融讯光通
RONG XUN GUANG TONG

视频云融合调度（指挥）系统建设（能源电力）

北京融讯光通科技有限公司

2023 年 12 月

目 录

一、建设目标

随着能源系统的数字化智能化进程的不断推进，对数据元素的利用越来越充分，各类制约能源数字化智能化发展的关键技术也在取得突破。因此，企业需要一个可以实现大数据的统一接入、数据的安全保密、各类信号的实时传输的视频云指挥调度系统。建设视频云指挥调度系统一套，将各单位现有的视频系统进行融合升级和智能化改造，整合现有各类视频监控、视频会议、视频指挥、单兵图传、卫星图传、无人机图像等各类视频资源，形成“应接尽接”的分层分级分权的融合视频云资源。在视频云平台上实现视频监控实时展现、视频会议、指挥调度、指挥值班等日常指挥工作，实现“指挥到底”，达到“一键管全网”。同时视频云平台还可以实现态势感知、数据呈现、智能应用、辅助决策等指挥场景化可视化，达到“一图展全貌”的效果，让领导机关实时掌控各部门工作动态。

二、建设内容

在现有视频会议系统、值班视频系统的基础上，整合包括监控在内的现有各类视频资源，在全国范围内部署分布式计算集群的视频云系统，实现指挥覆盖“横向到边、纵向到底”。

包括：

- ✓ 实现视频资源全面接入，视频监控无死角，将下级所有监控系统纳入视频云平台；
- ✓ 实现指挥、会议随呼随通，随叫随到，精准高效，指挥顺畅；
- ✓ 实现作战值班、重要岗位视频智能查岗；
- ✓ 实现任务保障全域可视，各部门态势实时呈现，领导机关一目了然。

三、建设规模

1）总部级规模：建设覆盖总部、省、市、区县四级的视频云指挥系统，采用分布式部署模式，总部级系统要求能够具备监控所有下级单位值班室、重点岗位、重要目标的视频能力，具备召开视频会议的能力、具备视频指挥调度的能力，具备智能巡视的能力，具备全局可视化呈现的能力，总部级视频云系统要求具备较大接入容量，且能够进行双机备份。

2）省级规模：建设覆盖省、市、区县三级所有单位的视频云指挥系统，采用分布式部署模式，省级系统要求能够具备监控所有下级单位值班室、重点岗位、重要目标的视频能力，具备召开视频会议的能力，具备智能巡视的能力，省级视频云系统要求具备一定的接入容量。

3）市级规模：建设覆盖市、区县两级所有单位的视频云指挥系统，采用分布式部署模式，具备监控所有下级单位值班室、重点岗位、重要目标的视频能力，具备召开视频会议的能力，具备智能巡视的能力。

4）区县级规模：建设覆盖区县级的视频云接入系统，具备监控系统、会议系统、指挥系统、单兵图传、无人设备、智能设备的安全接入能力。

四、建设改造原则

1）首先需要在满足企业信息化安全规范的前提下部署视频云平台；

2）结合现有网络通讯情况，合理使用链路和网络资源，具备网络通讯自适应能力；

3）适当冗余设计，确保系统具备可靠性；

4）系统需具备按需扩展能力。立足现有，适当补充，系统可以随着指挥规模的变化灵活扩展；

5）平滑部署，改造期间不影响关联系统的正常使用。

五、组网说明

系统基于 IP 网络，按照地理结构和管理层级，采用分布式部署。

1. 总部级组网

总部级系统按照一级中心规模部署。包含：

1）部署视频云中心管理服务器 2 台，互为热备，实现对视频云平台的整体管理和控制；

2）部署视频云流媒体管理服务器 2 台，实现满足对所有视频信息资源进行汇集和转发与分流；

3）部署视频云高清多源解码器 2 台，用于将系统内的视频信息解码还原到中心的电视墙、视频矩阵或拼接控制器上；

4）部署 AI 边缘服务器 1 台，实现智能查岗、哨位和重点目标的分析、识别、可视化事态展示等 AI 应用；

5）部署视频云指挥终端 2 台，用于视频会议和视频指挥；

6）部署视频云核心安全网关 1 台，实现视频监控平台及视频会议核心平台的网络防攻击、操作终端视频防泄密等功能；

7）部署视频云显示安全网关 1 台，实现指挥大屏视频水印添加；

8）部署视频云安全可视化平台 1 台，用于全网安全信息采集、设备统一管理、安全态势可视化展示等；

9）部署会议摄像机 1 台，用于视频会议；

10)部署 2 套万兆多功能安全网关互为热备（含防火墙功能、入侵防御/检测功能、防病毒功能等）；

11)部署 2 套主动风险防御设备。

2. 省级组网

在省级单位按照二级中心规格部署。包含：

1）部署视频云中心管理服务器 1 台，实现对视频云系统的整体管理和控制；

2）部署视频云流媒体管理服务器 1 台，实现满足对所有视频信息资源进行汇集和转发与分流；

3）部署视频云高清多源解码器 1 台，用于将系统内的视频信息解码还原到中心的电视墙、视频矩阵或拼接控制器上；

4）部署 AI 边缘服务器 1 台，实现智能查岗、哨位和重点目标的分析、识别、可视化事态展示等 AI 应用；

5）部署视频云指挥终端 2 台，用于视频会议和视频指挥；

6）部署视频云核心安全网关 1 台，实现视频监控平台网络防攻击、操作终端视频防泄密等功能；

7）部署视频云显示安全网关 1 台，实现指挥大屏视频水印添加；

8）部署会议摄像机 1 台，用于视频会议；

9）部署 2 套万兆多功能安全网关互为热备（含防火墙功能、入侵防御/检测功能、防病毒功能等）。

10）部署 1 套主动风险防御设备。

3. 市级组网

在市级单位按照三级中心规模部署。包含：

1）部署视频云中心管理服务器 1 台，实现对视频云系统的整体管理和控制；

2）部署视频云流媒体管理服务器 1 台，实现满足对所有视频信息资源进行汇集和转发与分流；

3）部署视频云高清多源解码器 1 台，用于将系统内的视频信息解码还原到中心的电视墙、视频矩阵或拼接控制器上；

4）部署 AI 边缘服务器 1 台，实现智能查岗、哨位和重点目标的分析、识别、可视化事态展示等 AI 应用；

5）部署视频云指挥终端 2 台，用于视频会议和视频指挥；

6）部署会议摄像机 1 台，用于视频会议；

7）部署视频云核心安全网关 1 台，实现视频监控平台网络防攻击、操作终端视频防泄密等功能；

8）部署 2 套千兆多功能安全网关互为热备（含防火墙功能、入侵防御/检测功能、防病毒功能等）。

9）部署 1 套低配型主动风险防御设备。

4. 区县级组网

在区县级单位按照点位规模部署。包括：

1）部署视频云接入管理服务器 1 台，实现提供标准协议产品接入和转换服务，接入并转换为视频云指挥系统内部协议，将所有摄像头、信息接入终端、会议终端、指挥终端、单兵图传等视频源进行统一汇聚，接入视频云指挥系统平台，形成本地资源池；

2）部署视频云指挥终端 1 台，用于视频会议和视频指挥；

3）部署 AI BOX 终端 1 台，用于实现智能查岗、哨位和重点目标的分析、识别、可视化事态展示等 AI 应用；

4）部署视频云终端接入安全网关 1 套，实现前端资产盘点、攻击防护、传输加密、端口隔离等；

5）部署会议摄像机 1 台，用于视频会议；

6）部署千兆多功能安全网关 2 套互为热备（含防火墙功能、入侵防御/检测功能、防病毒功能等）；

7）部署低配型主动风险防御设备 1 套。

在整个系统中，总部级、省级、市级、区县级都可以独立组网和管控，也可以级联成为一个大型的视频云系统，统一进行资源接入、资源访问、统一权限的分权分级调度和控制，灵活且便于管理。

六、视频云指挥建设典型预算清单

1. 总部级规模及预算

编 号	设备名称	规格型号	数 量	单 位	单价（万元）	总额(万元)	备 注
1	视频云中心管理服务器	VCS-CM9100-C	2	套	15.2	30.4	License 数量≤10w
2	视频云流媒体管理服务器	VCS-SM8100	2	套	14.3	28.6	
3	视频云高清多源解码器	VCS-HM1212	2	套	12.15	24.3	
4	AI 边缘服务器	YM-AI3300	1	套	29.45	29.45	
5	视频云指挥终端	VCT-VC501	2	台	1.265	2.53	

6	视频云核心安全网关	SP-MC6100	1	套	53.45	53.45	支持 60 个会议室双流会议；支持 100 路高清 IPC（4M 码流带宽）
7	视频云显示安全网关	SP-SG16	1	套	21.6	21.6	视频显示通道 16 路
8	视频云安全可视化平台	SP-VP6050	1	套	71.96	71.96	支持 50 台安全网关管理授权
9	会议摄像机	CVC-FP725	1	台	0.678	0.678	
10	万兆多功能安全网关		2	套	18	36	万兆安全网关（高配 40G）
11	主动风险防御设备（高配）		2	套	39.8	79.6	
	小计		**19**			**378.57**	

2. 省级规模及预算

编 号	设备名称	规格型号	数 量	单 位	单价（万元）	总额(万元)	备 注
1	视频云中心管理服务器	VCS-CM9100	1	套	12.3	12.3	License 数量≤1w
2	视频云流媒体管理服务器	VCS-SM8100	1	套	14.3	14.3	
3	视频云高清多源解码器	VCS-HM1212	1	套	12.15	12.15	
4	AI 边缘服务器	YM-AI2000	1	套	29.45	29.45	
5	视频云指挥终端	VCT-VC501	1	台	1.265	1.265	
6	视频云核心安全网关	SP-MC4064	1	套	13	13	支持 64 路高清 IPC（4M 码流带宽）
7	视频云显示安全网关	SP-SG08	1	套	12.88	12.88	视频显示通道 8 路
8	会议摄像机	CVC-FP725	1	台	0.678	0.678	
9	万兆多功能安全网关		2	套	9.4	18.8	万兆安全网关（10G）
10	主动风险防御设备（高配）		1	套	39.8	39.8	
	小计		**12**			**154.62**	

3. 市级规模及预算

编 号	设备名称	规格型号	数 量	单 位	单价（万元）	总额(万元)	备注
1	视频云中心管理服务器	VCS-CM9100	1	套	12.3	12.3	License 数量＜1w
2	视频云流媒体管理服务器	VCS-SM8100	1	套	14.3	14.3	
3	视频云高清多源解码器	VCS-HM1212	1	套	12.15	12.15	
4	AI 边缘服务器	YM-AI2000	1	套	29.45	29.45	
5	视频云指挥终端	VCT-VC501	2	台	1.265	2.53	
6	视频云核心安全网关	SP-MC2032	1	套	8.25	8.25	支持 32 路高清 IPC（4M 码流带宽）
7	会议摄像机	CVC-FP725	1	台	0.678	0.678	
8	千兆多功能安全网关		2	套	1.8	3.6	
9	主动风险防御设备（低配）		1	套	25.8	25.8	
	小计		**12**			**109.06**	

4. 区县级规模及预算

编 号	设备名称	规格型号	数 量	单 位	单价（万元）	总额(万元)	备 注
1	视频云接入管理服务器	VCS-AM8200	1	套	8.15	8.15	
2	视频云指挥终端	VCT-VC501	1	台	1.265	1.265	
3	AI BOX 终端	YM-AI100	1	台	3.68	3.68	
4	视频云终端接入安全网关	SP-AG04	1	套	0.592	0.592	
5	会议摄像机	CVC-FP725	1	台	0.678	0.678	
6	千兆多功能安全网关		2	套	1.8	3.6	
7	主动风险防御设备（低配）		1	套	25.8	25.8	
	小计		**8**			**43.765**	

七、典型案例

博鳌论坛

解决前指指挥中心至总指挥中心，视频传输通道资源不足问题，系统通过前端接入设备，将前进指挥所、警卫现场、公安天网、动态勤务等视频资源接入云端，实现总中心及授权单位的视频资源实时共享。

上合峰会

解决了前指指挥中心至 ZD 指挥中心和总指挥中心，视频传输通道资源不足，各级调用不便的问题，系统通过前端接入设备，将现场指挥所、警卫现场、公安天网、动态勤务等视频接入云端，实现总部、ZD 及授权单位的实时共享和指挥调用。

中非论坛

解决了峰会多个分会场，不同种类、协议的视频和多媒体信息的统一接入、管理和多级调用的问题，实现了各类视频资源不需前端转发，ZD、ZB 便可各取所需的保障模式。

澳门回归 20 周年庆典

- 方案是用于移动情况下，向警卫人员之间以及和后方指挥中心之间提供应急通信服务的无线视频指挥系统
- 保障部门及保障系统众多，且密级各不相同，需要将各单位音视频单独引接汇入，统一调度。
- 舰船上部署便携式基站设备和卫星设备，通过无线自组网和卫星链路将各船视频传输至指挥中心。

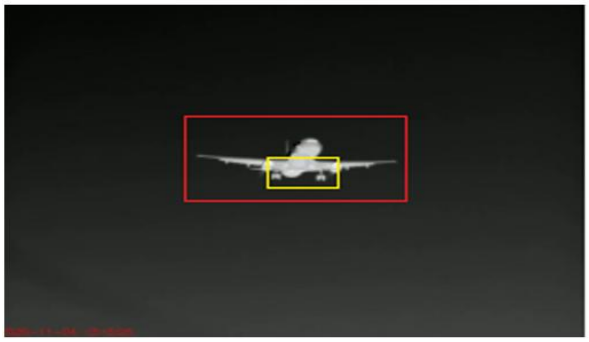
中国国际进口博览会

实现了视频指挥中心前移，跟随首长伴随保障的模式，通过 ZB 授权，ZD 可将周边各兄弟单位，空情海情，边境线，京、新、藏等重点地区各类视频资源的灵活调用，实现了首长走到哪，指挥中心跟到哪的目标。

2022 北京冬奥会

疫情防控下的 2022 北京冬奥会和冬残奥会，对人员进出要求严，保障难度大，对保障冬奥会的安全警卫工作提出了更高的要求，在场馆多且分散的情况下，采用场馆接入汇聚，ZD 实时指挥，ZB 统筹管理的模式，实现了冬奥警卫保障任务的圆满完成。

KJ 某机场 -飞机起降跟踪识别系统



以 YM- AI2300 高性能 AI 边缘主机为核心，构建高性能 AI 智能监控系统，简洁高效实现所需功能，赢得高度认可。

- 起降飞机自动检测 -对飞机进行自动检测、识别、跟踪和特写抓拍。
- 热成像视频探测和跟踪 -对飞机起飞、降落主动探测，识别并自动跟踪。
- 可见光视频跟踪 -系统将自动调整云台位置及摄像机焦距，确保飞机始终位于视场中心
- 起落架跟踪特征拍摄
- AI 智能学习-自动对飞机目标持续跟踪，并进行深度学习，自动识别飞机起落架。
- 历史数据回放

八、产品参数要求

1. 视频云中心管理服务器

1）软件架构：自主知识产权平台软件，具有高可靠性和稳定性，采用分布式设计，支持有中心或无中心部署，支持多级平台级联，支持双机热备。

2）设备管理：系统可以对前端设备和后端服务器设备执行添加、修改、删除操作，前端设

备在节点树中同一层级的先后顺序可调整。

3）用户管理：系统具有用户的添加、修改、删除以及临时禁用等功能。

4）权限管理：负责管理用户和设备的对应关系，可以针对每个用户授权同一设备的不同视频通道。

5）角色管理：负责管理角色的添加、修改、删除，可以自定义角色模板，并将之授权于用户。

6）时钟同步：中心可以实现对平台内所有服务器、所有前端采集设备、所有客户端进行统一校时。

7）别名管理：支持设备的别名管理，即设备注册到系统采用一种命名体系（比如编码），设备在客户端显示的名字则采用另一种命名体系（比如易于理解的地点、名称等）。

8）多网段地址映射：支持跨网段路由映射，根据来访用户的 IP 地址，自动将用户导向正确的网络地址。

9）客户端分辨率自适应：根据屏幕分辨率大小（1024*768 及以上分辨率），客户端界面支持自适应全屏显示模式。

10）网络传输时延控制：单向延迟低于 200ms（网络传输本身延迟不包括在内）。

11）网络传输差错控制：具备差错检测、错误隔离、限制延迟重发、强制恢复等一系列差错控制技术。

12）双向视频/视频会议：系统具有管理前端视频云指挥型终端双向点对点视音频通信；支持在多个指挥型终端间进行视频广播和组播的功能，主席可以禁言分会场；支持广播分会场的功能，可选择主席/分会场画中画模式，也可选择主席/分会场全屏模式。

13）网络带宽自适应：采用自适应算法可以实时检测网络带宽的拥塞程度，并可以动态对编码设备进行码流整形，调整输出码率以匹配网络带宽。

14）系统容错：分布式系统能够自动地通过自身的调度和协调，定位错误并通过任务迁移将原有任务从故障系统中迁移至正常系统中，从而达到容错的目的，避免系统因为某台设备出现故障而导致整个系统宕机的情况。

15）负载均衡：通过任务调度算法，保证了 CPU、网络、内存等重要计算资源在多机系统中的合理均衡的分配，从而使得系统整体性能达到最优。

16）★为指挥终端提供视频会议支撑；

17）★提供原厂盖章的售后服务承诺函。

2.视频云流媒体管理服务器

1）软件架构：自主知识产权平台软件，具有高可靠性和稳定性，采用分布式设计，支持多级级联，支持设备堆叠。

2）视频转/并发：支持 D1/720P/1080P/2K 各种分辨率的视频数据的转/并发与分发，单个媒体流≤8Mbps，单机最大支持 600Mbps 的流媒体转/并发（100 路 720P 4Mbps 或者 70 路 1080P 8Mbps 流媒体转/并发）；支持 RTP/RTSP、SIP、VAS2、ONVIF、GB-28181 等国际国内标准协议。

3）时延控制：单向延迟低于 200ms（网络传输本身延迟不包括在内）。

4）差错控制：具备差错检测、错误隔离、限制延迟重发、强制恢复等一系列差错控制技术。

5）带宽自适应：采用自适应算法可以实时检测网络带宽的拥塞程度，并可以动态对编码设备进行码流整形，调整输出码率以匹配网络带宽。

6）★提供原厂盖章的售后服务承诺函。

3.视频云接入管理服务器

1）软件架构：自主知识产权平台软件，具有高可靠性和稳定性，采用分布式设计，支持多级级联，支持设备堆叠。

2）多元融合接入：支持主流 IPC、视频编码设备、指挥终端、单兵终端和会议终端的接入，支持 RTP/RTSP、SIP、VAS2、ONVIF、GB-28181 等国际国内标准协议，单机支持≥100 路视频接入。

3）视频压缩：支持≥4 路视频码流超压缩，码流压缩倍率≥90%。

4）时延控制：单向延迟低于 200ms（网络传输本身延迟不包括在内）。

5）差错控制：具备差错检测、错误隔离、限制延迟重发、强制恢复等一系列差错控制技术。

6）带宽自适应：采用自适应算法可以实时检测网络带宽的拥塞程度，并可以动态对编码设备进行码流整形，调整输出码率以匹配网络带宽。

7）★与视频云中心管理服务器和视频云流媒体管理服务器同一品牌，支持视频云中心管理系统统一管理；

8）★提供原厂盖章的售后服务承诺函。

4.视频云高清多源解码器

1）软件架构：自主知识产权平台软件，具有高可靠性和稳定性，支持系统级联和设备堆叠。

2）视频切换：分为自动和手动切换两种方法，自动切换是通过预案实现的；手动切换视频可以通过拖拽方式进行，使信号源的视频显示在选择的显示窗口中。

3）视频分割：支持 12 通道单画面高清 1080P 输出、12 通道四画面 D1/4CIF 输出等多画面切换显示。

4)视频解码输出：支持同时解码主流设备厂前端设备，以及指挥型终端的视频，并支持扩展解码能力；单台设备支持最大 12 个 HDMI 的视频输出接口，最多同时解码输出 12 路最高分辨率为 1920×1080 的视频。

5)预案调用：用户选择预定义的轮巡预案，并可以启动或停止该预案。这样用户不需要手动进行视频切换，而由解码器自动负责在预定的时间内自动切换视频，达到自动轮巡的目的。

6)字幕叠加：可以自动接收视频源信息并以字幕台标方式叠加显示在解码画面上，并支持字幕的隐藏或显示操作。

7)★支持将视频云系统内网络数字信号解码为 12 路 HDMI 信号；

8)★与视频云中心管理服务器和视频云流媒体管理服务器同一品牌，支持视频云中心管理系统统一管理；

9)★提供原厂盖章的售后服务承诺函。

5.AI 边缘服务器

1）自主研发的硬件加速技术：芯片级硬件加速 ，自主知识产权 ，自主可控

2）国产化软硬件系统

3）定制 AI 算法：自有平台硬件加速技术，提供高性价比的解决方案。

4）CPU：飞腾 D2000，8 核

5）人工智能加速卡：寒武纪 270/370　INT8/TOPS：128T/

6）FPGA 加速卡：复旦微电子 690T

7）PCIE 扩展：板载 4 个 PCIE3.0x16 插槽、板载 1 个 M.2 2280 插槽、网口板载 2 个千兆以太网口

8）操作系统：银河麒麟 V10 桌面版

6.AI BOX 终端

1）自主研发的硬件加速技术：芯片级硬件加速，自主知识产权 ，国产化软硬件系统自主可控。

2）定制 AI 算法：自有平台硬件加速技术，提供高性价比的解决方案。

3）CPU： 8 核 A53@2.3GHz

4）计算能力：INT8:峰值算力 17TOPS；FP32:峰值算力 2.2TFLOPS

5）视频/图片编解码：视频解码：960fps 1080p（38 路 1080P@25FPS）、50fps 1080p（2 路 1080P@25FPS）；图片编解码：480 张/秒 1080P

6）内存与存储：内存：12GB；eMMC：32GB

7)外部接口：网口： 100/1000Mbps 自适应 *2；USB：USB3.1 *2；存储卡：MicroSD *1；显示：HDMI *1；凤凰端子：RS-232 *1 / RS-485 *1 /自定义 I/O

7.视频云指挥终端

1）视音频信号双向传输：支持 1 路 HDMI 接口视频信号编码输入、支持 1 路 HDMI 接口解码网络视频信号输出、支持 1 路 RCA 音频接口输入（双声道）、支持 1 路 RCA 音频接口输出（双声道）、支持会议功能、双通功能、脱网直通功能。

2）视频编码/分辨率：支持 H.264/ H.265，AVS2 编码；分辨率支持 1920*1080/1280*720；码流控制 32Kbps～8192Kbps，最大可自定义 8Mbps。

3）视频帧率控制：1/16 帧/秒~全帧率（全帧率包含 25/30/50/60 帧，视输入信号而定）。

4）自动视音频检测：系统自动识别是否有视频信号输入,设备上有相应指示灯指示；系统自动识别是否有音频信号输入，自动识别输入音频的信号大小，分 7 个级别显示音频强度。

5）字幕叠加：在解码端可以自动接收视频源信息并以字幕台标方式叠加显示在解码画面上，并支持字幕的隐藏或显示操作。

6）★支持视频云中心管理系统统一管理；

7）★提供原厂盖章的售后服务承诺函。

8.视频云超压接入终端

1）视频处理能力：4 路网络视频流输入，4 路压缩视频流输出，码流压倍率≥80%。

2）视频格式：H.264、H.265，分辨率支持 1920*1080/1280*720；

3）网络接口：1 个 100M/1000M 自适应以太网口，支持 3G、4G、5G 移动网络(可选配)

4）网络协议：HTTP，TCP/IP，UDP，DNS，SNTP，DHCP，FTP，SNMP,NTP，UPNP（可选）

5）存储拓展：支持 SD 卡存储，SD3.0 标准，最大支持 128G 卡（可选配）

6）★提供原厂盖章的售后服务承诺函。

9.视频云核心安全网关

1）前端摄像头准入控制：

- 基于 IP 地址、MAC 地址、应用协议、生产厂商、设备指纹等准入控制方式；
- 支持跨三层网络前端设备 MAC 地址识别与准入控制；
- 支持手工添加和批量导入准入规则，可根据用户需求灵活配置准入方案；
- 支持自动识别非法私接入侵、摄像机仿冒/替换攻击行为的检测与防护；

2）黑白名单控制：

- 支持黑名单和白名单流量过滤控制，支持 IP 地址、端口等多种防护方式；
- 支持策略联动，实现与接入安全网关或汇聚安全网关联动完成攻击源阻断；

3）终端设备准入控制：

- 支持终端身份认证体系，禁止黑客和非法用户接入视频监控系统；
- 支持对操作席终端用户进行安全权限管理，可以对视频监控数据的导出、下载、解密、外发操作进行安全控制；

4）录像/抓图导出防泄密：

- 录像/抓图数据导出时自动加密保护，对导出视频图像操作自动记录日志；
- 只有在授权的操作席终端上才可以正常使用，一旦带离授权环境则完全无法使用；

5）截屏/录屏防泄密：

- 禁止对操作席终端监控画面进行截屏和录屏操作；
- 可防各种截屏/录屏软件；
- 对截屏/录屏操作自动记录日志，对非法操作用户进行实时告警；

6）视频数据外发防泄密：

- 获得授权后操作席终端用户方可将视频数据制作成外发文件；
- 可对外发文件设置访问权限、时限和次数，并具备自动删除功能；
- 外发视频数据无需接收方预先安装专用软件，即可在时效和权限许可范围内使用；

7）拍摄屏幕防泄密：

- 支持显性水印、动态二维码水印，包含用户信息和设备信息，可威慑拍屏者并用于事后追溯；
- 支持隐性水印，包含用户信息，用于事后追溯；
- 支持屏幕全屏水印和监控画面水印；
- 支持下载视频/图片内嵌视频水印；

8）设备发现与识别：

- 支持全量网络流量监测、主动探测扫描等多种方式，准确发现网内前端设备；
- 支持多种设备识别检测技术，支持 IPC、NVR、监控系统、PC、网络设备等多种设备的检测；
- 支持厂商类型特征库，可识别海康、大华、宇视、科达等主流厂商，支持厂商自定义扩展；

- 支持在线前端设备信息检测功能，能实时监测前端设备的 IP 地址、MAC 地址、上线时间、厂商信息等；

9）安全检测：

- 支持前端设备弱口令检测功能，快速发现前端设备弱口令漏洞，密码字典支持在线编辑、加载更新；
- 支持多种违规外联检测技术，可自动检测操作终端同时连接内部网络和外部网络的违规行为；

10）资产管理：

- 支持资产列表，支持前端设备资产管理，自动获取前端设备指纹信息；
- 支持显示设备 IP 地址、设备类型、设备状态、添加时间、上级 IP 地址、单位名称、地理位置等信息。
- 支持视频资产批量导出/导入管理；
- 支持终端安全管理，实时显示安全防护终端信息统计；

11）运维管理：

- 支持链路质量检测，支持丢包率、时延等多维度检测，支持链路质量等级自定义；
- 支持 IP 地址资源热力图，支持按部门、地址段进行添加，支持批量导入导出，可实时显示 IP 地址的在线、离线、未使用等状态；
- 支持网络拓扑编辑模式，支持自动拓扑发现和绘制、拖拽方式完成拓扑连接；
- 支持软件升级、版本回退功能，支持对汇聚安全网关、接入安全网关、共享安全网关等进行软件升级操作；

12）网络攻击防护：

- 支持多种 DDoS 攻击、Flood 攻击、端口扫描等网络攻击防护方式；
- 支持攻击检测阈值设置，支持阻断和仅告警设置；
- 支持 FTP、TELNET 等多种应用协议识别防护方式；

- 支持基于五元组的网络访问控制功能；

13）传输加密防护：

- 支持与接入安全网关或汇聚安全网关联动实现传输加密防护；
- 支持国密 SM4 密码算法对视频信令报文、媒体流进行传输加解密；
- 支持视频数据加密传输功能，保证数据传输机密性；

14）系统管理：

- 内置安全管理模块，支持网络配置管理、用户管理、策略管理、终端管理、审批管理、日志管理和告警；
- 支持 NTP 时间管理功能，实现设备时间实时同步；
- 支持安全日志管理，支持系统日志、操作日志、终端日志、告警日志等，支持告警信息聚合、告警手工处置确认、批量处置确认；

15）统一管理：

- 支持接入安全网关、汇聚安全网关、显示安全网关、边界安全网关等统一管理；
- 支持网关信息、资产信息、日志告警信息采集汇总，集中展示所管理安全网关的在离线状态、上线时间等信息；
- 支持产品运行安全数据可视化，支持资产、安全事件、网络流量、链路时延、IP 使用率、告警等多种信息统计；

16）安全便捷的权限管理：

- 每个用户均可设置不同权限；
- 支持网络、客户端指定授权；

17）产品部署方式：

- 支持主路部署、旁路引流部署、端口镜像等部署方式；
- 支持级联部署；

◆ 支持 VLAN 场景部署。

18）★提供原厂盖章的售后服务承诺函。

10.视频云显示安全网关

1）水印功能：

◆ 支持显性水印，包含用户信息、时间信息和警示信息，可威慑拍屏者并用于事后追溯；

◆ 支持隐性水印，包含用户信息和时间信息，用于事后追溯；

2）分屏/全屏显示：

◆ 支持拼接屏幕防拍屏，支持分屏水印；

◆ 支持全屏幕防拍屏，支持整屏水印；

3）安全便捷的管理：

◆ 支持 GUI 人机交互界面控制，操作更便捷；

◆ 支持统一网管；

4）水印设置：

◆ 支持水印开关设置

◆ 支持水印位置设置，支持透明度设置，支持文本颜色设置；

◆ 支持水印字体样式、字体大小设置；

◆ 具有断电信息保存功能。

5）支持接口类型：VGA，HDMI，CVBS，YPbPr，DVI ；

6）冗余双电源。

7）★提供原厂盖章的售后服务承诺函。

11.视频云安全可视化平台

1）大屏展示：

- 支持安全态势总览，支持各类指标概览，支持按区域进行统计排行，支持区域地图展示。
- 支持查看告警统计、区域实时告警、告警分类、威胁趋势、资产数量、资产在线率、分区域 IPC 在线率、安全终端在线率。

2）设备管理：

- 支持设备的详细信息的展示，可查看设备的名称、IP 地址、MAC 地址、设备类型、设备状态、所属区域等信息。
- 支持设备信息的查询检索，可根据所属区域、设备类型、设备状态、IP 地址等属性信息进行组合查询，并以列表形式返回查询结果，可查看单个设备的详细信息。

3）资产管理：

- 支持资产信息上报，并以列表形式展示资产信息，包含资产的名称、IP 地址、MAC 地址、资产类型、资产状态、所属区域等信息。
- 支持资产的查询检索，可根据所属区域、设备类型、设备状态、IP 地址等属性信息进行组合查询，并以列表形式返回查询结果，可查看单个资产的详细信息。

4）设备拓扑：

- 支持网络拓扑状态展示，能够对网络拓扑进行移动、缩放、恢复居中展示。
- 支持网络拓扑编辑模式，可自定义拓扑结构，通过拖拽和点击的方式完成拓扑节点的添加、删除、连线、位置调整操作，可对调整后的拓扑进行保存。

5）离线 GIS 展示：

- 支持离线 GIS 地图显示，可按区域查看资产位置信息。
- 支持通过鼠标悬浮实时显示区域下的设备资产数量统计信息。

6）用户权限管理：

◆ 支持用户权限管理，支持包括系统管理员、策略管理员与日志管理员，分别对应系统管理、策略配置与日志检查。

7）告警日志：

◆ 支持全网设备告警日志、客户端日志采集，可按区域展示告警日志和客户端日志。
◆ 支持客户端日志审计功能，可对用户的截图、录屏、文件外发/还原等操作日志进行记录和查询。

8）区域管理：

◆ 支持按客户组织机构配置区域，并按区域进行管理。

9）★提供原厂盖章的售后服务承诺函。

12.视频云终端接入安全网关

1）前端摄像头准入控制：

◆ 基于 IP 地址、MAC 地址等准入控制方式；
◆ 支持手工添加和批量导入准入规则，可根据用户需求灵活配置准入方案；

2）黑白名单：

◆ 支持黑名单和白名单流量过滤控制，支持 IP 地址、端口等多种防护方式；
◆ 支持策略联动，实现与视频会议核心安全网关联动完成攻击源阻断；

3）网络攻击防护：

◆ 支持多种 DDoS 攻击、Flood 攻击、端口扫描等网络攻击防护方式；
◆ 支持攻击检测阈值设置，支持阻断和仅告警设置；
◆ 支持 FTP、TELNET 等多种应用协议识别防护方式；

4）端口隔离防护：

◆ 支持横向端口隔离功能，防止东西向摄像头跳板攻击；

5）传输加密防护：

◆ 支持与视频会议核心安全网关联动实现传输加密防护；
◆ 支持视频数据加密传输功能，保证数据传输机密性；

6）统一管理：

◆ 支持视频会议核心安全网关给前端监控点的视频会议接入安全网关进行配置策略下发；
◆ 支持视频会议接入安全网关将网关信息、资产信息、日志告警信息上报给视频会议核心安全网关，并有视频会议核心安全网关集中展示；
◆ 支持软件升级、版本回退功能，支持视频会议核心安全网关对视频会议接入安全网关进行软件升级操作；

7）4 路高清视频会议终端接入；5 个千兆电口；

8）★提供原厂盖章的售后服务承诺函。

13.会议摄像机

1）214 万像素 1/2.8 英寸 CMOS 传感器；

2）支持 H.265、H.264 网络视频编码；

3）支持全高清 1080P60 视频输出；

4）支持 3G-SDI、HDMI 高清视频输出；

5）12 倍光学变焦，最大广角 72.5°；

6）支持双码流，支持多级别视频质量配置；

7）支持 1 路音频输入和 1 路音频输出；

8）支持最大 64G TF 卡本地存储；

9）精密传动系统，定位精确，运行平稳；

10）支持多种协议及多种控制接口，支持菊花链组网；

11）配备多功能 IR 遥控器；

12）内置中英文操作菜单；

13）智能曝光有效解决投影、电视等设备对拍摄人物的影响；

14）支持桌面安装、壁挂安装和吸顶安装 3 种安装方式。

14.智能防火墙

1）安全防护：支持 4 种安全防护模式，基于网络、用户、应用；支持内嵌深度包检测引擎，针对数据包进行深度过滤检测；支持对穿透防火墙的 FTP 服务进行过滤审计；支持通过预定义过滤文件名实现对 FTP 数据流的区分控制；支持对 vpn 隧道内的内容检查和防护。

2）统一特征库：web 页面下统一对设备支持的特征库进行查看、更新及自定义操作；支持针对 webmail、应用特征库可以根据客户需求实现定制。

3）IPv6 支持：支持基于 IPv6 下的路由，包括：直连路由、静态路由、动态路由（OSPF、BGP 等）等；支持基于 IPv6 下的 IP 地址/地址组的包过滤、内容过滤、IPS 检测、流量控制以及关联时间控制等。

4）VPN：支持 PPTP、GRE、IPSEC 等 VPN；支持隧道热备份、负载均衡、单臂多线路、星形、网状、树状等多种组网方式。

5）应用管控：支持内置 URL 分类库，支持 80 多类、1000 多万条 URL 信息；支持对 URL 地址以及域名进行过滤，且支持黑名单和白名单；支持内置 1700 多种应用特征库，可准确识

别各种 IM、P2P、网络游戏、流媒体、股票等应用，并可自定义；支持基于安卓和苹果 OS 开发的多种聊天软件和社交软件，如，QQ、微信、新浪微博、YY 语音、糗粑、网易新闻等。

6）智能流量控制：支持基于优化的高速流匹配技术， 以多种依据对流量进行分类;支持将每条链路切割成多组彼此互不影响的通道(PIPE),每个通道可再分割多个虚拟通道(Virtual Channel），设定带宽管理规则；支持将流量通过镜像口镜像出去，供第三方设备存储、分析、审计等。

7）云计算安全：支持基于网络、用户、应用做安全防护；支持基于 VLAN、AAA、VXLAN、Trill、NVGRE 做安全防护。

8）安全虚拟化：支持基于租户提供 SecaaS 服务；支持基于租户提供虚机形态的防火墙系统；支持防火墙、抗 DDoS、IPS 等安全特性对外 Restful API 以便于在公有云提供安全服务。

9）高可靠性：支持主备模式(A/S)、主主模式(A/A)、非对称路由等多种热备方式，且切换时间小于 1 秒；支持不少于 4 个节点，使用虚拟 IP 地址技术，通过 VRRP 协议实现集群负载均衡；支持将任意物理接口设置为 HA 接口。

10）安全审计：支持将日志存储在本地，标配 1T 日志存储硬盘，完美满足公安部 82 号令，至少保留用户行为日志 60 天的要求；支持全部日志按天和统一格式（如：ozlog-20141013.log）存储，可以通过 web 页面查看、删除、导出历史日志列表；支持历史日志，保证设备掉电后仍然可以保留上次运行的日志记录。

11）API 接口：支持提供 API 联动接口，支持与第三方网管对接。

12）一级和二级节点采用万兆安全网关，三、四级节点采用千兆安全网关。

15.主动风险防御

1）硬件指标：

（高配）网口，8 个千兆网口；CPU，i7 系列；内存，16G；硬盘，500G SSD。

（低配）网口，2 个千兆网口；CPU，i7 系列；内存，8G；硬盘，500G SSD。

2）用户管理模块：添加、删除、修改系统的用户以及给用户分配角色。

3）资产管理模块：包含主机资源、服务资源、漏洞风险。可以通过主动发现收集主机资源，可以通过手动方式直接添加已知 IP 地址的主机，管理发现的所有安全风险资源。

4）资产监控模块（高配）：管理需要监控的主机资源；管理用户导入的站点资源；对平台管理的设备进行实时监控，及时发现预警异常问题。

5）信息收集模块：包含主机发现、端口扫描、服务识别、风险探测、主动收集五部分，用于收集目标环境 的相关资源信息。主机发现，发现某个网段内所有主机；端口扫描，发现某个主机所有开放的端口；服务识别，识别某个端口的应用或服务，以及其版本信息；风险探测，通过内置插件方式，探测资产或者应用是否存在相关安全风险；自动收集，自动完成“主机发现”、“端口扫描”、“服务识别、“漏洞探测”等功能；收集任务，查看所有收集任务。

6）风险发现模块：漏洞管理，内置最新的漏洞库；脚本库，内置检测脚本，检测脚本要求 48000 个以上，特有脚本 100 个以上，常见检测插件 40 个以上，常见 CMS 检测插件 300 个以上；自动扫描，后台自动对系统进行全面的风险扫描工作。

7）对抗验证模块：脚本管理，根据关键字查询相关的攻击脚本；脚本验证利用，利用内置渗透脚本进行利用验证；会话查询，查看并管理会话；自动攻击，新建“自动攻击”任务，后台自动将发现的所有漏洞进行尝试使用脚本进行利用验证。

8）基线保护模块（高配）：查看管理所有基线保护任务计划；查看所有作业运行情况；展示基线对比结果。

9）虚实仿真模块（高配）：含物理设备管理模块，虚拟实例模块和虚拟仿真模块。物理设备管理模块，包含增删改功能，设备信息包含设备名称，选择设备类型，输入管理 IP 等。虚拟实例模块包含镜像管理模块，支持镜像主动发现功能；虚拟模板模块，支持虚拟模板管理功能，支持新盘创建和镜像模板克隆生产功能。虚拟仿真模块，利用物理设备和虚拟实例

设定场景拓扑，查看并管理场景拓扑中生成的虚拟机。支持在浏览器上通过拖拽形式可视化的创建或编辑拓扑；

10）风险报告：生成总体报告、资产报告、风险报告。查看风险相关统计信息，并导出结果。