CMJS-NT-202601201

政府采购合同

项目名称：南通市经济技术开发区新一代电子政务外网建设项目包2安全部分

合同编号：

甲　　方：南通市经济技术开发区管理委员会办公室

乙　　方：江苏移动信息系统集成有限公司

签订时间：2026年3月17日

中国移动通信集团江苏有限公司

甲、乙双方根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律法规以及本采购项目的招标文件、乙方的《投标响应文件》以及《中标（成交）通知书》，甲乙双方同意签订本合同。

一、合同内容

1.1 采购项目名称： 南通市经济技术开发区新一代电子政务外网建设项目包2安全部分（采购项目编号：JSZC-320690-JSHL-G2025-0022）

1.2 合同履行期限：自合同签订之日起五年

1.3 履行地点：甲方指定地点

1.4 采购内容（参数要求详见附件）

序号	名称	规格型号	品牌	单位	数量	单价（元）	金额（元）
一、安全保障体系建设							
1	防火墙	NSG6300-KP45	奇安信	台	1	226494	226494
2	流量探针（动态安全资源池）	TSS10000-S93G	奇安信	套	2	187203	374406
3	零信任扩容	安全访问控制网关系统V5.0	奇安信	套	1	237734	237734
4	终端防病毒扩容	终端安全管理系统	奇安信	套	1	218153	218153
5	态势感知（核心产品）	NGSOC-LV	奇安信	套	1	504108	504108
6	终端准入扩容	ASM-S-6118K	盈高	套	1	386298	386298
7	备份一体机	DP2000	鼎甲	台	1	315107	315107
二、系统集成服务及其他							
1	系统集成服务（含辅材光纤、网线、光模块等）	配套	国产	项	1	99500	99500
	合计						2361800

二、合同金额

2.1 本合同金额为（大写）：贰佰叁拾陆万壹仟捌佰圆（2361800元）人民币（含税）。

2.2 合同履行

2.2.1 付款方式：分期付款

1）预付款支付时间：合同签订后30个工作日内，预付款支付比例：合同金额的20%。2）尾款支付时间：整体项目终验合格后30个工作日内支付至合同总金额的90%。3）剩余款项待5年运维期结束后30个工作日内付清。

2.2.2 合同履行：（1）自合同签订之日起，6个月内完成合同全部设备及服务的交货、安装、集成、调试工作。（2）交货方式：设备及软件货物及服务现场交货验货，并提交相关交付物。

2.2.3 组成合同的文件，协议书与下列文件一起构成合同文件，如下述文件有任何抵触、矛盾或歧义，应按以下顺序解释：

（1）政府采购合同协议书及变更、补充协议；

（2）政府采购合同专用条款；

（3）政府采购通用条款；

（4）中标（成交）通知书；

（5）投标（响应）文件；

（6）招标文件；

（7）有关技术文件、图纸；

（8）国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供使用货物（包含与货物相关的服务）的有关技术资料。

中国移动通信集团江苏有限公司

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同货物（包含与货物相关的服务）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的货物（包含与货物相关的服务）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、税费

6.1 本合同执行中相关的一切税费均由乙方负担。

七、质量保修范围和保修期及售后服务

7.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

7.2 乙方提供的货物在质量期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

(1)更换：由乙方承担所发生的全部费用。

(2)贬值处理：由甲乙双方合议定价。

(3)退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

7.3 如在使用过程中发生质量问题，乙方在接到甲方通知后在 24 小时内到达甲方现场。

7.4 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

7.5 上述的货物免费保修期为 5 年（自交货验收合格之日起计），因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

八、项目验收

8.1 甲方依法组织履约验收工作。

8.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

8.3 甲方邀请第三方专业机构或专家参与验收，相关意见将作为验收书的参考资料。

8.4 甲方按照采购合同的约定对乙方的履约情况进行验收。验收时间、验收标准见招标文件验收内容。验收时，甲方按照采购合同的约定对每一项技术、商务要求的履约情况进行确认。验收结束后，甲方出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付挂钩。履约验收的各项资料存档备查。

8.5 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项。验收不合格的项目，甲方有权不予付款并要求乙方在规定期限内达到验收合格标准，催告期限届满乙方仍未达到验收合格标准的，甲方有权解除合同，并要求乙方退还全部已收款项，并按合同金额的20%支付违约金。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

8.6 验收组织的其他事项：中标人提交货物验收申请，验收申请需列

明货物名称、规格型号、生产厂家、数量和相关产品技术参数说明书，提供产品合格证或在有效期内的具有CMA或ilac-MRA（中国认可国际互认检测标识）或CNAS的第三方检测机构出具的检测报告。在收到中标人货物验收申请，并经甲方审核同意后30个工作日内组织验收，必要时邀请行业专家或第三方专业机构验收，相关意见将作为验收书的参考资料。

九、货物的包装、发运及运输

9.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。乙方对货物的包装应符合《商品包装政府采购需求标准(试行)》、《快递包装政府采购需求标准（试行）》的规定。

9.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

9.3 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

9.4 货物在交付甲方前发生的风险均由乙方负责。

9.5 货物在规定的交付期限内由乙方送达甲方指定的地点并安装调试完成后视为交付。

十、违约责任

10.1 质量瑕疵的违约责任

乙方提供的产品不符合合同约定的质量标准或存在产品质量缺陷，甲方有权要求乙方根据【**政府采购合同专用条款**】要求及时修理、重作、更换，并承担由此给甲方造成的损失。

10.2 迟延交货的违约责任

（1）乙方应按照本合同规定的时间、地点交货和提供相关服务。在履行合同过程中，如果乙方遇到可能影响按时交货和提供服务的情形时，应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延长交货时间或延期提供服务。

（2）如果乙方没有按照合同规定的时间交货和提供相关服务，甲方有权从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按**【政府采购合同专用条款】**规定执行。如果涉及公共利益，且赔偿金额无法弥补公共利益损失，甲方可要求继续履行或者采取其他补救措施。

10.3 迟延支付的违约责任

甲方存在迟延支付乙方合同款项的，应当承担**【政府采购合同专用条款】**规定的逾期付款利息。

10.4 其他违约责任根据项目实际需要按**【政府采购合同专用条款】**规定执行。

十一、不可抗力事件处理

11.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

11.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

11.3 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

十二、解决争议的方法

签字盖章页，本页无正文。

甲方：南通市经济技术开发区管理委员会办公室

单位名称（公章或合同章）

法定代表人或其委托代理人（签章）

2026.3.23

住　所

联 系 人

联系电话

通信地址

邮政编码

电子邮箱

统一社会信用代码

乙方：江苏移动信息系统集成有限公司

单位名称（公章或合同章）

法定代表人或其委托代理人（签章）

2026.3.23

拥有者性别

住　所

联 系 人

联系电话

通信地址

邮政编码

电子邮箱

统一社会信用代码

开户名称　江苏移动信息系统集成有限公司

开户银行　中国银行股份有限公司南京云锦路支行

银行账号　479361758530

中国移动通信集团江苏有限公司

附件 1：设备参数要求

1、防火墙

指标项		指标要求
硬件和性能	硬件和性能	★国产硬件，产品实配最大吞吐量≥100Gbps，最大并发连接数≥4000W，最大新建连接数≥90W,同时开启入侵防御，防病毒，URL 过滤,实配 40GE 光接口≥4 个,10GE 光接口≥12 个,10GE 多模光模块≥10 个，冗余电源，五年威胁情报和特征库升级授权，下一代防火墙模块，五年质保。
基础组网	部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式；
	网络协议	支持 VTEP(VxLan Tunnel EndPoint)模式接入 VxLAN 网络,并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定；
		支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。
	路由协议	支持静态路由、策略路由及动态路由，策略路由支持用户自定义其优先级，动态路由应至少支持 RIP V1/V2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持 PIM-SM（稀疏模式）
	地址转换	支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 模式和 SYMMETRIC 模式。

	IPv6 支持	设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定。
	高可靠性	支持路由模式、透明模式的 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA 高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA 高可靠性部署支持配置接口权重；支持链路探测。
	虚拟化防火墙功能	支持对虚系统进行系统配置，包括管理设定、管理主机、证书管理、配置文件导入导出、日志配置；虚系统管理员可分权管理；
		支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。
访问控制	访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。
	应用识别与控制	支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 2800 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。
	流量管理	支持多调度类相互嵌套最大 5 级的带宽管理设置。支持设置每 IP 最大或最小带宽，可对每 IP 进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。

中国移动通信集团江苏有限公司

攻击防护	网络攻击防护	支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施。
		支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果。
		支持防御基于安全域的 IP 地址欺骗攻击，指定 IP 或网段必须从特定安全域流入。
	病毒防护	能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；
		支持对最多 6 级的压缩文件进行解压查杀；
		支持基于 MD5 的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀。
	入侵防御	支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护。
		支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息。
协同防御	云端协同	支持与互联网云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能

中国移动通信集团江苏有限公司

2、流量探针（动态安全资源池）

功能类别		招标要求
产品规格		国产化软硬件，2U 机箱，≥1*8 核 CPU，≥32G 内存，≥4T SATA，≥6*千兆电口+2*万兆光口；冗余电源，应用层流量处理能力≥3G；提供五年产品标准维保服务。含五年威胁情报与检测引擎规则升级授权。
部署方式	双协议栈检测	支持 IPv4 和 IPv6 网络环境下的部署，接口支持 IPv4、IPv6 配置，支持对 IPv4 路由监控和对 IPv6 路由监控，可同时对 IPv4 和 IPv6 网络流量分析检测。
流量采集与识别	离线数据采集	支持手动和 FTP 方式批量导入 PCAP 包对离线流量采集，文件大小不低于 1 个 G；并记录 PCAP 包导入记录及检测状态。
	流量过滤	支持通过 ip、ip 段、端口、协议、VLAN 等进行流量过滤，过滤条件支持 and、or、not 等逻辑运算创建的 BPF 过滤语法过滤数据。
	流量负载记录	支持记录 TCP，UDP，HTTP 协议流量日志中的负载信息：TCP,UDP 的上下行负载支持可配，不低于 10KB。HTTP 协议的请求头，请求体，响应头、响应体支持长度可配，不低于 8KB。
	网络协议识别	支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、sctp、sybase、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6、tidb、kingbase、mqtt 等。
	文件协议	支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、

中国移动通信集团江苏有限公司

	识别	NFS 等类型协议流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备
	隧道封装识别	支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测。云场景下，支持 GENEVE 协议双层隧道封装流量的解析检测。
	日志外发	支持配置网络日志外发的标准模式、精简模式、自定义模式，支持外发的网络日志的类型包括：TCP 流量、UDP 流量、异常流量、SSL 加密协商、登录行为、域名解析、文件传输、FTP 控制通道、LDAP 行为、web 访问、邮件行为、数据库操作、telnet 命令、旁路阻断、MQ 流量、Radius 行为、Kerberos 行为、ICMP 流量、syn 流量、DHCP 解析等 20 种网络日志。每种网络日志，都支持自定义配置外发的字段。
	规则更新	新增规则，在规则列表进行标签标记展示，新增规则产生的告警在告警详情进行标签标记展示。
流量威胁检测	检测模式	支持检测模式的标准模式、精简模式、自定义模式的切换；支持手动配置各类检测引擎、机器学习模型的开关。
	WEB 攻击检测	支持常见攻击行为检测，支持 HTTP 双向流量动态检测，检出类型包括：SQL 注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等。
	WEBSHELL 攻击检测	支持基于工具特征的 WebShell 检测，检出类型包括：中国菜刀、蚁剑、冰蝎、哥斯拉、小马生成器 webshell 上传攻击检测，HTTP 代理程序等。
	网络攻击	支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解、Mysql

中国移动通信集团江苏有限公司

	检测	UDF 提权攻击、Microsoft Windows NetLogon 权限提升漏洞攻击，向日葵、TeamViewer，psexec 远程执行、smbexec 在目标上远程执行命令，DCSync_DCShadow 疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat 后门程序变种通信行为、Cobaltstrike HTTPS beacon 通信等
	加密流量攻击检测	支持隐秘信道检测。检测类型包括：ICMP、DNS 协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密 web 应用的流量检测，非法应用加密通信的检测，SSL 加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持 JA3 指纹检测。
	AI 检测能力	支持灵活开启机器学习模型，增强检测精度，模型至少包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测。
	远程工具检测能力	支持远控/远程工具检测，工具类型包括：向日葵、ToDesk、Sorillus、Stowaway、CcRemote、DWservice 等
	弱口令检测能力	支持基于自定义正则表达式以及自定义弱口令字典的弱口令登录行为检测，同时要支持不同协议弱口令分析。自定义弱口令正则表达式方式支持自定义弱口令强度、复杂度规则。支持配置多条弱口令检测的正则表达式。
	挖矿检测能力	支持门罗币、莱特币、以太坊、比特币、斯特币等 24+多种币种的检测。
	混淆攻击检测	支持对使用 base64、unicode、url 编码等混淆手段攻击检测。

中国移动通信集团江苏有限公司

	shiro 反序列化密钥配置	支持针对 shiro 反序列化，自定义添加密钥展示解密内容。
	内置规则编辑	系统内置规则支持进行编辑，支持自定义威胁类型、威胁等级、攻击结果。
	自定义检测漏洞规则	支持自定义漏洞规则 支持根据攻击载荷自定义漏洞检测规则，可自定义检测规则的四元组、检测规则的协议类型，包括：TCP/UDP/HTTP 协议。HTTP 协议可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）、匹配载荷内容，TCP/UDP 协议可自定义上下行 payload。并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE 编号、CNNVD 编号、漏洞描述、漏洞危害、解决方案。
	自定义检测威胁情报	支持自定义威胁情报 支持根据威胁类型、威胁名称、威胁级别、置信度、情报类型、IP、域名等自定义添加威胁情报，支持 STIX、OPENIOC、JSON、XLSX 格式的批量导入。
	敏感信息识别及加密展示	支持根据正则/机器学习来判断告警详情是否包含身份证号、用户名、密码等敏感信息，敏感信息加密展示。
	攻击特征显示	支持攻击特征高亮展示，方便分析人员事件分析

中国移动通信集团江苏有限公司

3、零信任扩容

指标项	指标子项	指标要求
产品扩容	原设备型号	LXR-TAC1500 零信任身份系统 V5.0
	软件客户端扩容	扩容 1000 个零信任并发用户授权，提供 1500 个多网切换授权，新增授权质保跟随原设备质保。
网络隐身	网络隐身	支持 TCP 单包授权机制
		支持 UDP+TCP 单包授权机制，UDP+TCP 方式默认不开放端口，可避免业务应用的端口被扫描，进而避免利用端口对业务应用发起攻击的风险
		支持通过输入安全码激活客户端，完成 SPA 敲门。安全码可支持共享码、一人一码两种模式，以满足不.景的需求。
用户身份管理	用户身份管理	提供用户概览统计能力，包括用户总数、启用用户数、锁定用户数、禁用用户数等信息，提升管理员运维能力。
		支持用户身份打标签，以实现对不同的用户打不同标签，并可以基于标签进行细粒度访问控制
终端管理	终端管理	提供设备概览统计能力，包括终端总数、启用终端数、锁定终端数、禁用终端数等信息，提升管理员运维能力。
		支持建立用户设备清单，支持对 PC 终端、移动终端进行统一查看和管理。
		支持用户自助解绑设置，可设置是否允许用户自助解绑，以及解绑是否要求做多因子认证，进一步加强设备解绑的管控。
		支持设备打标签，并可将标签用于访问控制策略，从而灵活实现对

中国移动通信集团江苏有限公司

		设备进行归类并实施不同程度的管控措施
终端环境感知	终端环境感知	支持 X86 架构下的 Windows 端环境采集，通过零信任客户端采集终端设备操作系统、类型、IP、MAC 等基础属性，支持采集运行进程、运行的虚拟机软件、运行的录屏软件、运行的远控软件、运行的杀毒软件、域、端口、防火墙设置等信息并作为访问控制策略项，以实现基于 Windows 终端安全状况的访问控制措施。
		支持 MacOS 端高危端口，开启屏幕共享，开启文件共享，开启互联网共享，开启蓝牙共享，开启打印机共享，开启内容缓存，开启远程管理，开启远程登录，开启操作系统防火墙，开启远程 APPLE 事件等环境感知和采集，以实现基于 MacOS 终端安全状况的访问控制措施。
		支持 ARM/X86 架构下的统信 UOS 和麒麟 Kylin PC 端操高危端口、运行的软件、零信任客户端版本、运行的杀毒软件、运行的远控软件、运行的虚拟机软件、安装的防病毒软件等环境感知和采集，以实现基于终端安全状况的访问控制措施。
资源管理	资源管理	支持应用概览统计能力，包括应用总数、WEB 应用数、隧道应用数等信息，提升管理员的运维能力。
		支持 WEB 应用(7 层）、隧道应用(3、4 层 TCP/UDP 应用)的代理和发布，以满足不同业务应用发布的需要
		支持 WEB 应用支持数据传递，可通过 URL、Header、Cookie 自定参数传递，以满足应用对特定参数的需要，从而实现对现网应用无需修改即可正常访问

中国移动通信集团江苏有限公司

自适应认证	自适应认证	支持用户名+密码、AD、LDAP 用户登录认证
		支持动态口令、短信、邮箱的多因子认证方式
		支持认证策略的优先级排序设置，可支持单用户目录认证策略的优先级、跨多个用户目录的全局优先级排序设置，以实现用户登录认证时，可按照设置优先级顺序展示相应的认证方式，以方便用户登录认证时使用。
		支持设备认证，提供认证策略配置，可根据是否签发设备、导入设备、绑定设备进行设备认证
		当用户以弱密码、非信任位置、非信任时间、闲置账号进行登录时，建立增强认证规则，需要进行多因子认证，以加强并提升用户身份的安全
权限管理	权限管理	支持用户直接授权访问的资源以及资源角色
		支持按照组织机构授权访问的资源以及资源角色
		支持按用户组授权访问的资源以及资源角色，以实现组内用户的批量授权，减轻管理的负担
		支持从应用资源、资源角色选择用户、组织机构、用户组，以实现角色内资源的被批量授予用户，减轻管理员的负担
		支持从资源角色选择用户、组织机构、用户组，以实现角色内资源的被批量授予用户，减轻管理员的负担
		支持继承其父组织机构权限，以实现用户的授权管理
安全准入控制	安全准入控制	支持从用户属性、环境属性、行为属性、终端属性维度设置准入策略，便于对用户准入进行控制

中国移动通信集团江苏有限公司

		支持按访问时间、访问地点、网段设置环境属性，以实现从环境属性维度对用户准入控制，确保只有在安全环境下才能正常进入系统。
		支持用户两次登录设备发生变化、异常旅行速度设置行为属性，以实现从用户行为维度进行准入控制，缓解因用户账号被盗用、身份被仿冒的用户进入系统的安全风险。
		支持基于设备标签设置准入控制策略，以满足用户在特定场景的安全控制规则
动态访问控制	动态访问控制	支持从用户属性、环境属性、应用属性、终端属性等维度设置访问策略，便于对用户访问资源进行控制
		支持访问策略模板，便于基于策略模块快速配置
		支持基于设备标签，设置访问控制策略，从而灵活实现对设备进行归类并实施不同程度的管控措施。
		支持基于设备归属，设置访问控制策略，从而实现针对企业签发、个人自带设备实施不同程度的管控
		支持基于认证方式、人员标签的用户属性设置访问控制策略
终端数据安全	PC安全空间	多空间：支持同一用户可配置多个安全空间，不同安全空间之间的应用相互隔离，可同时运行且互不干扰
		空间等级：安全空间可以设置不同的安全等级，支持控制不同安全等级的空间之间的数据流转
		数据加密：安全空间的数据在全生命周期都需要加密保存
		授信进程：安全空间提供应用权限管理能力，空间外的普通应用只能访问空间外的数据，不能访问空间内的数据；空间外的白名单应

中国移动通信集团江苏有限公司

		用可以访问空间内的数据。
		安全空间内支持应用黑/白名单控制
		进程隔离：安全空间内应用与空间外应用通信隔离，包括：文件通信隔离、服务通信隔离、命名对象通信隔离、剪切板进程通信隔离、注册表隔离
		数据隔离：安全空间内的应用产生的数据只能保存在空间内，且只能在空间内查看；个人空间内不可查看安全空间内数据。
		水印功能：空间内支持屏幕水印、打印水印功能。同时支持设置不同的水印参数，包括不限于水印内容、字体、密度、字色、角度等
		网络隔离：安全空间内支持网络白/黑名单模式，仅允许访问指定的IP、IP段、域名、IPV6。同时可以禁止在安全空间外访问空间白名单网址
终端数据安全	许可回收	支持安全空间、多网切换的许可数占用情况的展示，以及按策略进行许可数回收，便于回收和重复利用不再使用的许可点数，从而减少的成本
应用安全防护	应用安全防护	提供应用限流限速，支持通过限制请求并发设置相应阈值进行限流限速，缓解大量并发访问给业务应用造成的压力和资源消耗，从而确保业务的连续性、可用性。
		提供应用限流限速，支持通过限制响应传输速率设置相应阈值进行限流限速，缓解快速返回响应导致业务应用造成的压力和资源消耗，从而确保业务的连续性、可用性。
日志审计	日志审计	提供用户日志、管理日志、系统日志、访问日志等信息采集、管理

中国移动通信集团江苏有限公司

		及审计
		支持日志按照 SYSLOG 形式外发上报，可以设置多个远程日志服务器
业务监控	业务监控	提供用户维度业务监控，支持用户总数、用户锁定数统计，支持用户来源、用户组分布、用户上线趋势包含过去 1 个月、过去 7 小时、过去 24 小时。
系统管理	系统管理	支持用户会话、管理员会话、应用连接会话等会话的监控和管控，可手工强制下线，以便管理员能查看并及时对存在异常用户进行下线处置
		提供控制中心、网关的 CPU、进程 CPU、内存、进程内存、磁盘等系统资源的监控，便于管理员能够及时掌握系统当前的健康状况
		提供系统在备份，以保证系统在故障时可以通过备份进行恢复；提供升级功能，以保证系统可以根据需要更新到最新的版本状态，从而更好的提供安全服务和保障能力。
安全防护	安全防护	支持预防 syn flood 攻击、忽略 icmp 回显请求、并支持开启 ProxyProtocol 来识别并传递源 IP 地址。
		提供暴力破解防护，支持在 2 分钟内同一 IP 错误登陆 SSH 后台 10 次，该 IP 将被锁定 1 小时，从而缓解暴力攻击尝试登录管理后台，对零信任系统进行攻击的安全风险。

2、终端防病毒扩容

项目	指标项	技术参数
平台环境要求	原产品型号	终端安全管理系统 V6.0

中国移动通信集团江苏有限公司

	产品授权扩容	软件形态，与原有控制中心统一平台管理。提供国产化客户端扩容授权数 2000 个点，五年软件升级维保。
	控制中心要求	控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展； 管理中心操作系统支持 Windows Server 2012 R2/2016/2019/2022 的 64 位版本（简体中文版）； 支持 CentOS 7 系统；
	winpc 客户端	操作系统：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10/windows 11
	winserver 客户端	操作系统：Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；
	linux 客户端	操作系统：CentOS 5~8/Red Hat Enterprise Linux 5~8/Ubuntu1610
	macos 客户端	操作系统：macOS X 10.15、macOS 11.1、macOS 12.0.1、macOS 12.1
	国产化客户端	中标麒麟、银河麒麟、麒麟 V10、统信 UOS v20
基础功能	终端许可管理	支持按照终端类型/分组统计及分配管理每个功能的终端授权使用数量。
	语言要求	产品全功能支持简体中文/繁体中体/英语自由切换。
	基础功能	支持根据分组、计算机名称、IP 地址、MAC 地址、通信 IP 地址、接入点、客户端类型、操作系统类型、操作系统版本等条件的组合筛选出符合条件的终端进行管理，自由对终端进行转移分组、删除终端、重启系统和终端跃迁。

中国移动通信集团江苏有限公司

		支持定时公告功能，可配置开机显示、周期显示和立即推送。
		支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态、资产品牌、设备出厂日期； 硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息； 实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息； 网络信息展示，包括 IP 获取方式、IP 地址、子网掩码、默认网关、DNS 等信息；
		客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。
	客户端管理	支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。
防病毒防护	病毒防护概况	病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。
	病毒扫描	支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。

中国移动通信集团江苏有限公司

		病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
		支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务
		支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。
		支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。
	主动防御	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
		勒索软件防护：支持勒索病毒免疫防护，同时支持诱饵文件防护、预防勒索病毒变种
	网络防护	支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。
		支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。
	杀毒引擎	支持不少于三个杀毒引擎混合使用，提高病毒检出率。
勒索防护		支持通过家族免疫、智能诱捕、自主诱捕、行为追踪、智能秘钥、隐形灾备、云主防严格模式等，实现勒索病毒识别、诱捕、拦截，并实现加密文件备份和恢复。

中国移动通信集团江苏有限公司

		支持设置处置方式，自动处理、询问用户、不处理仅上报日志，支持设置备份文件的大小、历史文件清理。
补丁管理	补丁类型	支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC 等软件进行补丁修复。
		支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁。支持仅安装指定补丁设置。
	灰度发布	支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。
	漏洞修复设置	支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
主机防火墙		支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围，支持对设定进程名称、进程路径，支持模糊规则。

中国移动通信集团江苏有限公司

		支持根据需要来设置是否接管系统防火墙，支持根据规则的重要程度设置规则的优先级。
终端管控	外设管理	支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。
		支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。
	进程管理	支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、支持远程结束进程。支持远程查看计算机各个网卡配置信息。
		支持终端进程红名单、黑名单、白名单功能。可保护核心进程不被结束。
	能耗管理	支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。
日志		管理员可以按分组、按时间查看弹窗拦截的日志，日志详细记录被拦截弹窗的信息，同时支持日志的导出

5、态势感知

指标项	指标子项	指标要求
产品形态	软硬件要求	主机:国产化硬件，内存≥ 256G DDR4；硬盘≥2 块 960G SSD+12*4TB

中国移动通信集团江苏有限公司

		SATA，网络接口：4个千兆电口、2个万兆光口。 软件免费升级5年；产品质保5年。
系统对接	系统对接	**本次新建态势感知平台，与南通市统一安全管理平台进行对接。**
功能支持	功能支持	支持监控中心（态势感知、安全概览、仪表板、运维工作台）、分析中心（日志检索、告警分析）、威胁检测（威胁告警、事件管理、模型管理、威胁情报）、响应中心（自动化响应、威胁预警、工单管理）、资产中心（资产管理、脆弱性管理、风险资产）、统计报表、系统管理、威胁情报升级、漏洞知识库等功能，内置态势感知大屏，支持接入并解析的数据源数量至少为50个。
信创	国产化适配	软件支持国产化部署
数据采集与存储	数据采集	支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集；默认支持接入并解析的数据源数量50个，支持按需扩容数据源数量。
	数据存储	支持新增日志类型功能，可在线新增字段信息，支持数据存储类型的配置，包括：ES、Hive、mysql，支持存储基础信息的配置：包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的
	资产管理	支持从资产分组、组织架构、业务分组、地理位置及网段视角展示主机资产详情信息。
		支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期、资产唯一标识等属性进行配置。支持查看DHCP场景下资产IP的变更记录。

中国移动通信集团江苏有限公司

	资产风险	支持对资产风险值的自定义计算，计算范围包括威胁告警及脆弱性的危害等级、时间范围、处置状态等纬度。支持对风险计算周期进行配置。
威胁情报	本地情报	支持本地威胁情报的检索，检索类型支持域名、URL、IP地址；威胁情报内容支持IOC、攻击链阶段、ID、置信度、类型描述、定向攻击、风险等级、恶意家族、发布时间、攻击事件/团伙、影响平台、情报当前状态、威胁描述等；
威胁检测	威胁建模	支持自定义关联规则，支持类VISIO的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；提供1100+条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警。
	告警模式	支持配置告警模式，告警模式包括全量告警、精选告警，两种模式。精选告警的配置包括：告警置信度、告警攻击结果、告警危害等级，其中告警置信度包括：高、中、低，告警攻击结果包括：成功、企图、失败，告警危害等级包括：危急、高危、中危、低危。
	关联分析场景	支持预置关联分析场景，包括不限于：攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动、威胁情报命中等不同威胁场景的分析；支持将VPN、沙箱、流量传感器、Linux、Windows、AD域、WAF、NIPS、防火墙、HIDS、蜜罐等日志类型定义为标签，支持按照标签一键筛选定位关联规则。
	智能分诊规则	提供智能分诊能力，达到告警的降噪目的。智能分诊模型支持分诊规则、加白分诊规则两种规则的创建，分诊规则支持配置过滤条件

中国移动通信集团江苏有限公司

		和配置过滤条件组，过滤内容包括：告警名称、首次告警时间、源IP、目的IP、源端口、目的端口、通信方向、攻击者等信息；智能分诊支持生效时间配置，包括：永久生效和自定义时间。
威胁预警	预警配置	支持对重大网络安全事件（如Log4j漏洞）进行威胁预警功能。厂商针对重大网络安全事件生成威胁预警包，通过系统自动升级的方式分发给平台用户。也支持通过导入威胁预警包并启动威胁预警任务，完成网络安全事件的影响面评估和分析。
分析溯源	告警分析	具备独立的告警分析管理模块，该模块支持基于多视角进行聚合分析，预置分析视角至少包含告警名称分析、攻击者分析（含外部攻击者、内部攻击者）、失陷情报分析、挖矿木马分析、勒索软件分析、ATT&CK分析。
	事件调查	支持事件调查管理，支持查看事件详情信息；事件详情包括事件概览、受影响资产，ATT&CK战术，攻击技术及攻击者信息列表，关键攻击痕迹，证据库（包含：告警、资产及脆弱性信息、添加的证据及描述信息等）、处置建议。支持在证据库-告警列表页面进行告警搜索过滤，支持在证据库-资产列表页面进行资产搜索过滤。
	事件响应	支持按时间范围查询响应事件，并按照响应状态（待解决、解决中、已解决）统计响应事件的数量，快速了解当前平台响应事件的情况；支持按照事件属性字段查询响应事件。支持查看事件响应详情信息、事件响应处置的时间轴信息和事件响应阶段信息；事件响应详情包括事件调查基本信息（如：事件类型、攻击技术、事件描述、事件时间、调查结论和处置建议）。

中国移动通信集团江苏有限公司

	日志检索	支持通过热数据、冷数据方式对存储时间不同的日志进行分类搜索
		支持高级模式、Lucene、QAL 三种模式进行搜索。
响应处置	响应预案	支持对威胁告警和安全事件新增自动化响应策略，支持类 VISO 的图形化连线拖拽交互，通过将数据过滤和联动处置、syslog 外发、通知响应、工单 5 个计算单元进行灵活组合从而对告警实现自动化的、不同方式的响应场景；其中数据过滤计算单元支持引用对象资源、资产信息。支持通过列表的方式管理自动化响应策略，支持对策略进行停用、启用、批量删除等操作。
	工单响应	支持通过工单对安全事件进行跟踪处理，工单类型包括：通用、弱口令、告警、配置核查、漏洞、WEB 漏洞。工单流转中支持添加附件，支持 zip,.rar,.pdf,.doc,.docx,.xls,.xlsx,.ppt,.pptx,.txt,.png,.jpeg,.jpg 格式。工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销。
	联动处置	支持联动第三方防火墙进行威胁处置，可编写策略进行联动处置。
态势大屏	态势首页	提供态势感知大屏统一入口，态势首页集中展示至少 8 块态势大屏；支持大屏配置、轮播投放，内置大屏介绍文档，可供用户线上查看和下载；
		支持对态势大屏的内网地理位置、重点关注区域进行修改；支持自定义大屏 LOGO；支持设置大屏启停、轮播间隔时间、大屏轮播顺序
统计报表	报表管理	自定义报表模板：支持自定义模板可加入多种统计分析视图（含自定义）和智能备注信息（可根据数据不同展示不同的备注说明）；支持灵活编辑和布局调整以形成整体报表；可添加不限于告警统计、

中国移动通信集团江苏有限公司

		工单统计、异常行为统计、弱口令统计、攻击者统计、日志统计、系统维护、脆弱性统计、调查统计、资产统计、风险统计等；报表模板可被快速报表和周期报表任务引用
系统管理	升级管理	支持统一系统软件版本、威胁情报、漏洞知识库、IP地址定位库、巡检规则包、威胁预警包等数据的升级，支持配置升级地址并展示当前版本和升级相关信息，支持手动/自动升级方式
	知识库	支持自定义知识库，支持对自定义知识库字段的管理和配置，字段包含文本框、富文本、数值、密码、附件等表现形式，支持自定义知识库的增删改查等基础配置。

6、终端准入扩容

指标项	指标子项	指标要求
终端准入扩容	原设备型号	ASM-S-6118K
	基础架构	国产化硬件、麒麟操作系统及自研功能软件。 原硬件配置如下：飞腾 CPU:cpu:D-2000+ 8 核 内存:16G 硬盘 4T 单电源。
	性能参数	扩增 1000 点授权，由原来 1000 点扩容至 2000 点，每秒事务数（TPS）：≥2000（次/秒），最大吞吐量：≥1.5Gbps，最大并发连接数：2000（条）；新增授权质保跟随原设备质保。
	扩容功能要求	扩增授权部分需要支持原设备中可选模块：远程运维，违规外联，国产化适配等增配功能。
		扩增授权部分需要支持国产化终端：身份认证模块、访问控制模块、安全检查及智能修复模块、补丁库及规范刷更新等基础功能模块。

中国移动通信集团江苏有限公司

		扩增授权后，需原厂支持服务，含正式授权提供及上门设备调试客户端适配等工作。
		支持高级模式、Lucene、QAL 三种模式进行搜索。

7、备份一体机

指标项	指标要求
硬件要求	机型：2U 机架式 CPU：国产 内存：64GB 系统盘：2*480GB SSD 数据盘：6*8TB SATA 阵列卡：2GB 缓存 RAID 卡（含掉电保护） 网络接口：2*1GE 电口 2*10GE 光口（含多模光纤模块） 提供原厂商 5 年硬件质保服务（7*24 服务）
软件授权需求	不限制受保护的服务器类型、不限制被保护的数据库类型和数据库部署架构(双机、集群、RAC 等)、不限制操作系统的备份和恢复功能。 配置不少于 30T 备份容量许可（提供承诺函，格式自拟，并加盖供应商公章）
文件保护	支持 windows、linux、UNIX 以及国产化操作系统中的文件备份和恢复。
	海量小文件备份恢复性能：当海量小文件达到 10 万级时，备份速度≥100MB、s，恢复速度≥1000MB/s。
操作系统备份	支持 windows、linux 以及国产化操作系统的备份和恢复
	支持操作系统恢复过程中提供驱动程序更换界面，允许客户针对不同的驱动程

中国移动通信集团江苏有限公司

	序做调整。
数据库保护	支持 Windows、Linux 以及国产化操作系统下国内外主流数据库如 oracle、sqlserver、mysql、达梦、人大金仓、南大通用、神舟通用、GaussDB、TBase、瀚高、等数据库的备份与恢复；
	支持对 Oracle 的日志进行详细解析，可以查看每条日志数据的实际执行内容，包括：时间、 SCN、 用户名、 表名、 操作类型、 SQL 语句等。在数据恢复作业中可以选择准确的 SCN 来确定数据恢复点。
	针对 Oracle 中已经提交的事务，根据日志解析后得到的 SQL 语句，采用图形化界面来创建撤销处理，把数据回滚到事务提交前的状态。
	支持 MySQL 的逻辑备份和物理备份（完全备份、增量备份、日志备份、连续日志备份），通过物理备份实现对数据库的热备份。支持 MySQL 基于物理备份的备份数据（非 CDP 备份数据），实现任意时间点的恢复。
云平台保护	支持国内外主流如 vmware、hyper-V、KVM、ZStack、SmartX、华为、华三、浪潮 InCloud Sphere、深信服 HCI 等虚拟机的无代理备份与恢复；
	支持与 vmware 联动功能，，无需登录到备份管理平台，可以在 vmware 的管理平台上管理虚拟化备份运行状态和运行情况。
可用性验证	支持对 Oracle、SQL Server、MySQL、DB2、PostgreSQL、Informix、Sybase、达梦、Kingbase、Gbase、Domino 等主流数据库的备份集进行定时容灾演练，以此检验备份集的可用性。
管理方式	采用先进的运维管理架构，要求所有功能的管理和监控，都在备份软件中采用同一可视化界面实现。
	持使用 Access Key 的用户登录模式，有效解决用户应用系统密码定期自动变更

中国移动通信集团江苏有限公司

	和无密码场景下备份作业的按期执行。
	支持通过管理控制台，集中更新所有客户端，无须对每台客户端单独进行操作。
	智能报表，能够自定义报表。自主选择字段来源以及需要显示的字段等，并能够自定义新字段。支持筛选，排序等动作。
	为确保恢复演练时杜绝出现误操作的问题，需要提供资源保护设置演示：标记资源为受保护对象后，不能对资源进行恢复操作。
	备份系统在多作业同时备份时平均备份速率≥3GB/s。
	确保备份产品自身具有高安全性，具有国家权威机构出具的源代码安全审计报告。
告警方式	支持以邮件告警的方式，针对于备份存储系统的硬件故障、软件故障等等信息及时通知管理员

中国移动通信集团江苏有限公司