政府采购合同

（服务类）

第一部分 合同专用条款

项目名称:常州经济开发区人民检察院工作网安全防御系统(等保三级)

甲方：常州经济开发区人民检察院

乙方：中电鸿信信息科技有限公司

签订地：江苏常州

签订日期：_____年_____月_____日

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定及常州市政府采购中心采购编号为　　采购文件及投标（响应）文件，按照平等、自愿、公平和诚实信用的原则，经甲乙双方协商一致，约定以下合同条款，以兹共同遵守、全面履行。

1.1 合同组成部分

下列文件为本合同的有效组成部分，对甲乙双方均具有法律约束力。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标通知书；

1.1.3 投标文件（含澄清或者说明文件）；

1.1.4 招标文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

1.2 服务

1.2.1 服务名称：常州经济开发区人民检察院工作网安全防御系统（等保三级）；

1.2.2 服务标准:依据国家等级保护 2.0 技术要求,以及检察院的业务特点,需进行工作网安全防御系统建设服务,保护范围包括但不限于网络基础设施、本地计算环境及边界、信息安全基础设施等。服务期为三年。

1.3 价款

本合同总价为：¥941800 元（大写：玖拾肆万壹仟捌佰元人民币）。全额为安全服务费用，开具 6%税率发票。

分项价格：详见附件系统清单。

1.4 结算方式

序号	阶段	付款条件	付款期限	付款比例	备注
1	1	项目签订合同后	自接收到发票之日起 15 日内	30	合同签订后自接收到发票之日起 15 日内，支付至合同价的 30%
2	2	运维服务期间第一年支付合同金额的 30%	自接收到发票之日起 15 日内	30	合同签订后自接收到发票之日起 15 日内，支付至合同价的 60%
3	3	运维服务期间第二年支付合同金额的 20%	自接收到发票之日起 15 日内	20	合同签订后自接收到发票之日起 15 日内，支付至合同价的 80%
4	4	运维服务期间第三年支付合同金额的 20%	自接收到发票之日起 15 日内	20	合同签订后自接收到发票之日起 15 日内，支付至合同价的 100%

甲方支付乙方每笔款项的另一前提是收到乙方开具的正式发票,甲方应自接收到乙方开具的正式发票之日后 15 日内按照约定支付资金。如有特殊情况，双方协商决定。

1.5 服务提供时间、地点和方式

1.5.1 提供时间：设备部分合同签订后 45 个日历日内完成供货、安装、调试和验收。整体服务期为三年。；

1.5.2 服务地点：甲方指定地点；

1.5.3 服务方式：提供现场及运维服务，具体详见附件清单。

1.6 检验和验收

项目涉及的全部软硬件部署完成、系统联调正常后，根据采购人的安排进行试点工作，采购人对系统功能、性能等基本满意后，进行验收。准备项目验收交付物，验收文档的提交应覆盖以下内容：

项目实施前：项目实施方案（包括技术方案）、项目实施计划等；

项目实施期间：项目实施工作单、故障诊断及排除记录、项目实施过程中衍生的其他相关资料；

项目实施后：项目竣工报告、系统运行报告、故障诊断与排除手册、工作总结报告；

培训期间：培训计划、用户使用手册、管理员使用手册。

1.7 违约责任

1.7.1 除不可抗力外，若乙方未按照本合同约定的时间、地点和方式提供服务，则视为乙方违约，每延迟一日，乙方应当按照延期提供服务总价格的 0.5% 向甲方支付违约金，违约金总额不超过本合同总价的 5%；乙方延迟提供服务

天以上，甲方除了有权按照以上标准向乙方主张违约金外，还有权单方解除本合同，因此产生的相关损失全部由乙方承担，解除通知送达对方时本合同即解除；

1.7.2 除不可抗力外，若甲方未按照本合同约定时间支付价款，则视为甲方违约，每迟延一日，甲方应当按照逾期付款金额的0.5%向乙方支付违约金；违约金总额不超过本合同总价的5%，甲方迟延付款90天以上，则乙方有权单方解除本合同，解除通知送达对方时本合同即解除。

1.7.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经对方催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段来影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同，解除通知送达对方时，本合同即解除；

1.7.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式。

1.7.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式。

1.7.6 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

1.8 合同争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，应当选择下列第 2 种方式解决：

1.8.1 将争议提交/仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.8.2 向标的物所在地的人民法院起诉解决。

1.9 合同生效

本合同自甲乙双方签字盖章后生效，一式四份，双方各执两份，具有同等法律效力。

甲方：

统一社会信用代码或身份证号码：

住所：

法定代表人或授权代表（签字）：

联系人：

约定送达地址：

邮政编码：

乙方：

统一社会信用代码或身份证号码：

91320000668382125D

住所：南京市玄武大道699-1号

法定代表人或授权代表（签字）：

联系人：周峰

约定送达地址：常州市潞城街道141号

邮政编码：213025

电话:	电话:15301509710
传真:	传真:025-86588940
电子邮箱:	电子邮箱：15301509710@189.cn
开户银行:	开户银行：南京市建设银行湖北路支行
开户名称:	开户名称：中电鸿信信息科技有限公司
开户账号:	开户账号：32001881436059000588

第二部分 合同一般条款

2.1 定义

本合同中的下列词语应按以下内容进行解释:

2.1.1 “合同”系指采购人和中标供应商签订的载明双方当事人所达成的协议，并包括所有的附件、附录和构成合同的其他文件。

2.1.2 “合同价”系指根据合同约定，中标供应商在完全履行合同义务后，采购人应支付给中标供应商的价格。

2.1.3 “服务”系指中标供应商根据合同约定应向采购人履行的除货物和工程以外的其他政府采购对象,包括采购人自身需要的服务和向社会公众提供的公共服务。

2.1.4 “甲方”系指与中标供应商签署合同的采购人；采购人委托采购代理机构代表其与乙方签订合同的，采购人的授权委托书作为合同附件。

2.1.5 “乙方”系指根据合同约定提供服务的中标供应商；两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购的，联合体各方均应为乙方或者与乙方相同地位的合同当事人，并就合同约定的事项对甲方承担连带责任。

2.1.6 “现场”系指合同约定提供服务的地点。

2.2 技术规范

服务所应遵守的技术规范应与采购文件规定的技术规范和技术规范附件(如果有的话)及其技术规范偏差表(如果被甲方接受的话)相一致；如果采购文件中没有技术规范的相应说明，那么应以国家有关部门最新颁布的相应标准和规范为准。

2.3 知识产权

2.3.1 乙方应保证其提供的服务全部或部分不存在任何侵犯第三方知识产权的行为；若因乙方提供的服务的知识产权问题导致甲方被追究法律责任，则乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿；

2.3.2 合同涉及技术成果的归属和收益的分成办法的，详见***合同专用及补充条款***。

2.4 履约检查和问题反馈

2.4.1 甲方有权在其认为必要时，对乙方是否能够按照合同约定提供服务进行履约检查，以确保乙方所提供的服务能够依约满足甲方之项目需求，但不得因履约检查妨碍乙方的正常工作，乙方应予积极配合；

2.4.2 合同履行期间，甲方有权将履行过程中出现的问题反馈给乙方，双方当事人应以书面形式约定需要完善和改进的内容。

2.5 结算方式和付款条件

详见***合同专用及补充条款***。

2.6 技术资料和保密义务

2.6.1 乙方有权依据合同约定和项目需要，向甲方了解有关情况，调阅有关资料等，甲方应予积极配合；

2.6.2 乙方有义务妥善保管和保护由甲方提供的前款信息和资料等；

2.6.3 除非依照法律规定或者对方当事人的书面同意，任何一方均应保证不向任何第三方提供或披露有关合同的或者履行合同过程中知悉的对方当事人任何未公开的信息和资料，包括但不限于技术情报、技术资料、商业秘密和商业信息等，并采取一切合理和必要措施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。

2.7 质量保证

2.7.1 乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2.7.2 乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

2.7.3 乙方应保证提供的服务符合国家、行业标准，同时符合甲方提供的规范标准。

2.8 延迟履行

在合同履行过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长履行的具体时间，否则，视为乙方违约，按照合同专用及补充条款承担相应违约责任。

2.9 合同变更

2.9.1 双方当事人协商一致，可以签订书面补充合同的形式变更合同，但不得违背采购文件确定的事项，且如果系追加与合同标的相同的服务的，那么所有补充合同的采购金额不得超过原合同价的 10%；

2.9.2 合同继续履行将损害国家利益或社会公共利益的，双方当事人应当以书面形式变更合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，按各自过错承担相应的责任。

2.10 合同转让和分包

合同的权利义务依法不得转让，但经甲方书面同意，乙方可以依法采取分包方式履行合同，即：依法可以将合同项下的部分非主体、非关键性工作分包给他人完成，接受分包的人应当具备相应的资格条件，并不得再次分包，且乙方应就分包项目向甲方负责，即与分包供应商就分包项目向甲方承担连带责任。

2.11 不可抗力

2.11.1 如果任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限相应顺延，顺延的期限即为不可抗力期间；

2.11.2 因不可抗力致使不能实现合同目的的，当事人可以解除合同；

2.11.3 因不可抗力致使合同有变更必要的，双方当事人应在***合同专用及补充条款***约定时间内以书面形式变更合同；

2.11.4 受不可抗力影响的一方在不可抗力发生后，应在***合同专用及补充条款***约定时间内以书面形式通知对方当事人，并在***合同专用及补充条款***约定时间内，将有关部门出具的证明文件送达对方当事人。

2.12 税费

与合同有关的一切税费，均按照中华人民共和国法律的相关规定缴纳。

2.13 乙方破产

如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同且不给予乙方任何补偿和赔偿，同时甲方有权要求乙方支付违约金　　元，若该违约金不足以弥补甲方各项损失，则甲方还有权就各项损失向乙方主张赔偿责任。

2.14 合同中止、终止

2.14.1 双方当事人不得无故擅自中止或者终止合同；

2.14.2 合同继续履行将损害国家利益或社会公共利益的，双方当事人应当中止或者终止合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，双方按各自过错承担相应的责任。

2.15 检验和验收

2.15.1 乙方按照***合同专用及补充条款***的约定，定期提交服务报告，甲方按照***合同专用及补充条款***的约定进行定期验收；

2.15.2 合同期满或者履行完毕后，甲方有权组织（包括依法邀请国家认可的质量检测机构参加）对乙方履约情况进行验收，即：按照合同约定的标准，组织对乙方履约情况进行验收，并出具验收报告；向社会公众提供的公共服务项目，验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告；

2.15.3 检验和验收标准、程序等具体内容以及前述验收报告的效力详见***合同专用及补充条款***。

2.16 通知和送达

2.16.1 甲乙双方确认，合同第一部分尾部所载明地址为其法定送达地址，双方往来中所有通知、文件、材料送达该地址，即视为送达，包括但不限于邮寄送达、拒绝签收等；任何一方变更上述送达地址的，应于变更前15个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达地址仍视为有效。

2.16.2 以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

2.17 合同使用的文字和适用的法律

2.17.1 合同使用汉语书就、变更和解释；

2.17.2 合同适用中华人民共和国法律。

2.18 履约保证金

2.18.1 采购文件要求乙方提交履约保证金的，乙方应按***合同专用及补充条款***约定的方式，以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式，提交不超过合同价5%的履约保证金；

2.18.2 履约保证金在***合同专用及补充条款***约定期间内不予退还或者应完全有效，前述约定期间届满之日起/个工作日内，甲方应将履约保证金无息退还乙方；

2.18.3 如果乙方不履行合同，履约保证金不予退还；如果乙方未能按合同约定全面履行义务，那么甲方有权从履约保证金中取得补偿或赔偿，同时不影响甲方要求乙方承担合同约定的超过履约保证金的违约责任的权利。

2.18.4 除2.18.3所述情形以外，甲方如逾期未退还乙方履约保证金的，除了全部退还履约保证金以外，超期时间还应当按照中国人民银行同期贷款基准利率向乙方支付利息。

2.19 合同份数

合同份数按***合同专用条款***规定，每份均具有同等法律效力。

第三部分　合同专用及补充条款

本部分是对前两部分的补充和修改，如果前两部分和本部分的约定不一致，应以本部分的约定为准。本部分的条款号应与前两部分的条款号保持对应；与前两部分无对应关系的内容可另行编制条款号。

条款号	约定内容
2.3.2	具有知识产权的计算机软件等货物的知识产权归属，项目验收合格并支付验收款后，产权归甲方所有。
2.5	结算方式和付款条件：详见合同正文1.4条款。
2.11.3	因不可抗力致使合同有变更必要的，双方当事人应在7天内以书面形式变更合同；
2.11.4	受不可抗力影响的一方在不可抗力发生后，应在7天内以书面形式通知对方当事人，并在7天内，将有关部门出具的证明文件送达对方当事人。
2.15.1	货物交付前，乙方应对货物的质量、数量等方面进行详细、全面的检验，并向甲方出具证明货物符合合同约定的文件；货物交付时，甲方在15天内组织验收，并可依法邀请相关方参加，验收应出具验收书。
2.15.3	检验和验收标准、程序等具体内容以及前述验收书的效力详见投标文件。
2.18	本项目无需履约保证金。
2.22	合同份数：本合同一式四份，甲乙双方各执两份，具有同等法律效力。

附件：系统清单

序号	分项名称	服务内容		数量	单位	响应价格	
						单价	合价
1	下一代防火墙	性能参数	网络层吞吐量≥8Gbps，应用层吞吐量≥1.6Gbps，并发连接数≥250 万，新建连接数≥10 万；	2	台	73900	147800
		硬件参数	标准 1U 设备；国产 CPU，CPU 核数≥4，CPU 主频≥1.5GHz，国产操作系统；内存≥8GB；标配≥6 个千兆电口+4 个千兆光口；3 年软硬件维保，3 年特征库升级。				
		入侵防御	产品须开启 IPS 模块，具备入侵防御功能。				
		Web 应用防护	产品须开启 web 应用防护模块，具备 web 应用防护功能。				
		工作模式	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。				
		路由特性	产品支持策略路由负载来支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，总共需要支持加权流量、带宽比例、线路优先等负载均衡调度算法。				
		访问控制	产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求				
		地域访问控制	产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。				

			NAT 功能	产品支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能，支持一对一、一对多、多对一等形式的 NAT。支持IPv4 / v6 NAT 地址转换。				
			应用控制	产品内置应用特征识别库，支持不少于 2980 种应用规则，支持对游戏、下载工具、IM 聊天工具、视频软件、股票软件等类型应用进行检测与控制。（需提供产品功能截图证明）				
			Web 应用防护	产品具备 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为，安全特征规则超过 3320 种。（需提供产品功能截图证明）				
				▲具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。需提供国家权威机构出具的关于“漏洞防扫描”的相关证书。				
			入侵防护	支持对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 WEB 攻击行为进行有效防护；				
				支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等 DoS/DDoS 攻击防护；支持 IP 地址扫描和端口扫描防护；				
				支持 Land、Smurf、WinNuke、Tear Drop、IP 数据块分片传输、超大				

				ICMP 数据攻击等攻击基于数据包攻击防护；支持 IP 协议异常报文检测和 TCP 协议异常报文检测；				
				支持对常见应用服务（FTP、SSH、SMTP、IMAP、POP3、RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；				
				支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间；（提供相关证明材料）				
				▲产品支持僵尸网络检测功能，防止失陷主机威胁内网扩散。需提供国家权威机构出具的关于“僵尸网络检测”的相关证书。				
			防病毒模块	产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。（需提供产品功能截图证明）				
			对象智能识别	产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。（需提供产品功能截图证明）				
			策略生命周期管理	▲产品支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。需提供国家权威机构出具的关于“安全策略管理”的相关证书。				
			基本要求	★要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。				
				▲所投产品需具备《计算				

			机软件著作权登记证书》，提供有效的证书复印件。				
			★所投产品具备中国国家信息安全产品认证证书，提供有效证书复印件。				
2	路由器	IPv4 转发性能	≥3Mpps	2	台	9000	18000
		硬件规格	▲提供不低于 13 个千兆电口，2 个千兆光口，如外支持不低于 2 个业务扩展插槽，交流电源。（提供原厂截图）				
		路由协议	支持静态路由，RIP/RIPng，OSPF/OSPFv3，BGP4/BGP4+，IS-IS/IS-ISv6。				
		虚拟化	▲支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备。当单台设备故障时，流量可以迅速切换，保证网络业务的稳定性。提供国家确定的认证机构出具的处于有效期内的检测报告复印件。				
		广域网	支持 TCP 传输优化，数据压缩解压，冗余数据消除等技术对广域网流量传输优化，提供广域网带宽利用率和减少链路抖动和延迟。				
		VXLAN	支持可扩展虚拟局域网络，实现跨三层公网的二层转发。				
		IPv6 NetStream	▲基于流的统计技术，可以对网络中的业务流量进行统计和分析。它将具有相同特征的报文作为一条流，对各个流进行统计，记录流的统计信息并输出。也可以把多个具有某些相同特征的流聚合成一条聚合流，记录聚合流的统计信息并输出。提供国家确定的认证机构出具的				

			处于有效期内的检测报告复印件。				
		攻击防御	支持 ND 攻击防御，防止 IPv6 终端仿冒攻击。支持 ND 协议报文源 MAC 地址一致性检查功能。				
3	核心交换机	基本要求	▲交换容量≥730Gbps，包转发率≥220Mpps，以官网最小值为准；（提供原厂截图）	2	台	28500	57000
			▲提供不低于 24 个千兆光口，8 个千兆电口，12 个万兆光口；（提供原厂截图）				
		安全认证	支持同时开启 802.1X、MAC 认证及 Portal 认证；				
		堆叠	支持堆叠技术，支持最大堆叠数量≥9 台；				
		VLAN 特性	支持基于端口的 VLAN、支持基于协议的 VLAN、支持基于 MAC 的 VLAN				
		链路聚合	支持链路聚合功能及聚合零丢包；				
		镜像功能	支持流镜像、端口镜像、远程镜像；				
		路由协议	支持静态路由，RIP/RIPng，OSPF v2/v3，BGP4，BGP4+ for IPv6，IS-IS，IS-IS V6				
		可靠性	▲支持 RRPP，环网故障恢复时间≤50ms；支持 Smartlink，收敛时间≤50ms；支持 RSTP、MSTP、PVST，收敛时间≤50ms，以上要求提供国家确定的认证机构出具的处于有效期内的检测报告复印件。				
		MACsec 硬件加密	支持 MACsec 硬件加密技术，实现报文加密、防重放攻击、防篡改，无需软件授权；				
		VXLAN 功能	支持通过 VXLAN 技术实现不同交换机的二层或三层互通功能；				

		运维能力	▲设备内置及图形化操作的方式，实现对网络的统一运维及管理，要求提供国家确定的认证机构出具的处于有效期内的检测报告复印件。				
		管理和维护	支持 Telnet、SNMP 及支持 RMON 告警、事件、历史记录;				
		配置要求	配置模块化双风扇、双电源，实配 MACsec 硬件加密功能。				
4	光模块	万兆模块(1310nm,10km,LC)		26	块	1000	26000
5	堡垒机	硬件配置要求	整机规格：1U 机箱，采用国产处理器（主频：1.5GHz，4 核）,国产操作系统; 接口配置：6 个千兆电口、4 个千兆光口,冗余电源;	1	台	100000	100000
		授权	50 个主机/设备许可，最大可扩容至 100; 16GB 内存，1T 硬盘 用户数不限制。				
		资产管理	支持中标麒麟、银河麒麟、Windows 等操作系统，支持网络设备、安全设备、数据库等的资产管理				
			支持修改管理协议默认端口，支持资产的批量导入导出。				
			支持资产组的增删改查				
		用户管理	支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出				
			采用三员管理，支持系统管理员、安全审计员和安全操作员，并且三员之间权限相互制约				
			支持本地认证和三方认证服务器接入认证，如 AD、LDAP、Radius 服务器				
			▲支持数字证书等方式进行双因子认证。支持中标				

				麒麟或银河麒麟客户端采用数字证书双因子认证（提供产品功能截图证明）				
				支持用户组的增删改查				
			资产账号	▲自动对 Windows、Linux 等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成（提供产品功能截图证明）				
			权限管理	支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权				
				支持会话、指令、剪切板上下行、文件上传下载的约束行为；				
				支持用户会话超时退出；支持用户密码连续鉴权失败锁定，到期自动解锁；支持用户强密码策略，密码长度 8 位以上，包含字母、数字、特殊字符等；支持对用户登录 IP 地址、MAC 地址、时间的限定				
				支持内置工单运维，操作员可根据工作需求临时申请设备运维工单，管理员审批后可直接运维，过期失效；				
				支持对运维时间、运维地址、运维操作指令的限定，触发策略后进行告警				
			单点登录	支持访问 SSH、RDP、Telnet、FTP、SFTP、VNC、数据库等资产；支持账号密码的自动代填登录，支持半自动登录和手动登录；				
				设备访问支持最新的 html5 技术，在同一 WEB				

				窗口页签中，无需 JAVA 应用插件或调用本地应用客户端，即可实现对目标设备的快速运维；				
				支持 SecureCRT、XShell、WinSCP 等客户端直接连接堡垒机进行代理运维目标资产				
			审计管理	支持对用户和管理员的认证登录、操作和配置管理进行日志记录				
				支持对 Windows、VNC 等图形界面的运维操作进行录屏审计，支持图形和字符协议的视频回放				
				▲支持对图形和字符协议的操作进行文本记录，如鼠标操作、文本内容操作等，Linux 命令操作等（提供产品功能截图证明）				
				支持对在线会话的实时监控和即时阻断，避免违规操作				
				支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。				
				报表针从会话、指令等多个维度进行统计； 系统内置丰富报表统计模板：协议运维排名、资产运维次数 top10、资产运维趋势 top10、用户运维趋势 top10、协议运维趋势、用户运维次数 top10、指令分布 top10、top10 指令资产分布、指令用户分布 top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令				

				top10 等多种类型报表模板。				
			系统管理	支持 HTTPS 方式和 Console 方式进行管理				
				支持管理口与业务口分离。				
				支持将本机日志、告警日志通过 SYSLOG、邮箱等进行外发和告警				
				支持配置数据和审计数据的备份、自动清理，支持备份数据通过 FTP 方式远程备份				
				支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性				
			产品资质	▲具备计算机软件著作权登记证书				
				★具备中华人民共和国公安部颁发的《计算机信息系统安全产品销售许可证》（增强级），提供有效的证书复印件。				
				▲具备飞腾 CPU 兼容性证明				
				▲具备银河麒麟或麒麟软件操作系统兼容性认证				
				▲CMMI 5 级，提供证书复印件并加盖供应商公章				
				▲网络安全应急服务支撑单位证书（国家级），提供证书复印件				
6	日志审计		硬件配置要求	整机规格：2U 机箱 采用国产 CPU：主频：2.3GHz，8 核；采用国产操作系统，内存：32GB 系统盘：256GB Msata 数据盘：4T 网络接口； 接口配置：6 千兆电（含 1 个管理口、1 个 HA 口）+4 千兆光+2 万兆光，冗余电源；	1	台	98000	98000
			性能要	日志采集处理均值				

			求	3000EPS，默认包含 50 个日志源。				
			部署方式	支持单级部署；支持代理分布式部署采集日志；各级完全自制，独立管理本级日志；？ 下级不需要把日志传到上级，上级可以直接远程查看、统计各级日志，节省网络带宽；				
			基本要求	支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 26 类 300 种日志对象的日志数据采集；				
				对所管理设备的日志原始数据完整存储，支持数据本地集中存储；				
				内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则；				
			功能要求	支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。				
				支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；				
				▲支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；（提供产品功能截图证明）				
				支持独立展示每个被采集源最近 24 小时的日志数量趋势，便于掌握设备的安				

				全事件情况， 支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态				
				支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储;				
				支持日志备份功能，支持本地备份和 FTP 备份方式，支持自动备份和手动备份;				
				▲支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数;（提供产品功能截图证明）				
				支持为不同类型日志设置不同的查询条件和显示条件。				
				支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类;				
				▲支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析；（提供产品功能截图证明）				
				支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数。				
				支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作;				
				▲支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集				

				日志总量、最近接收时间、业务组等基础信息；（提供产品功能截图证明）					
				支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。					
				支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰；					
			产品资质	▲具备计算机软件著作权登记证书					
				★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》，提供证书复印件					
				▲具备飞腾 CPU 兼容性证明					
				▲具备银河麒麟或麒麟软件操作系统兼容性认证					
				▲CMMI 5 级，提供证书复印件					
				▲网络安全应急服务支撑单位证书（国家级），提供证书复印件					
7	天烛高级攻击检测防御系统 ADS 高级版		终端 Agent 程序兼容情况	Windows PC 客户端支持	Windows7、Windows8、Windows8.1、Windows10	1	套	150000	150000
				Windows 服务器客户端支持	WindowsServer2008、WindowsServer2008R2、WindowsServer2012、WindowsServer2012R2、WindowsServer2016、WindowsServer2019				
				Linux 客户端支持	Centos/Rad Hat/Ubuntu/Suse15/中标麒麟/银河麒麟/统信 UOS				
			部署要求	平台及其他组件必须支持部署在物理机、虚拟机/云的计					

				算环境					
			威胁概览	综合概览	可按照最近 7 天、最近 10 天、最近 30 天等不同时间段，展示终端、服务器产生告警总数、已处置告警数、未处置告警数、全网异常文件拦截告警总数等数据				
				态势大屏展示	从宏观的角度对威胁攻击进行观察分析，展示出综合评分、威胁告警等级、风险资产走势、威胁占比等，能够快速定位终端风险				
					支持通过热力图颜色渐变形式显示命中 ATT&CK 指标项的分布情况				
					支持实时展示终端安全事件、恶意文件、异常命令等多个层面对终端进行安全态势分析。通过逻辑的风险拓扑，展示全网风险终端分布状态。				
			资产管理	资产管理	支持将资产以组织架构形式进行分组管理；可通过树形组织形式查看公司组织架构				
					自动获取已安装探针终端的软硬件资产信息，展示并采集终端资产的基础信息（包括终端 IP 地址列表、终端 MAC 地址列表、终端历史 IP 地址列表、终端用户列表、进程列表、服务列表、网络信息、软件资产、历史操作、自启动项、				

					USB 设备、漏洞补丁）实时了解全网终端资产状况。支持提供资产数据导出，便于资产管理				
					支持新上线或从未手动分配过部门分组的终端上线后将根据本地 IP 地址自动分配到相应部门分组				
				终端登录日志	支持查看网内各终端完整的用户登录日志，监控终端账号登录成功、失败情况				
				性能监控	支持对终端 CPU、内存、磁盘性能进行监控，CPU、内存超过阈值进行预警提示				
			安全策略管理	安全策略配置	可对安全策略进行编辑、新增、查看操作，以及在编辑、新增时，定制当前使用的策略规则和功能的开关配置，并将配置保存为安全策略下发至终端进行安全响应				
				自定义策略配置	对当前使用的策略规则进行自定义开关配置，并可将该策略应用到目前公司组织结构中的不同分组				
				移动存储设备管理	移动存储设备管理，可限制终端移动存储设备的访问				
				主机防火墙	支持对终端主机防火墙规则进行自定义配置，自定义控制主机防火墙规则的启用停用				
			风险检测	系统风险检测	对操作系统的注册表变更记录、系统权限篡改检测、流量异常、会话劫持、系统服务、				

					创建自启动项、计划任务程序等进行实时检测，以及对操作系统的漏洞补丁、系统异常和配置文件进行检测				
				终端异常行为检测	▲通过终端行为实时检测，对异常提升用户操作权限行为、脚本类程序执行行为、非法访问黑 IP、常见命令行程序执行及操作行为进行实时检测和告警，可追溯执行用户、网络连接信息、执行的进程、系统模块调用，还原威胁命令执行的上下文内容，呈现事件发生过程，对事件定位追踪（提供产品功能截图）				
				专项威胁检测	支持基于进程行为的方式对勒索病毒加密篡改文件检测				
					支持挖矿木马矿池访问检测				
					支持伪造系统程序木马的检测				
					支持钓鱼木马程序及快捷方式的检测				
					支持常见 APT 攻击方式的检测				
				基线检测	提供基线检查功能，针对终端操作系统、数据库的配置进行安全检测，结合终端行为检测引擎对安全基线进行检测，支持查看基线检测进度与检测项内容				
					支持查看基线检测结果和历史安全基线检测记录，发起重新检				

					测，以及导出本地检测结果				
			入侵防御	威胁防护	主动防御型查杀，可在不依赖病毒特征库的情况下，对恶意程序、免杀木马、钓鱼程序、挖矿程序、勒索病毒、黑名单程序等进行检测、拦截				
				全网威胁自动管理	▲支持全网威胁自动管理，有效预防已知/未知恶意程序（例如勒索、挖矿、木马、蠕虫、病毒等所有恶意程序）在网内的扩散，查看某一个文件的MD5在公司全网范围以内的分布情况，能看到每一个终端首次出现该文件的时间（首次将文件上传至云端扫描的时间）、主机、文件路径信息熵等信息；支持一处发现威胁，全网拦截（提供产品功能截图）				
				网站后门防护	支持 webshell 越权执行防护和后门文件检测。提供查杀和实时防护，可自定义文件扫描方式，支持检测常见的 PHP、JSP、ASP 等后门文件类型				
				黑白名单管理	支持文件黑白名单，并提供文件黑白名单快速查询工具，支持批量导入和移除操作				
				病毒查杀	支持通过多病毒分析引擎实时扫描的终端新增文件，同时允许自定义对文件进行恢复、删除，允许手动设置扫描部门、文件				

					路径、文件类型，并选择是否隔离异常文件，并且支持查看扫描进度、导出扫描结果，且可选择是否停止当前扫描。				
			勒索专项防护	勒索诱饵防护	▲在系统关键目录投放诱饵文件，并监控诱饵文件的读写操作，当勒索病毒诱饵文件进行读写操作时（加密、修改等）会触发客户端行为检测，从而进行拦截，有效阻止勒索病毒的加密行为（提供产品功能截图）				
				勒索恶意行为	支持检测勒索恶意行为，包括但不限于删除卷影副本、删除系统还原点、删除数据库备份、恶意结束进程、篡改系统服务项等危险指令，对恶意进程文件发送多病毒分析引擎进行检测				
			威胁告警溯源	威胁告警	▲提供实时的威胁告警信息，可以自动地对已知和未知威胁进行处置。支持查看全网内所有终端产生的告警信息及告警等级；告警详情包括：文件操作（新建、访问、删除)、注册表操作（新建项、删除项、删除值、重命名项、设置项）、网络通信（连入 ip、连出 ip、首次通讯时间、端口、相关域名）、系统模块加载（加载时间、模块文件 MD5、文件类型、病毒类型）（提				

					供产品功能截图）				
					▲支持通过图表模式以及时序图模式两种方式对告警中所有源威胁事件所命中的ATT&CK 指标情况进行查看，各个指标项的时候可显示指标详情以及命中情况（提供产品功能截）				
					支持网络通信、系统模块加载命中 IOC 并高亮显示				
					支持以安全事件时间轴进行排序展示，快速提取当前终端所有安全事件数据				
				终端安全事件溯源	▲以树形结构展示威胁文件进程的调用关系，对事件详情进行描述，可追溯恶意进程的运行时间、详细路径、以及文件信息详情，并可手动加入黑白名单。支持对威胁事件追溯分析，可记录事件发生时间、发生数量、关联终端名称、登录的用户账户、事件行为描述、事件关联文件详细路径、关联文件加载的模块信息、行为发生时的调用信息（提供产品功能截图）				
				网络安全事件溯源	▲支持对每一个网络安全事件进行详细记录，包括事件类型、发生次数、源目的 IP、端口、关联终端、关联文件等（提供产品				

					功能截图）				
				安全事件关键进程标记	支持对触发当前安全事件的进程进行标记，并展示出当前进程所有的详细信息；联系上下文，以时间轴的方式查看所有与当前进程相关的安全事件，做到关键进程上下文关联查询				
				安全事件过滤	通过安全事件的数据库，经过灵活的自定义过滤条件，筛选出相关上下文的安全事件，并通过安全事件详情中的进程路径查看整个安全事件的全流程				
			威胁响应	响应处置	根据安全策略开关，对终端威胁行为检测到之后进行自动处置、结束进程、文件黑白名单控制、网络隔离、远程关机等				
					支持断网情况下的威胁行为检测，即使终端掉线、断网依然可以提供有效防护				
				远程调查取证	支持通过命令行把终端相关文件通过远程下载方式传输到服务端				
			安全运维	实时进程管理	支持实时对终端内正在运行的进程进行检测，可以显示每个进程文件的详细路径、进程启动、进程加载、进程执行命令等，可手动远程进行在线停止、隔离和进程文件删除操作				

				全局文件检索	支持全局新增文件检索，可显示所查找的文件所在终端名、文件描述、版本、HASH值、文件签名、文件安全级别等信息				
				客户端升级	支持灵活的按照组织架构主动、被动、静默方式对终端 Agent 进行升级，支持 IO 风暴智能削峰，在既定版本服务端硬件支撑范围内所有客户端可同时上线				
				服务端升级	支持在不中断业务情况下升级服务端				
				用户管理	支持配置三权分立账号权限，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限				
				报表管理	提供详细的报表记录和多种报表输出。分为威胁报表和资产报表、自定义报表，支持实时导出报表和定期导出报表				
				告警邮件管理	支持邮件告警、支持告警通过 Syslog 外发，可自定义告警类型				
				备份与恢复管理	提供系统备份与恢复功能，备份支持自动备份恢复和远程备份两种模式				
				标准数据接口	支持三方软件通过接口获取采集的数据				
				系统软件扩容	支持授权数量的增加以及在不中断业务的情况下扩容				
				硬件	支持不停机扩容				

			系统扩容	系统组件支持分布式部署				
8	运维综合管理系统		基础构架	采用 J2EE 架构，支持多系统部署，可部署到 Window、linux 等操作系统平台上，能够提供多数据部署接口（Mysql、ORACLE、MongoDB），方便数据对接。	1	套	135000	135000
				▲支持分布式部署，支持 100 节点监控管理（网络设备（含安全设备、传输设备）、实体机（虚拟机）、系统应用数量（基础类软件或应用系统）等）（需提技术白皮书或截图加盖公章）				
				▲支持分级管理，支持自动方式同步下级系统的资源、告警、报表，提供功能截图				
				对网络可用性指标的采集使用 SNMP，PING 进行监控，同时使用 SYSLOG,TRAP 等日志信息进行分析判断。				
			拓扑管理	可自动发现网络设备，正确识别网络中设备的厂商、设备的类型				
				支持 MSTP 协议的链路可用性状态监控				
				支持 IPv4、IPv6 双协议的设备发现和管理，提供功能截图				
				支持对设备的分组拓扑构建。				
				支持设备及链路的手工发现方式和自动发现方式				
			网络资源管理	能够提供设备、IP、MAC、端口、链路、Vlan 等丰富的资源管理功能，并提供 IP-MAC、IP-PORT 绑定检测。				

				能够定期自动备份关键网络设备的配置信息，实现对配置文件进行统一的归档管理，配置文件可导出。				
			主机服务器监控	系统必须支持包括windows2000\2003\2008\2012、Linux、IBM AIX、Sun Solaris 、HP-Unix 、SCO Unixware 、SCO Openserver 、FreeBSD 、OpenBSD 、AS400 、IBM Power 等各版本操作系统的监控。				
				支持 IPMI 协议、SNMP 协议等方式对服务器硬件的监测，包括风扇转速、电源、电压、内存变化、磁盘变化、磁盘坏道检测、工作温度等。				
				支持 eventlog、syslog 等系统日志的监控，可根据日志告警级别以及日志中出现的特定的关键字信息进行报警。				
			国产化适配	▲适配国产操作系统，包括统信 UOS 系统（海光服务器）、统信 UOS 系统（兆芯服务器），需提供官方兼容证书或互认证明				
				▲适配国产中间件，包括东方通 Tongweb、中创中间件，需提供官方兼容证书或互认证明				
				▲适配国产关系数据库，包括达梦 DM 数据库，需提供官方兼容证书或互认证明				
				▲适配 NoSQL 数据库，包括巨杉 SquoiaDB 数据库，需提供官方兼容证书或互认证明				
			数据库监控	系统必须支持 Oracle、Microsoft SQL Server、				

				MySQL、DB2、Sybase、Informix、PostgreSql、Cassandra、达梦等数据库的监控。				
			中间件监控	系统必须支持 Tomcat、Jboss、WebLogic、Websphere、WebLogic 集群、Websphere 集群、Resin、IBM MQ、MSMQ、Tuxedo、Sharepoint、Tonglink、Tongweb、Microsoft.NET、Glassfish 等中间件的监控。				
			其他应用	系统必须支持对 AD 活动目录、DNS 服务器、FTP 服务器、LDAP 服务器、Exchange、Mail 邮件服务器的监控				
				能够通过自定义脚本的方式对特殊的业务应用进行监视, 如 bat、shell 等脚本, 并且脚本执行结果可生成为趋势图用以分析。				
			告警管理	可设置故障等级，按设备通断、端口 up/down 状态、端口流量、cpu/内存等性能指标设置故障等级。				
				可提供多种告警方式。包括颜色、声音、邮件、短信等手段。应支持根据不同的告警级别、设备类型、设备名称、用户角色等进行短信接收人的配置，还可进行消息过滤。				
				告警需要按级别划分，如紧急告警、重要告警、次要告警等，并能在拓扑图上用颜色区分不同的告警等级。				
				提供 syslog、Trap、eventlog 接收功能				
			自动巡检	按照监控类型对制定范围的监控资源进行定时（按				

			天、周、月）自动巡检后生成巡检报告。巡检报告可随时在页面查看，也可设定邮箱自动发送到指定邮箱				
			安全机制	系统支持对登录过程中的数据加密,以保障管理员远程登录监控系统的安全性;			
				▲提供 HTTPS 安全登录方式和登录输入验证码登陆；（需提技术白皮书或截图）			
				用户管理可以集成第三方 LDAP			
			操作审计	满足审计要求，支持审计功能，可以多种方式查阅到用户在系统中的操作时间和操作内容等。			
				系统应支持对用户特定操作行为进行日志记录，并做事后审计;			
				产品有 ITSS 信息技术服务工具产品注册符合性评估证书，提供证书。			
				厂商具有 ITSS 服务认证，提供证书。			
专业技术服务							
9	等保测评费用	工作网等级保护三级的测评服务费		1	项	80000	80000
10	漏洞扫描服务	针对主机系统、WEB 应用、弱口令等开展漏扫服务，不低于 1 年 4 次漏扫服务		1	项	20000	20000
11	应急响应服务	针对突发的安全事件时，应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏。并在此基础上，安全服务实施人员协助检查所有受影响的系统，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。		1	项	10000	10000
12	全流量分析服务	对全网进行全流量分析，并提供分析报告，便于技术科对单位网络的		1	项	20000	20000

		整体健康状况有个全面的了解。				
13	系统集成服务	1.网络线缆、光缆应急保障线路铺设，备用线缆跳纤，光缆熔接包等备品备件 2.改造同时不得影响机房业务需安排人员现场保障 3.对整个项目所涉及到的产品提供安装调试以及 3 年质保，维保等服务	1	项	80000	80000
总价			941800			