用户需求书

1、软硬件设备及材料采购

序号	名称	技术参数	单位	数量	备注
一	服务器				
1	服务器机箱	19 英寸 2U 高标准机架式服务器机箱，最大可插 4 个计算节点，共 24 个硬盘槽位； 含两个冗余白金电源，电源输入范围：100-127VAC、200-240VAC,50/60Hz；	台	2	
2	应用服务器 2.4T SAS 硬盘	SAS 盘，容量 2.4TB，规格 2.5 吋，SAS 接口，10500rpm	块	6	
3	应用服务器计算节点	2 颗 Intel Xeon Silver 4110 (8 核/16 线程，主频 2.1GHz,up to 3.0GHz，11MB 缓存)；64G 内存；1 块 2.4TB SAS 盘，1 块 960GB SSD 盘；2 个 SFP+光接口，含光模块；	套	3	
4	大数据服务器 2.4T SAS 硬盘	SAS 盘，容量 2.4TB，规格 2.5 吋，SAS 接口，10500rpm	块	4	
5	大数据服务器 3.2T U.2 SSD 硬盘	SSD 盘，容量 3.2TB，U.2 接口，3200MB/S	块	1	
6	大数据服务器服务器计算节点	2 颗 Intel Xeon Silver 4110 (8 核/16 线程，主频 2.1GHz,up to 3.0GHz，11MB 缓存)；64G 内存；1 块 2.4TB SAS 盘，1 块 960GB SSD 盘；2 个 SFP+光接口，含光模块；	套	1	

序号	名称	技术参数	单位	数量	备注
7	四电口千兆网卡	以太网电口网卡，配置 4 个 1000M RJ45 以太网电口	块	4	
8	核心交换机	三层核心交换机，交换容量：2.4/24Tbps；包转发率：477/705Mpps；18 个 1000BASE-X SFP 端口，6 个 1G/10GBase-X SFP Plus 端口，2 个 40G QSFP+端口	台	1	
9	接入交换机	24 个 10/100/1000M 自适应电口，4 个 1000M/10G SFP+光口，固化单交流电源，无风扇，1 个 SFP-XG-LX-SM1310 SFP+ 万兆模块(1310nm,10km,LC)	台	2	
二	**安全设备**				
1	安全网关（下一代防火墙）	双交流电源；含 12*GE 电口,12*SFP 光口，500G 硬盘，网络吞吐量 8Gbps；最大并发连接数大于 300 万，每秒新建 HTTP 连接数大于 10 万。（默认 SFP 接口不带光模块）。支持大病毒文件的扫描，实时病毒连接阻断，病毒事件记录，支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描。基于状态、精准的高性能攻击检测和防御，实时攻击源阻断、IP 屏蔽、攻击事件记录，支持针对多种协议和应用的攻击检测和防御，支持 SQL 注入和 XSS 防御、外链防护和 Web 访问控制。	台	2	
2	综合日志审计平台（日志审计系统）	标配：标准 1U 硬件，1 个 console 口 网口类别：6 个千兆工作管理口(1 管理口+1HA 口+4 审计口) 硬盘：1T，内存：8G，单电源。 日志处理能力 200EPS。资产授权数量：20 个	台	1	
3	运维审计与风险控制系统（运维审	标准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口,硬盘:1T，硬盘不可扩展；1*RJ45 串口，单电源。最大资产数 100 个，最大字符连接 100 个，最大图型连接 20 个。	台	1	

序号	名称	技术参数	单位	数量	备注
	计系统）				
4	APT 攻击预警平台（未知威胁预警平台）	硬件外形：软硬一体化 1U 标准机架式设备； 电源：单电源，PU：2 核 4 线程*1,内存：8G,硬盘容量：1T*1； 接口：千兆 RJ45 网口*2(管理口*2)、千兆 RJ45 网口*4 吞吐率：网络层：500Mbps,应用层：100Mbps； WEB 检测：HTTP 最大并发数 1 万/秒； 邮件检测：邮件处理数：50 万封/24 小时； 文件检测：1 万个/24 小时	台	1	
5	数据库审计与风险控制系统（数据库审计系统）	硬件尺寸：标准 1U；CPU 数量：2 核；内存容量：8GB 硬盘容量：1TB；硬盘接口：企业级 SATA；网口：1 管理口+1HA 口+4 审计口（4 个千兆电）； 网口类型：1000M 电口*6；电源配置：单电源　　总网络吞吐量：500Mbps；双向审计最大数据库流量：100Mbps；峰值事务处理能力 TPS：6000 条/秒；日志数量存储：10 亿条； 功能描述：全功能开放 数据库实例授权许可数量：4；硬件是否可扩容：否	台	1	
6	主机安全及管理系统（主机安全及管理系统）	包含终端管理中心硬件及软件一套 规格 1U、CPU 二核四线程、内存 8G、硬盘 1T、单电源 实现对终端的统一管理和策略下发	台	1	
		适用于 Windows PC 防护	台	20	

序号	名称	技术参数	单位	数量	备注
		支持 Windows XP、Windows 7、Windows 8、Windows 10 等操作系统			
		适用于各类型服务器防护 支持 Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、 Ubuntu 14 +等操作系统	台	15	
三	云平台				
1	云计算平台管理软件	1）提供图形化的综合云计算管理平台，对管理员和用户呈现集中的计算、存储和网络物理资源管理视图和虚拟资源视图，提供完善的资源的分区管理、虚拟机和容器的创建调度管理、以及对外开放兼容的开发服务接口； 2）提供硬件资源的即插即用能力，并支持硬件资源使用率查询、实时使用量告警等功能，为数据中心管理提供智能化硬件资源管理。 3）支持虚拟资源管理，能对虚拟资源进行配额管理，虚拟资源的使用率查询与监控告警，以及基于业务对虚拟资源使用率的情况。 4）支持对数据中心的服务器资源进行分域管理，并能根据资源的分配配置，满足业务可靠性、服务 Qos 以及业务的最大性能和特定需求部署保障。 5）提供完善的虚拟机镜像管理，包括镜像的存储方式，镜像的格式管理。 6）提供完善的虚拟机调度方法，支持基于 CPU、内存、磁盘需求以及相同主机、不同主机的调度，满足业务部署的灵活性。 7）支持对虚拟设备包括状态监控、设置、迁移和服务监控等全面的管理能力。	套	1	

序号	名称	技术参数	单位	数量	备注
		8）提供完善的服务接口，支持通过 REST 接口的方式开放给上层应用。用户可以灵活的基于开放的服务接口开发业务的管理应用。 9）大规模管理，支持数百台的物理服务器规模的虚拟机的管理能力。 10）支持物理服务器动态扩容，系统性能呈线性增长。 11）采用国产产品技术，实现对物理设备的计算虚拟化、网络虚拟化、存储虚拟化，以及相关的虚拟化资源兼容性，可靠性要求； 12）支持内存分配，并通过优化或者容器技术减少虚拟软件的性能损耗。 13）支持虚拟机/容器的 CPU QoS 控制，能控制虚拟机/容器获得的计算资源能力，控制虚拟机/容器获得的最大计算能力以及修改虚拟机的配置参数。 14）云平台可以对虚拟机/容器进行内存 QoS 控制，控制虚拟机/容器可获取的物理内存，并能完整的对虚拟机或容器的生命周期进行管理，并且支持查询、创建、删除、启动、关闭、重启、克隆虚拟机/容器等一系列功能。 15）虚拟化平台支持主流设备厂商提供的 X86 服务器，部署的虚拟机平台能支持主流的 X86 架构的操作系统，包括 Windows Server 2003 /2008 R2 及以上版本服务器操作系统，Windows XP、Windows 7 操作系统， Redhat、SUSE、CentOS、Ubuntu、Fedora 等业界主流 OS 操作系统。 16）虚拟化软件支持主流设备厂商提供的共享存储，支持业务与数据相分离，保证业务数据安全；支持各种 IPSAN/FCSAN 块存储设备，支持基于 NFS 的各种存储系统，支持主流云存储系统。			

序号	名称	技术参数	单位	数量	备注
2	云计算平台虚拟化授权	含云计算平台 License 授权，部署软件后，可支持： 1）采用国产产品技术，实现对物理设备的计算虚拟化、网络虚拟化、存储虚拟化，以及相关的虚拟化资源兼容性，可靠性要求； 2）支持内存分配，并通过优化或者容器技术减少虚拟软件的性能损耗。 3）支持虚拟机/容器的 CPU QoS 控制，能控制虚拟机/容器获得的计算资源能力，控制虚拟机/容器获得的最大计算能力以及修改虚拟机的配置参数。 4）云平台可以对虚拟机/容器进行内存 QoS 控制，控制虚拟机/容器可获取的物理内存，并能完整的对虚拟机或容器的生命周期进行管理，并且支持查询、创建、删除、启动、关闭、重启、克隆虚拟机/容器等一系列功能。 5）虚拟化平台支持主流设备厂商提供的 X86 服务器，部署的虚拟机平台能支持主流的 X86 架构的操作系统，包括 Windows Server 2003 /2008 R2 及以上版本服务器操作系统，Windows XP、Windows 7 操作系统， Redhat、SUSE、CentOS、Ubuntu、Fedora 等业界主流 OS 操作系统。 6）虚拟化软件支持主流设备厂商提供的共享存储，支持业务与数据相分离，保证业务数据安全；支持各种 IPSAN/FCSAN 块存储设备，支持基于 NFS 的各种存储系统，支持主流云存储系统。	个	128	
四	**指挥中心改造**				

序号	名称	技术参数	单位	数量	备注
1	无缝高清矩阵机箱	1.矩阵采用纯硬件标准化机箱设计，支持配置 36×36 路信号切换，支持 HDMI、DVI、VGA、SDI、HDBaseT、光纤的任意输入/输出信号卡，其中 DVI 输入卡兼容 CVBS，YUV,S-VIDEO 信号，VGA 输入/输出卡均兼容 CVBS，YUV,S-VIDEO。 2.采用板卡模块化设计，支持接入 9 块输入卡、9 块输出卡、1 块控制卡；通过定制配置各类相同或不同的输入输出卡可以组成单一接口类型或多接口类型的矩阵，如 HDMI 矩阵，DVI 矩阵，VGA 矩阵，YUV 矩阵，Video 矩阵等。 3.支持无缝切换功能，切换过程无黑屏信号。 4.支持 1080P 分辨率，最大可支持 4Kx2K。支持断电记忆功能，免除上电重复设置动作。支持智能温控，控制矩阵风扇的运行；系统内可存储多组预切换指令，调用时可以一键切换。 5.支持模拟音频与 HDMI 内嵌音频选择输入、支持模拟音频与 HDMI 内嵌音频同时输出。 6.支持接入 1 块控制板卡，具有 1 路 RS-232,1 路 RS-485,1 路 TCP/IP 端口（PC 软件）。 7.HDBaseT 输入输出信号支持双向 RS-232 和双向 IR 信号传输，可对 RS-232 和 IR 信号选择随视频信号切换，或分离切换模式，支持 POC 对外供电。 8.支持 KVM 坐席管理功能，通过一套键盘鼠标显示器切换、管理多台计算机设备。	台	1	
	高清无缝混插矩阵切换内嵌软件	1.软件内嵌于高清混插矩阵切换系统，实现各类高清晰数字/模拟信号的处理、切换等功能。 2.支持分辨率高达 1920×1080P@60Hz 的处理能力。 3.支持信号无缝切换，切换过程无黑屏信号。	套		

序号	名称	技术参数	单位	数量	备注
		4.支持通过专业的 PC 上位机管理软件控制。 5.通过矩阵切换信号或通过软件切换信号。			
	嵌入式控制面板	1.支持由矩阵主机远程供电，无需配独立适配器。 2.支持编程图片、图形、文字、按键等更具人性化的界面。 3.面板显示屏尺寸为 3.5 英寸，TFT 液晶屏。 4.分辨率支持 320*240。	个	1	
	无缝矩阵 DVI 输入卡	1.支持 4 路 DVI-I 母接口无缝输入；支持热插拔。。 2.支持快速无缝切换，无闪烁，无黑屏。 3.支持多格式信号输出，可支持 HDMI/DVI、VGA、CVBS、YPbPr 任意一种信号。支持分辨率达 1920X1200P@60。 4.支持断电现场切换记忆保护功能，特有 ESD 静电保护功能。 5.兼容 HDMI1.3a 的标准，HDCP1.3 协议，DVI1.0 协议。	块	9	
	高清 HDMI 矩阵输入板卡内嵌软件	1.软件内嵌于高清矩阵系统板卡设备，实现信号的处理功能。 2.支持分辨率高达 1920×1080P@60Hz 的处理能力。 3.通过矩阵切换信号或通过软件切换信号。	套		
	无缝矩阵 4 路 DVI 输出卡	功能特点： 支持 4 路 DVI 信号无缝输出，4 路立体声音频输出； 实时无缝切换效果；最大分辨率支持 1920×1200@60hz； 带增益 25 米线长，带独立音频输出；	块	8	

序号	名称	技术参数	单位	数量	备注
		支持输出分辨率可调，支持图像参数修改； 兼容 HDMI1.3 和 HDCP1.4 标准。 所有板卡和主板，采用 10G 进口专业高速连接器，非普通金手指连接； 输出支持高清 CVBS / S-VIDEO / YUV/VGA/DVI（需要转接线）			
	高清 HDMI 矩阵输出板卡内嵌软件	1.软件内嵌于高清矩阵系统板卡设备，实现信号的处理功能。 2.支持分辨率高达 1920×1080P@60Hz 的处理能力。 3.通过矩阵切换信号或通过软件切换信号。	套		
2	队站智能联动控制终端	满足自动联动消防警铃、警灯、车库门等功能，满足接处警系统接口应用功能。	套	12	
3	指挥中心智能接处警终端	Intel i7-8700/8G/1T/显卡：4G 显存，带 3 个 HDMI 输出口/win10 系统/含有线键鼠/3 年硬件上门服务/显示器：三屏 23.8 英寸微边框 2K；三屏电脑显示器支架	台	6	
4	队站智能接处警终端	Intel i7-8700/8G/1T/GT730-2G 独显/win10 系统/含有线键鼠/3 年硬件上门服务/显示器：23.8 英寸微边框 2K	台	15	
5	坐席控制台	1800×900×750 定制控制台	套	8	
6	土建费用	控制室土建改造和 lcd 拼接屏拆除	批	1	
7	装饰费用	按原风格装饰（含 1 套实木门 2100*1200mm）	批	1	
8	12mm 透视玻璃		平方	5.6	
9	线缆改造	含矩阵 DVI、坐席、控制台的线缆改造	批	1	

2、软件开发

序号	系统模块	子模块	功能项	功能描述	备注
1	接处警业务系统	综合报警审理	警情动态	提供城市远程监控、互联网应用报警信息实时刷新功能，支持合并警情信息集合显示，支持对重要警情设为关注置顶显示。	
2			警情核实与跟踪	提供对警情动态信息中的多个警情核实与跟踪警情功能。	
3			警情转入	核实警情后，提供转入功能，将警情推送到警情受理模块进行统一处置调派。	
4			同警整理	针对互联网信息传播特点，同一警情多报情况频发，提供警情合并整理功能。	
5			警情历史查询	提供警情历史查询功能，提供受理信息参考。	
6		警情受理模块	电话排队和早释提醒	通过对已经拨入 119 接警台的电话进行自动时序排队，显示未分配到座席且处于等待状态的电话信息，支持对接通前主动挂断的电话进行记录和手动回拨。	
7			综合定位	系统结合定位云服务平台提供定位信息、运营商基站定位、短信定位、地址智能识别等多种方式，快速帮助接警员获取警情地址。接警员可根据语音识别出的警情地址在辅助地图上完成搜索定位，也可进行警情地址的手动定位及地址文本匹配，精确、高效完成警情地址定位操作。	
8			来电提醒	根据综合报警定位服务、智能接警服务和三字段信息、历史警情等信息提取报警信息，实现来电提醒。	
9			错位接警	如果报警信息不属本辖区，可以使用错位接警功能，将该警情转给其他支队，同时与警情归属辖区建立三方通话，实现语音与信息的推送。	

序号	系统模块	子模块	功能项	功能描述	备注
10			人工报警（警情补录）	如遇现场报警等特殊情况，接警员可通过此功能手动创建警单。	
11			接警要点提醒	根据警情类别、警情地址、警情等级、气象信息、处置对象等建立预置规则，自动匹配不同的接警用语进行辅助提醒，规范接警员在接警对话中的话语内容，同时支持根据实时对话内容的沟通程度判断接警用语优先级，自动调整接警用语排序和显示状态，达到提升接警效率的目的；对于报警人寻求现场帮助的场景，也支持匹配对应现场自我救援指引方案，有效辅助接警员对报警人进行引导。具备条件的单位可设立学习因子，通过各接警员日常操作习惯，利用机器学习算法建立要点提醒研判模型，实现智能匹配。	
12			智能语音识别	接警通话过程中调用后台支撑服务进行实时语音转写，通过获取报警人及接警员的对话语音流信息，实现无延迟自动语音转文字，准确还原双方对话内容，并且支持对话音频中实现精准话者分离，实时语音转写响应时间控制在 300 毫秒以下。对于本地口音普通话，需要有不断提升识别率的完整系统流程机制支撑。	
13			警情要素提取	利用警情语音转写内容，使用专用自然语言解译模型，对关键信息进行完整的实时识别提取，内容包括警情地址、警情类型、燃烧物、被困人员、燃烧楼层、火灾场所、烟雾状况等，由接警员确认后自动填入警情单，达到高效率辅助填单的目标。 警情要素提取的精准度是提高立案效率的关键点，对报警电话内容要求精准提	

序号	系统模块	子模块	功能项	功能描述	备注
				取所有警情要素，对警情要素内容提取的结论与报警对话内容信息必须匹配。其中警情地址的准确性和完整性是第一优先级，对警情地址的提取，可根据地址智能匹配机制，对原报警电话内容残缺的地址信息进行自动补全，保证地址信息更符合地图定位的检索条件要求。 提取各类警情信息，为深度学习模型提供训练样本，不断提高转义文本信息提取准确率。	
14			单位识别	通过识别与提取环节获取到单位信息，同时基于“一张图”实时分析单位及周边情况。	
15			重点单位匹配	智能接处警在语音识别与信息提取环节,能够通过语音识别技术产出的关键单位信息，与系统自建的信息库进行对比和判断,快速检索定位位置附近高层地下建筑、人员密集场所、危化品生产存储场所等重点单位,当识别出来的所在地理地理信息周边范围内出现重点护具,系统将会通过 POI 分库信息快速搜索地理范围内部100米范围内的周边建筑,不但同时匹配重点单位,还能实时查询周边单位的信息，为警情立案做到智能筛选,精准匹配，辅助了解周边情况，为灭火救援工作提供可视化的前置数据支撑。	
16			地址快速匹配	录入地址信息时，实时检索选择匹配度最高的地址，辅助接警员锁定警情地址，同时在“一张图”进行位置展示。	

序号	系统模块	子模块	功能项	功能描述	备注
17			多报提示及归并	基于同一电话在同一时段报警次数超过两次，进行多次报警提示。 针对同一号码重复报警与多个电话重复报同一警情这两种情况，根据一定时间范围内的位置、报警电话、报警人、警情类型自动分析出是否为重复警情，判定为重复警情时进行提示，以第一警情为主进行合并，形成同灾警情集。	
18			交接班管理	提供交接班信息记录功能。	
19		智能调度模块	首批力量调派	接警员在初步向报警人确认警情类型以及警情位置后，系统将结合空间位置自动推算处置力量，快速调派首战力量出动。	
20			群呼通报	在警情确定后，对辖区其他社会救援力量实现一键语音或文字通报。	
21			联动设备控制	结合智能调派方案自动通知对应消防救援站出警，对警铃、警灯、广播等设备发出控制指令。	
22			警情推送	根据现场情况及不同等级的警情，采用语音、文字等形式，向消防救援队伍、联勤联动单位等所有参战力量推送警情。	
23			警情升级提醒	结合现场实时反馈、记录的信息要点，通过警情等级分析模型提醒接警员进行警情升级。	
24			增援调派	根据警情等级和调度模型自动生成调派方案，支持人工修改。	
25			跨区域增援请求	对警情现场情况研判后，可向上级单位发送增援请求、推送增援信息。	
26			警情结案	对处置完毕的警情信息进行归档保存。	
27		警情受	设备联动	消防救援站接收警情时实现营区广播、警灯、警铃等同步联动。	

序号	系统模块	子模块	功能项	功能描述	备注
28		理终端模块	群呼通报	在接到指令后，对辖区其他社会救援力量实现一键语音或文字通报。	
29			出车单通知	警情出车单显示当前警情、出动力量清单等信息。	
30			警情处理列表	警情处理列表展示处置过程中的警情信息，包括警情编号、警情状态、警情类型、警情等级、报警时间、地址等。	
31			处置信息反馈	系统提供处置信息回填功能，支持消防救援站值班人员录入该警情的“现场信息”、“火场文书”、“文电信息”等。	
32			一张图模块	提供地形地貌、交通路况、警情信息、实力状态等信息一张图展示。	
33		警情受理移动终端模块	警情信息	接收警情相关信息，并能显示警情地址、警情电话等其他相关信息。	
34			报警录音	提供移动终端收听报警录音功能。	
35			群呼通报	在接到指令后，对辖区其他社会救援力量实现一键语音或文字通报。	
36			处置指令	提供移动终端接收相关指令信息功能。	
37			二次定位	提供警情二次定位和指挥中心信息同步功能。	
38			处置对象关联	处置对象关联后自动下发对象基本信息到移动作战终端，支持实时查看。	
39			周边资源	自动分析周边的资源，如水源、重点防护目标、消防设施信息，并在地图上展示分布地点。	
40			现场处置信息反馈	支持现场人员录入该警情的“现场信息”、“火场文书”、“文电信息”等；支持反馈出警、到场、出水、归队等信息，实现与指挥中心的处置交互。	
41			交接班管理	提供交接班信息记录功能。	

序号	系统模块	子模块	功能项	功能描述	备注
42			人员信息维护	提供消防救援站人员信息增、删、改及状态调整操作。	
43			车辆信息维护	提供消防救援站车辆信息增、删、改及状态调整操作。	
44			器材装备信息维护	提供消防器材装备信息增、删、改及状态调整操作。	
45			值班报备	提供人员和车辆信息的报备功能。	
46		救援预案智能模块	预案信息展示	展示预案的基础信息，包括预案名称、编号、类型、等级、调派的力量情况等信息。	
47			预案信息维护	支持对预案信息进行编辑修改、增加、删除等基本操作。	
48			预案智能匹配	根据警情信息，系统从预案库智能匹配对应的预案，形成完整的力量调派方案，快速完成力量调派并出警，同时支持查看详细的预案内容。	
49	接处警业务信息支撑	全过程信息管理模块	时序化警情过程	自动记录警情受理、调度、处置的全过程信息，同时支持接警员对处置信息进行快速回填。	
50			人员装备动态监控	对现场参战人员和装备的数量、状态等信息进行实时掌握，有定位、监控设备的进行实时跟踪，可接入车联网信息等，实现相关信息自动更新。	
51			录音录时服务	提供录音录时服务，对接处警过程中的所有通话进行全程录音、备份。	
52		接处警一张图模块	地图功能	提供地形地貌、一张图展示方式及地图基本操作功能。	
53			资源信息分析	支持在地图上展示当前警情定位信息，同时叠加辖区图层供接警员参考研判；支持对周边消火栓、重点单位等资源进行分析；事发地为重点单位则需提供对应的特殊标识。	

序号	系统模块	子模块	功能项	功能描述	备注
54			车辆导航	根据警情发生地点及调派的消防救援站位置，充分整合实时路况信息，使用卡车、特种车模式规划行车路径，规避限高，限重，限行路段，选择最优路径，快速到达现场。	
55			气象信息	根据警情发生地点的地理信息数据，实时展示辖区天气情况、风力、风向、气温等信息。具备条件的总队或支队可接入该区域水文信息，根据警情发生地点的地理信息数据，自动分析该区域气水文情况，实时展示辖区降水量。	
56			周边建筑	根据警情发生地点的地理信息数据，自动分析和展示周边建筑标识信息。	
57			图层管理	提供消防图层目录和图层显示管理控制功能，支持图层数据动态配置，可接入互联网图层资源和其他单位的图层资源。	
58		警情展示模块	当日警情	支持按照警情类型、时段（当日、本年、本月、小时）对辖区范围内警情进行统计，同时可对消防救援站的数据进行分区域展示，支持按照柱状图、饼状图等进行可视化统计展示。	
59			警情统计	支持警情数量、突出警情、警情类型等数据统计。	
60			重要警情提醒及状态	支持辖区范围内重要警情提醒，按级别以列表方式显示重大警情当前处置状态。	
61			力量统计	支持对辖区范围内各级力量监控统计。	
62			伤亡人数统计	支持按照时间段对辖区范围内灾害事故伤亡人数统计。	
63			值班信息	提供循环展示值班信息功能，支持对辖区内各级值班信息进行展示。	

序号	系统模块	子模块	功能项	功能描述	备注
64			车辆装备统计	支持对辖区内装备车辆按消防救援站分区统计。	
65			系统实时监控	支持对各模块状态进行实时监控。	
66			数据质量监控	支持对警情数据质量进行监控，提供数据异常提醒功能。	
67		数据管理模块	系统数据管理	提供对系统配置、短信参数配置、座席管理、角色权限管理、用户信息管理、值班报备、阈值管理、接警提示管理、首批调派力量管理、力量信息管理、调度方案管理和黑名单管理功能。	
68			数据字典管理	提供对警情类型、性质、警情状态、火灾场所、建筑火灾类型、建筑结构、建筑物分类、警情等级、车辆等级、车辆状态、车辆作战功能、车辆作战状态等一系列业务应用字典和基础字典的管理功能。	
69			业务数据管理	业务数据管理的目标是保障数据实时与准确，已建成作战基础数据管理相关系统，可以提供实时、准确数据的建设单位，应按照智能接处警系统数据标准和接入标准，与接处警系统同步数据；未建成作战基础数据管理相关系统，或虽有相关系统但无法提供准确数据的建设单位，应在接处警系统建设过程中，同步建设或升级作战基础数据管理系统或功能模块，以确保接入智能接处警系统的数据准确性和实时性。维护数据主要涉及：专职队管理、消防人员管理、车辆信息管理、装备器材管理、联勤保障单位管理、应急联动单位管理、专家信息管理、重点单位管理、预案管理和图层数据管理如消火栓、消防水池、消防码头、微型消防站等。	

序号	系统模块	子模块	功能项	功能描述	备注
70			统计报表	提供警情全流程报表、日报表、周报表、自定义报表、接警员接警统计、综合查询、伤亡人数统计、火灾类型分析等基础报表，支持单个警情接、调、处信息汇总报告生成和日常各类警情统计分析报表。	
71	智能化后台支撑	综合报警定位服务模块	报警电话定位	优先依托现有先进的定位云服务平台，或协调运营商，提供报警电话定位数据，实现手机及固话报警定位。	
72			地名地址定位	地名地址定位是依托人类活动中产生的各类信息数据，如：详细区域、街道、门牌号、建筑物名称等，通过相似度匹配，找到最相似的地址信息获得地理坐标信息，返回的地址信息包括完整地址、经纬坐标、所属管辖区域等信息。	
73			地理要素定位	通过“一张图”服务提供的关键字、周边 POI 搜索、以及行政区划等查询功能，实现报警时常用位置识别信息比对定位，同时，支持多类别的精准搜索匹配和模糊搜索查询，满足目的化、多样化的地图搜索需求。	
74			移动应用定位	移动应用报警系统在报警时，可通用移动终端设备利用 AGPS 技术或 WIFI 定位技术取得当前位置信息，并将报警信息推送至综合报警定位服务中，实现手机报警实时定位。	
75			智能融合定位	以“一张图”服务为基础，充分利用互联网数据资源，整合报警电话定位、辖区范围、地理要素定位、地名地址定位、移动应用定位等多类定位手段，逐渐缩小空间区域，将各类位置信息互为补充，建立优先规则，自动计算警情位置，提供定位服务，同时结合手动定位，以提高定位精准度，达到快速准确定位警	

序号	系统模块	子模块	功能项	功能描述	备注
				情的目的。	
76		智能接警模型	警情语音识别	结合人工智能技术，建立消防语料库、接警关键信息识别模型和本地口音普通话训练模型，支持智能语音服务本地私有化部署，支持双声道语音流话者分离，实现警情无延迟精准语音识别。	
77			警情信息提取	结合消防语料库、消防关键词匹配等技术手段，通过本地私有化部署的自然语义解析服务，以智能警情要素提取模型实现实时警情信息精准提取。	
78			警情等级分析模型	根据警情信息反馈内容动态运算分析给出警情等级，结合人工修正记录并比对历史同类警情进行自我优化，完善系统智能分析模型。	
79			重复警情提醒模型	根据一定时间范围内的位置、报警电话、报警人、警情类型等自动分析出是否有重复警情，对重复警情自动发出提醒。	
80		智能调度模型	智能调派模型	针对当地消防救援力量、灾害类型及分布特点，结合空间位置、路径、时间等要素，建立满足当地消防救援需要的智能调派模型。通过智能调派模型，可自动生成辅助推荐调派方案，支持根据实际调派方案数据，自动预警并提醒接警员核实差异原因(如车辆正在维修，道路限高、限重、限行等），同时进行记录，以接警员修改及确认的调派优化方案作为训练数据不断优化智能调派模型。具备条件的单位可建立模型自我训练的模式，以不断提高模型自动生成调	

序号	系统模块	子模块	功能项	功能描述	备注
				派方案的精准度，整体提升指挥中心的调度效率。	
81			智能路径规划模型	建立智能路径规划模型，结合地图分析辖区内交通道路拥堵畅通情况，桥梁隧道及高速公路入口的通行能力等信息，利用卡车、特种车模式合理规划行车路径，合理规避限高、限重、限行路段，指引消防救援车辆以最佳、最快捷的行驶路线到达警情现场，具备条件的单位可根据实时路况提供备选方案，同时结合实际历史行车轨迹数据，结合深度学习技术，不断自行训练，提升优化智能路径规划模型的正确性和可靠性。	
82			调派优化模型	建立调派优化模型，系统自动核对实际出警车辆与推荐出警车辆存在的差异，自动预警并提醒接警员核实差异原因(如车辆正在维修，道路限高、限重、限行等），同时进行记录，以接警员修改及确认的调派优化方案作为训练数据不断优化调派模型。	
83		语音模型智能训练		建立本地口音普通话语音模型训练机制，在确保语音数据保密性的基础上，提供适应各地本地口音普通话的纠偏机制，提供语音标注工具，并支持智能语音识别模型本地自动化数据训练、模型效果评估、模型发布、自动应用至智能接处警系统，以持续提高本地口音普通话语音识别效果。	
84		多源报警转入服务模块		提供多源报警统一接入接口，与接警端应用模块分离，对各类报警源的信息进	

序号	系统模块	子模块	功能项	功能描述	备注
				行统一转换，如城市远程监控、微信、APP 报警信息。	
85	联网汇聚模块	消息服务		提供统一消息服务为各系统和模块之间提供消息传递服务，保证系统之间数据即时快速交换，实现警情受理、处置、调度、反馈的全流程通信。	
86		数据接入		对外部一体化业务信息系统、一张图等各类系统数据源以配置方式进行数据接入，分别采用数据库、接口方式对接。数据源配置支持数据字段映射能力，能够对数据进行一定的转换，保证数据中心数据库的时效性、权威性和一致性。	
87		数据分发		提供主动的数据分发服务，将从外部或上级获取的数据即时分发到本级业务模块或下级联网汇聚模块中。通过本服务可将外部接入数据或内部相关数据推送至指定位置。	
88		数据共享		提供一套统一的数据共享服务进行对外共享。	
89		数据汇聚子模块		提供实时与定时数据汇聚功能，同时支持指定时间段补传功能。	
90		数据可视化子模块	数据汇聚总览	通过数据可视化模块对数据进行展示，并提供智能化报表功能，为辅助决策提供数据依据。	
91			数据综合查询	查询支队的各维度数据情况，及时获取相关数据详细信息。提供重要警情提醒，实时预警，并支持按级别以列表方式显示重大警情当前处置状态并及时跟踪。	
92			数据汇聚统计	以辖区为单位，统计、查询各维度数据情况，直观、准确的获取辖区内的数据汇聚统计情况。	
93		数据质	警情数据填写完整性	数据汇聚采用可靠协议接口，包含有交互式应答及消息推送反馈功能，对汇聚	

序号	系统模块	子模块	功能项	功能描述	备注
		量分析子模块	分析	的警情数据的完整性和质量进行实时监测、分析以及异常告警。	
94			数据汇聚异常记录	对汇聚数据过程中可能出现的抽取失败、数据缺失等问题进行记录及提示。	
95	运行监控模块	监控总览		提供对主要的服务器设备、座席、中继网关、服务等主要指标信息总览展示。	
96		设备监控		提供对服务器、座席、网络、中继网关等主要设备各项指标信息实时监控，异常数据告警。	
97		服务监控		提供对服务各项指标信息实时监控，异常数据告警。	
98	数据迁移	将老旧系统数据 2012 年至今数据全部迁移至新系统数据库中			

3、性能要求

3.1 系统综合性能指标

服务能力（平台满足用户需求的能力）	最大并发用户数	1000
	响应时间	≤3 秒
	每秒事务数	≥3000 个
	服务失效率	≤0.001%
服务扩展性（评价平台在负荷超过设计容量 120%后的性能变化）	每秒事务数	下降不超过 10%
服务稳定性（评价平台在负荷超过设计容量 120%后是否稳定）	响应时间	≤5 秒

另外系统不得出现以下情况：无故退出系统；发生系统不可控制的故障提示；因系统故障导致操作系统或机器无法正常工作。

3.2 数据平台性能指标

（1）结构化数据：并行加载速度达到 1.2GB/秒；

（2）非结构化数据：并行加载速度达到 2.1GB/秒；

（3）条件检索速度：总量在 100 万条以上记录时，条件检索响应时间小于 3 秒；

（4）各种比对、分析等复杂事务处理≤4s；

（5）统计分析速度：总量在 100 万条以上记录时，统计分析响应时间小于 60 秒；

（6）创建分词索引：中文分词建立索引速度在 100MB/秒；

（7）关键词检索速度：总量在 13TB 的文本数据，关键词检索响应时间小于 3 秒；

（8）索引膨胀比率：10%~30%；

（9）数据压缩比率：5% ~30%。

3.3 智能化能力指标

以对模拟报警录音 10 起、随机抽取历史报警录音 10 起，总计 20 起报警录音进行智能识别为例：

（1）智能语音识别准确率不低于 95%；

（2）警情地址识别准确率不低于 90%；

（3）警情重要元素识别准确率不低于 90%。

4、网络要求

建设和完善海口市救援支队网络支撑平台，同时对接上级总队指挥网，为海口市救援支队日常工作提供网络系统、救援音视频信息管理和应用系统运行环境的支撑与服务，保障网络与信息的安全传输与可信交换。

本期网络建设采用“核心+接入”二层网络结构和“万兆骨干，千兆桌面”组网模式。如拓扑图所示。核心交换机，负责接入交换机。接入交换机通过万兆光纤接入核心交换机，接入交换机通过千兆网线连接到每个信息点。

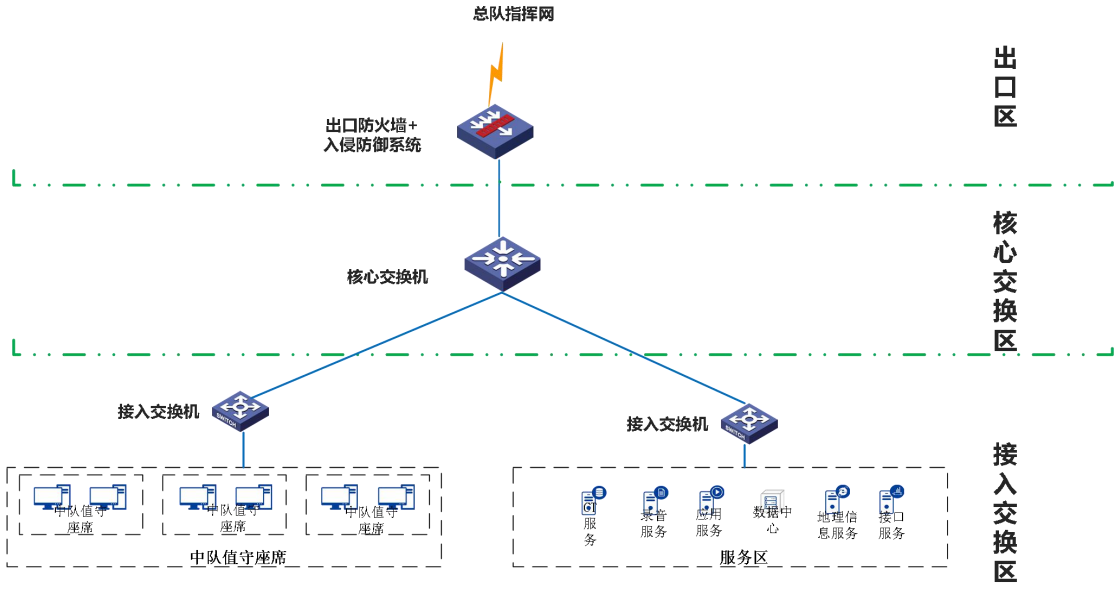

图 1　网络结构拓扑图

5、安全要求

5.1 安全技术框架设计

根据国家等级保护策略，结合信息系统的安全保护等级，设计支撑体系框架的安全目标和安全要求，安全要求和技术方法符合国家等级保护相关标准，基本满足等级保护的基本目标、控制项和控制点。

信息系统安全体系建设的思路是根据分区分域防护的原则，按照一个中心下的三重防御体系，建设信息安全等级保护纵深防御体系。

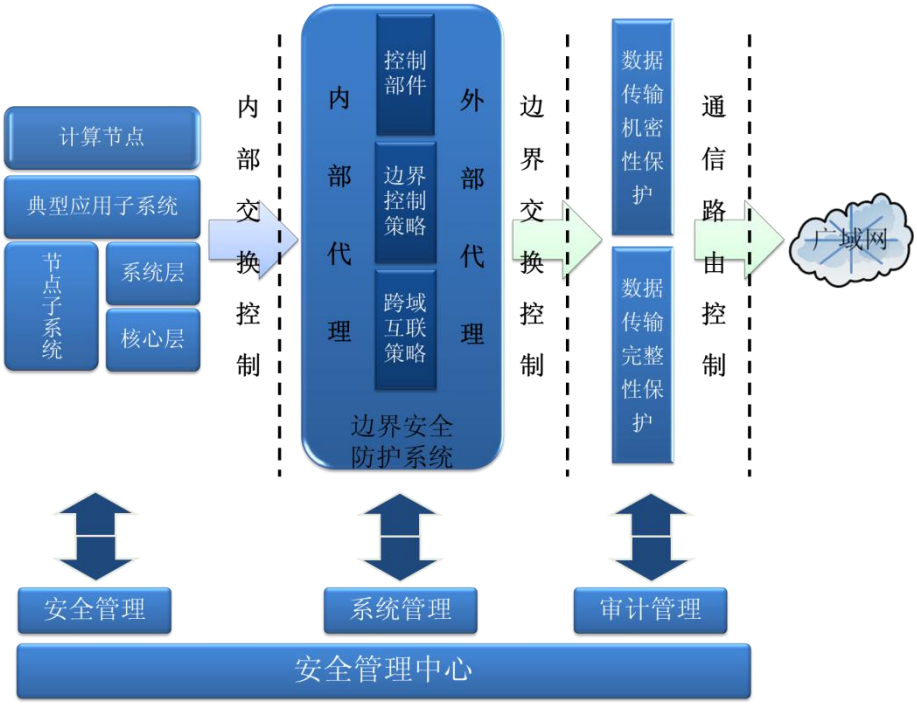

图 2　安全管理示意图

按照信息系统业务处理过程将系统划分成计算环境、区域边界和通信网络三部分，以终端安全为基础对这三部分实施保护，构成有安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的“一个中心”管理下的“三重防御体系”。

5.2 安全域规划设计

安全域是根据保护要求、信息性质、使用主体、安全目标和策略等的不同来划分的，是具有相近的安全属性需求的网络实体的集合。

一个安全域内可进一步被划分为安全子域，安全子域也可继续依次细化为次级安全域、三级安全域等等。同一级安全域之间的安全需求包括两个方面：隔离需求和连接需求。隔离需求对应着网络边界的身份认证、访问控制、不可抵赖、审计等安全服务；连接需求对应着传输过程中保密性、完整性、可用性等安全服务。下级安全域继承上级安全域的隔离和连接需求。

因此，网络中应该划分不同级别的安全域，并对不同级别的安全域实行分级的保护。

5.2.1 安全域划分方法

在进行解决方案设计时，首先要对系统的安全域进行划分，使相同业务需求或相同保护级别的系统分离出来。通过逐一对组织机构应用系统的安全域划分和多系统安全域整合，形成组织机构的安全域架构。

安全域的定义是同一安全域内的系统有相同的安全保护需求、并相互信任。安全区域划分分析是以结构化的方法为基础进行分解性分析，所谓结构化就是通过特定的结构

将问题拆分成若干个子问题的迭代方法。结构化方法包括以下几条基本原则：

1、充分覆盖

所有子问题的总和必须覆盖原问题。如果不能充分覆盖，那么解决问题的方法就可能出现遗漏，严重影响本方法的可行性。

2、互不重叠

所有子问题都不允许出现重复，类似以下的情况不应出现在一个框架中：

两个不同的子问题其实是同一个子问题的两种表述；某一个子问题其实是另外两个问题或多个问题的合并。

3、不可再细分

所有子问题都必须细分到不能再被细分。当一个问题经过框架分析后，所有不可再细分的子问题构成了一个“框架”。

安全域划分是将系统作为一个安全域，通过对网络和信息系统的梳理和整合，将此安全域划分为子安全域和子安全域的子安全域。以此类推，形成系统的结构化的安全域划分结构。安全域结构化划分须遵守充分覆盖、互不重叠、不可再细分的原则。

划分一个独立的业务信息系统的内部安全域，主要参考如下步骤：

1）查看网络上承载的业务系统的访问终端与业务主机的访问关系以及业务主机之间的访问关系，若业务主机之间没有任何访问关系的则单独考虑各业务系统安全域的划分，若业务主机之间有访问关系，则几个业务系统一起考虑安全域的划分；

2）划分安全计算域：根据业务系统的业务功能实现机制、保护等级程度进行安全计算域的划分，一般分为核心处理域和访问域，其中数据库服务器等后台处理设备归入核心处理域，前台直接面对用户的应用服务器归入访问域；局域网访问域可以有多种类型，包括：开发区，测试区，数据共享区，数据交换区，第三方维护管理区，VPN 接入区等；局域网的内部核心处理域包括：数据库，安全控制管理，后台维护区（网管工作区）等，核心处理域应具有隔离设备对该区域进行安全隔离，如防火墙，路由器（使用 ACL），交换机（使用 VLAN）等；

3）划分安全用户域：根据业务系统的访问用户分类进行安全用户域的划分，访问同类数据的用户终端、需要进行相同级别保护划为一类安全用户域，一般分为管理用户域、内部用户域、外部用户域；

4）划分安全网络域：安全网络域是由连接具有相同安全等级的计算域和（或）用户域组成的网络域。网络域的安全等级的确定与网络所连接的安全用户域和（或）安全计算域的安全等级有关。一般同一网络内化分三种安全域：外部域、接入域、内部域。

5.2.2 安全域划分原则

安全域应该以业务的逻辑为主要原则，辅以安全的原则，才能合理地对网络系统进

行梳理，在不损失或较小损失业务运作效率的前提下来保障安全。安全的主要目的是为了保障业务系统的正常运行，超越业务逻辑来谈安全是没有意义的。安全域划分采用的原则如下：

安全域仅对资产所有者为本部门的资产进行划分，对部属本部门资产的访问端通过边界进行保护安全域内资产。

1、业务和功能特性

业务系统逻辑和应用关联性；

业务系统所属的管理部门和行政结构；

2、安全特性的要求

安全要求差异：可用、保密和完整三性的要求差异，如有保密性要求的资产单独划区域；

面临威胁的差异：面临主要威胁不同，如第三方接入区单独划区域；

资产价值差异：重要与不重要资产分离，如核心生产区和管理终端区分离；

参照现有状况；

现有网络结构的状况：现有网络结构、地域和机房等；

参照现有的管理部门职权划分。

3、其他要求

具体到某一业务系统，安全域划分原则可以继续细化为:

功能相似、资产价值相似属于同一区域；

功能存在差异、资产价值相似，对可以提炼出功能中共同的属性的资产同属一各区域，对于不能提炼出共性的资产划分到不同区域；

功能相似、资产价值存在差异，可以判断威胁来源和影响程度，对于威胁来源和影响相似的资产同属一个区域，不同程度的划分到不同区域；

功能存在差异、资产价值存在差异，划分为不同区域；

整合业务系统到同一外部网络的所有物理边界；

根据威胁分析结果，从逻辑上整合威胁相近的外部逻辑边界。

对于同一组织机构的多个业务系统，首先逐一分析应用系统，划分安全域。分析每个应用系统安全域划分结果，充分考虑实施可行性和管理可行性，将多个系统的安全域进行合并和边界整合。多个系统安全域合并和边界整合需充分考虑以下因素：

- 网络结构、地域和机房等；
- 网络和应用管理可行性；
- 多系统间可能的影响；
- 安全技术手段实施可控制范围；

- 多系统等级和安全域重要程度差异；
- 功能相似性和威胁相似性；
- 安全要求相似性。

5.3 网络安全拓扑

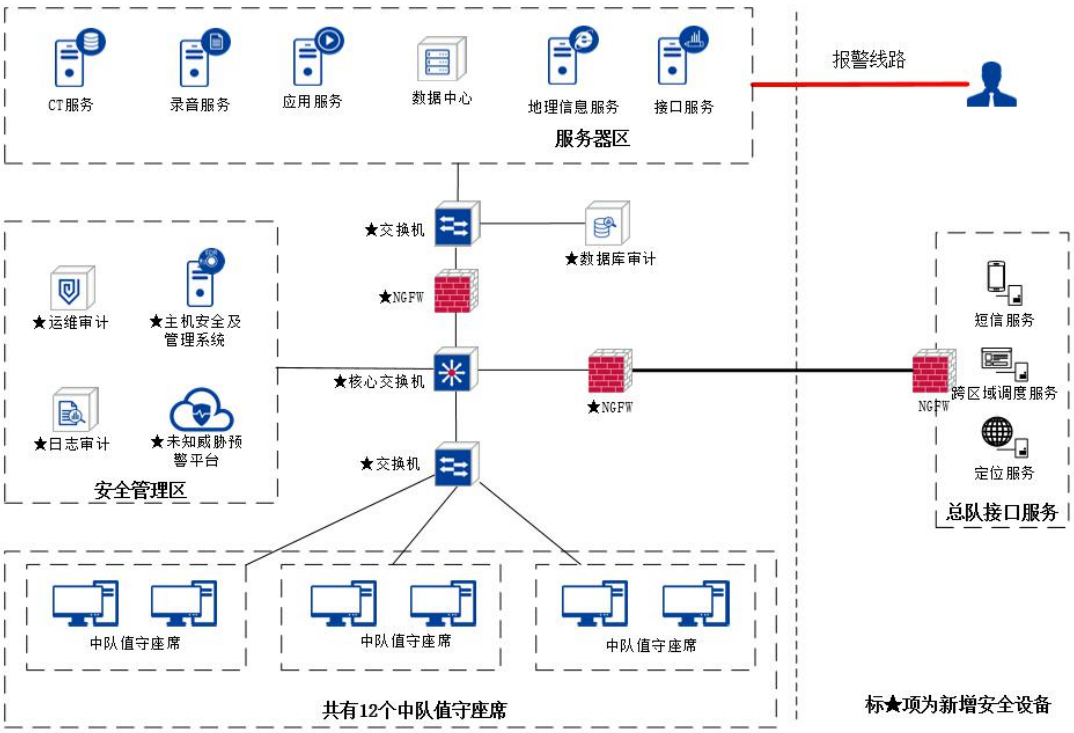

图 3　网络安全拓扑图

通过在海口市消防救援支队内网出口边界部署下一代防火墙，实现对外进出站流量的安全访问控制防护，以及部署数据库审计设备实现对所有数据库访问及操作行为的安全审计预警，以保障服务器的数据安全及应用系统安全。

在安全管理区部署主机安全及管理系统实现对内多重要服务器及办公终端的安全防护，东西向流量的访问控制及防病毒等功能。

部署日志审计及运维审计设备，实现对内网重要设备的安全日志及运维操作进行审计分析预警，并通过未知威胁预警平台对网内流量进行全流量多维分析，并与访问控制设备及主机防护系统实现联动处置，以实现对网络安全的动态防护。

5.4 安全技术体系建设

5.4.1 安全计算环境建设

5.4.1.1 主机安全及管理系统

1、等保 2.0 控制项对应

控制点	条目细项	产品符合
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	符合
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	符合
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	符合
	d）应对审计进程进行保护，防止未经授权的中断。	符合
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	符合
	b）应关闭不需要的系统服务、默认共享和高危端口；	符合
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	符合
	d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	符合
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	符合
	f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	符合
恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	符合
	b）应定期验证防范恶意代码攻击的技术措施的有效性。	符合

2、产品部署：

将产品管理端部署在安全管理区配合客户终端实现网络内部的主机安全防护。本产品部署主要有服务端与终端两部分组成，服务端提供统一的控制与协调。以实现服务器、虚拟云及办公终端的主机防护。

3、产品功能：

主机安全及管理系统是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。主机安全及管理系统通过文件诱饵引擎，具有勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。目前广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全等各个场景。

主机安全及管理系统主要需求指标参数：支持对服务器进行防护。防护内容包括：病毒查杀、漏洞管理、网络防护、勒索防护等。支持 Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、 Suse11 +、 Ubuntu 14 +等操作系统。

系统防护：病毒查杀，使用自主研发的多引擎，多方来源病毒库，病毒、木马文件识别率达到 99%以上。

漏洞管理：依赖管理平台的强大推送功能，能够及时检测及安装官方发布的系统补丁，使操作系统免受黑客攻击。对操作系统进行全面漏洞扫描，并对漏洞补丁进行一键修复或单个修复。

登录防护：可对系统账户登录进行精准的策略设置，支持对访问来源（账户、地理位置、远程 IP 或域名、远程计算机名）、访问时间的配置，实时阻断非法登录。采用系统级插件技术，及时发现并阻断暴力破解行为，不依赖系统日志。可周期性执行弱口令检测或立即执行一次检测，检测字典包括常见弱口令、同用户名的口令和空口令。

进程防护：进程启动防护是进程启动时的主动防御机制，在进程启动、文件创建时自动触发，阻断恶意程序运行。开启进程白名单，通过配置进程白名单，只允许受信任的进程启动，对其他进程可以做仅记录、阻断并记录两种设置。

文件访问控制：文件变化审计，监控目标文件/目录的改写操作，记录到日志中。

网络防护：微隔离，采用内核级网络防火墙技术，对不同的业务之间的流量进行精准识别、针对非法流量可以精准阻断，该功能广泛应用在云数据中心。快捷操作直接输入需要关闭的端口或需要屏蔽的恶意 IP，自动生成隔离规则。

防端口扫描：为了防止对终端服务器上端口进行恶意探测，某个 IP 在指定时间内对某个端口进行恶意探测超过设置次数，将恶意探测 IP 地址进行锁定，防止其对终端服务器有下一步的恶意行为。可以查看已临时锁定的 IP 清单。

防违规外联：开启防违规外联功能，配置白名单 IP，除白名单 IP 以外实时阻断或仅记录。

Web 应用防护：网站漏洞防护，一是网站漏洞防护，可防护常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞、文件名解析漏洞、自定义规则等；二是网站满数据防护，可禁止浏览畸形文件、敏感信息防泄漏、自动屏蔽扫描器等：

CC 攻击防护：具有高、中、低三档防护策略，智能检测并防御 CC 攻击。

网站访问控制可通过灵活配置的 IP 或页面路径，可对特定的访问者或页面进行放行或拦截。

网站后门查杀：静态检查与动态执行检测结合，可对网站目录下所有文件进行深入检测，清扫隐藏的 WebShell，解除后顾之忧。通过路径配置对 Web 应用目录进行深入检测，对扫描出的风险文件进行立即隔离或添加信任、删除操作。

工具箱：勒索防御，勒索病毒使用高强度非对称加密算法对用户关键数据加密并索取赎金，勒索防御功能通过对恶意进程、弱口令、系统漏洞、高危端口的检测，给出感染勒索病毒的可能性，并且通过双重防御引擎，阻断勒索软件的启动和加密行为，实时抵御勒索病毒。

挖矿防御：挖矿病毒会大量消耗系统运行资源非法挖矿，挖矿防御功能通过对弱口令、系统漏洞、资源占用、恶意进程、DNS 历史查询和异常外联几项的检测，给出感染挖矿病毒的可能性，并通过主动防御机制，实时阻断挖矿病毒的运行。

性能监控：对终端的 CPU、内存、磁盘及网络入站、出站流量进行监控，并在达到用户配置的阈值时及时发出告警，防止系统资源耗尽。

外设管理：监控外设的插入与拔出，控制外设的权限包括禁用、只读、放行，对外设对文件的操作进行审计。

批量配置：批量配置通过将录制的模板，应用给大量资产，达到快速配置大量资产的目的。内置 10 个常用模板：开启进程启动防护、关闭外设文件审计、永恒之蓝勒索挖矿防御、开启网站漏洞防护、启用防端口扫描检查、启动外设文件审计、禁止外设写入、开启勒索加密防护引擎、关闭网站漏洞防护、解除外设写入限制。

定期巡检：设置需要定期批量执行的检测任务，内容包括任务名称、执行巡检的内容，要巡检的资产，执行周期和备注。

病毒查杀：可查看所有资产病毒查杀情况。可在此页对所有资产批量进行立即扫描（快速扫描/全盘扫描）、停止扫描、立即隔离。

5.4.1.2 数据库审计系统

1、等保 2.0 控制项对应

控制点	条目细项	产品符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事	符合

	件进行审计；	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	符合
	d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	符合
系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计	符合
	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	符合
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计	符合
	b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	符合
安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计	符合
	b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	符合

2、产品部署

部署 1 台数据库审计系统，采用旁路模式部署，需要在交换机上镜像被审计数据库的进出流量。

3、产品功能

数据库审计系统是结合各类法令法规（如等级保护、分级保护、企业内控、SOX、PCI 等）对数据库安全的要求，自主研发的细粒度审计、双向审计、全方位风险控制的数据库安全审计产品，可以全面记录数据库访问行为，识别越权操作等违规行为，并完成追踪溯源；跟踪敏感数据访问行为轨迹，构建行为模型，及时发现敏感数据泄漏；检测数据库配置弱点、发现 SQL 注入等漏洞、提供解决建议；为数据库安全管理与性能优化提供决策依据；提供符合法律法规的报告，满足等级保护审计要求。

数据库审计与风险控制系统对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果，以可视化的方式将所有的访问都呈现在管理者的面前，数据库不再处于不可知、不可控的情况，数据威胁将被迅速发现和响应。

1）事前安全风险评估

数据库审计与风险控制系统依托权威性的数据库安全规则库，自动完成对几百种不当的数据库配置、潜在弱点、数据库用户弱口令、数据库软件补丁等等的漏洞检测。

2）实时行为监控

数据库审计与风险控制系统可保护业界主流的数据库系统，防止受到特权滥用、已知漏洞攻击、人为失误等等的侵害。当用户与数据库进行交互时，数据库审计与风险控制系统会自动根据预设置的风险控制策略，结合对数据库活动的实时监控信息，进行特征检测及审计规则检测，任何尝试的攻击或违反审计规则的操作都会被检测到并实时阻断或告警。

3）细粒度协议解析与双向审计

系统通过对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时审计，而且还可对数据库系统返回结果进行完整的还原和审计，包括数据库命令执行时长、执行的结果集等内容。

4）双重审计

用户只需要将 web 服务器的流量镜像到数据库审计与风险控制系统，就能够对所有基于 web 的应用的访问行为进行解析还原，形成数据库审计和 web 审计的双重审计模式。

5）应用三层关联审计

数据库审计与风险控制系统能够将 web 审计记录与数据库审计记录进行关联，直接追溯到应用层的原始访问者及请求信息，从而实现将威胁来源定位到最前端的终端用户的三层审计的效果，通过三层审计能更精确地定位事件发生前后所有层面的访问及操作请求。

6）灵活的审计规则

数据库审计与风险控制系统提供细粒度的审计规则，如精细到表、字段、具体报文内容的细粒度审计规则，实现对敏感信息的精细监控；基于 IP 地址、MAC 地址和端口号审计；提供可定义作用数量动作门限、可设定关联表数目动作门限、根据 SQL 执行时间长短、根据 SQL 执行回应以及具体报文内容等设定规则。

7）高效的行为检索

数据库审计与风险控制系统在已审计的海量记录中设计了通过各种要素多重组合的方式进行查询，能够快速精确地定位到威胁记录的位置，帮助管理者做出响应。

5.4.2 全区域边界建设

下一代防火墙

1、等保 2.0 控制项对应：

控制点	条目细项	产品符合
网络架构	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	符合
	d）应避免将重要网络区域部署在网络边界处，重要网络区域和其他网络区域之间应采取可靠的技术隔离手段；	符合
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	符合
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	符合
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	符合
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	符合
	e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	符合
入侵防范	a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c)应采取技术措施对网络行为进行分析，实现对	符合

	网络攻击特别是新型网络攻击行为的分析； d)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	

2、产品部署

在海口市消防救援支队与总队的通信边界以及服务器安全域边界各部署1台下一代防火墙，开启入侵防御、防病毒模块，实现对服务器区的安全防护及整个内网的进出站边界进行整体安全防护。

3、产品能力

在面对日益增长的应用和流量以及网络安全的需求下，传统的网络防火墙已经无论在功能还是在性能方面都显得力不从心。通过部署下一代防火墙，对重要节点和网段进行边界保护，可以对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，防范各类攻击行为，杜绝越权访问，防止非法攻击，抵御可能的 DOS 和 DDOS 攻击。通过合理布局，形成多级的纵深防御体系。

1）防火墙功能

防火墙实现不同安全域之间的访问控制，可以达到等级保护中要求根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级，保护服务器脆弱的服务、控制对系统的访问、实现区域划分和阻止网络攻击。

2）入侵防御系统

入侵防御系统多种攻击特征，能够检测常见的病毒、蠕虫、后门、木马、僵尸网络攻击以及缓冲区溢出攻击和漏洞攻击；封堵主流的高级逃逸攻击；检测和防御主流的异常流量，含各类Flood攻击；提供用户自定义攻击特征码功能，可指定网络层到应用层的对比内容；提供虚拟补丁功能，让没有及时修补漏洞的客户，能够保障网络安全正常运行。

3）防病毒

采用高效的病毒防御引擎和国内知名病毒厂商特征库，可检测不少于300万以上种病毒。可以根据不同的源IP地址、目的IP地址、服务、时间、接口、用户等，采用不同的病毒防御策略。

可以过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒特征库定时更新，支持病毒库本地升级，病毒库可实时在线升级。

支持基于病毒防护策略设置阻断、清除、记录日志，发送电子邮件报警。

5.4.3 安全通信网络建设

1、等保2.0控制项对应

控制点	条目细项	产品符合
通信传输	a)应采用校验技术或密码技术保证通信过程中数据的完整性； b)应采用密码技术保证通信过程中数据的保密性。	符合

2、部署：

开启下一代防火墙的 VPN 功能进行前端设备的 VPN 接入。

网络建成后，大量的业务信息依托网络平台。有的人员，往往需要在公网上进行内网信息的获取。这种传输方式十分容易被非法窃取、篡改或删除。移动办公用户无法有效的访问单位资源，单位流程办公无法执行，比如需要通过单位 OA 系统进行申请相关工作事项，由于外出办公无法进行及时申请，公司会议无法及时收到通知等相关的工作。为此公司把内部办公系统发布到外网服务会带来一些非法用户的攻击访问，访问公司内部资源时传输过程中容易被窃取信息，造成无法挽回的损失，因此需要通过网络通信加密/认证技术手段对相关应用系统进行保护。对于移动办公用户必须要建立 SSL VPN 安全通道，更好的为移动用户提供服务并具备更强的安全性和可控性。

网络的 VPN 应用有两种：防火墙到防火墙、移动用户到 IPsec VPN/防火墙或 SSL VPN 网关设备。前者是针对单位各分支机构，应用在各分支机构有固定 IP 地址的防火墙系统之间，供分支结构之间互通信息；后者针对移动办公的 IP 地址不固定的单位员工从 Internet 上对单位内部资源的访问，其中 SSL VPN 可以更好地为移动用户提供服务并且具备更强的安全性和可控性，是移动用户安全访问应用的技术趋势。

而 SSL VPN 网关可以让单位员工随时随地，以任意接入方式，受控地安全访问单位的信息，是单位提高工作效率、保障信息安全、降低 IT 成本的最佳选择。

5.4.4 安全管理中心建设

5.4.4.1 日志审计系统

1、等保 2.0 控制项对应

条目号	控制点	条目细项	产品符合
8.1.3.5	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	符合
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	符合

		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	符合
		d）应对审计进程进行保护，防止未经授权的中断。	符合
8.1.5.4	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控	符合
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理	符合
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测	符合
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求	符合 符合
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理	符合
		f）应能对网络中发生的各类安全事件进行识别、报警和分析	符合

2、产品部署

在内网的安全管理区部署 1 台日志审计设备，实现网络环境安全类、管理类、流量数据以及资产、用户的基本数据的采集、ETL 和集中存储。并将日志转发给安全威胁分析平台进行分析。

采集方式：通过使用 Syslog、SNMP Trap、OPSec、FTP 协议在日志采集引擎上对各种日志进行采集，包括资产日志、安全设备的日志、主机服务器的日志以及应用系统的日志采集。支持主动采集和被动接收等多种方式对日志进行采集。

3、产品能力

日志审计系统通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营安全；日志采集探针通过基于国际标准化的关联分析引擎，为客户提供全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，为客户提供真正可信赖的事件追责依据和业务运行的深度安全。同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，协助用户全面审计信息系统整体安全状况。

1）全面的智能收集功能

不断的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控；可配置过滤和聚合功能可以消除无关数据，并且合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

2）全面日志采集

支持 200 多个品牌。2000 多种设备的日志接入。日志接入兼容性能力强。覆盖主流硬件设备、主机及应用，保障日志信息的全面收集。实现信息资产（网络设备、安全设备、主机、应用及数据库）的日志获取。

3）大规模安全存储

采用先进的全文索引和文件型高性能日志存储技术。内置 T 级别存储设备，可以选配各种 RAID 级别进行数据冗余和安全保障。系统拥有多项自主知识产权的存储加密机制和查询机制，十分合适等保、密保等行业的应用要求。

4）智能关联分析

自研高效关联分析引擎，具备多项核心专利技术。实现全维度、跨设备、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，客户可轻松实现各资产间的关联分析。

5）脆弱性管理

具备多厂商资产脆弱性管理，兼容性较强。支持主流漏洞扫描工具的漏洞管理分析，可结合日志和资产进行关联分析。支持收集和管理来自各种 Web 漏洞扫描、主机漏洞扫描工具、网络漏洞扫描工具的产生的扫描结果，并实时和用户资产收到的攻击危险进行风险关联分析。

6）数据挖掘和数据预测

具备多种数据挖掘和数据预测核心分析模型。对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。

7）合规能力

满足各类法规日志留存、分析的要求。如《中华人民共和国网络安全法》、《信息安全等级保护管理办法》、SOX 法案等。具备 1000+相关法案的审计报表。

5.4.4.2 运维审计系统

1、等保 2.0 控制项对应

控制点	条目细项	产品符合
安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	符合

	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	符合
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	符合
	d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	符合
身份鉴别	d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	符合
系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计	符合
	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	符合
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计	符合
	b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	符合
安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计	符合
	b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	符合

2、产品部署

在安全管理区各部署 1 台运维审计系统（堡垒机），采用旁路的网络部署模式，不影响网络拓扑和业务系统的运行，可通过网络访问控制系统（如：防火墙、带有 ACL 功

能的交换机）的配合下，让堡垒机成为唯一的入口，确保“终端至运维审计系统的管理端口可达、运维审计系统与目标主机的运维协议可达”。

3、产品功能

随着信息化的大力普及，信息化内控建设方面存在一定的滞后性，信息化设备的运维方面存在众多的安全隐患，如系统账号滥用、弱密码、越权访问、权限管理混乱、运维过程不透明、误操作、恶意数据泄露等众多安全问题，运维的服务器普遍存储着各种重要的业务数据，业务的稳定安全运行至关重要，运维过程中一旦误操作或者遭受恶意操作，没有任何访问控制和审计，将会导致事中无法管控、事后无法追溯调查取证，存在着极大的管理风险，随着国家对网络安全的重视，运维内控也变得日趋重要，如何管控内部各种运维人员的日常操作行为已经是信息化建设和管理必须重点考虑和解决的问题。

运维审计是结合各类法令法规（如 SOX、PCI、企业内控管理、等级保护、ISO/IEC 27001 等）对运维审计的要求，采用 B/S 架构，集统一帐户管理与单点登录于一体，支持多种字符终端协议、文件传输协议与图形终端协议的实时监控与历史查询，具备全方位运维风险控制能力的统一运维安全管理与审计产品。

1）运维协议

目前已经支持 SSH、RDP、VNC、FTP、SFTP、Telnet 等六种协议近 200 个协议版本，兼容目前数据中心各种服务器、交换机、路由器等主要资产设备。

2）身份鉴别

通过手机 APP 动态口令、动态令牌卡、USBKEY、短信口令、等多种鉴别方式保证用户访问的合法性，确保账号无法盗用。同时支持同第三方认证平台 AD/LDAP/RADIUS 的认证对接。

3）自动建模授权

通过智能学习建模方式，建立运维人员的权限模型，智能完成授权，并自动添加资产和账号。大大减少部署工作量，保障系统快速有效上线。

4）运维接入

支持 Web 单点登录、C/S 登录、网关代理、Web H5 运维等四种方式运维接入，能友好的兼容各种终端、各种环境、各种不同使用习惯的运维接入要求。

5）文件传输审计

可以完整保存 SFTP、FTP、SCP、RZ、SZ、RDP 协议传输的文件，支持细粒度的文件审计控制，一旦发生数据窃取、拖库、上恶意病毒干扰等事件，可以快速定位追踪。

6）数据库运维审计

对 Oracle、SQLServer、Mysql、DB2 等主流数据库的运维操作进行运维访问控制和

审计，用户运维体验、审计完整性和细粒度有较为明显的技术优势。

7）运维统计报表

系统内置丰富的报表统计，包含操作重要性、异常用户、行为告警、会话数量、法律法规符合性等维度统计的多种报表，报表形式包含柱状图、饼图、曲线图等多种形式，提供可关联、可回放、可追溯等深度分析的报表。

8）灵活的部署模式

支持单机、HA、异地灾备、大型集群、分布式等多种方式的部署模式，适应各种大小规模、多数据中心等复杂环境的高可用部署要求。

5.4.4.3 未知威胁预警平台

1、等保 2.0 控制项对应

条目号	所属等级	控制点	条目细项	产品符合
8.1.3.3	第三级安全要求	入侵防范	a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警	符合
8.1.3.4	第三级安全要求	恶意代码和垃圾邮件防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	符合
8.2.3.2	第三级安全要求	入侵防范	a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量	符合

			等； b)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； d）应在检测到网络攻击行为、异常流量情况时进行告警。	

2、产品部署

在内网的安全管理区部署 1 台未知威胁预警平台设备，未知威胁预警平台旁路部署在核心交换机上，通过核心网络镜像，把所通过该汇聚的所有网络访问进行审计，重点在于发现网络攻击特别是未知的新型网络攻击的检测和分析。通过部署未知威胁预警平台产品对邮件协议、应用协议进行解析，在协议中分离文件，通过内置动态沙箱分析技术发现文件中的恶意行为。以及 WEBSHELL 后门、高危恶意代码样本传播、内部主机被控回连进行预警，对攻击进行取证分析，帮助持续完善安全防护策略。对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接；
同时通过未知威胁预警平台可以实现与访问控制设备及主机防护系统实现联动处置，以实现对网络安全的动态防护。

3、产品功能

未知威胁预警平台使用深度威胁检测技术，对流量进行深度解析，发现流量中的恶意攻击，提供了全面的检测和预警的能力。相对于仅依靠特征检测的传统安全产品，本产品可发现零日漏洞利用、未知恶意代码等高级攻击手段，能检测到传统安全设备无法检测的攻击，为用户提供更高级的安全保障。

平台具备以下功能：

- WEB 威胁深度检测
- 邮件威胁深度检测
- 病毒木马深度检测
- 0day 攻击检测
- 异常行为分析
- 云端高级分析

通过综合关联分析综合判断 APT 攻击的行为和攻击路径。

图 4　未知威胁预警平台检测流程

1）WEB 威胁深度检测

未知威胁预警平台通过对 Web 流量和应用进行深度检测，提供全面的入侵检测能力。

未知威胁预警平台能在攻击到达 Web 服务器之前进行检测，并进行实时的攻击预警。安恒 APT 攻击(网络战)预警平台能解码所有进入的请求，检查这些请求是否合法或合乎规定；仅允许正确的格式或 RFC 遵从的请求通过。已知的恶意请求将被阻断，非法植入到 Header、Form 和 URL 中的脚本将被阻止。未知威胁预警平台还能进行 Web 地址翻译、请求限制、URL 格式定义及 Cookie 安全。

未知威胁预警平台能通过与 WAF 联动防护一系列的攻击，无论是已知的或未知的。实现阻止那些的攻击如跨站点脚本攻击、缓冲区溢出攻击、恶意浏览、SQL 注入等。

2）邮件威胁深度检测

未知威胁预警平台对邮件协议进行深度分析，记录并分析每个邮件，并对其中的附件进行分析并检测，发现其中的安全问题。包括 WEBMail 漏洞利用、邮件欺骗、邮件恶意链接、恶意邮件附件等威胁。

通过对附件进行对已知攻击特征的扫描、未知攻击漏洞的扫描和动态分析的方式进行测试，发现其中的攻击。

3）病毒木马深度检测

未知威胁预警平台对应用协议解析，在协议中分离文件，通过对病毒木马进行扫描，快速发现各种已知特征的恶意文件攻击行为。

未知威胁预警平台内部集成了 300 万+的病毒木马特征库，可有效发现网络中存在的僵木蠕，包含各种 CVE 漏洞利用、病毒感染、恶意代码传播、远控工具和恶意回连行为，分析网络中主机的威胁趋势，感知主机的威胁指数，进一步发现各种恶意样本的传播规律，预警网络安全状况。

4）利用 0day 漏洞攻击检测

安恒通过长期的研究，总结并提权各类 0day 攻击的特点。在网络流量中分析关心的文件。采用 shellcode 静态行为分析和沙箱动态行为分析的检测机制，弥补特征检测

的不足，并输出完整的二进制分析报告，全过程解析文件在运行过程中存在的各种隐藏行为。

通过定位目标文件中的 shellcode 以及脚本类文件中的溢出代码，进行静态执行分析，对目标文件进行检测，发现其中的 0day 攻击样本。

产品内置动态沙箱分析技术发现文件中的恶意行为，内部虚拟机可实现完全模拟真实桌面环境，所有恶意文件的注册表行为、敏感路径操作行为、进程行为、导入表信息、资源信息、段信息、字符串信息及运行截图等行为都将被发现，综合分析这些恶意行为，判断其中的可疑操作，再结合加权值分析技术，在保证发现所有恶意行为的同时，极大降低了误报。

5）异常行为分析

APT 攻击通常会结合人工渗透攻击，在人工渗透攻击中经常使用扫描或病毒扩散的过程。这些过程中，通常会产生大量的恶意流量。利用这些恶意流量特征，能检测攻击行为。

目前检测基于多个维度，如：

- 基于时间的检测
- 基于 ip 的检测
- 基于端口的检测
- 基于协议的检测
- 基于 DNS 异常检测
- 基于木马回连行为的分析

… …

6）云端高级分析

未知威胁预警平台云端可提供更为深层的威胁分析服务、安全预警服务和情报共享服务，依托于云端的海量数据、高级的机器学习和大数据分析能力，可及时共享最新的安全威胁情报，提供更为精准的威胁分析能力，用户也可直接访问云端，上传、查询和确认样本的分析结果，感知最新的安全态势。

APT 的对抗是以时间对抗时间，云端是产品的重要补充，是对用户提供的一种更为高级的服务，可更为及时有效的利用大数据的能力提升 APT 检测的效果。

6、云服务要求

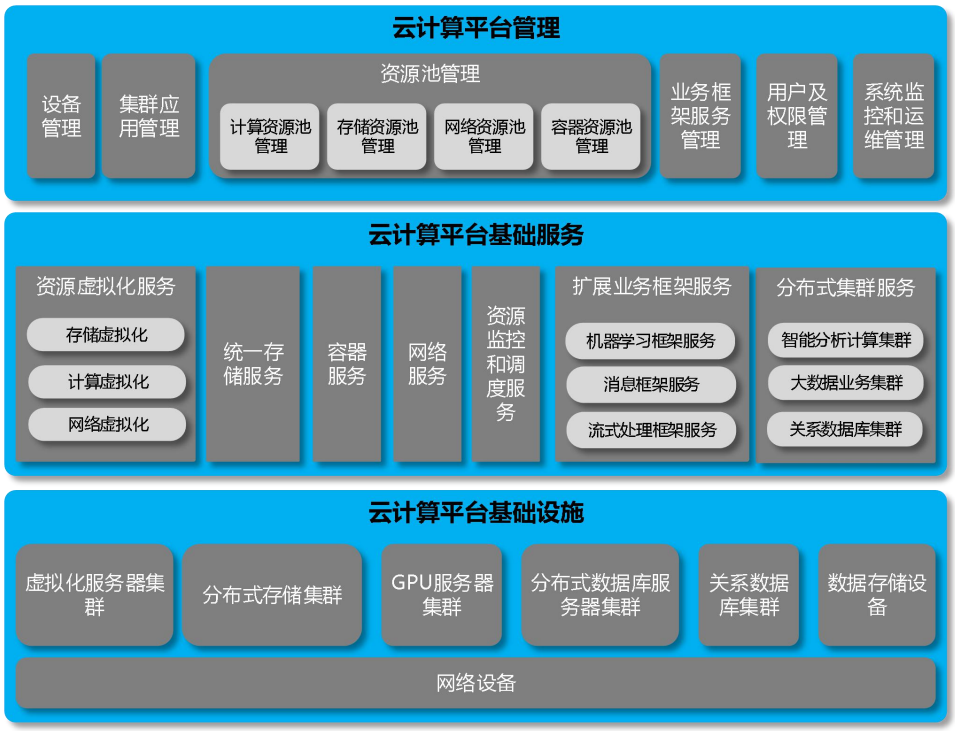

图 5　云平台基础设施服务层架构

6.1 云计算平台基础设施

云计算基础设施是各中心的计算资源、存储资源与网络资源的集合。包括各中心运营所需的服务器硬件、网络、存储、安全设备等基础设施。服务器主要分为计算虚拟化服务器设备、GPU 服务器集群以及关系数据库集群服务器，计算虚拟化服务器设备用于计算资源虚拟化，GPU 集群服务器设备用于部署集群化的智能分析应用，关系数据库集群用于部署关系数据库集群系统。分布式存储集群主要提供全局统一的分布式数据存储服务。数据存储设备主要用于分布式数据库服务器集群的共享数据存储以及云计算管理平台的镜像以及管理数据存储。网络设备主要有用于安全防护的防火墙设备、用于网络交换的网络交换机、用于构建存储网的光纤交换机组成。硬件基础设施层中，所涉及的虚拟化软件、硬件、网络、各类存储硬件可根据需要提供相关的接口与服务，以便统一集成到云管理平台内，以构建完整的计算资源中心资源管理体系。

6.2 云计算平台基础服务

云计算平台基础服务为云计算环境内所有的应用与服务提供全局服务的接口以便对各类服务实现监控、调度与管理。云基础服务包括了资源虚拟化服务、容器服务、统一存储服务、网络服务、资源监控和分布式集群服务等。

6.2.1 计算资源虚拟化和容器服务

云计算平台通过资源虚拟化实现对物理设备资源的管理和调度。虚拟化软件即虚拟化宿主操作系统，提供对服务器的虚拟化的功能实现。

在考虑虚拟化消耗及业务应用特点的基础上，系统采用传统虚拟机及 Docker 容器相结合的解决方案，负责对底层硬件资源进行抽象，统一调度计算、存储、网络资源池。其中，虚拟化核心是提供主机 CPU、内存、I/O 的虚拟化，通过共享文件系统保证虚拟主机或者容器的迁移、HA 集群和动态资源调度。

容器服务采用 Docker 容器技术实现，Docker 容器基于轻量级 Linux + 容器的方式，通过在云计算平台实现集群层面的服务调度、管理。

基于虚拟机的虚拟化服务则是在一台物理主机上虚拟出多个 VM（虚拟机），各个 VM 之间相互隔离，并能同时运行相互独立的操作系统，这些虚拟客户操作系统通过虚拟化层中间件访问实际的物理资源，并进行管理。云平台系统提供基于 Linux 内核的 KVM 虚拟机服务，可以很好地应用在服务器虚拟化整合，硬件抽象，Unix 向 Linux 迁移，结合硬件服务器的大数据开发/混合模式，虚拟桌面架构等。虚拟化宿主操作系统，只具备和虚拟化有关的功能，可以更高效稳定及安全地运行虚机系统。在虚拟化层，可以支持各类虚拟机操作系统，以及包括能提高性能的半虚拟化的网络驱动、块驱动、内存优化驱动等附加组件，以保证公安云计算中心在虚拟化系统中高效稳定地运行。

图 6　虚拟机和容器统一部署

资源虚拟化实现 IT 资源虚拟化整合和统一管理，基于 Docker 容器以及 KVM 进行调度，经过定制化的改进和开发，提供针对各类硬件的高性能虚拟化应用能力，完成计算资源、网络资源、存储资源的虚拟化，并且充分考虑系统的兼容性、可扩展性和可靠性。资源虚拟化主要有如下功能特性：

1) 支持在云计算管理平台上对 Docker 容器的创建、查询、启动、关闭、重启、删除；

2） 支持 KVM 虚拟机的创建、查询、启动、暂停、关闭、重启、删除；

3） 支持指定物理节点或者指定的域内创建 Docker 容器；

4） 支持指定物理节点创建 KVM 虚拟机；

5） KVM 虚拟机平台支持主流的 X86 架构的操作系统，包括 Windows Server 2003 /2008 R2 及以上版本服务器操作系统,Windows XP、Windows 7 操作系统，Redhat、SUSE、CentOS、Ubuntu、Fedora 等业界主流 OS 操作系统。

6） 支持 Host、Bridge、None 等多种网络模式，支持虚拟网络的创建和管理，支持给 Docker 容器以及 KVM 虚拟机添加多个网络；

7） 创建 Docker 容器或 KVM 虚拟机时，可指定 CPU，内存等资源配置；

8） 支持内存分配功能，支持不同虚机内存资源的共享和复用；支持虚机的内存 QoS 控制，控制虚拟机最低可获取的物理内存。

9） 支持虚机的 CPU QoS 控制，包括控制虚拟机获得的最低计算能力，控制虚拟机获得的最大计算能力。

10） 虚拟化平台提供统一的跨节点分布式数据存储能力，可不使用外部存储设备。若使用外部存储设备时，可支持主流设备厂商提供的共享存储，如 IPSAN，NFS，CIFS 等外部存储；

11） 虚拟化平台可提供 NFS，HDFS，S3，FTP 等不同的数据协议接口，并支持跨不同协议接口的数据共享能力；

12） 支持存储精简配置功能，支持为客户虚拟出比实际物理存储更大的虚拟存储空间，只有写入数据的虚拟存储空间才会为之真正分配物理存储，未写入的虚拟存储空间不占用物理存储资源。

13） 支持虚机热迁移功能，可以在不停机的状态下，手工或自动地实现虚机在集群之内的不同物理机之间迁移，保障业务连续性，迁移速度不小于 10 秒；

14） 支持 KVM 虚拟机的快照和备份；

15） 支持虚拟机在线克隆为模板。

多台服务器虚拟化后连接到共享存储，构建成云计算资源池，通过网络按需为用户提供计算资源服务。同一个资源池内的虚拟机可以共享资源池内物理服务器的 CPU、内存、存储、网络等资源，并可在资源池内物理服务器上动态漂移，实现资源动态调配。

计算资源以池化方式可以细粒度，根据需要划分为不同的按照实体硬件对应的应用资源池：比如测试资源池、冗余资源池、生产资源池等，同时为了满足桌面虚拟化平台建设的要求，也可以划分出部分资源作为虚拟桌面所需资源，即桌面虚拟化资源池。对不同区域的实体硬件部署纳入不同资源池，并可以分列管理，各自横向扩充。

6.2.2 存储资源虚拟化和统一存储服务

统一存储服务是云计算中心的全局服务，通过统一存储服务，云计算中心对其应用服务系统的数据存储进行资源整合、数据结构梳理、数据合理化存储使数据在存储综合后进行存储管理、权限管理、事件管理、容量管理、策略管理等功能。

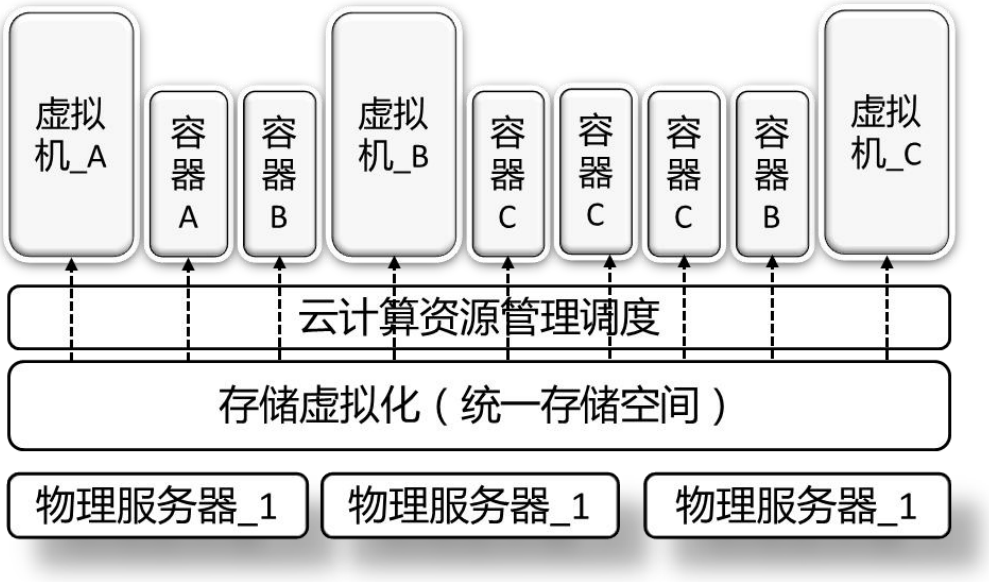

图 7　云平台统一存储服务

统一存储服务采用分布式并行存储系统，采用全冗余设计，支持多副本、N+M 纠删码等数据保护技术，支持单一存储命名空间、支持容量海量扩展，性能线性扩展，能够满足高性能计算中心海量文件并发读写需求。统一存储服务可提供 NFS，FTP，S3，HDFS 等开放标准的接口，可以直接与各类应用系统直接挂载使用。云计算平台系统中的视频图像综合运用管理平台、视频图像侦控作战平台、情报实战研判平台、执法办案信息管理平台、合成行动指挥作战平台、运行维护管理平台、警务综合系统、PGIS 系统、部门间信息共享平台、综合情报平台、执法办案信息管理平台等各种应用所需的图片、视频、纯文本文档、电子表格、PDF 文件、PPT 等各种资料文件都可以通过标准接口直接存储到统一云存储系统中。

6.2.3 网络虚拟化服务

云平台的网络服务可以为不同的用户或者节点创建隔离的网络环境，在隔离的网络环境下，用户或者节点集群可以独立使用私有网络。同时，通过网络服务也可以创建共享的网络环境，此时不同的节点集群和用户可以共享系统的网络。

云平台的网络服务功能可支持 Host 模式、Bridge 模式和 None 模式。用户可以根据业务需求，选择合适的网络模式。

- Bridge 模式

Bridge 模式可以为虚拟机或者容器提供独立的网络，保证各个容器中的进程服务的网络环境相互不受影响。同时，通过宿主机上的虚拟网桥来联通虚拟机或容器与宿主机的网络，实现虚拟机或容器与宿主机以及外部网络的通信。

- Host 模式

Host 模式下，虚拟机或者容器可以与宿主机共享一个网络命名空间，可以直接使用宿主机的物理网卡，和外部进行通信。宿主机上，Host 模式和 Bridge 模式可以共存，而并不会冲突。

- None 模式

None 模式下的容器，默认不会创建任何的网络环境。在没有网络配置的情况下，可以根据业务平台的需要，为虚拟机或者容器提供更多的网络定制策略，在虚拟机或者容器任务启动的过程中，动态配置所需的网络环境。

6.2.4 资源监控和集群服务

资源监控是对云平台系统内所有设备节点、虚拟机运行信息包括 CPU，内存，以及网络信息的监控服务。节点监控服务提供了跨平台的系统信息收集的 API，可以监控包括 windows 系列、linux 系列系统的运行信息。

分布式集群服务主要提供集群的监控和管理调度服务。通过在云平台上对设备以及虚拟机进行集群分域，实现集群的管理。分布式集群服务可监控集群内各个节点的状态，并响应系统对集群节点的调度管理。

通过监控服务和分布式集群服务，云计算管理平台可以收集各种节点的工作状态，为分布式集群服务以及资源调度服务提供决策信息，决定集群和资源调度的策略，结合分布式调度与集群负载均衡技术，保证云平台的资源高效使用，保证业务系统运行的可靠性与服务水平的一致性。

6.3 云计算平台管理

云计算平台管理提供涉及设备、计算、网络与存储所需的各类资源、业务框架、用户权限、系统监控和运维等各类管理服务，为各类应用在云服务平台内发布、应用运行、系统维护提供所需的技术环境与流程化管理人机操作界面，实现设备管理、资源管理、用户管理、运行维护管理等功能。云计算中心内的计算资源主要有虚拟化资源池、容器以及由实体物理服务器构建的技术环境构成。统一由云管理平台进行资源的管理与分配。

云管理系统是云管理平台的基础核心系统，采用多中心的扁平化部署模式，提供

统一的分布式服务系统。分布式服务系统上层面向所有的云服务，下层面向基础设施架构，提供一个具备分布式部署模式的消息交互、具备资源监控与调度能力的系统。应用服务的部署与发布统一由分布式调度服务进行调度，服务所需的资源由基础设施资源调度服务对服务集群进行调度。云计算管理单元可以对基础设施设备硬件资源进行虚拟化的管理，可通过虚拟机或者轻量级的容器技术实现硬件资源的统一管理以及快速的业务部署和应用，为整个云计算平台提供大容量、可灵活获取并可便捷扩展的计算资源，存储资源以及网络资源，支撑上层的各类业务服务系统和业务软件模块的部署。具体功能要求如下：

6.3.1 设备管理

支持对物理设备以及虚拟设备的监控管理服务，包括设备的状态监控、设置、迁移和服务监控等全面的管理能力。虚拟平台支持节点服务器的故障检测与迁移机制。在服务器发生物理故障或者网络异常时，云平台管理集群可以检测节点的服务异常，将失效服务器上的虚拟机或者容器迁移至其他可用服务节点，实现业务服务的高可用。

6.3.2 资源管理

云计算管理单元支持虚拟资源管理，能对虚拟资源进行配额管理，虚拟资源的使用率查询与监控告警，以及基于业务对虚拟资源使用率的情况。提供智能 HDD/SSD 混合存储，极致 I/O 性能，数据安全可靠。实现计算资源与存储资源的横向扩展功能，支持动态添加和删除数据节点，数据节点能够支持上千个。

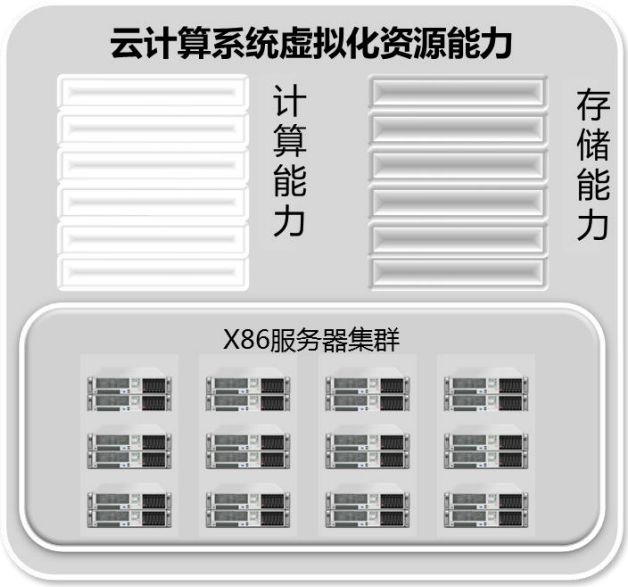

图 8　计算和存储能力横向扩展

6.3.3 网络管理

云计算管理单元网络管理能提供网络创建和物理和虚拟网络配置管理等功能。通过与物理、虚拟网络的配合管理，支持基于数据中心全网的网络设备管理、拓扑管理能力，提高网络设备带宽利用率。系统提供基于 WEB 的集中运维软件，可以实现对虚拟机以及容器集中监控和管理，同时提供告警能力。

6.3.4 镜像管理

云计算管理单元能提供完善的虚拟机镜像管理，包括镜像的存储方式，镜像的格式管理等。

6.3.5 用户管理

部署的云计算管理单元能提供系统管理员、业务管理员等多种用户角色。系统管理员负责整个云平台的管理，并对租户实现按需求的资源配额分配以及对租户的权限和角色管理。

6.3.6 资源调度管理

提供完善的虚拟机以及 Docker 容器调度方法，支持基于 CPU、内存、磁盘需求以及相同主机、不同主机的调度，满足业务部署的灵活性。实现服务 HA 功能，自动迁移故障服务，快速恢复服务，实现计算资源和存储资源的负载均衡。

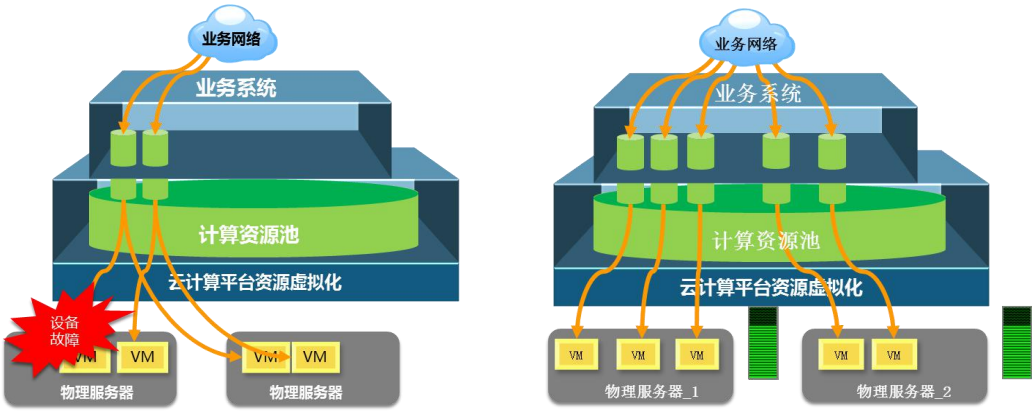

图 9　云平台容错和业务均衡

6.3.7 动态扩展

支持大规模设备管理，支持数百台的物理服务器规模的虚拟机的管理和调度。支持物理服务器动态扩容，系统性能呈线性增长。

6.3.8 界面应用

云计算管理单元提供图形化的管理操作界面，管理人员能基于图形化简易的操作，进行物理资源的查询，物理设备的状态监控，虚拟机/容器的创建和状态查询与监控等。

同时，可以基于图形化的管理平台，进行虚拟机/容器以及框架的配置、资源的管理、基于业务的部署配置等。

6.3.9 开放服务接口

云计算管理单元提供完善的服务接口，支持通过 REST 接口的方式开放给上层应用。用户可以灵活的基于开放的服务接口开发业务的管理应用。

7、数据标准

依据应急管理部消防救援局《消防智能接处警系统数据标准》执行。

8、接口标准

依据应急管理部消防救援局《消防智能接处警系统接口标准》执行。

9、警情地图要求

警情地图服务使用应急管理部消防救援局统一部署的消防“一张图”地图相关数据及服务。

10、利旧要求

保留原有正常使用的服务器加入资源池，提高计算和存储资源；原有的 G450 网关继续利旧，作为主要话务交换手段使用，其他手段作为辅助或备用。具体利旧清单如下：

序号	应用类型	数量	品牌型号	利旧要求	购置时间	使用时间	使用情况
1	服务器	1	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常
2	服务器	2	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常
3	服务器	1	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常
4	服务器	1	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常
5	服务器	1	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常
6	服务器	1	HP DL388e-G7	加入资源池	2012 年 6 月	8 年	正常

序号	应用类型	数量	品牌型号	利旧要求	购置时间	使用时间	使用情况
7	服务器	1	HP DL580-G7	加入资源池	2012年6月	8年	正常
8	服务器	1	HP DL580-G7	加入资源池	2012年6月	8年	正常
9	G450网关	1	MB450	语音网关	2012年6月	8年	正常

11、系统迁移要求

11.1 新旧系统切换

新旧系统切换采用并行运行，无缝切换的模式。新系统部署完成后，先由试点区域人员进行试用，对系统进行熟悉，并提出试运行建议，然后再全面推行。在完全切换之前，新系统进行试行、试用，测试数据可以进行保留，在完全切换之后，用户全部使用新系统，并对旧系统进行数据迁移。

11.1.1 切换时间

新旧系统双轨运行期为2个月；

新旧系统切换时间为3天，安排在节假日或周末进行切换。

11.1.2 切换要求

新系统在试运行过程中满足试行区域的工作要求，并针对试运行提出的意见进行修改，满足新系统全面试运行的条件。

11.1.3 切换计划

序号	阶段	时间	主要工作
1	旧系统数据采集阶段	两周	完成旧系统数据的收集，包括部门、人员、部件、分类等数据
2	新系统部署阶段	两个月	完成新系统的部署工作，录入旧系统的数据和新采集的数据
3	新旧系统切	一个月	对旧系统中的数据和接口对接进行系统

	换测试阶段		联调，进行功能测试
4	新系统培训阶段	两周	对试运行区域人员进行新系统培训
5	新系统区域试行阶段	一个月	在试运行区域对系统进行试运行，针对试运行问题进行调整和优化
6	正式切换到新系统	3 天	正式切换到新系统，旧系统不在使用

图表 1　新旧系统切换计划

11.1.4 详细步骤

11.1.4.1 旧系统数据采集阶段

完成旧系统数据的收集，包括部门、人员、案件、分类等数据。

11.1.4.2 新系统数据导入阶段

完成新系统的部署和数据导入工作，录入旧系统的数据和新采集的数据，将部门、人员、部件、分类等数据录入到新系统，并根据用户最新的管理要求和考核要求，对数据进行调整。

11.1.4.3 新旧系统切换测试阶段

对旧系统中的数据和接口对接进行系统联调，进行功能测试。

主要测试内容包括运行环境的测试、服务器压力测试、网络环境测试、第三方历史对接接口测试等。

11.1.4.4 新系统培训阶段

针对试运行提出的问题，对系统调整优化完成后，全面面向所有人员进行新系统培训，培训人员包括指挥中心接警员、调度员、网络管理员、职能部门等。培训内容包括新系统的功能、新系统如何操作、新旧系统切换注意事项等。

11.1.4.5 新系统试行阶段

在试运行区域对系统进行试运行，针对试运行问题进行调整和优化。

11.1.4.5.1 非试运行区域

旧系统仍旧正常运行。针对非试运行区域，仍旧使用旧系统。

11.1.4.5.2 试运行区域

同时并行使用新系统和旧系统。对试运行区域人员进行培训，试用新系统。

11.1.4.6 正式切换到新系统

正式切换到新系统，旧系统不录入新数据，保留旧系统的正常运行一个月时间，在此期间，能够进入旧系统查看历史案件信息和统计历史数据，同时对历史数据进行数据迁移。

12、运维要求

12.1 运行管理单位

项目建成后质保期内由承建单位全面负责系统的运行、维护。建设单位负责监督、组织和工作协调。

12.2 运维管理规范

建设单位成立运行维护组织机构，在工作领导小组的领导下，将全面负责系统的运维指导、监督和组织管理。

12.3 运维服务内容

12.3.1 网络系统的运行和维护

本项目不涉及此项。

12.3.2 服务器、存储设备及机房的运行维护

数据库由系统管理员负责，集中管理。管理员口令专人负责，在最小的范围内使用，记录存档，口令定期修改。超级管理员口令原则上只允许在服务器上使用。

数据库设置不同的用户和用户组，每个用户组要设置数据库各用户表的访问权限。用户通过账号和密码登录系统，操作均在数据库中保留有日志。数据库中要设置使用角色，限制个用户的使用权限。

对重要保密数据进行加密处理后在存储，对存储在磁性介质或其他介质的文件和

数据，系统必须提供相关的保护措施。

定期备份数据库、数据看日志，数据备份可以用磁带或硬盘和光盘等介质备份。备份文件应异地存放，保证数据的安全性。

服务器的网络操作系统应能满足海口救援队的业务要求和用户数要求。

建立数据质量控制的管理机制，确定质量管理的专门负责人。

根据系统的功能要求，检查核对软件系统工作流程和数据结构以及数据流程，特别是检查数据的更新和存盘操作流程。

对数据的更新进行核对，定期检查数据的完整性，重点测试应用系统中可能出现的各种故障，发现问题及时更正，并对系统的容错方式提出解决方案，确保的数据的一致性。

系统在经过一定时间的运行之后，如果需要更新程序和更改数据存盘流程，则必须经过严格测试，跟踪存储的数据，直到确保数据的准确和完整。

服务器硬件至少每年保养维护一次，清理硬盘数据（包括文件系统和数据库系统），清理灰尘，检查电源系统，ups 系统以及其他附属设备（如空调系统、接地防雷系统、绝缘系统）。

12.3.3 系统的升级与扩展

结合海口市消防救援支队的实际，不断升级和扩展业务模块，使系统更加完善和实用。

根据实用性的原则和海口救援支队实际情况，升级与扩展海口救援支队系统和硬件设施。

确保系统在升级和扩展中对历史数据的向下兼容，建立完整的数据迁移方案，在通过审核和测试的前提下进行。

13、其他要求：

1、交付时间：合同签订生效之日起 90 天内。

2、交付地点：用户指定地点。

3、产品质保期为 2 年，产品质量保证期内，所有设备维修服务均为上门服务，由此产生的费用均不再收取。如出现非人为及不可抗力因素(如雷击等)造成的质量问题，乙方不负责免费维修。

4、质保期内提供全天候上门保修，免费更换全部配件；提供 7×24 小时技术支持和

服务；遇系统故障必须 1 小时内解决问题，恢复系统工作。

5、在质保期内，承建商必须免费对业主单位在系统运行过程中所出现的各种软件、硬件问题及时跟进、解决，不断完善、优化本系统；

6、每月进行一次系统全面巡检；重大安保任务、重大节假日前必须进行全面巡检，确保系统安全运行。

7、对供应设备的安装调试、操作运行、使用、维护、故障排除和修理、结构原理、数据处理系统、软件使用等方面提供培训，提供相应培训资料，并承担因此产生的费用。

8、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。