50mm 镜头**

定焦，50mm

- **红外白光一体式闪光灯**

进口 LED 灯珠，支持 LED 频闪，白光气体爆闪，红外气体爆闪。
可覆盖 1 个车道。
采用进口高亮度 LED 芯片，寿命长，稳定性好，发光效率高
采用步进电机功能，实现红外滤片的切换
气体光源回电时间小于 67ms，支持超速连拍，
气体补光控制具有峰值抑制功能
支持 LED 灯频闪、白光气体爆闪，红外气体爆闪
支持相机误触发保护功能，触发信号输入异常时自动保护、且自动恢复

结构采用 IP66 设计

- **终端管理设备**

嵌入式操作系统；
内置 1 块 3.5 寸 2T 硬盘；支持 12 路 IPC 接入；双网卡，内置 8 个 100M 以太网接口及 2 个 1000M 网络接口；
支持 VGA 输出；1 个 RS485、2 个 RS232、2 个 USB、4 路报警输入\报警输出、1 个 eSATA 接口；电源:DC12V；
支持对通行车辆的信息（记录和图片）存储；
支持录像存储功能；
可配置多种字符叠加、图片合成模式；
支持区间测速功能；
支持配置增加 GPS 校时模块；

1.1.4 送站平台标准卡口

- **900 万一体化抓拍单元**

图像传感器：采用 1 英寸 GMOS 支持视频帧率在 1～25fps 可调
视频压缩标准：H.264/H.265/MJPEG
输出图片格式：JPEG
主码流 4096*2160@25fps
支持识别：民用车牌，警用车牌，2012 式新军用车牌，2012 式武警车牌，新能源车牌。
最大图像尺寸≥4096×2160 像素，字符叠加时最大可支持 4096×2800
支持机动车、二轮车（摩托车、自行车、电动二轮车）、三轮车和行人分类检测 支持车前窗挂坠、年检标识、抽烟、驾驶员人脸识别、驾驶室人脸抠图、遮阳板识别等检测功能 支持车辆捕获抓拍功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的捕获率均≥95% 支持车牌识别功能，在天气晴朗无雾，号牌无遮挡、无污损，白天和晚上的识别准确率均≥95% 使用闪光灯补光时，抓拍图片可看清司乘人员人脸 支持主副驾驶人脸抠图功能 外壳防护等级应不低于 IP66
工作环境温度支持：-30℃～+60℃
工作环境湿度：5%~95%@40℃，无凝结

- **1 英寸 50mm 镜头**

定焦，50mm

- **红外白光一体式闪光灯**

进口 LED 灯珠，支持 LED 频闪，白光气体爆闪，红外气体爆闪。
可覆盖 1 个车道。
采用进口高亮度 LED 芯片，寿命长，稳定性好，发光效率高
采用步进电机功能，实现红外滤片的切换
气体光源回电时间小于 67ms，支持超速连拍，
气体补光控制具有峰值抑制功能
支持 LED 灯频闪、白光气体爆闪，红外气体爆闪
支持相机误触发保护功能，触发信号输入异常时自动保护、且自动恢复
结构采用 IP66 设计

- **终端管理设备**

嵌入式操作系统；

内置 1 块 3.5 寸 2T 硬盘；支持 12 路 IPC 接入；双网卡，内置 8 个 100M 以太网接口及 2 个 1000M 网络接口；
支持 VGA 输出；1 个 RS485、2 个 RS232、2 个 USB、4 路报警输入\报警输出、1 个 eSATA 接口；电源:DC12V；
支持对通行车辆的信息（记录和图片）存储；
支持录像存储功能；
可配置多种字符叠加、图片合成模式；
支持区间测速功能；
支持配置增加 GPS 校时模块；

1.1.5 增强型微热点

因项目保密性需求，投标人在下载投标文件后，须携带授权委托书、保密承诺 函（格式不限）至采购代理机构领取纸质版。

1.2 视频图像智能综合应用服务平台

1.2.1 市级视频图像汇聚平台（视频专网）

- **市级视频图像汇聚平台**

支持 B 端和 C 端统一云账户访问，B 端支持设备、用户、组织及存储管理（支持 Web 无插件化），C 端支持丰富的高级业务功能

- **平台计算分析单元模块**

外形规格 2U 机架式
处理器 2 颗 Intel Xeon 4108 1.8G 9.6UPI 11M 8 核 85W
内存 2 条 32GB DDR4 2666 REG 内存
硬盘 2 块 2TB 3.5 吋 7200 转 6Gb SAT 企业级机械硬盘 RAID1
4 个硬盘托架（其中自带 2 块硬盘）
SSD 盘 2 块 Micron SSD SATA 5100 MAX 240G 2.5 英寸-SATA 接口

- **平台数据分析单元模块**

处理器英特尔 至强 双路处理器 E5-2640 8 核 * 8；标配：16GB DDR3 ECC 内存 * 32；8 个内存插槽 * 4；标配：1T SATA 盘 2.5’ * 4；480G SSD 固态硬盘 2.5’ * 12；最大可扩展 24 块 SATA/SAS/SSD 2.5’ 硬盘；嵌入式网卡集成 2 个高性能千兆以太网控制器；集成 I/O 端口（2 个 USB 接口，1 个标准 VGA 接口，1 个串口，2 个 RJ45 网络接口）* 4；内置：（1 个 USB 接口）* 4

- **流媒体控制、转发单元模块**

支持视频流的转发、存储、回放及下载
支持以 RTSP、HLS 协议、FLV 协议、国际协议获取实时码流

- **GIS 地图服务**

点位秒级加载，主流地图矢量影像图离线支持（天地图、高德地图、腾讯地图、、超图、PGIS、arcgis），多业务系统共用，人员车辆轨迹按道路渲染，道路搜索，路口定位

- **平台接入网关**

支持 10 万路视频级联，支持加密狗授权机制；
支持 Web 方式访问，配置、管理网关设备；
多平台多层次级联，跨域互联互通与资源共享；
支持联网标准协议 GBT28181/DB33/DB41/GBT28059，具备符合上述协议的快速接入能力；支持至少 3 级级联部署，最大可支持 16 个外域的接入

1.2.2 市级视频图像汇聚平台（公安网）

- **市级视频图像汇聚平台**

支持 B 端和 C 端统一云账户访问，B 端支持设备、用户、组织及存储管理（支持 Web 无插件化），C 端支持丰富的高级业务功能
支持千兆网络绑定，实现业务网络和存储网络分离，充分利用网口资源；
采用分布式非对称式架构，元数据处理与数据存储的松耦合分析架构。

- **平台计算分析单元模块**

外形规格 2U 机架式
处理器 2 颗 Intel Xeon 4108 1.8G 9.6UPI 11M 8 核 85W
内存 2 条 32GB DDR4 2666 REG 内存
硬盘 2 块 2TB 3.5 吋 7200 转 6Gb SAT 企业级机械硬盘 RAID1
4 个硬盘托架（其中自带 2 块硬盘）
SSD 盘 2 块 Micron SSD SATA 5100 MAX 240G 2.5 英寸-SATA 接口

- **平台数据分析单元模块**

处理器英特尔 至强 双路处理器 E5-2640 8 核 * 8；标配：16GB DDR3 ECC 内存 * 32；8 个内存插槽 * 4；标配：1T SATA 盘 2.5’ * 4；480G SSD 固态硬盘 2.5’ * 12；最大可扩展 24 块 SATA/SAS/SSD 2.5’ 硬盘；嵌入式网卡集成 2 个高性能千兆以太网控制器；集成 I/O 端口（2 个 USB 接口，1 个标准 VGA 接口，1 个串口，2 个 RJ45 网络接口）* 4；内置：（1 个 USB 接口）* 4

- **流媒体控制、转发单元模块**

支持视频流的转发、存储、回放及下载
支持以 RTSP、HLS 协议、FLV 协议、国际协议获取实时码流

- **GIS 地图服务**

点位秒级加载，主流地图矢量影像图离线支持（天地图、高德地图、腾讯地图、、超图、PGIS、arcgis），多业务系统共用，人员车辆轨迹按道路渲染，道路搜索，路口定位

1.2.3 存储系统

- **视频云存储节点（市局）**

配置要求：
本次配置 21 个云存储节点；
★单节点配置不少于 2 颗处理器，每颗处理器核数不少于 24 核，主频不低于 2.6GHz；
单节点配置≥80 GB 内存；
单节点配置≥2 块 600G SAS 系统盘，配置≥1 块 1.92TB SSD 缓存盘， 配置≥35 块 10TB 7.2K rpm SATA 硬盘；
单节点配置≥4 个 10GE 接口、≥1 个 IPMI 管理网口；
配置≥2 台内部组网交换机（含 48*万兆接口,6*100G 接口）和对应的光模块和堆叠线缆；
架构要求：全对称分布式架构，无独立元数据节点，性能、容量随节点数增加而线性增加；
★前后端网络隔离：为了避免数据重构、动态分级等内部流量对前端业务产生影响，同时基于网络安全等因素，必须配置前端网络/后端网络双平面组网；
★数据保护 支持跨节点网络 RAID，最多可接受 4 个节点同时失效；
视频监控：开放虚拟机架构，可同时支持自研或第三方流媒体软件；

存储软件功能：支持基于文件级的动态分级存储功能用于数据生命周期管理，支持跨层透明移动数据，分级策略支持基于 I/O 热度自动分级；
支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率、网络带宽、TCP/IP 连接数、轮询、节点能力值；
支持基于用户、用户组、目录的空间配额管理功能；
支持快照功能，目录级快照功能；
支持视频监控图像修复功能；
支持防病毒功能；
支持企业级 WORM；
★远程复制功能：支持配置集群间目录级的远程复制功能，支持集群一对多、多对一复制模式，支持实时监控远程复制任务的健康状态、运行状态、数据状态等；
★掉电保护：具有异常掉电时数据不丢失功能；
管理特性：支持并提供功能全面的图形化 GUI 管理软件，支持 Web 或其它图形化方式进行远程管理，可视化系统结构图，提供对整个存储系统各个部分的监测；可以提供统计报表、监控分析、趋势预测、性能对比、诊断分析等；
运维特性：支持对软件版本、硬件状态、系统容量使用情况进行实时监控，对于节点/硬盘故障等，自动感知和处理，无需人工干预；
服务：5 年原厂保修服务，国内设有 24 小时 400 服务支持电话，提供原厂针对本项目的授权委托书与质保函。

- **视频云存储节点（县分局）**

本次配置 27 个云存储节点；
★单节点配置不少于 2 颗处理器，每颗处理器核数不少于 24 核，主频不低于 2.6GHz；
★单节点内存配置不低于 64GB，采用 DDR4、2933MHZ 及以上规格，可提供不低于 32 个内存插槽（单卡槽最大支持 64G），可组成不低于 16 个 DDR4 通道；
单节点配置不少于 36 块 14TB SATA 盘；
单节点配备两个独立元数据盘 960G SSD，组成 RAID1；
电源模块支持 1+1 冗余备份，支持独立维护；
配置冗余白金牌电源；
★在一台实体机器虚拟化后的多台逻辑机器上，应能支持部署不同功能以及数量的存储、转发等模块；
硬件资源按照计算资源、存储资源、网络资源分类，业务应用部署在容器上；
支持视频流和图片流直存，无需额外接入单独的转发；
支持不同容器业务隔离，并提供独立的虚拟的操作系统运行环境和接口，容器内业务进程不占用系统内存；
★支持 N+0 集群，单集群内云节点不需要独立的集群管理，当任意一个节点故障时，支持将故障节点上的业务负载分担到其他节点，可在 30s 之内完成；
★单节点同时支持 2Gbps 接入存储、2Gbps 转发、1Gbps 下载；
采用企业级 Linux 通用操作系统；
系统应能支持不少于 30 万路摄像机的接入，并同时支持不少于 30 万路第三方平台摄像机的接入；
系统应能支持 5000 个用户注册，可支持 2000 个用户同时登陆，支持 200 个用户同时操作；可设置用户单位、角色及用户基本信息；

系统应能支持多级多域管理，可支持整网不少于 200 个上下级域，同时支持不少于 128 个外域对接，平台互联最大可支持不小于 8 级；
实时浏览：前端支持多码流的情况下，支持选择某个码流进行实时浏览；
录像回放：支持按照指定设备、通道、时间、报警信息等要素检索联网设备历史图像资料进行跨域远程回放和下载，回放支持正常播放、快速播放、慢速播放、画面暂停、图像抓拍、缩放显示等；
服务：5 年原厂保修服务，国内设有 24 小时 400 服务支持电话，提供原厂针对本项目的授权委托书与质保函。

1.2.4 视图库（视频专网）

- **视频图像信息库管理平台（市区）**

与云存储结合，支持海量视频、图片信息的上传。支持通过多种关键字字段对非结构化得视频、图片信息进行结构化描述。支持海量数据的快速检索。可配置多台组成视图库集群，数量根据单台 3000 万/天纯结构化数据接入量计算 800 万/天带图片结构化数据接入量计算，支持上下级视图库数据汇聚，单节点每日汇聚量达 5000 万。

- **视频图像信息库管理平台（各县区）**

与云存储结合，支持海量视频、图片信息的上传。支持通过多种关键字字段对非结构化得视频、图片信息进行结构化描述。支持海量数据的快速检索。可配置多台组成视图库集群，数量根据单台 3000 万/天纯结构化数据接入量计算 800 万/天带图片结构化数据接入量计算，支持上下级视图库数据汇聚，单节点每日汇聚量达 5000 万。

- **视频库平台配套数据分析单元模块（各县区）**

配套云数据库服务完成数据的接入和查询 API，支撑上层业务平台进行数据的查询
支持接入的数据提供生命周期的管理；
针对实时流数据提供安全，可靠，可弹性扩展的数据传输平台，以消息流方式接入其他结构化数据；
支持对数据进行远程的备份功能;
支持对接入的数据进行流量统计，包括正常入库数据和异常入库数据等；
支持车辆、人像、Mac、RFID、交通业务等数据实时接入，支持数据入库前运维上自动建表
数据查询服务为上层服务提供统一 REST 接口，支持车辆、人像、Mac、RFID、交通业务的抓拍记录模糊查询、精确查询、关联查询；

1.2.5 视图库（公安网）

- **视频图像信息库管理平台**

与云存储结合，支持海量视频、图片信息的上传。支持通过多种关键字字段对非结构化的视频、图片信息进行结构化描述。支持海量数据的快速检索。可配置多台组成视图库集群，数量根据单台 3000 万/天纯结构化数据接入量计算 800 万/天带图片结构化数据接入量计算

- **平台数据分析单元模块**

英特尔至强双路处理器 4110 每路 8 核；64GB DDR4，可扩展至 768GB, ECC 内存；2 块 2.5 英寸 SATA 1TB 企业级机械硬盘，2 块 2.5 英寸 SATA 960GB 数据中心级固态硬盘，可扩展至 10 块 2.5 英寸硬盘；RAID 控制器：H730P；1Gbps*8；3

个 USB 3.0，1 个串口；2 个 VGA 接口；1+1 冗余电源；550W，白金级能效，满负荷小于 450W；

- **平台数据分析单元模块**

单控制器；高速缓存标配 16G；设备高度 4U；支持硬盘 36 个；1 个管理口 4 个千兆口 2 个万兆口；1 个 USB2.0 和 eSATA 复用接口；1 个 RS232 和 1 个 RS485

- **硬盘**

3.5inch 硬盘-容量 6000GB-缓存 128MB-SATA 接口

- **视频云业务存储网交换机**

L3 万兆以太网交换机，48 个 10/100/1000Base-T 以太网端口，4 个 10G Base-X SFP+万兆端口

- **多模光模块**

多模，双纤双向，10G，850nm，300m，-40~85 度,3.3V,LC 接口

- **单模光模块**

单模，双纤双向，10G，1310,20km，-40~85 度,3.3V,LC 接口

1.2.6 AR 全景指挥系统

- **云景实战指挥平台软件**

基于视频云架构，实现视频 AR 打标，通过关联视频、卡口、人脸、警情警力、周边资源等实现立体化全景监控；结合 AI（人脸识别、车辆二次分析）技术，替代原本观看监控视频录像的实战体验，提供全景浸入式指挥实战体验。

支持对下级平台标注的 AR 标签进行标签级联，上次不需要对点位进行二次标签处理；支持与 VR 场景的联动，做到 AR 与 VR 的联动；支持标签的防漂移和防抖动;支持事件报警、订阅人脸布控以及车辆布控报警并联动展示周边的警力资源。在全景画面不动的情况下，使用球机快速放大细节和跟踪目标；）

- **平台计算分析单元模块**

预装 Centor OS 6.7 操作系统；内存 2 条 32GB DDR4 2666 REG 内存；硬盘 2 块 2TB 3.5 寸 7200 转 6Gb SATA 企业级机械硬盘 ；RAID1 ；SSD 盘 2 块 Micron SSD SATA 5100 MAX 240G 2.5 英寸-SATA 接口 数据中心级固态硬盘

- **视频平台接入网关**

软硬一体化设计的联网网关设备。可基于 GB/T28181 等联网标准实现视频监控平台间的级联、互联功能，支持多平台多层次级联，实现平台之间的跨域互联互通与资源共享,具备高度的开放性与灵活性,为各行业视频监控业务提供高效易用、可靠。

1.3 视频图像综合支撑体系

1.3.1 视频计算分析单元模块

- **分析单元（1 型）**

2 颗 Intel 5120(2.2GHz/14 核/19.25MB/105W) CPU ；

32GB*12 DDR4-2666 内存；

1.92TB*1 6G SATA SSD ；600GB*2 12G SAS 10K ；4TB*5 6G SATA 7.2K ；标配 SAS RAID 阵列卡，支持 RAID0/1/10/5/6/50/60/1E/Simple Volume；配置 RAID 卡≥2GB 缓存；

4 个 10/100/1000M-BaseT 以太网接口+1 块双端口万兆以太网光口（含模块）

服务：提供原厂安装实施服务、五年原厂质保，提供原厂针对本项目的授权委托书与质保函。

- **分析单元（2 型）**

2 颗 Intel 4114(2.2GHz/10 核/13.75MB/85W) CPU ；
32GB*8 DDR4-2666 内存；
600GB*2 12G SAS 10K ；
标配 SAS RAID 阵列卡，支持 RAID0/1/10/5/6/50/60/1E/Simple Volume；配置 RAID 卡≥2GB 缓存；
4 个 10/100/1000M-BaseT 以太网接口+1 块双端口万兆以太网光口（含模块）
服务：提供原厂安装实施服务、五年原厂质保，提供原厂针对本项目的授权委托书与质保函。

- **分析单元（3 型）**

2 颗 Intel 5120(2.2GHz/14 核/19.25MB/105W) CPU ；
32GB*8 DDR4-2666 内存；
600GB*2 12G SAS 10K ；4TB*10 6G SATA 7.2K ；
标配 SAS RAID 阵列卡，支持 RAID0/1/10/5/6/50/60/1E/Simple Volume；配置 RAID 卡≥2GB 缓存；
4 个 10/100/1000M-BaseT 以太网接口+1 块双端口万兆以太网光口（含模块）
服务：提供原厂安装实施服务、五年原厂质保，提供原厂针对本项目的授权委托书与质保函。

- **分析单元（4 型）**

机架式设备，非刀片或高密度产品
处理器：2 颗 Intel Xeon Gold 5118 处理器（每处理器主频≥2.3GHz，核数≥12）。
内存：8 根 32GB ECC DDR4 2666 内存，最大支持 16 个内存插槽。
硬盘：5 块 1.2TB 10K 2.5 寸 SAS 硬盘+2 块 240G 2.5 寸 SSD；
Raid 卡：配置不少于 1 块 2GB SAS Raid 卡。
万兆网络接口：提供 2 个万兆 RJ45 网络接口+2 个万兆光纤网卡（含模块）。
配置显卡卡槽:配置 4 块 NVIDIA Tesla T4 16G 显卡
电源：满配 2 块 2200W 80plus 认证钛金级电源，1+1 冗余，支持 240V 高压直流。
服务：提供原厂安装实施服务、五年原厂质保，提供原厂针对本项目的授权委托书与质保函。

- **身份证解码分析单元**

身份证解码分析单元配备不少于 24 个解码模块。双电源供电，确保设备稳定工作。
解码分析单元内部每个身份证解码模块都直接由独自的 CPU 处理器控制，确保身份认证过程更快捷，更稳定，用户体验更好。

规格：
工作温度：-20 ~ +70 ℃
储存温度：-40 ~ +95 ℃
相对湿度：20 ~ 90% RH
大气压力: 86 ~ 106 Kpa
输入电压：双电源 100-240V
额定电流： 1.5A
最大功率：200W
内置 SAM： ≧24 个安全模块（SAM）
支撑不少于 2000 个前端用户应用

功能性要求：

1)支持多种采集方式：系统同时支持蓝牙终端设备、OTG 终端设备、NFC 手机等设备的对接解码要求；

2)可监控：可以通过网管协议对解码设备进行性能检测。可通过管理软件界面直观有效监控设备运行情况和当前使用情况，可统计使用数据。

3)易于开发：提供 SDK 包方式供各公安业务调用二代身份证识别系统接口；提供专用 APP 可直接只读取身份证信息并显示；提供公安网内的第三方系统调用接口。

性能性说明：

1)稳定性：网络解码设备不使用电脑主板和操作系统，以保障系统稳定，系统实现 7*24 长时间稳定运行。

2)准确性：准确解析二代身份证内的所有信息，完整返回所有解析结果。

3)健壮性：各个 SAM 模块由独立的 MCU 控制工作，各个 SAM 有独立的嵌入式操作系统。保证每个内部解码模块能独立工作，一块解码模块出现运行问题时不能影响其他解码模块正常工作。

4)自恢复性：网络解码设备的每个 sam 模块应具备自恢复能力，在运行出现问题后 5 分钟之内能够自动恢复。

5)响应迅速：手持终端从刷卡到后台反馈证件信息到终端不超过 5 秒。

6)安全性：服务端不做数据存储，网络解码设备不能带有硬盘，以确保不能存储身份证信息，保证信息不会外泄确保信息安全。

7）线性平滑扩展：通过增加解码分析单元满足线性扩容要求，且要求多台设备之间通过级联方式连接。扩容简便，扩容时无需停止运行中的服务。

含部署应用过程中所需的所有配套软硬件，并按照用户要求完成与相关系统对接。

- **大数据计算单元节点**

序号	设备名称	设备配置	数量
1	大数据在线集群计算节点	大数据在线集群计算节点，配合机框使用，固定配置包含节点框、主板、散热器、风扇、电源板、背板接口板，支持 BMC 远程管理，支持 Raid0、1 主板自带 2 个 GE 网口，具体配置如下： CPU： Intel Xeon Silver 4110*2 内存：256G 硬盘：1T SATA*2 Raid1 网卡：双口万兆网卡	20
2	大数据在线集群主机阵列卡 HBA	含 1 块主机卡 x8 Gen 3.0/双口 SF8644	20
3	大数据在线集群数据节点（SATA）	扩展接口：高速专用存储总线 盘位：支持 48*4T 7.2K SATA，支持 raid0、raid5 以及硬盘直连，支持断电保护。 主机接口：4 个 HD SAS 专用高速接口，每个接口对应 12 个盘位，和主机对点连接。 含三年硬盘不返还服务	5

4	大数据接入预处理节点	CPU:Intel Xeon Silver E5-2620v4*2 内存: 128G 系统盘：150G SSD 存储盘：1TB SATA*2 Raid：支持 Raid0、1 网卡：2 个万兆，2 个千兆网卡，1 个千兆设备管理口 预处理专用模块：专用多核 Cavium 66 系列硬件加速模块，10 核 MIPS64 r2 IntegerCore，每核支持 1 条并行硬件流水线；8G 流水线缓存，支持多流水线共享，也支持每流水线独立分配 HFA DPI Engine 加速的文本信息提取、规则匹配支持千万级虚拟身份实时比对 1 个千兆管理网口	2
5	大数据接入预处理节点	CPU:Intel Xeon Silver E5-2620v4*2 内存: 128G 系统盘：150G SSD 存储盘：1TB SATA*2 Raid：支持 Raid0、1 网卡：2 个万兆，2 个千兆网卡，1 个千兆设备管理口 预处理专用模块：专用多核 Cavium 66 系列硬件加速模块，10 核 MIPS64 r2 IntegerCore，每核支持 1 条并行硬件流水线；8G 流水线缓存，支持多流水线共享，也支持每流水线独立分配 HFA DPI Engine 加速的文本信息提取、规则匹配支持千万级虚拟身份实时比对 1 个千兆管理网口	1
7	大数据网络接入设备	32 万兆光口，千兆万兆自适应.	2
8	光模块-万兆单模	SFP+万兆单模/接收-14.4dBm	2
9	光模块-万兆多模	SFP+万兆多模/接收-11dBm	32

1.3.2 联网共享设备

- **市区核心联网共享设备**

1.性能：交换容量≥730Tbps，包转发能力≥460000Mpps；主控引擎数量≥2，独立的交换网板数量≥6，独立的业务槽位数量≥16。

2. 产品基于正交 CLOS 架构设计，主控与网板工作分离，采用无背板设计。

3.端口性能：支持 10G 光口、10G 电口、40G 光口、100G 光口，400G 光口。

4.IP 路由：支持 RIP、OSPF、IS-IS、BGP 等 IPv4 路由协议；支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。

5.虚拟化特性 支持 N:1 虚拟化技术（N≥4）。

6.跨设备链路聚合：支持跨设备链路聚合，能够实现多台设备间的链路聚合，从而把链路可靠性从单板级提升到设备级。
7.业务扩展：支持以独立业务插卡方式扩展防火墙、IPS、负载均衡、应用控制网关等功能，非功能授权方式。
8.业务性能:支持丰富的SDN特性,支持VXLAN二/三层网关功能,支持通过VXLAN结合EVPN实现DC内及DC间业务部署。
9.硬件加密技术：支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。
10.安全可靠：支持微分段、支持硬件BFD。
11.运维功能：支持Telemetry、支持INT（In-band Network Telemetry）。
12.安全和管理：支持故障后报警和自恢复；支持电源智能管理；支持802.3az高效节能以太网；支持RMON、NTP时钟；支持SNMP v1/v2/v3。
13.绿色环保：设备采用严格的前后通风设计，通风散热效率高。
14.10G端口功耗≤4.5W，40G端口功耗≤8W。
15.配置要求：配置双主控，满配独立的交换网板，满配电源，96个万兆光口，48个千兆光接口，48个千兆电口，24个万兆多模光模块，32个万兆单模光模块，24个千兆多模光模块,要求所有实配端口均为业务端口。
16.成熟度：为了保证设备的成熟性，设备入网时间不得低于3年，提供产品入网证证书，并加盖设备生产厂家公章。
17.服务要求：提供设备生产厂商5年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **区县核心联网共享设备**

1.性能：交换容量≥250Tbps，包转发能力≥72000Mpps；主控引擎数量≥2，独立的交换网板数量≥2，独立的业务槽位数量≥10。
2.架构：产品基于正交CLOS架构设计，主控与网板工作分离.
3.端口性能 支持10G光口、10G电口、40G光口、100G光口 。
4.IP路由：支持RIP、OSPF、IS-IS、BGP等IPv4路由协议；支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议。
5.虚拟化特性：支持N:1虚拟化技术（N≥4）支持1：N虚拟化技术。
6.跨设备链路聚合：支持跨设备链路聚合，能够实现多台设备间的链路聚合，从而把链路可靠性从单板级提升到设备级。
7.业务扩展：支持以独立业务插卡方式扩展防火墙、无线控制器、IPS、负载均衡、应用控制网关等功能，非功能授权方式。
8.业务性能:支持丰富的SDN特性,支持VXLAN二/三层网关功能,支持通过VXLAN结合EVPN实现DC内及DC间业务部署。
9.融合AC功能：支持融合AC功能，无需额外配置单独硬件，并且能在交换机上对所有上线的AP进行管理和配置。
10.硬件加密技术：支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。
11.安全可靠：支持CPU防攻击能力，保障CPU工作安全；支持BFD for VRRP/BGP/IS-IS/OSPF/RSVP/静态路由等，实现各协议的快速故障检测机制，故障检测时间小于50m
支持ISSU技术，升级过程中保障业务不中断。

12.安全和管理：支持故障后报警和自恢复；支持电源智能管理；支持 802.3az 高效节能以太网；支持 RMON、NTP 时钟；支持 SNMP v1/v2/v3。
13.配置要求：配置双主控，满配独立的交换网板，满配电源，52 个万兆光口，20 个千兆光接口，24 个千兆电口，16 个万兆多模光模块，24 个万兆单模光模块，8 个千兆多模光模块,要求所有实配端口均为业务端口，配置 1 块独立的防火墙板卡（要求吞吐量≥60G）。
14.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **区县汇聚联网设备**

1.整体要求：交换容量≥590Gbps，包转发能力≥220Mpps.
2.端口要求：千兆光口≥24，万兆光口≥4，扩展插槽≥1。
3.路由功能：支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP。
4.虚拟化特性：支持 N:1 虚拟化技术。
5.跨设备链路聚合：支持跨设备链路聚合技术，通过将两台物理设备在转发层面虚拟成一台设备来实现跨设备链路聚合，保持控制层面互相独立，提供设备级冗余保护和流量负载分担，同时提高系统的可靠性。
6.VXLAN 功能：支持 VxLAN 二层交换、路由交换和网关功能。
7.硬件加密技术：支持 802.1ae Macsec 安全加密，实现 MAC 层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验
8.管理和维护：支持 SNMP V1/V2/V3、RMON、SSHV2；支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准。
9.安全扩展功能：设备扩展槽位可集成防火墙插卡。
10.可视化能力：支持 Telemetry 技术，可通过 GRPC 协议将交换机的实时资源信息与告警信息上送至运维平台。
11.防雷功能：支持业界领先的 10KV 业务端口防雷能力。
12.配置要求：配置双电源，双风扇，实配 1 块独立的防火墙板卡（吞吐量≥4G），24 个千兆单模光模块，2 个万兆单模光模块。
13.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **网管一体机**

1.基本功能：统一平台实现网络、主机、应用、虚拟化等的统一管理。产品及组件为自主研发产品，不得采用 OEM 第三方产品；系统支持部署到 windows、linux 平台，支持使用 MS SQL、Oracle 数据库，采用 B/S 架构；系统支持分布式部署：要求资源拓扑、告警、性能等功能模块支持多设备分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理。单套软件可管理资源数>2000 个（含网络、主机、应用等）。
2.网络管理：支持多厂商设备管理，包含 Cisco、H3C、华为等，可对设备状态和基本信息的管理，包含了设备的基本信息、接口信息、性能数据和告警信息等。可提供直观的设备的面板视图，支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；支持网络设备存储空间管理，可浏览网络设备中存储的文件，提供整理建议。支持超长离线设备自动删除，可设置离线删除时间；可接收分析 Syslog，完成基本格式的解析，并入库。提供 Syslog 特征分析及策略注册能力，支持基于统计规则进行聚合生成告警（Trap）；可接收分析各类 SNMP trap 告警，完成基本格式

的解析，并入库，系统预定义解析各类 trap 类型不小于 6000 条，例如光模块失效告警、硬件故障告警、NBAD(网络行为异常检查)告警等。可对重复、闪断、未定义等 trap 告警进行过滤，可按照 trap 类型、trap 发送时间等进行 trap 告警过滤。提供 snmp trap 特征分析及策略注册能力，支持基于统计规则进行聚合生成告警；支持管理第三方设备：新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份、软件升级（使用 TCL/ Expect /Perl 模板自定制），第三方设备管理系统集成。

3.拓扑管理：自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等；支持 IP 拓扑、二层拓扑、自定义拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、全景拓扑、Vxlan 拓扑等多种拓扑类型；二层拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息。

4.性能管理：支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。

5.故障管理：支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转 E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能；

6.报表管理：支持多种图表展示：提供多种报表样式，包括普通的行列报表、主/子报表、图形摘要报表、交叉表、TopN 和 BottomN 报表。支持多种图形展示：包括条形图、饼图、曲线图、甘特图、面积图、圆环图、三维梯形图、三维曲面图、XY 散点图、雷达图、气泡图、股票图、漏斗图等。周期性报表机制：支持天报表、周报表、月报表、季度报表、半年报表、年报表。可以设定周期性报表的开始时间、失效时间。可以将自身的组织名称和 Logo 融入到发布的报表中，可以定时生成后 Email 到指定邮箱。

7.配置要求：配置软件一套，配置 500 个节点的管理授权，一体机的硬件配置不得低于：2 颗 intel 10 核 CPU，128G 内存，3 块 1.2T 10K SAS 硬盘，1 块 2Gb 缓存 Raid 卡，4 个千兆电接口，双电源。

8.服务要求：提供设备生产厂家商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

1.3.3 联网准入设备

- **联网准入控制设备**

1.硬件架构：采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块；采用控制、数据、业务相分离的全分布式架构，主控引擎、业务引擎、交换引擎、接口单元均硬件槽位分离;所有交换引擎必须为独立形态(非主控集成)，占用专用的硬件槽位，独立交换引擎 N+1 冗余，N≥3。

2.接口要求：独立的业务槽位数≥6，配置万兆光口≥32,40G 接口≥4。

3.性能要求：吞吐量≥260G，每秒新建连接数≥60 万，最大并发连接数≥4000 万。

4.部署模式：支持路由模式、透明（网桥）模式、混合模式。

5.路由功能：实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。

6.攻击防护：实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。
7.虚拟化功能：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（包含主备/主主模式）部署；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。
8.IPv6 功能：实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能；支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能；
9.NAT 功能：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。
10.攻击防护：实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。
11.安全策略 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；支持策略冗余分析， 冲突策略分析以及命中率统计
支持策略风险调优，定期分析用户策略，结合应用状况和流量情况，给出优化建议。
12.入侵检测：实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类；支持超过 7000 种特征的攻击检测和防御。
13.防病毒：可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表；支持超过 37000 条病毒规则。
14.诊断中心 支持报文示踪功能，可对原始报文进行回放；支持丢包统计，提供详细分析丢包原因。
15.设备管理：支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等；提供开放 API 接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。
16.配置要求：配置双主控，4 块独立的交换网板，32 个万兆光口,4 个 40G 接口，满配电源，满配风扇，8 个万兆多模光模块，设备需同时具备防火墙、IPS、防病毒三种功能。
17.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **防 DDOS**

1.设备形态；流量清洗系统结构一体化，应采用 B/S 架构，运行与管理无需外置环境配合，所有功能操作均能够在设备内置的管理接口上完成；
2.硬件规格：采用非 X86 多核架构，前后通风设计，具备可插拔冗余电源模块，可插拔冗余风扇模块；
3.设备可清洗混合攻击流量≥20Gbps，64 字节小包清洗容量≥12Gbps。
4.接口数：千兆 Combo 接口≥4，万兆光口≥2。
5.攻击防护能力：支持对欺骗与非欺骗的 TCP (SYN, SYN-ACK, ACK, FIN, fragments) 、UDP (random port floods, fragments)、ICMP (unreachable, echo,

fragments)、(M)Stream Flood 及混合类型攻击的防护；支持针对 SYN、UDP、ICMP、SYN/ACK、FIN/RST、IP Fragment、ACK 等网络层 Flood 类型的攻击防护；支持针对 HTTP GET/POST、HTTPS、DNS Query、DNS Reply、SIP 等应用层攻击的防护；支持针对 CC 攻击、慢速攻击、连接耗尽等连接型攻击的防护；支持每域名限速 DNS 合法性检查、DNS 过滤、TCP 校验、重传校验、Reply 状态防护、递归防护。
6.IPv6 攻击防护：设备必须支持 IPv6 基本组网功能及 IPv6 攻击的防御功能，包括支持 ISISv6、OSPFv3、BGP4+协议；支持 IPv6 Syn Flood、IPv6 DNS Query Flood、IPv6 UDP flood、IPv6 ICMPv6 Flood 攻击防御。
7.FLOOD 攻击防御：支持识别并防御各类 FLOOD 攻击，如 UDP Flood，UDP Fragment，ACK Flood，SYN Flood，FIN/RST Flood，TCP Misuse，TCP Connection Flood，TCP Fragment，ICMP Flood，ICMP Fragment。
8.HTTP 类防护：支持 HTTP 协议的清洗，包括但不限于：HTTP GET FLOOD、HTTP POST FLOOD、HTTP 代理攻击。
9.指纹防护：支持自动挖掘攻击特征功能，能自动发现攻击特征用于攻击防御。
10.管理功能：管理界面要友好、易用性强，应支持本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息；系统具备统一管理平台，在集群部署时支持对多台设备的集中管理，日志收集，运行状态监控，策略下发；针对防御主机 IP 能够进行流量排名、链接排名、攻击状态筛选等功能；支持手动指定参数抓包；手动抓包参数至少支持源目的 IP、源目的端口、协议类型、抓包时长、抓包数量等；支持自动抓包，当发生攻击事件时自动抓取报文留作回溯取证；抓包文件支持通过 wireshark 等分析软件进行解析分析
牵引方式 支持静态和动态牵引方式，并且支持 BGP、OSPF 路由协议；支持二层回注、三层回注、GRE 回注、MPLS LSP 回注、MPLS VPN 回注等多种回注方式。
11.资质要求：具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》。
12.配置要求：配置双电源，双风扇，2 个万兆多模光模块。
13.服务要求：提供设备生产厂家商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **数据库审计**

1.硬件架构：2U 高机架式硬件架构，支持冗余电源；内存≥16G，硬盘≥4T。
2.接口要求：业务接口：≥6 个千兆电口，≥8 个千兆光口，端口扩展槽位≥2。
3.性能要求：数据库吞吐量≥8Gbps，SQL 峰值处理能力≥6 万条/秒，日志存储数量≥18 亿条，可支持审计数据库实例无限制。
4.管理模式:支持对系统全集和分量（模块）的配置信息，执行备份与还原，分量信息包括： SQL 模版、报表任务、事件报表过滤规则、监听配置、事件定义、对象管理、客户端信息、敏感信息、事件响应、入侵检测规则、交换机信息、用户管理、数据归档参数、日志响应、集中管理平台配置、网络配置、管理主机、引擎相关配置、数据库相关配置，备份与还原；界面直观展示设备运行态势，通过五个色块动态展示服务运行状况、审计数据总量、告警总量、健康度（根据健康度自动变化颜色）、系统连续运行时间等重要信息。可在长达 90 日的时间范围内手动选择展示区间，同时支持以 1 分钟、10 分钟、1 小时作为统计单元。系统运行态势，包含 SQL 事务数（会话数据、明细数据、告警数据）、CPU、内存、负载。支持磁盘和固态盘的 I/O 使用率、存储状态实时展示，要求存储状态支持类型占比，类型包括数据库文件、备份文件、索引文件、交换文件、数据库缓存、

其他，以及提供磁盘健康状态和可用容量预测。以上内容需在同一界面中展示；支持系统自检功能且提供独立界面，当系统自身侦测到日志存储空间不足、昨日业务数据量超标、磁盘错误、license 过期、无配置备份、系统掉电、监听网卡断开等 18 类，涵盖系统运维中的各项重要消息时，独立弹窗提示用户并包含快捷处理方式；支持极简升级，提供友好的升级界面、并提供升级时长的预测。升级界面要求包含升级提示、升级进度、涉及数据量、升级时间预测及升级过程日志信息；支持对不同的数据库采用不同的编码格式解析，同时能对数据库实现自动的编码识别；支持在 IPV6 环境下部署和管理，且支持在纯 IPV4 环境、纯 IPV6 环境及 IPV4 与 IPV6 混杂环境下对数据库进行审计。

5.数据分析：支持对以下内容实现完全审计，包括超长语句、注释内容、多嵌套语句、绑定变量、RPC 等；支持对 TELNET、FTP、SSH、VNC、RDP 等远程操作行为的会话审计；提供力导向图，可实时查看当前数据库的连接情况，并通过对节点的点击展示更加详细的信息；支持事件告警，发现异常或非法行为。提供事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与该事件一样对应。支持快捷规则配置；同时，支持对审计数据的多种响应方式，包含过滤、记录、windows 消息、邮件、syslog、SNMP、屏幕录像、网关联动等多种事件告警和提示方式，第一时间向负责人发送告警信息；支持对异常操作行为进行追踪定位，审计到真实的 MAC 地址，而非网关路由的 MAC 地址；查询结果实时分析，系统支持在海量数据中，定义不少于 27 类条件进行查询，对查询结果实时统计分析，并以图表方式展示。在 1 亿条查询结果条件下，10 秒内生成统计分析结果。分析结果包括：分类统计（涉及源 IP、目标 IP、数据库用户名、数据名、应用程序名、协议类型、计算机名）、日期统计（按小时、日、周、月、年统计）、性能统计（包括单会话中语句种类数量、单会话的重复程度和单会话语句数量）。此外用户可自定义统计分析结果的展示内容，展示前 N 条数据、以升序或降序方式展示；支持因子监测功能，对数据库中突发增加的内容提供独立展示页面。因子内容包括：IP 地址、应用程序名、计算机名、存储过程、数据库用户名、数据名、数据库主机。系统记录因子出现次数，且能排序，可多维快速定位因子；支持 SQL 模板，系统能自动识别并抽取数据库句式语意相同但参数不同的语句，并通过独立页面展示，同时记录该模板的状态、触发规则名、总记录数、总告警数、上次告警记录数、上次出现时间、最后出现时间，并能设置该模板别名，通过模板直接进行过滤操作；支持网络审计，可定期获知数据库服务器是否存在非数据库的访问通讯，以协助判断潜在风险

支持基于 SQL 模板设置模板状态，过滤匹配该模板的语句，并能根据以下条件查询模板信息：关键字查找模板、触发规则、状态，且可根据所需选择排序字段。同时支持 SQL 模版和关联的具体语句的相互跳转查看；提供可视化、透明化的历史数据分析能力，让历史数据动起来。提供 30 分钟、1 小时、2 小时、8 小时、12 小时、1 天、7 天、30 天、90 天等时间范围内的数据选择，同时可根据需要，支持 1 分钟、10 分钟、1 小时、8 小时、1 天、1 周等 6 种细分度的统计间隔；支持审计数据中敏感数据的模糊化处理，系统内置常见敏感数据的掩码规则。

6.数据安全：产品拥有强大的数据库入侵检测规则库，能够对数十种针对数据库的常见漏洞和攻击手法进行检测，比如 SQL 注入，存储过程攻击，版本检测攻击，缓冲区溢出攻击，目录遍历攻击，拒绝服务攻击，权限绕过攻击，文件异常攻击等。

7.报表与查询：支持普通查询、模糊查询、明细查询、词组查询、流水号查询五种匹配命中方式，同时可叠加多达 27 种查询条件，其中包含会话语句种类、重复程度、耗时、数量、排除关键字及时段选择，查询结果支持多种格式导出；支持 TB 级海量数据多关键字秒级快速检索，检索速度小于 10 秒，并能实时对查询结果以图表方式进行统计排序；支持对高危报表元素进行二次编辑，使之产生更精确的报表，以图表方式展示各个字段，包括源 IP、目标 IP、SQL 相似度、操作方式、操作对象、规则编号、应用程序名的统计情况；提供报表缩略图展示，可快速一览报表结果，同时支持快速打开报表。
8.资质：具备公安部《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级。
9.配置要求：配置双电源，4 个千兆多模光模块。
服务要求 提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **堡垒机**

1.硬件规格：2U 高机架式硬件架构，支持冗余电源；内存≥16G，≥2 块 2T 硬盘。
2.接口数：配置≥8 个千兆电口，≥8 个千兆光口，支持≥2 个接口扩展槽位。
3.性能要求：最大图形并发连接数≥400，最大字符并发连接数≥1500，标准配置支持≥600 个资产的管理能力，支持无限个资产管理的扩容能力。
4.兼容性：支持 Chrome、Firefox、IE、Safrai 等主流浏览器；操作终端支持 Winddows 及 Mac OS 操作系统。
5.角色管理:系统支持账号分权管理，包括超级管理员、配置管理员、操作员、审计员及自动化人员等多种角色，并可根据功能自定义用户角色。
6.身份认证：支持与 Ldap、AD 域、Radius、短信网关等第三方认证平台对接，实现统一身份认证；支持双因素组合认证，可以将两种认证方式自定义组合为全新的认证方式；
支持 AD 账号的自动化同步，可将未纳管的 AD 账号自动添加到系统中并自动赋予指定角色，无需管理员干预。
7.账号安全：具备账号密码的防爆力破解功能，可在用户持续输错三次（可自定义）密码后自动锁定和自动解锁；支持基于用户来源 IP 及 Mac 地址限制用户的登录行为。
8.协议类型：支持 SSH、Telnet、RDP、SFTP、XDMCP、VNC 等多种协议，支持通过应用发布方式实现对 BS、CS 应用的纳管。
9.动态视图:支持按不同属性对资产进行多级分类并自动生成树状结构的资源视图。
10.跳转管理：支持不同资产之间的联动配置，彼此之间可实现自动跳转访问。
11.资产维护：支持资源信息批量导入、导出、修改、删除管理。
12.资源分权：支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同的部门（子部门）。
13.权限分权：支持访问控制策略按部门分权，不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置。
14.审计分权：支持审计功能按部门分权，使得不同部门的审计管理员只能审计自己部门、自己直属子部门设备上的操作日志。
15.访问权限：支持以用户（用户组）、目标设备（设备组、程序）、系统账号、服务等维度灵活设置访问策略；支持动态权限管控，管理员可基于用户属性、设

备属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、设备、账号即会被自动赋予对应访问权限；支持变更单管理功能，管理员可以基于使用人、资源、系统账号、到期时间，来上传、创建值班表模式的权限变更单，变更单无需审批，但可以自动生成时效性的访问权限；支持资源访问工单：用户填写包含工单标题、工单描述、需要访问的设备、需要使用的系统账号、需要访问的时间段的电子工单，经审批通过后可自动生成时效性的访问权限。
16.高危操作：可跟据用户（用户组）、目标设备（设备组）、系统帐号、命令集来设置详细的命令权限控制策略，支持命令黑白名单、命令批复、告警通知等多种模式；支持基于 A/B 角管理模式的双人复核，当用户登录到目标设备时，必须经过复核人的复核确认后才能正常操作当会话复核人发现操作存在风险，可实时暂停。
17.密码工单：支持密码工单管理，可通过工单申请相应资源的明文密码，审批通过后可通过邮件方式向申请人发送相应提示信息，有效期后平台会自动回收相应账号密码，并自动触发密码变更操作。
18.权限查看：支持按用户、资源统计查看权限分配情况。
19：资源展示：支持通过 web 页面以树状结构方式展现用户可访问的设备资源信息。
20.访问管理：支持 Web、Mstsc、SSH Client 等多种访问模式；支持批量启动功能，可一次性登录选择好的目标设备；支持设备收藏功能，用户可以对经常需要访问的目标设备做一键收藏，以便于下次可以直接在收藏夹中找到。
21.图形操作审计：支持图形化操作智能审计，可在审计回放界面上，同步显示关键的键盘操作、标题栏操作、剪贴板操作等文字信息，并能在点击任意文字信息，可直接定位到相关画面；支持图形操作的关键事件切片，管理员点击任意切片，即可直接定位到对应操作片段。
22.字符操作审计：支持以录像方式完整展示用户的指令操作，同时支持命令输入、输出分层管理。
23.文件传输审计：支持文件传输审计，可以完整记录用户通过系统进行的文件传输操作，并可对传输的文件信息进行留存，以便于事后审计。
24：数据库审计:支持 sqlserver、mysql、oracle 等数据库操作行为审计，可通过录像及 sql 语句方式查看用户相关操作。
25.审计分析：支持以 topN 模型展示用户的操作热点，如高危指令热度、用户操作热度分析等；支持资源、用户、操作三个维度审计智能检索，其中在操作检索层面，支持多关键字检索，检索结果直接定位到相关操作片段，并能将多个会话的操作片段进行一键合并和基于时间的操作排序重组。
26.事件审计：支持记录登录、配置及审计行为。
27.报表管理：支持用户、资产、系统账号、会话等信息的统计报表；支持自动化报表，可依据报表模板自动生成日报、周报、月报等自动化报表。
28.部署管理：支持主、备双机部署模式，支持三台及三台以上设备的多 A 集群化部署。
29.资质：具备公安部《计算机信息系统安全专用产品销售许可证》，要求提供中国信息安全认证中心《IT 产品信息安全认证证书》。
30.配置要求 配置双电源，4 个千兆多模光模块。
31.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **漏洞扫描**

1.硬件规格 2U 高机架式硬件架构，支持冗余电源；内存≥8G，≥1T 硬盘。
2.接口数：配置≥8 个千兆电口，≥8 个千兆光口，支持≥2 个接口扩展槽位。
3.功能要求：系统需支持主机漏洞扫描、数据库漏洞扫描功能和 WEB 漏洞扫描功能。
4.性能要求：系统漏洞扫描：扫描目标并发数量≥120 个，扫描进程并发数量≥200 个;数据库漏洞扫描:扫描目标并发数量≥120 个,扫描进程并发数量≥200 个；WEB 漏洞扫描支持：扫描目标并发数量≥10 个，扫描进程并发数量≥20 个；支持扫描任务并发数量≥10 个;最大可扫描无限个无限制范围的 IP 地址或域名，本次实际配置 512 个。
5.系统管理：系统采用 B/S 设计架构，并采用 SSL 加密通信方式，通过浏览器方便对产品进行远程管理；支持系统数据备份、恢复机制，支持对系统的数据，包括对扫描任务、扫描结果、扫描日志、扫描模板、参数配置文件等进行备份和恢复。
6.分布式管理：支持多级管理（3 级及 3 级以上），可以分布式大规模部署，可通过统一平台进行集中化管理；支持查看每个下级引擎节点的漏洞信息、资产风险概况；支持对各个引擎节点进行单独任务下发；各个引擎节点可以接收上级任务进行负载均衡扫描，提高扫描效率；支持创建分布式任务时可以对下级引擎节点进行过滤设置，让必要的引擎节点执行扫描任务，同时也可以对下级引擎节点设置特定的扫描目标；支持通告管理功能，上级结点可以对各个引擎节点发布消息。
7.资产管理：支持资产分组管理，可以增加、删除、编辑分组的功能；支持资产管理功能，包含增加、删除、修改等资产操作功能；支持资产导入、导出功能；支持资产自动发现功能，发现存活的目标自动添加到资产列表中，便于管理员对资产的管理；支持从资产管理直接选择目标资产进行创建扫描任务；支持查看各资产的风险等级、各种风险等级的漏洞统计、所有资产的风险等级统计功能。
8.告警管理：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。
9.主机漏洞扫描：主机漏洞知识库可检测漏洞数量≥50000+，其中可检测 CVE 漏洞数≥48000+个，非 CVE 漏洞数≥3000+个,漏洞信息全中文支持，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案；应提供漏洞规则查询的功能，方便用户查看；支持主机漏洞知识库与 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等国内外主流标准兼容；支持在扫描过程中人工指定包括 SMB、SSH、Telnet、SNMP 等常见协议的登陆口令，登陆到相应的系统中对特定应用进行深入扫描；支持 IPV4、IPV6 双协议栈地址扫描；支持不少于 5 种文件格式报表输出，如 HTML、PDF、WORD、XML、WPS。
10.数据库漏洞扫描：数据库漏洞知识库可检测漏洞数量 1500+，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案；应提供漏洞规则查询的功能，方便用户查看；支持 MSSQL Server、Oracle、MySQL、DB2、Informix、Sybase、达梦、人大金仓等主流数据库漏洞扫描；支持对数据库进行帐户口令认证登陆，登陆到相应的数据库中对特定应用进行深入扫描，其中主流数据库类型支持包括不局限于 Oracle、Mysql、MSSQL、DB2、Informix、Sybase、达梦等 7 种数据库类型；支持不少于 5 种文件格式报表输出，如 HTML、PDF、WORD、XML、WPS。

11.扫描任务：支持多个扫描任务多个目标并发执行；支持扫描计划任务管理，并将扫描结果自动发送给管理人员；支持断点恢复扫描，扫描过程意外中断恢复后支持自动继续扫描任务

支持多样化扫描任务管理，至少包括合并任务、导入任务、任务删除、重扫、复制扫描任务、暂停任务、中止任务、导出任务、扫描结果对比分析等；支持立即执行、暂不执行、定时执行、每日执行、每周执行、每月执行等不低于 6 种执行计划；支持任务优先级高、中、低三个级别。

12.扫描策略：支持扫描策略模板管理功能，包括对策略的增加、修改和删除等功能；系统内置多种扫描策略，分别针对不同的扫描对象，至少包括 Windows 系统、Linux 系统、Unix 系统、工控设备、WEB 服务、数据库、移动终端、网络设备等检测策略；系统内置多种的扫描方式，至少包括快速扫描、完全扫描等方式，以适应不同的网络环境需求。

13.报表管理：支持报表模板管理，用户可以根据实际需要，预先设定各种报表模板，满足不同场景的需求；支持用户自定义报表样式，可以对报表封面、任务综述、风险类别、风险分布、主机概述、端口信息、服务等信息进行分类，自定义报告封面 信息(包括不限于：报表的标题、描述、页眉、页脚等相关信息)；支持主机的漏洞分布、风险值和风险等级等信息展示，并列出主机的详细漏洞描述和解决建议；支持报表在线预览，批量下载报表。

14.安全管理：应提供系统管理员、安全管理员、操作员、审计员四种不同的角色，每个角色权限相互制约；分配给不同使用需要的用户，合理管理系统的使用权限，防止权限的滥用和误用，只有审计员可登录，对系统的操作日志进行增、删、改、检索、导出等操作；支持登录 IP 限制，限制用户只能在指定某些 IP 的主机上登录使用，支持限制用户可的扫描 IP 范围；支持登录时间限制，限制用户只能在指定的时间段使用；支持屏幕锁定功能，在扫描过程中，用户离开停止操作 15 分钟，程序将自动锁定屏幕（锁屏时间可配置）；支持用户锁定功能，在登录过程中，当用户连续输错密码 3 次，程序自动锁定用户（输错次数和锁定时间可配置）；支持任务锁定解锁功能，可以对任务进行锁定，防止其他用户对其任务进行操作，如果要对任务操作必须输入正解密码进行解锁；应提供数据备份功能，定期的数据备份，保护用户的数据。

15.产品升级：升级方式必须支持在线升级、离线升级和定时升级等方式；

16.资质要求：具备公安部《计算机信息系统安全专用产品销售许可证》。

17.配置要求：配置双电源，4 个千兆多模光模块。

18.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **访问准入控制设备**

1.硬件规格 2U 高机架式硬件架构，支持冗余电源；内存≥16G，≥1 块 1T 硬盘。

2.接口数：配置≥4 个千兆电口，≥4 个千兆光口，支持≥4 个接口扩展槽位，具备至少 16 个以太网千兆接口及 8 个万兆接口的扩展能力。

3.性能要求：HTTP 吞吐量≥5Gbps，HTTP 并发连接数≥100 万、HTTP 每秒新建连接数≥8 万，保护网站站点数量无限制。

4.系统管理：系统采用 B/S 设计架构，并采用 SSL 加密通信方式，通过浏览器方便对产品进行远程管理；产品界面友好，所有的图形界面、报警信息、报表与文档、技术资料要求均支持简体中文；支持 IPv4、IPv6 双栈防护；支持旁路镜像模式下，对检测到的攻击进行旁路阻断。

5.Web 安全防护：支持 HTTP 协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据；支持 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求；支持识别和阻断注入攻击；支持设置扫描陷阱，防止恶意扫描；支持爬虫防护；支持 LDAP、XPATH、struct2/xworks 检测和防护；支持识别阻断跨站脚本(XSS)注入式攻击；支持识别阻断盗链攻击；支持识别阻断跨站请求伪造攻击；支持非法上传检测阻断，包括恶意 WebShell 防护；支持对网页请求/响应内容中的非法关键字进行检测、过滤；支持识别和防止敏感信息泄露；且可自定义敏感信息特征，如用户名、密码、邮箱、身份证信息、MD5 密码等；支持敏感词防护并可自定义敏感词库；支持恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、缓冲区溢出攻击防护；支持虚拟补丁功能，支持导入 appscan 等第三方扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护；支持 cookie 加固及加密保护；支持页面访问顺序规则防护；
支持网站自学习建模，可通过学习 URL、host 等信息展示网站结构树形图，并支持对 URL 的访问量和响应健康度进行图形化统计； 支持通过自学习的 URL 参数的长度、类型、范围及请求方法等数据特点创建黑白名单模型，如果参数违反模型则判断为非法流量，直接执行阻断或封禁动作；支持自定义防护模板，提供通用、增强、专家的初始防护策略模板；支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作；支持第三方威胁情报库更新，支持利用威胁情报规则进行防护，并支持基于威胁情报的日志查询。
6.审计及告警：要求具备独立的审计日志、流量日志、攻击日志、DDoS 防护日志及威胁情报日志模块，且支持按不同日志分类进行 syslog 外发，至少支持字符串和 json 两种数据格式；支持日志定期自动备份导出；要求攻击日志具备详细的攻击和原始报文摘要；支持日志可视化，可对访问日志、攻击日志及安全情报等日志进行二次分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计；支持日志、trap、邮件、短信等告警方式。
7.监控及报表：支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计；态势监测支持对监测范围、防护区域和防护对象的自定义设置；系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名；能够根据网站的访问防护的网站、被篡改内容、篡改内容的类型、试图进行的篡改、成功的篡改、发现的日期、事件发生的日期等条件进行详细信息的查询 支持以 Word、PDF、HTML 等通用格式导出报表。
8.Web 漏洞扫描：提供 Web 站点安全扫描功能；支持自定义 Web 安全扫描任务，定期进行 Web 安全扫描。
9.高可用性：支持硬件 bypass 功能，支持软件 bypass 负载保护机制，设备达到峰值时，切换 bypass 功能。
10.管理方式：支持 HTTPS、SSH、Console、WebShell 多种管理方式。
11.资质要求：具备公安部《计算机信息系统安全专用产品 销售许可证》-增强级。
12.配置要求：配置双电源，4 个千兆多模光模块。
13.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **日志审计**

1.硬件规格：≥1 颗 8 物理核 CPU，内存≥64GB，存储容量≥12TB；实配 4 个千兆电接口，2 个万兆光口，冗余电源。
2.性能要求：事件入库性能≥4000，≥512 日志源。
3.系统管理：支持 WEB 界面管理，通过 WEB 界面全程进行设备配置、回溯、查询等操作。
4.全局概览：顶栏显示采集器数、日志源数、日志数、告警事件数、关联规则统计，并且支持下钻查看详细信息；图表显示：日志按设备类型分布、日志按等级分布、日志按类型分布，并且支持下钻查看详细信；可实时展示关联事件数量趋势、平台自身性能实时监控图（CPU、内存、磁盘）；可选择基于一天、一周、30 天进行展示；首页数据支持自动刷新，无需人工刷新界面。
5.日志查看：具备日志收集实时监控，可基于设备类型、日志类型、日志等级进行监控查看
支持按照设备类型（交换机、路由器、FW/IPS/LB/WAF、数据库、中间件、主机等设备）列表查看日志范式化分析结果，支持查看日志详情；支持基于时间、日志类别进行筛选；支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、主机日志等 11 大类 70 子标签进行分类；支持多条件查询，包含开始时间、结束时间、动作类型、设备名称、日志等级、用户名、源 IP、目的 IP、协议等条件进行过滤查询展示；支持按照日志等级（调试、通知、重要、警告、错误、严重、设备故障、设备不可用及其他信息）列表展示日志范式化分析结果、下钻支持日志详情。
6.日志分析：支持多类型、多厂商安全设备、网络设备、操作系统、应用日志适配分析；对原始日志的日志内容进行适配分析，分析结果范式化展示：可对多源日志进行递归关联、时序关联、统计关联等方式关联分析，提升安全分析结果准确性。
7.日志概览：预定义日志概览：支持默认展示操作日志设备 IP 分布、审计日志审计类型分布、威胁日志攻击分类分布、威胁日志设备名称分布、威胁日志严重等级分布、安全控制日志目的 IP 分布；支持按照时间周期（一天、一周、30 天）进行过滤展示；自定义日志概览：支持用户自定义统计维度展示日志审计结果，具备多种日志类型、统计属性交叉统计 160 种图形展示可选择；可同时展示 6 个维度审计结果；支持用户自定义统计效果，可选择饼状分布图、折线趋势图、柱状比较图；支持按照时间周期（一天、一周、30 天）进行过滤展。
8.全文检索：支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式。
9.关联规则：支持新增、删除、修改和导入关联规则，对关联规则进行启用和停用管理；支持按照规则名称，事件名称，使用状态，威胁等级进行检索查询；支持查看规则详情；支持安全策略命中次数统计。
10.事件概览：支持预定义事件概览和自定义事件概览；支持用户自定义统计维度展示关联事件审计结果，最多同时展示 6 个维度审计结果；支持用户自定义统计效果，可选择饼状分布图、折线趋势图、柱状比较图；支持按照时间周期（一天、一周、30 天）进行过滤展示。
11.事件明细：列表显示安全事件明细的详细信息，主要包括发生时间、过滤类型、事件等级、事件名称、源 IP 地址、目的 IP 地址、规则名称、事件描述、原始事件数、处理状态、支持操作等信息，支持查看原始事件详情进行追溯；查询

支持按照开始时间，结束时间，事件等级，处理状态条件进行检索查询；基于事件状态进行批量处理，确认安全事件状态；支持安全事件导出。
12.报表：报表查看：支持按照报表任务和模板名称进行查询；支持配置报表自动转发至用户邮箱；支持自定义定时清理历史报表，节省系统空间；支持报表任务的新增/删除/修改/启用/停用等管理；支持按照任务类型/任务状态/任务名称进行查询；预定义报表模板：默认报表模板为日志统计报表、事件统计报表；显示报表模板和报表名称的对应关系，支持预览报表模板，支持按照模板类型和模板名称进行查询；自定义报表模板：支持自定义报表中日志统计维度、统计方式（柱状图、饼状图、折线图、表格）；支持用户自定义报表样式，可基于日志、关联事件结果生成 50 多种维度的自定义统计报告；支持报表自定义时预览，方便用户定义理想报表。
13.数据清理：支持对数据清理进行时间阈值或空间阈值设置。
14.角色及权限管理：展示当前系统用户列表和用户状态，可对用户进行增删改查操作；对系统用户角色进行管理；可查看系统当前在线用户即访问时间；展示当前系统用户列表和用户状态，可对用户进行增删改查操作。
15.日志采集:被动日志采集：支持包括 SYSLOG、HTTP、NetFlow；支持日志源增删改功能；支持列表展示日志源的详细信息，包括名称、IP、设备类型、型号、厂商名称、关联采集器、上报端口（支持特定用户绑定特定的日志源）等信息；支持按照 IP、设备类型、厂商名称、设备型号进行检索查询；主动日志采集：支持包括 FTP、JDBC\ODBC、Agent 终端采集；支持增删改查共享文件主动采集日志源、数据库主动采集日志源；支持列表展示日志源的详细信息，包括日志类别、日志源名称、类型、IP、采集器地址；支持按照名称、日志源类型检索查询。
16.日志管理：可导入文件类型日志（txt、log）；可新增、删除日志转发策略，支持转发频率调控。
17.告警管理：支持配置告警规则、告警方式；支持告警策略新增/删除/修改/启用/停用管理；支持告警策略高级查询，基于策略名称、告警类型、策略状态等信息进行查询；支持告警记录高级查询，基于开始/结束时间、策略名称、告警类型、处理状态等进行查询。
18.资质要求：具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，能提供有效证书的复印件。
19.配置要求：配置双电源，4 个千兆电口，2 个万兆光口，2 个万兆多模光模块。
20.服务要求：提供设备生产厂商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **行为管理**

1.硬件架构：多核架构设计，不允许采用 X86 架构，功能采用模块化结构设计，提供 CPU 型号、频率，双电源；内置软件 Bypass 模块，内置两路电口 Bypass；在设备流量异常时，可自动切换到 Bypass 状态，当设备恢复时，可自动切换回工作状态。
2.接口要求：千兆电口≥12，千兆光口≥12，万兆光口≥4。
3.部署模式：支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备。
4.路由协议：支持静态路由、策略路由、RIP、OSPF、ISP 路由，其中 ISP 路由支持自定义，并可提供基于应用的策略路由。
5.NAT 功能：支持源地址转换、目的地址转换、双向地址转换、NAT44。

6.IPv6 功能：支持接入 IPv6 网络，支持配置基于用户和应用均为任意的 7 元组的 IPv6 策略

支持 IPv6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。

7.应用协议识别：支持主流 P2P、IM、在线视频、网络游戏、网络炒股等应用识别；支持 BYOD 特征库，可识别 ios 版和安卓版移动互联网软件如腾讯微博、QQ 空间等特征；支持基于 IP、端口等自定义协议服务；应用特征库可提供在线升级和手动升级。

8.用户行为控制：支持自定义关键字对象，提供基于关键的邮件、http 等相关内容的关键字过滤功能;支持用户应用的精细化控制,例如微信的:“微信”“微信语音”“微信发消息”“微信收消息”“微信登录”“微信发文件”“微信收文件”；支持邮件详细控制，针对 smtp 发邮件方式，支持针对发件人、收件人黑白名单过滤，针对标题正文支持关键字控制，针对邮件大小和附件个数支持相关控制；支持针对 web 相关行为的关键字过滤，支持针对 web 搜索引擎、web http 上传、web 网页内容的关键字控制；支持针对虚拟账号的黑白名单控制。

9.用户行为审计：支持一键化快速审计策略配置；支持 http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计；http 类审计支持网页访问、网络社区（微博、论坛）、网页搜索、http 外发文件、http 文件下载、web 网盘上传文件、web 网盘下载文件等细粒度的审计；邮件类审计支持 smtp 的发邮件，imap&pop3 收邮件、外发的 web mail 邮件内容、外发的 web mail 邮件附件、接受的 webmail 邮件内容、接受的 webmail 邮件附件等细粒度的审计；即时通讯类审计支持 IM 聊天行为审计、网页版微信审计、移动飞信审计、其他即时通讯类软件审计等细粒度的审计;基础协议类审计支持 FTP 的账号和文件名相关审计；娱乐股票类审计，支持娱乐类的账号和评论审计，支持股票类的账号审计；其他应用行为审计，支持管理员选择相关审计的应用大类。

10.流量管理支持高性能的限制通道，限制通道支持基于接口、地址、用户、用户组、应用、服务、时间维护的条件匹配，支持每 IP 和每用户限速配置；支持惩罚通道建立、支持惩罚通道内限制每 IP 和每用户限速；支持通道化的 QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每 IP 带宽、流量限额、带宽优先级等 QoS 动作，时间选择支持基于日计划、周计划、单次计划等；支持 4 级层次化 QoS、支持多级用户/用户组嵌套；支持用户（用户组）+应用（应用组）+时间等条件的组合进行多线路带宽管理；支持进行 IP、整机会话限制；支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现,可查看某一应用的流量趋势图和其 Top 流量用户；支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义；支持流量和时长的月限额。

11.用户管理:支持同步 LDAP 用户,支持 AD 域单点登录,标准 AD 设备和 OPEN LDAP 设备的用户导入，支持针对同步的用户和用户组配置策略；支持与 AD 的自动同步用户，支持定时、配置及手动同步第三方用户；支持通过 LDAP 方式、SNMP 方式、ARP 方式获取用户同步；支持针对上网用户一段时间 URL 排名，生成用户标签。

12.统计报表：支持定时的邮件统计报表发送，支持 pdf 和 html 格式；支持针对实时行为管理数据生成统计报表，并支持导出；支持日报表、周报表、月报表、一次报表任务创建；

13.系统日志要求：支持本地日志记录和远程日志输出、支持专用的日志审计管理软件、支持中文日志、支持日志导出。
14.业务告警：支持针对设备健康状态，业务信息等维度告警；告警事件入库支持展示，查询，导出；告警事件支持弹窗，邮件；弹窗默认展示最近 10 条告警记录。
15.配置要求：配置双电源，5 年特征库升级服务，4 个万兆多模光模块。
16.服务要求：提供设备生产厂家商 5 年技术支持服务。提供原厂针对本项目的授权委托书与质保函。

- **终端安全准入**

1. 设备规格：硬件一体化专用设备，外观尺寸 2U，支持旁路部署；双路 Intel 至强 CPU，16 核，内存 32G，存储空间不少于 1TB，支持 RAID1；配置 2 个千兆自适应电口，支持 8 个端口扩展插槽；1+1 冗余双电源。
2.端点发现：能够对网络中的未知设备（无法提供设备管理权限）、未知端点、未产生流量的端点主动发现。包括但不限于交换机、路由器、防火墙、服务器、PC 终端、打印机、摄像头、配电终端、RSU 等等。
3.端点识别：、能够自动识别接入网络所有 IP 端点，识别信息包括端点 IP、MAC、所属区域、端点类型、操作系统、厂商信息，在线状态、合规状态等；接入端点的上联交换机端口信息发生变化（up/down），能够立刻发现，并对接入端点进行识别。
4.端点识别种类：能够识别出至少 10 家主流摄像头信息。
5.网络设备识别：能够识别出至少 10 家主流网络设备厂家及类型。
6.识别规则自定义：端点识别策略能够自定义：按 IP 地址段、端口深度、协议深度、场景（只识别某种特定端点）并支持 NAT 场景下的识别。
7.端点准入控制：能够自动识别非法私接、仿冒的端点，并实时告警，告警方式包括但不限于：大屏、短信、邮件、手机 APP；同时能够主动将非法端点加入黑名单，阻断非法终端的接入；为了确保接入端点的合规，保障在网端点的安全，新的端点接入网络后，即使没有产生流量，也能够对此端点合规性进行判断，并主动对非法端点阻断。
8.端点状态统一监控：网络中所有 IP 端点类型、数量、在线状态、合规状态、告警信息统一图形化展示。
9.资产报表：可以从端口信息、端点状态、在线状态、端点类型、某类端点状态、厂商、新发现端点等多个维度输出资产报表。
10.端点拓扑：能够展示整网拓扑；端点拓扑可展示：在线状态，合规状态，终端及设备类型，厂商。
11.资质：提供公安部计算机信息系统安全专用销售许可证（准入控制二级）及测试报告，并加盖设备生产厂家公章。
12.本次配置 5 台扫描器，扫描器设备规格：硬件一体化专用设备，支持旁路部署；单路 Intel 至强 CPU，8 核，内存 16G；配置 6 个千兆电口，2 个千兆 Combo 接口，固化电源。
13.原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **视频与数据安全接入平台**

1	万兆安全数据交换	硬件形态：标准机架式机箱，双主机架构，专用安全加固 Linux 操作系统，冗余电源。	4

	系统	内网接口：标配 1 个 100/1000M Base-TX 管理接口，1 个 10000M SFP+多模光模块网闸接口，1 个 10000M SFP+多模光模块网络接口，1 个 100/1000M Base-TX 网络接口。	
		外网接口：标配 1 个 100/1000M Base-TX 管理接口，1 个 10000M SFP+多模光模块网闸接口，1 个 10000M SFP+多模光模块网络接口，1 个 100/1000M Base-TX 网络接口。至强四核 CPU，主频 2GHz 或以上，内存≥16GB. 数据影射最大字段数≥256	
		数据库到数据库交换记录数（≥400Kb/记录）≥1,5000 条/秒；	
		数据文件处理文件数（≥400Kb/文件）≥1,5000 个/秒；	
		系统吞吐量≥4000Mbps	
		最大支持服务≥80	
		产品原厂商必须入围《通过公安部组织测试的接入平台厂商名单》，提供公安部网站截图。	
		产品具备《商用密码产品型号证书》	
2	隔离网闸	硬件形态：万兆标准型，标准 2U 机箱，双冗余电源；整机配备液晶屏和设备健康监控声光报警装置；	4
		内网接口：标配 1 个万兆 XFP 接口（包含万兆光纤模块），4 个 10/100/1000M Base-TX 网络接口，1 个 10/100/1000M Base-TX 管理接口，1 个 10/100/1000M Base-TX HA 接口（双机热备口）；	
		外网接口：标配 1 个万兆 XFP 接口（包含万兆光纤模块），4 个 10/100/1000M Base-TX 网络接口，1 个 10/100/1000M Base-TX 管理接口，1 个 10/100/1000M Base-TX HA 接口（双机热备口）；	
		最大传输延时<=20μs	
		最大硬件数据吞吐量≥30Gbps	
		应用层数据传输率≥4000Mbps	
		最大支持服务≥80	
		主要功能：	
		1、符合等级保护三级要求，支持三权分立的管理；	
		2、支持 HTTP、TCP、FTP 等多种通道服务；	
		3、支持共享、客户端、FTP 等多种模式的文件同步服务，实现文件实时同步；	
		4、支持文件同步断点续传；	
		5、支持数据库同步；	
		6、支持查看各个服务的运行性能及流量；	
		7、支持病毒过滤，对病毒数据进行隔离处理并报警；	
		8、支持 SNMP V2/V3 协议，实现网闸与标准网管平台的无缝集成；	

		9、具有完善的日志记录和检索功能，完整地记录传输、报警、操作员操作等审计数据；	
		10、支持 IPV6。	
3	万兆交换机	24 个 10/100/1000 以太网端口，万兆接口 4 个；	2
4	万兆防火墙	机架式硬件万兆防火墙，专用硬件平台。网络处理能力>15G，标准机架式，标配 6 个 10/100/1000BASE-T 接口，1 个扩展插槽，并含 2 个高速 USB2.0 接口，可接移动存储进行日志存储。可支持 4 个万兆光口。	4
5	集控探针	标准 1U 机架式机箱，集成 4 个 10M/100M/1000Mbps 千兆网络接口，安全加固 Linux 系统。	2
		MTBF(平均无故障时间间隔)> 50000 小时，支持 SYSLOG 协议	
		支持 SNMP v2/SNMP v3 协议	
		必须支持与徐州市局集中监控系统对接，报送数据。	
6	视频安全接入系统	视频安全隔离设备：2U、内外网各支持 6 个千兆电口，4 千兆光口；2 个万兆光口。	4
		产品原厂商必须入围《通过公安部组织测试的接入平台厂商名单》，提供公安部网站截图。必须具备网络关键设备和网络安全专用产品安全认证及中国国家信息安全产品认证	
		系统性能参数	
		≥4000 路并发（标清：每路 D1 画质，1Mbps） ≥1000 路并发（高清：每路 D4 画质，4Mbps） 主要功能 1、支持集群、容错功能。 2、支持双机热备、负载均衡。 3、支持标准 TCP、UDP 协议。 4、支持 DB33、GB/T28181-2011 规范标准。 5、支持大华、海康威视、星望、天视、先进视讯、博康、华为 3COM、浙江贝尔等多数主流视频系统。 6、支持视频信令与协议的分析、过滤。 7、支持视频数据单向传输、控制信令双向传输。 8、支持同时承载若干个不同的视频传输服务，每个服务可以单独启停。 9、支持认证公安警用硬件数字证书。 10、支持对视频服务器的认证。 11、支持用户域、可信域管理方法。 12、具有完善的日志管理功能，提供详尽的开机、传输、管理员操作等日志的查询及显示功能。 13、支持高速传输通道，支持多路视频并发。	

		14、支持功能定制，提供扩展接口，满足不同用户的个性化要求。 15、支持 M-JEPG，MPEG4、H.264 等编码格式，D4、D1、VGA、2/3D1、1/2D1、SIF、3/4D1、CIF、QCIF 等视频分辨率。	

原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **防毒墙**

硬件指标　三层吞吐量 14Gbps，应用层吞吐量 4Gbps；并发连接数 250W，新建连接数 22W；　硬件指标：2U；64G SSD+SATA 1T 存储；双电源；1 个串口（RJ45），2 个 USB 2.0，6 个千兆电口+2 个万兆光口（含光模块），≥2 个扩展槽，

部署方式　支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；

网络特性　支持静态 ARP、ARP 代理、DNS、DNS 代理、DHCP server、DHCP 中继、SNMPV1/V2/V3/Traps、TCP MSS 配置；

支持 IPV6 环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS 漏洞防御，WEB 应用防护等，支持协议一致性（包括但不限于 Core、NDP、Autoconfig、PMTU、ICMPV6）和协议健壮性检测（IPv6 畸形报文、ICMPv6 畸形报文、其他协议畸形报文），支持 IPV6 的地址转换、双栈的过渡技术。

路由支持　支持静态路由，ECMP 等价路由；

支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；

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；

基础功能　访问控制规则支持模拟策略匹配，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；

内容安全　支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，并给出恶意邮件的提示，支持根据邮件附件类型进行文件过滤；

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；

支持识别管控的应用识别规则总数超过 9500 条，并支持自定义应用规则；

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 SMB v1/v2 协议传输的文件杀毒；

支持非 PE 文件的杀毒；

支持不少于 7 层的压缩文件查杀；

僵尸主机检测　设备具备独立的僵尸网络与病毒防护库，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 104 万条以上；

支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测；

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；

支持对未知域名进行拦截，防止中毒主机访问恶意的域名；

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；

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；
支持基于勒索病毒的攻击链提供勒索病毒防护配置向导，包含防护对象、勒索病毒常用端口、漏洞、弱口令的自定义定时识别及自动生成包含 WEB 应用防护、漏洞防护、内容安全、僵尸网络检测、慢速爆破防御等勒索病毒防护策略。
支持通过专门页面进行基于问题主机 IP 的勒索病毒风险管理，并针对不同事件进行风险定级，在提供处置建议的同时应具终端处置的能力。
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；
原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **敏感数据保护**

硬件指标　1U 机架式；6 个千兆电口，1 个扩展插槽，峰值运维 SQL 吞吐量 3000 条/秒，峰值 SQL 审计吞吐量 4500 条/秒,在线会话 5000 个,
80 亿条在线 SQL 语句存储。
>=2T 存储空间
敏感数据发现　内置多种敏感数据发现策略，可自动梳理发现敏感数据
敏感数据分类和管理　　持自定义敏感数据范围，可在表级和列级两个粒度进行配置，多个数据表格归类成为敏感数据集合，进行独立安全管理
多因素身份登陆管理　　支持多维身份管理，至少支持应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U 盾等因素进行任意组合，形成新的登陆认证规则
支持对管理工具或客户端应用程序进行签名登陆验证，防止恶意和仿冒的工具或程序登陆。
　　支持为敏感数据管理人员身份分配唯一的数字证书，每张数字证书只能载入一个唯一的 U 盾。
权限分离　特权用户权限分离：支持禁止特权用户（DBA\SYSDBA\Schema User\any 权限等用户）访问和操作敏感数据集合，实现特权用户权限分离管理
访问控制
　　针对敏感数据集合的访问，需要通过授权才可以访问，不具备访问权限的操作，明确阻断拒绝，并提示“安全权限不足错误”
　　账户管理操作（Create user、Alter user、drop user 等），授权管理操作(Grant)，业务对象操作（Truncat table，drop table）以及业务代码操作（修改 Package，修改 view）只有具备操作权限的安全管理员和授权人员才可以进行操作。
　　支持访问返回行数控制，对批量下载、更新等操作的控制，避免海量数据泄漏
　　支持访问频次控制，避免一定时间内的高批次访问，避免非法人员通过高频访问快速窃取业务数据
　　具有敏感 SQL 特征库，能够对勒索等恶意代码进行快速识别和防御
细粒度审计分析　　支持 SQL 命令的细粒度审计和分析，并详细记录管理用户的行为信息，包括该语句执行的时间、机器名、用户名、IP 地址、MAC 地址、客户

端程序名以及 SQL 语句等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控

动态脱敏　运维管理端数据脱敏：支持 SQLPLUS、PLSQLDEV 等 SQL 管理工具查询数据时的动态脱敏，根据用户的身份与访问的数据库对象以及对应的脱敏规则，对不同授权的用户可返回真实数据、部分遮盖、全部遮盖以及其他脱敏算法得到的结果。

运维管理端数据脱敏需支持如下几种模式：

放行：对于已授权用户，返回真实数据；

返回空：对含有敏感表格或敏感列的数据结果返回为空值；

遮盖：全遮盖：默认以遮盖符‘*’替换敏感列的值；

部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；

随机映射：对数值、字符或字符串进行随机映射处理；

口令猜测防御　密码猜证检测防御：支持检测和审计密码猜测行为，通过设置密码猜测次数限制进行防护。达到密码猜测限制，锁定猜测终端，支持自动解锁和手工解锁

SQL 语句翻译　SQL 语句提供直译和意译的不同翻译引擎，从英文翻译成中文，增加阅读性直观性。

运维工单　通过工作流的方式对表格和 SQL 访问授权，使整个过程更加透明，有迹可寻。简化安全管理流程，使安全管理更加便捷。

产品资质　具备公安部颁发的《计算机信息系统安全专用产品销售许可证》；

具备 ISCCC 信息安全认证中心颁发的《中国国家信息安全产品认证证书》；

具备保密局颁发的《涉密信息系统产品检测证书》

原厂商资质 ISO27001 信息安全管理体系认证证书。

ISO20000 信息技术服务管理体系认证证书。

原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **数据脱敏**

硬件指标　1U 机架式；6 个千兆电口，1 个扩展槽，脱敏速度至少每秒 40 万个数据单元，>=2T 存储空间

支持类型　支持市面上主流的关系型数据库作为脱敏的源和目标,具体包括 Oracle，mysql，ms sqlserver，greenplum ,ingre vectorwise ,intersystems cache ， kingbaseEs ， lucaidDb ， mariadb ， maxdb(sap db) ， monetdb ， msaccess , native mondrian , neoview ,netezza , oracle rdb , postgresql , redshit ， sybase ,terdata ,vertica；sqllite；支持 hdfs,hive,impala 和 kafka 等大数据平台

支持 txt,csv,dmp,dbf 等文件类型作为脱敏源和目标,且支持远程 ftp 和 sftp 发现

脱敏方式　支持将 Oracle dump 文件作为脱敏源,支持 dump 到 dump,dump 到库的脱敏方式

支持库到库脱敏、库到文件脱敏、文件到文件脱敏、文件到数据库脱敏

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。数据脱敏系统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：姓名,身份证,银行卡,cvv,医生资格证书,医师执业证书,护照,军官证,护照,组织机构代码,组织机构名称,营业执照,社会统一信用代码,

税务登记,开户许可证,证券名,证券代码,基金代码,基金名,电话,邮箱,ip 地址,车牌号,邮箱

脱敏规则管理　支持客户根据自身特殊数据进行脱敏发现规则定义,并且可设置类型名称。

脱敏系统需内置丰富的脱敏规则，包括确定随机、遮盖、仿真脱敏（包含姓名、地址、电话、证件号码、邮箱、邮编、银行账号、组织机构代码、营业执照等）等规则；脱敏规则在界面方便管理，自定义增加（如：支持字符串和数字的映射、截取、截断、位移等）；支持依赖脱敏，即：混合字段依赖类型字段的脱敏。

对敏感数据进行多个分段处理,对指定的分段进行脱敏,其余保留原指. 如身份证可以分为地址码（省）、地址码（市）、地址码（区）、出生日期码（年）、出生日期码（月）、出生日期码（日）、顺序码.

脱敏算法秘钥机制，即脱敏算法加秘钥生成新脱敏算法，并且秘钥每隔一段时间脱敏管理员可自定义手工修改,修改秘钥后脱敏后的数据和原脱敏算法脱敏后的数据不同，便于脱敏规则安全管理。

支持表、主键、外键、索引、约束、视图、同义词、序列、自定义类型、存储过程、函数、触发器、包等数据库对象脱敏后在目标库中自动创建。

脱敏策略　对于字符型敏感数据对象，支持随机、固定映射、遮盖、截取、截断方式脱敏；对于数值型敏感数据对象，支持随机、移位、截断、取整方式脱敏

同一列数据中包含多种数据类型(如证件号码列中包含身份证、军官证、护照),脱敏后仍然能够生成和对应源数据一致的数据特征.

对敏感数据进行多个分段处理,对指定的分段进行脱敏,其余保留如：身份证可以分为地址码（省）、地址码（市）、地址码（区）、出生日期码（年）、出生日期码（月）、出生日期码（日）、顺序码.

支持脱敏前某个字段值为多个字段之和，脱敏后仍然保持脱敏前的数据计算关系。

支持多域类型的敏感信息脱敏（将多种类型的敏感数据拼装成一个字符串进行存储，例如：联系方式中的手机号码与固定电话。

一个字段内包括身份证、军官证和护照等数据集合时，支持按照不同的数据特征采取不同的脱敏规则进行脱敏。

数据子集用于控制数据脱敏的范围，数据子集外的数据不需要经过脱敏平台，防止大量的无关信息被操作。

在选择表格生成脱敏源的过程中,要求能够对源端表格通过关键字进行筛选,减少人工肉眼筛选的工作量.

不落地脱敏 数据脱敏过程完全不落地：

（1）不存在数据中间泄漏风险（2）无需额外存储存放中间数据。

原厂商资质 原厂商具有 ISO27001 信息安全管理体系认证证书；

原厂商具有 ISO20000 信息技术服务管理体系认证证书；

产品资质　具备公安部颁发的《计算机信息系统安全专用产品销售许可证》；

原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **数据库加密**

硬件指标　1U 机架式；6 个千兆电口，1 个扩展槽，峰值 SQL 吞吐量 15000 条/秒，在线会话 6000 个,80 亿条在线 SQL 语句存储，>=2T 存储空间

支持类型　支持 Oracle、SQL Server、MySQL 等数据库加密。防止明文存储引起的数据泄密
加密粒度　支持以表、列、库为单位进行数据加密
加密算法　支持 DES、AES 等国际密码算法
密钥管理　支持密钥统一自动备份功能
透明加密　加密数据对应用透明，业务系统及数据库访问工具如：PL/SQL、JDBC、ODBC 等访问过程不受影响，不涉及业务系统的二次开发。
同时对于增删改查操作，函数、存储过程等均透明；对于主外键、唯一索引、NOTNULL 等重要约束透明。
支持随机盐加密策略
一致性存储加密　Oracle、SQL Server 等数据库重要日志文件以密文形式存在、数据库备份以密文形式存在、索引数据以密文形式存在
支持以下所有特殊数据类型和索引类型的加密正常读写、相等和范围查询：BLOB 数据、CLOB 数据、IOT 表的 Mapping 表、B*Tree 索引、Bitmap 索引、全局索引、IOT 表主键索引、IOT 表 Secondry Index、LOB Index
多因子身份管理　支持多维身份管理，至少包括应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U 盾等要素，任何一个要素不合法，可以进行阻断访问
支持对 SQLPLUS、PLSQLDEV 等 SQL 管理工具或客户端应用程序进行登陆验证，防止恶意和仿冒的工具登陆数据库
直连管控　针对直接连接数据库的行为进行管控，防止违规登陆
身份权限管理　支持针对不同身份设置明文访问、密文访问模式
动态脱敏　支持 SQLPLUS、PLSQLDEV 等 SQL 管理工具查询加密数据时的动态屏蔽，根据用户的身份以及设置的屏蔽规则，对不同授权的用户可返回真实数据、部分遮盖、全部遮盖以及其他屏蔽算法得到的结果。
屏蔽规则支持以下算法：
放行：对于已授权用户，返回真实数据；
返回空：对含有敏感表格或敏感列的数据结果返回为空值；
遮盖：全遮盖：默认以遮盖符‘*’替换敏感列的值；
部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；
随机映射：对数值、字符或字符串进行随机映射处理。
原厂商资质 原厂商具有 ISO27001 信息安全管理体系认证证书；
原厂商具有 ISO20000 信息技术服务管理体系认证证书；
产品资质　具备公安部颁发的《计算机信息系统安全专用产品销售许可证》；
原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **数据库安全准入设备**

硬件规格　1U 机架式；6 个千兆电口，1 个扩展槽，峰值 SQL 吞吐量 15000 条/秒，在线会话 6000 个，SQL 请求响应延时小于 1ms，80 亿条在线 SQL 语句存储，>=2T 存储空间
部署模式　支持旁路部署、透明代理、透明网桥、混合部署等模式
配置管理　黑白名单规则配置：内置 SQL 白名单和黑名单规则库，支持自定义配置，自带智能化学习模型，支持策略修正配置。
提供 SQL 白名单功能，采用白名单的规则机制可以自学习 SQL 语句，通过上下文判断来自非法的黑客攻击行为，能有效的拦截未知的 SQL 注入攻击行为。

内置 SQL 注入特征规则库，特征库存储常见的 SQL 注入行为特征规则，支持特征码自定义配置，自带智能化学习模型，支持策略修正配置。

内置数据库漏洞规则库，内置市场主流数据库已公开的数据库漏洞，至少包括 CVE 上已公开的所有漏洞，同时支持自定义配置，支持漏洞库定期升级。

数据库攻击防御　　支持学习模式、激活模式和模拟模式等多种模式。学习模式运行，支持 SQL 的自学习，识别安全 SQL；模拟模式运行，可以提升安全策略准确性，避免对生产库的影响，在学习一定周期后，系统自动转激活运行，避免人工操作，简单快捷

支持应用的多要素协同管理，包括 IP 地址、主机名、数据库账户等要素

严格管控 SQLPLUS、PLSQLDEV 等 SQL 工具连接数据库，防止工具随意连接数据库

支持对假冒应用与恶意应用的识别和拦截，防止非法人员利用假冒应用登陆数据库、窃取数据。

符合白名单规则库内的 SQL 语句，最高级别优先放行；符合黑名单规则库内的 SQL 语句被阻断防御。

来自应用端 SQL 语句，没有匹配在 SQL 白名单的，会进行 SQL 注入特征模式匹配，只要符合 SQL 注入特征的，SQL 语句被阻断防御。

支持虚拟补丁功能，针对数据库漏洞攻击行为进行阻断，拦截 SQL 语句。

支持危险操作放行和防御控制，遇到危险操作时，SQL 语句被阻断防御。

可以深度解析数据库操作内容，准确解析出语句中的表名，操作方式,SQL 语句及绑定变量，并根据策略名、SQL 语句、日期进行归类和统计分析。

事件查询和搜索　　以搜索引擎条的方式进行搜索，提供类似于百度，谷歌的搜索方式以方便使用；提供高级搜索，进行精确匹配搜索；提供搜索注册功能，方便下次使用。

实现海量审计信息内，自动分级管理来迅速获得有价值的安全可疑行为分析信息；基于规则进行分级配置，使用者可以按级别或规则来快速找到其需要的安全审计信息。

订阅和告警 安全告警必须支持基于订阅的模式，每个人可以订阅自己的安全告警事件，安全告警事件发送支持短信、邮件以及页面。

丰富的事件响应处理能力　提供一致性回溯分析、相同事件查看分析。

SQL 语句翻译　SQL 语句提供直译和意译的不同翻译引擎，从英文翻译成中文，增加阅读性直观性；

产品资质　具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。

具备保密局颁发的《涉密信息系统产品检测证书》；

原厂商资质 ISO27001 信息安全管理体系认证证书。

ISO20000 信息技术服务管理体系认证证书。

原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

- **数据库运行管理系统**

硬件指标　1U 机架式设备， 4 个电口，16G 内存，2T 存储空间。

部署方式　监控对象采用无代理方式部署，支持 SNMP、SSH、JMX 等采集模式，采集过程要求不影响监控对象的性能。

状态监控　支持数据库运行健康状态监控，包括：

可用性监控：监听、实例、表空间的可用性；

错误监控：数据库运行过程中的错误数量；

性能监控：数据块逻辑读指标直观反映数据库性能；
变化监控：对象（表、索引、视图等）、权限（用户、表）、空间（对象、表空间、归档）的变化量；
可靠性监控：备份及容灾系统的运行状态。
SQL 执行监控　支持 SQL 执行生命周期完整监控，包括：登录、解析、执行、提交，通过 SQL 执行次数、SQL 执行时间，主观展示 SQL 执行性能瓶颈。
关联资源监控　支持数据库关联资源监控，包括：
数据库资源监控：processes、session、DB files、jobs。
三大资源锁监控：Mutex、 Latch、 Lock。
主机资源监控，包括：CPU、内存、存储、网络。
数据库巡检 支持业务系统、数据库类型、实例名、操作系统、IP 地址、巡检完成时间等信息进行全面巡检
支持巡检对象的异常信息数量统计，运维人员可及时掌控各系统数据库的健康状况
整合资深数据库专家的多年运维经验，形成专家智能系统，根据数据库的健康状态，给出专业的分析，对数据库可能存在的故障和问题进行快速定位，对每个异常指标提供专业解读和排错建议
1. 支持一键操作实现全面巡检
2. 全面巡检的报告内容至少包括：数据库可用性、空间管理、安全性、可靠性、性能、错误、主机资源、数据库资源、数据库软件、数据库参数、系统参数等信息
3. 支持在线和以 PDF 文档导出两种方式查看巡检报告
中间件监控 支持 WebLogic、Tomcat 等主流业务中间件监控。采用 JMX 直接监控 Java 应用程序服务器的功能，无需第三方模块或集成层。使用高效的 Java 网关监视 Tomcat 等应用服务器，包括：JVM 可用内存、JVM 最大内存、JVM 总的内存、线程等。
虚拟机监控 支持 VMware 虚拟机状态监控，包括：VMware 物理主机硬件状态、虚拟机在线状态、CPU 利用率、内存大小及利用率、磁盘空间大小及利用率等。
其它监控　支持操作系统、服务器、存储、交换机、路由器、安全设备、网络等监控
预封装模版 预先封装不同监控对象的大屏展示模版，包括：中间件、数据库、操作系统、虚拟机、物理服务器等。实现常见运维故障（80%以上）及隐患能从大屏中直观展示及告警。
其中数据库监控模版，要求实现：
1. 一张大屏可以直观显示监控对象的健康指数，并根据阀值自动告警。
从流程及时间模型的角度联动展示各项指标，清晰定位问题环节。
云服务功能 提供和运维一体机配套的线上运维云服务，实现告警订阅、告警推送、工单流转、数据库专家在线服务等功能
工单服务　提供新建工单、工单流转、工单升级、工单统计报表等功能。
与告警订阅和服务授权紧耦合。
针对“待处理告警”，支持一键发起服务工单。
自动巡检　白天巡检获取一份有关数据库、主机在巡检时间段内所有指标的状态信息，并和上一次白天巡检的结果进行比对，针对异常突变指标进行告警，确保当日所有业务正常运行所需要的主机和数据库资源健康度：

1. 主机巡检信息至少包括：业务系统、数据库类型、实例名、主机名、操作系统、CPU、内存等；
2. 数据库巡检信息至少包括：健康和风险两大指标评分体系，从可用性、性能、可靠性、变更、错误、告警等维度进行分类展示，指标项大于 30 项；
3. 支持自定义时间及周期的数据库自动巡检；
4. 支持告警和错误统计，不同颜色进行正常、告警、错误的分类展示，支持告警详细信息在界面展示；
5. 支持问题下钻溯源，并根据定位问题自动匹配解决方案和工具。

晚上巡检获取一份有关数据库、主机在巡检时间段内所有资源使用趋势信息和指标状态信息，并和上一次晚上巡检的结果进行比对，针对异常突变指标进行告警，确保当晚的所有业务正常运行所需要的主机和数据库资源健康度：
1. 晚上巡检的内容至少覆盖白天巡检中主机和数据库的所有指标信息；
2. 晚上巡检支持自定义时间及周期、告警错误统计、问题下钻；
3. 晚上巡检至少提供巡检时间段内的 CPU、内存、I/O、进程、表空间、日志、逻辑读趋势分析图，分析当天主机和数据库的资源使用情况，以确保主机和数据库的资源能否在“无人值守”的情况下，支撑业务端正常运行。

巡检记录　支持保存数据库对象至少 90 天的自动巡检和全面巡检记录。
支持自定义时间，IP、实例名和业务系统名称等关键字智能查询巡检记录。
AWR 报告生成与解读　　支持至少 7 天内任意时间点（间隔为 1 小时）AWR 报告生成。
需要对数据库对象的业务系统、数据库类型、实例名、操作系统、IP 地址、报告开始时间和结束时间等信息进行展示。

支持 AWR 报告全中文解读，解读内容至少包括：主机资源、数据库内存、会话登录、SQL 解析、SQL 执行、事务提交、RAC 统计、数据库参数建议等。
整合资深数据库专家的多年数据库性能优化经验，形成专家智能分析系统，根据数据库的性能状况，给出专业的分析，对数据库可能存在的性能瓶颈进行快速定位，对每个异常指标提供专业解读和优化建议。
提供在线和 PDF 文档两种方式查看解读报告。
归档日志清理　支持数据库归档和非归档模式查询。
提供归档路径、归档空间使用率、备份成功开始时间、最近归档时间等信息。
提供至少 2 种方式清理归档日志，涵盖紧急和普通两种情景。
清理策略：清理最近一次全备份成功开始时间之前的全部归档日志或清理一小时以外的归档日志。
SQL 诊断　　支持单个 SQL ID 诊断。
提供 SQL 诊断报告，报告内容至少包括：SQL ID、SQL 文本、SQL 执行计划和 SQL 优化建议。
支持在线和 PDF 文档两种方式查看 SQL 诊断报告。
锁处理 当遇到两个事务竞争同一资源而发生锁故障时，会严重影响业务系统连续性及性能，需提供自动锁处理工具：
1. 支持自动定位锁源及被锁源阻塞的会话；
2. 支持 SQL 锁源现场保留；

支持一键杀锁操作。
错误日志　支持数据库错误日志统计和关联分析。
支持图表分析统计。

支持错误日志历史数据查询，自定义查询。
趋势分析　支持数据库运行趋势的智能分析，提供运行趋势图，至少包括：主机资源使用趋势、数据库性能趋势、业务波动趋势等分析。
原厂商资质 ISO27001 信息安全管理体系认证证书。
ISO20000 信息技术服务管理体系认证证书。
原厂 5 年质保，提供原厂针对本项目的授权委托书与质保函。

1.3.4　机房租赁

1. 需提供覆盖徐州全市域的本地化机房进行公安视频专网上云存储、大数据分析等设备的部署，本期按 70 个标准机柜【单机柜功率不小于 3.0KW】规模设计建设；同时满足未来 5 年的项目扩容需求，具备提供 100 个标准机柜的供应能力。机房及机柜的租赁服务要求如下：

机房租赁指标	服务要求
基本要求	（1）机房应位于徐州市行政区内。 （2）提供独立封闭区域供项目使用，设置独立门禁和视频监控系统，与外单位租赁区域物理隔离。 （3）本期项目机柜使用需求数量为 70 个，预留后续机柜扩展区域（不少于 100 个机柜）。
机房建筑	（1）租赁机房为电子信息系统专用的区域，可有效隔离租赁机房与周围的建筑。 （2）租赁机房抗震设防分类应不低于乙类，抗震设防烈度不小于 6 度。 （3）机房使用防静电、活动可提升的架空地板，高度不低于 400mm。 （4）租赁机房建筑的入口至租赁机房应设无障碍通道及专用货梯，通道以及专用货梯的宽度与门的尺寸应满足设备和材料运输要求，通道宽度不低于 1500mm，货梯承重不小于 2000kg。 （5）提供独立、集中的租用区域，并与外单位租赁区域物理隔离。未经授权，其他人员无权进入。 （6）租赁机房建筑物应距离燃气主管道、地铁运行线路及站点至少 800 米， 500 米内不能有加油站。租赁机房本身及周围没有强污染源、强放射源、强振动源、火灾易发点等安全隐患的地点。 （7）系统接地符合《建筑物防雷设计规范》GB50057-2010 和《建筑物电子信息系统防雷技术规范》GB50343-2012 设计要求。
供电系统	（1）机房供电以 220v 单相交流供或高压直流电。 （2）至少 2 路高压专线接入租赁机房，每条不小于 500KVA，不同变电站引入，每路市电均满足全负载容量，市电可随时互切互投。 （3）需配备发电机组。发电机不低于 N+1 台配置，发电机组互为备份，每台发电机组输出功率不得小于 1000KW，满足应急供电需求。 （4）租赁机房要求使用不间断电源模块及进线列头柜（不计

	入本项目租赁机柜数量）。 （5）各级配电柜均应按照负载情况装设浪涌避雷装置，装设应符合国家相应标准规范的要求。机房内所有机箱、机柜、配电箱柜、线槽、桥架均应按照规范要求作可靠的接地。
空调系统	（1）租赁机房区域提供独立的空调（水冷室外机可共用），N+X 配置（X≥1），制冷能力满足租赁机房区域最大负荷制冷需要，机房（开机时）温度 18～28℃，湿度 35%～75%；机房（停机时）温度 5℃～35℃，湿度 35%～75%。 （2）空调系统设备安装于独立设备的专属区域内，与机柜和设备分隔，且设置漏水检测装置。
消防系统	（1）租赁机房设置独立防区消防系统；温感/烟感双路感应，可以定点报警，消防系统配置独立气体灭火钢瓶间，配置灾后排烟系统，配置自动报警与消防系统联动； （2）通过公安消防机构验收。 （3）租赁机房应设置洁净气体消防灭火系统；租赁机房应安装自动报警装置和应急设施；需配置手持机房专用气体灭火器，租赁机房需配置匹配数量防毒面具。 （5）租赁机房配置专门的消防监控系统；实时将远程监控数据采集显示到监控系统，并有统一声光报警功能。
安防系统	（1)机房租赁区域配置独立 7×24 小时无死角视频监控系统。应保证对所有门口进出的监控，包括应急通道门。 （2）配备 24 小时专业安保人员及机房管理人员。 （3）监控机房区域的 CCTV 监控可远程调用，禁止无关人员查看机柜区域内的录像。 （4）提供区域独立门禁，仅授权人员可以进入，不得赋予任何人进出的权限，门禁系统与消防系统联动。区域需配置多重门禁，并有登记制度和记录备查。
集中监控	（1）配置机房基础设施 7×24 小时集中监控系统，必须具备声光告警功能。 （2）专业人员 7*24 小时在岗，随时巡视。 （3）7*24 小时的机房授权进入服务、入侵检测、保安人员 7*24 小时值班，定时巡逻。 （4）对所有可能出现异常情况的动态画面进行捕捉和存储，视频资料存储周期最短为 3 个月。 （5)对机房和其他房间出入口设置门禁读卡器、门锁及门磁，同时有一套完整的管理体系，能够实现对所有人员的入室权限进行严格的管理和控制。 （6）消防系统的报警信号与门禁控制器的联动扩展端口沟通，实现消防报警信号输入、强制电锁动作输出等功能。
机柜资源	（1）单机柜静态载荷不低于 800kg。 （2）提供 19 英寸标准服务器机柜，容量不少于 42U，机柜宽不低于 600mm，机柜深度不低于 1000mm，应根据实际需要提供相应层板和托架。 （3)单机柜配置 AB 两路 PDU，每路提供不少于 16 个插座（按

	需配置 10A 或 16A），输入 32A。 （4）在不影响机房动环、配电结构、消防要求情况下，提供租赁机房改造服务。
综合布线	（1）可以在租赁区域内进行综合布线。若布线涉及租赁区域内、外部，须提供必要的协助。 （2）机房安装专用走线槽，强电主线槽主要用于从 UPS 入交流电源；强电支线槽用于给各机柜里的 PDU 从列头柜接线引入走线；弱电线槽用于布放综合配线柜到设备机柜的网线等信号线缆，布放 ODF 到设备机柜的光缆。 （3）提供的综合布线产品（包括线缆、跳线、配线架、光纤等材料）必须具有产品质量检验合格证，网线须采用六类非屏蔽线缆。 （4）缆线的布放应自然平直，不得产生扭绞、打圈接头等现象，不应受外力的挤压和损伤。 （5）缆线两端应贴有标签，应标明编号，标签书写应清晰，端正和正确。标签应选用不易损坏的材料。
日常管理	（1）具备明确的进出入登记制度及完整清晰的进出入机房授权审批记录。 （2）机房日常巡检 4 小时/次，包含但不限于主要安全通道、消防设施、所有基础设施、动环设备等，保留巡检记录；机房运行日志记录保存时间≥1 年。 （3）安排专人协助安装线路，进行配合工作；当运营商线路出现问题时，需积极协助处理线路故障；涉及物业相关费用，由承租机房方承担。 （4）配合开展机柜、综合布线及其配套设施日常运维工作。具有详细的巡检流程规范及操作流程规范。各项巡检操作规定均需符合设备原厂规范要求。 （5）对数据中心关键基础设施设备建有标准维护作业程序、标准操作流程。 （6）租赁机房需建立完善的事件管理制度，对可能出现的突发事件按照影响程度和紧急程度的不同进行分级处置。
安全管理	（1）数据信息安全要求 加强机房运维人员管理，禁止发生以下安全事件：数据泄露、存放机密数据和信息的介质丢失、数据损坏且无法恢复、发生有影响的信息安全突发事件等。 （2）系统网络安全要求 加强机房运维人员管理，禁止发生以下安全事件：非授权网络连接、非授权系统访问、非授权软件安装、非授权系统、网络、应用激活、非授权人员开启用户方机柜等事件。 （3）机房动力环境监控系统：配电、空调、环境、门禁、摄像、漏水等系统状态实时处于自动监控状态，一旦故障立刻以多种经形式报警，包括拨打值班电话、短信发送等，保证即时通知相关人员。 （4）对所有可能出现的异常情况的动态画面进行捕捉和存

	储。
服务报告	（1）定期编写、交付租赁机房运行月报、季报、半年报、年报，以及其他涉及服务区域所需要的文档材料。 （2）按要求每月提交运维报告数据。定期提交设备相关的运维数据，包括基础设施巡检数据、演练计划、演练记录与总结报告等。 （3）各项报告涉及的数据必须真实、准确、完整。
机房搬迁服务	当前,徐州市公安局青年路机房视频专网的设备全部分布在2楼和5楼，同公安网的部分设备混排在不同的机柜中。且2个楼层的机柜使用空间使用率已接近95%,无法满足未来公安视频业务发展对机房空间的需求，因此需考虑将青年路机房中的视频专网设施搬迁。 机房搬迁应尽量将方案实施过程中产生的影响降到最低，在目标时间内完成对服务器、网络设备、存储等设备的拆卸、搬迁、安装及测试。保证重要的应用系统、设备停机时间最小范围内，尽量缩小其它系统的停机时间，减少因此带来的不便和损失。并且在开机后，继续跟踪系统的运行情况，随时处理系统运行的异常情况。确保各个系统设备正常有序的运行。 中标人五年内需提供两次同等规模的搬迁服务。

2. 物理安全：独立区域设置(进行物理隔离和围挡)，设置独立人脸门禁管理(门禁授权由公安局管理)；

3. 安保措施：独立区域内视频监控无盲区，视频录像记录存储时长不小于3个月（录像查看需经公安局授权）；视频信号可通过公安视频专网推送至本项目统一运维平台监控和管理；

4. 环境安全：可提供机房内温湿度、供配电等数据至本项目统一运维平台。

1.4 视频图像基础保障体系

1.4.1 统一运维管控平台

·集中账号管理

身份鉴别及审计系统可实现对所有服务器、网络设备账号的集中管理。可以完成对账号整个生命周期的监控和管理，降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。单位可以实现将账号与具体的自然人相关联。

·集中身份认证

身份鉴别及审计系统为用户提供统一的认证接口,支持多种认证方式。采用统一的认证接口对用户进行认证管理（支持AD域认证、LDAP认证、radius认证、数字证书认证），即方便了用户身份认证，又提高了认证的安全性和可靠性。

·统一资源授权

身份鉴别及审计系统提供统一的界面,对相应用户、角色及行为和资源进行授权,系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权，最大限度保护用户资源的安全。

·集中访问控制

身份鉴别及审计系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，用来分配给具体的用户限制其系统行为，管理员根据其自身的角色为其指定相应的控制策略来限定用户，真正做到 who、where、when、what。然而更好的提高系统的安全性。做到运维用户多次登录失败自动锁定账号功能，支持限制运维用户访问源 IP、访问时间段的功能。

• 集中操作审计

身份鉴别及审计系统操作审计日志分为登录日志、会话日志和系统日志三部分，登录日志是对用户登录堡垒机的情况进行日志记录；会话日志记录用户对资源的访问及操作，支持指令识别和视频录像；系统日志是针对堡垒机自身的操作情况的审计，包括创建/删除、锁定/激活用户(组)、资产(组)、授权关系、策略等。生成的日志支持丰富的查询和操作方式。

• 工单审批

身份鉴别及审计系统支持工单审批模式，第三方运维人员或普通运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行运维操作，更好的提高运维流程简单并记录相应操作。

1.4.2 网络运行分析平台

• 中间件监控

利用 JMX 实现监控 Java 应用服务功能，无需安装任何第三方软件或插件。使用高效的 Java 网关监视 Tomcat，Weblogic，ACTIVEMQ 等，包括运行状态、JVM 可用内存、JVM 最大内存、JVM 总内存、线程等。

• 操作系统监控

实现对 Windows、Linux、AIX、HP-UX、Solaris 主机的运行状况监控，包括主机的在线状态、CPU 利用率、内存大小及利用率、磁盘空间大小及利用率等状态信息。

• 主机硬件监控

通过 IPMI 收集 CPU 温度，风扇转速、电压和磁盘状态等统计信息，可以独立于操作系统外直接从带外管理口监控硬件状态。

IPMI 监控仅适用于支持 IPMI 的设备。

• 网络监控

实现网络设备（包括网络安全设备）的在线状态监控和网络链路状态监控，包括：线路联通性、线路响应时间、线路流量、线路带宽利用率、线路错包率、线路丢包率等信息。对网络设备接口状态进行监管，包括接口状态、接口流量性能等信息。持续监视、报告网络的运行情况，发现异常及时告警。

• 存储监控

存储监控的信息包括存储控制器、磁盘、电源、风扇等健康状态，支持对 EMC、IBM、NETAPP、海康、大华、华为等厂家存储设备的监控。

• 虚拟机监控

实现对虚拟机的监控，包括配置数据和性能数据。支持使用自动发现规则来发现虚拟机，并根据预定义的模型创建主机节点来监控它们，包括物理主机硬件状态、虚拟机在线状态、CPU 的信息（核心数量、利用率、频率）、内存大小及利用率、磁盘空间大小及利用率等信息。

1.4.3 视频质量分析诊断

支持 1 万路视频分析接入。基于平台的后端智能视频质量诊断服务设备，视频诊断系统对海量视频的轮训监控和分析，得到各路视频的运行状态，并对出现的异常现象进行统计和报警。

支持对视频模糊、高亮异常、低亮异常、偏色、低对比度异常、视频抖动运动、噪声过大、条纹干扰、视频丢失、视频冻结、视频遮挡和场景变化等异常现象进行报警统计。

1.4.4 融合显控设备

- **显控设备**

P1.25mm LED 拼接单元

参数：

1) 输入功率（最大值)：500 W/m²
2) 箱体结构：压铸铝
3) 工作温湿度：-20℃~+50℃/10%~90%RH
4) 灰度等级：16384 levels per color

- **专用工作站**

i7-9700/16G/2T+256G M.2 SSD/RTX2070/RW/W10）+27 英寸显示器+无线键鼠套装