郑州市气象局郑州智慧气象项目（A包）

合同书

甲方：郑州市气象局

乙方：河南省丰之汇信息技术有限公司

二零二三 年 十二 月

（一）合同协议书

买方：郑州市气象局

卖方：河南省丰之汇信息技术有限公司

郑州市气象局（采购人名称）的 郑州市气象局郑州智慧气象（项目名称）A 包，经国内公开采购（采购项目编号：郑财招标采购-2023-298）。经评标委员会评定 河南省丰之汇信息技术有限公司（中标人）为中标人。买、卖双方同意按照下面的条款和条件，签署本合同。

1.货物和数量

分项名称	规格型号	制造厂家及原产地	单位	数量	单价	总价
飞思网巡 IT 运维管理系统软件 V5.0（智能网络可视化系统）	飞思网巡网管软件-50 授权	深信服	套	1	38000	38000
云镜网络资产脆弱性扫描系统（漏洞扫描）	YJ-1000-B1075	深信服	套	1	79000	79000
防火墙（防火墙）	AF-2000-FH2130B	深信服	套	2	69200	138400
防火墙（可信边界接入网关）	AF-1000-FH1200B	深信服	套	1	18000	18000
防火墙（内网安全接入模块）	AF-1000-FH1800A	深信服	套	5	34500	172500
全网行为管理系统（内网威胁诊断模块）	AC-1000-SK2100	深信服	套	1	178000	178000
Web 应用防护系统（web 应用防火墙）	WAF-1000-FH1800A	深信服	套	1	81200	81200
潜伏威胁探针系统（威胁情报超融合流量探针）	STA-100-B2100	深信服	套	1	70000	70000
安全感知管理平台（安全态势感知平台）	SIP-1000-A3300	深信服	套	1	219000	219000
托管检测与响应服务（安全自查工具）	MDR	深信服	项	1	129000	129000
技术服务费（安全集成服务）		丰之汇	项	1	36900	36900
总价	壹佰壹拾陆万元整	（￥：1160000.00）				
项目 1-9 含 13%税率、项目 10-11 含 6%税率						

2.合同总价

本合同总价为人民币 壹佰壹拾陆万元整（大写）元整（￥1160000.00 元），本合同为固定单价合同，在整个合同有效期内单价不予调整。

序号	合同履行期限	交货地点	交货期	质量标准	验收标准	质保期
1	自合同签订之日起至质保期结束止	采购人指定地点	自合同订立之日起 60 日历天	合格	符合行业现行相关标准，满足项目需求	自验收合格之日起 36 个月

3. 支付方式

3.1 合同签订后 15 个工作日内，买方向卖方支付合同总价的 50%（具体支付金额以财政实际拨付金额为准），即人民币￥：580000.00 元，大写：伍拾捌万元整。

3.2 卖方全部货物到货，产品到货验收合格后，买方向卖方支付合同价款的 47%（具体支付金额以财政实际拨付金额为准），即人民币￥：545200.00 元，大写：伍拾肆万伍仟贰佰元整 。

3.3 自验收合格起 36 个月后，买方向卖方支付合同价款的 3%（具体支付金额以财政实际拨付金额为准），即人民币￥：34800.00 元，大写：叁万肆仟捌佰元整 。

4. 合同的生效

本合同经双方全权代表签署、加盖单位印章生效。

买方：郑州市气象局

（印章）

2023 年 12 月 28 日

卖方：河南省丰之汇信息技术有限公司

（印章）

2023 年 12 月 28 日

授权代表（签字）：

授权代表（签字）：

地址：

地址：郑州市金水区金水路 226 号楷林国际 20 层 2011 号

邮政编码：

邮政编码：450000

电话：

电话：0371-56066689

开户银行：

开户银行：中国银行股份有限公司郑州财富广场支行

帐号：

帐号：253360546672

（二）合同条款

1.定义

1.1 本合同下列术语应解释为：

1）“合同”系指买卖双方签署的、合同格式中载明的买卖双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

2）“合同价”系指根据本合同规定，卖方在完全履行合同义务后买方应支付给卖方的价格。

3）“货物（设备）”系指卖方根据合同约定须向买方提供的货物、仪器仪表、备品备件、专业工具、手册及其它技术资料和材料。

4）“服务”系指按合同规定供应商须承担的设计、制造、安装、检验、调试、技术支持、提供技术援助、培训、售后服务以及其他类似的义务服务。

5）“合同条款”系指本合同条款。

6）“买方”系指购买设备和服务的单位。

7）“卖方”系指提供本合同项下设备和服务的公司或实体。

8）“现场”系指合同约定设备将要运至和安装的地点。

9）“交货”是指卖方按照合同规定，向买方提供设备。

10）“安装”是指有关设备、备件、材料和软件的安装工作，包括按照图纸将零部件放置在适当的位置并连接起来。

11）“调试”指卖方在完成了安装之后，为准备验收而进行的设备运转测试。

12）“验收”系指合同双方依据强制性的国家标准、技术质量规范和合同约定，确认合同项下的设备符合合同规定的活动。

13）“项目现场”系指本合同项下设备安装、运行的现场。

14）“天”指日历天数。

15）“质量保证期”是指自合同验收之日起一定时间内，卖方保证所供设备的适当和稳定运行，并负责消除存在的任何缺陷。

2.适用性

2.1 本合同条款适用于买方和卖方在合同协议书上签字生效所包含的所有时间和内容。

3.原产地

本条款所述的“原产地”是指设备开采、生长或生产或提供有关服务的来源地。所述的“设备”是指制造、加工或实质上装配了主要部件而形成的设备。商业上公认的产品是指在基本特征、性能或功能上与部件有着实质性区别的产品。

4.标准

4.1 本合同下交付的设备应符合技术规格所述的标准。如果没有提及适用标准，则应符合中国国家标准或设备来源国适用的官方标准。这些标准必须是有关机构发布的最新版本的标准。

4.2 除非技术规格中另有规定，计量单位均采用中华人民共和国法定计量单位。

5.使用合同文件和资料

5.1 未经买方事先书面同意，卖方不得将由买方或代表买方提供的有关合同或任何合同条文、规格、计划、图纸、模型、样品或资料提供给与履行本合同无关的任何其他人。即使向与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必须的范围。

5.2 未经买方事先书面同意，除了履行本合同之外，卖方不应使用合同条款第 5.1 所列举的任何文件和资料。

6. 包装

6.1 卖方应提供设备运至合同规定的最终目的地所需要的包装，以防止设备在转运中损坏或变质。这类包装应采取防潮、防晒、防锈防腐蚀、防震动及防止其它损坏的必要保护措施，从而保护设备能够经受多次搬运、装卸及长途运输。卖方应承担由于其包装或其防护措施不妥而引起设备锈蚀、损坏和丢失的任何损失的责任或费用。

7. 合同履行期限

7.1 本项目合同履行期限为 36 个月 。

8. 协调

8.1 卖方应与其他承包商（包括安装承包商）进行技术协调，以保证正确地完成本合同的安装、调试与验收工作。

9. 保险

9.1 本合同下提供的设备应对其在制造、购置、运输、存放及交货过程中的丢失或损坏按本条款规定的方式，以人民币投保全面保险。交货前的一切保险由卖方负责。

10. 运输

10.1 合同要求卖方将设备运至买方指定的目的地或项目现场，卖方应负责办理、支付将设备运至目的地或项目现场，包括合同约定的保险和储存在内的一切事项，有关费用应包括在合同价中。

11. 备品备件

11.1 正如合同条款所规定，卖方可能被要求提供下列与备件有关的材料、通知和资料：

①买方从卖方选购备件，但前提条件是该选择并不能免除卖方在合同保证期内所承担的义务；

②在备件停止生产的情况下，卖方应事先将要停止生产的计划通知买方使买方有足够的时间采购所需的备件；

③在备件停止生产后，如果买方要求，卖方应免费向买方提供备件的蓝图、图纸和规格。

11.2 卖方应提供为系统的正常运行提供必要的备品和备件。

12. 质量保证要求与售后服务

12.1 卖方应保证合同项下所供货物是全新的、未使用过的，除非合同另有规定，货物应含有设计上和材料的全部最新改进。卖方进一步保证，合同项下提供的全部货物没有设计、材料或工艺上的缺陷（由于按买方的要求设计或按买方的规格提供的材料所产生的缺陷除外），或者没有因卖方的行为或疏忽而产生的缺陷，这些缺陷是所供货物在最终目的地国家现行条件下正常使用可能产生的。

12.2 卖方同意在本合同规定的质保期内，向买方人提供系统维护和支持服务。卖方应保证系统的现场技术服务。

12.3 卖方应明确其承诺的质保期内、质保期外售后服务方式、响应时间、到达现场时间、修复

时间，包括远程访问与现场服务形式，乙方自收到甲方反馈30分钟响应，2小时内到达现场。

12.4 卖方应在质保期内提供免费上门维修和技术支持的服务。

13. 索赔

13.1 如果卖方对偏差负有责任而买方在合同条款第18或合同的其他条款规定的检验、安装、调试、验收和质量保证期内提出了索赔，卖方应按照买方同意的下列一种或几种方式结合起来解决索赔事宜：

①卖方同意退货并用合同规定的货币将货款退还给买方，并承担由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为看管和保护退回货物所需的其它必要费用。

②根据货物的偏差情况，损坏程度以及买方所遭受损失的金额，经买方与卖方双方商定降低货物的价格。

③用符合合同规定的规格、质量和性能要求的新零件、部件和/或货物来更换有缺陷的部分和/或修补缺陷部分，卖方应承担一切费用和风险并负担买方蒙受的全部直接损失费用。

13.2 如果在买方发出索赔通知后3天，卖方未作答复，上述索赔应视为已被卖方接受。如卖方未能在买方发出索赔通知后3天内或买方同意的延长期限内，按照买方同意的上述规定的任何一种方法解决索赔事宜，买方将从未付货款或从卖方开具的履约保证金中扣回索赔金额。

14. 合同价

14.1 本合同采用固定单价承包方式。卖方的投标总报价（评审时发现算术错误，修正后经采购人和乙方认可的报价）即为合同价。

14.2 卖方应对其投标报价考虑周全，本合同实施过程中（非设计变更造成）出现的未列、漏列项目及费用由卖方自行承担。

14.3 除买方提出的项目增加外，本合同价不允许调整。

15. 合同履行期限延误

15.1 如因买方原因逾期完工卖方不承担违约责任，如因卖方原因逾期完工，买方有权解除合同。

16. 违约终止合同

16.1 如果卖方未能履行合同规定的其它任何义务；

16.2 如果买方认为卖方在本合同的竞争和实施过程中有腐败和欺诈行为。

为此目的，定义下述条件：

①“腐败行为”是指提供、给予、接受或索取任何有价值的物品来影响有关人员在采购过程或合同实施过程中的行为；

②“欺诈行为”是指为了影响采购过程或合同实施过程而谎报事实，损害买方的利益的行为。

17. 不可抗力

17.1 签约双方任一方由于受不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，其延长的期限应相当于事件所影响的时间。不可抗力事件系指买方与卖方双方在缔结合同时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事件，诸如战争、严重火灾、洪水、台风、地震等。

17.2 受阻一方应在不可抗力事件发生后尽快用电报、传真或电传通知对方，并于事件发生后15天内将有关当局出具的证明文件用特快专递或挂号信寄给对方审阅确认。一旦不可抗力事

件的影响持续 15 天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

18. 违约责任

18.1 甲方无正当理由拒收货物、拒付货款的，甲方应向乙方偿付拒付货款 1‰的违约金。

18.2 乙方无正当理由逾期交付货物的，每逾期 1 天，乙方向甲方偿付逾期交货部分货款总额的 3 ‰的违约金。如乙方逾期交货达 15 天，甲方有权解除合同，甲方解除合同的通知自到达乙方时生效。

18.3 甲方未按合同规定的期限向乙方支付货款的，每逾期 1 天甲方向乙方偿付欠款总额的 3 ‰违约金。

19. 争议的解决

19.1 合同实施或与合同有关的一切争议应通过双方协商解决。

19.2 如协商不成，可向买、卖双方所在地人民法院提起诉讼。

19.3 在争议期间，除存在争议的部分外，本合同其它部分应继续执行。

20. 适用法律

20.1 本合同应按照中华人民共和国的法律进行解释。

21. 合同生效

21.1 本合同经双方全权代表签署并加盖单位印章后生效。

22.2 本合同一式 陆 份，具有同等法律效力。

（三）合同附件

3.1 中标通知书

中标通知书

采购项目编号：郑财招标采购-2023-298

河南省丰之汇信息技术有限公司：

你方于 2023 年 12 月 21 日所递交的 郑州市气象局郑州智慧气象项目A包 投标文件已被我方接受，被确定为中标人。

采购人（盖章）
2023 年 12 月 26 日

采购代理机构（盖章）
2023 年 12 月 26 日

中标主要内容

中标人名称	河南省丰之汇信息技术有限公司
中标价	大写：壹佰壹拾陆万元整 小写：1160000.00 元
中标内容	所投标包的货物采购、供货、包装、运输及运输保险、安装、调试、检验、检测、备品备件、易耗品、技术服务（包括技术资料的提供）、现场服务、技术培训、满足货物的安装调试及运行维护、参加验收、售后服务、系统集成和其它相关内容等
交货期	自合同订立之日起 60 日历天
交货地点	采购人指定地点
质保期	自验收合格之日起 36 个月
质量标准	合格
合同履行期限	自合同签订之日起至质保期结束止

请你方在接到本中标通知书后的 2 个工作日内与郑州市气象局签订合同。

特此通知。

3.2 设备清单及实施要求

1.采购清单

序号	名称	单位	数量	备注
1	防火墙	套	2	安全产品
2	Web 应用防火墙	套	1	安全产品
3	漏洞扫描	套	1	安全产品
4	可信边界接入网关	套	1	安全产品
5	安全态势感知平台	套	1	安全产品
6	威胁情报超融合流量探针	套	1	安全产品
7	内网安全接入模块	台	5	安全产品
8	内网威胁诊断模块	套	1	安全产品
9	智能网络可视化系统	套	1	安全产品
10	安全自查工具	项	1	安全服务
11	安全集成服务	项	1	安全服务

2.主要产品参数要求

序号	名称	主要规格参数
1	防火墙	1、整机吞吐量≥20Gbps,最大并发连接数≥200 万，每秒新建连接数≥9 万，支持虚拟防火墙； 2、标准机架式，设备接口满足项目配置需要并可扩展，千兆电口≥8 个，万兆光接口≥2 个，具有扩展槽位；≥2 个高速 USB2.0 接口，≥1 个 RJ45 串口； 3、支持二层模式(透明模式)、三层模式(路由和 NAT 模式)和混合模式； 4、支持静态路由，等价路由，支持 RIP、RIPng、OSPFv2/v3 动态路由协议，支持多链路出站负载，支持基于 ISP 的智能路由选路； 5、DDoS 攻击防护：支持 Land、Smurf、Fraggle、WinNuke、PingofDeath、TearDrop、IPSpoofing 攻击防护、支持 SYNFlood、ICMPFlood、UDPFlood、ARPFlood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测;支持对信任区域主机外发的异常流量进行检测,如 ICMP，UDP，SYN，DNSFlood 等 DDoS 攻击行为； 6、支持对被保护对象的流量进行分析，发现被保护对象的不同业务流量情况，支持生成和导出相关报告； 7、支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过

		滤策略，提高运维人员工作效率； 8、支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能；通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计；支持所有安全设备的安全日志汇总，并能够通过时间、严重等级、动作、ip、用户、特征/漏洞 ID 等多个条件查询过滤日志； 9、双机支持 A/S，A/A 方式部署，支持配置同步，会话同步和用户状态同步；双机模式下，支持主备两台设备采用同一套 IP 地址，简化配置，节约公网地址； 10、★具备勒索病毒防护专项，对勒索软件进行检测和防护。 11、★具备 C&C 攻击防护能力，支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。 12、★产品支持联动安全自查工具，支持流量日志分析、事件聚合，安全事件微信端就可接受预警和处置。
2	Web 应用防火墙	1.吞吐量≥5Gbps，并发连接≥200 万，每秒新建≥5 万，配置千兆电口≥4 个，全部开启 bypass 功能，开启全部接口 WAF 功能使用许可，配置 3 年特征库升级服务，配置固态硬盘，包含策略调优服务； 2.支持透明模式、代理模式和网关模式； 3.支持协议正规化，至少包括请求行正规化、Cookie 正规化、头域负载正规化等，可设置 Host、Referer、Accept、User-Agent、Range、Content-Length、Accept-Charset、Content-Encoding 等参数，支持识别 HTTP/1.1、HTTP/1.0、HTTP/0.9 等版本； 4.支持对上传文件的检查，可基于上传方法、文件类型、上传文件个数、单个文件大小、文件大小总和等参数进行配置。可识别类型至少包括 PE、asp、aspx、php、jsp、sh、py、ELF、rb、pl、Webshell 等； 5.支持 Web 层面的漏洞攻击防护，防护类型至少包含 SQL、XSS、命令注入、目录遍历、CSRF 等。支持例外页面、例外参数配置，且支持与黑名单联动，可设置联动阈值、联动周期及禁封时间； 6.支持服务器信息隐藏，隐藏信息至少包括 Server 头域信息、5xx 信息、4xx 信息、网站目录信息、关键文件信息、数据库信息、源码信息、账号信息(银行卡号、身份证号)； 7.支持网站自学习功能，可学习到 URL 地址、请求频率、最大长度、参数个数、cookie 总长度、Cookie 个数、参数名称、参数类型、最大值、最小值等信息，生成相应的白名单策略，且可按需调整白名单，并设置阻断或告警动作； 8.支持站点自动发现功能，可自动学习命中的防护策略，并将学习到的新 IP、新端口、新域名自动添加到防护策略中； 9.支持网络爬虫防护，支持配置预定义爬虫类型，自定义爬虫类型，爬虫白名单； 10.支持配置用户组(IPv4/IPv6)，开启/关闭预定义弱口令，防护资源(HOST、URL、用户名前缀、密码前缀)、安全级别(中、强、极强)、动作(提示、告警、阻断、阻断

		并推送告警)； 11.支持配置服务器、防护IP、防护域名、防护URL、网页预取状态、基于域名/URL查询记录；支持开启/关闭强制防护，支持批量开启/关闭； 12.支持在线查看报表，可查看整网安全分析、近期攻击趋势、全局攻击分布、Web应用系统统计、Web攻击源IP统计等，可以通过地图的形式展示国内及全球的攻击分布情况，且可以查看国内各省攻击数量、百分比及全球各国的攻击数量、百分比。支持报表的导出； 13.★支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 14.★支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 15.★需原生支持BOT防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义URL保护范围和保护阈值。 16.★支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。
3	漏洞扫描	1.标准机架式,千兆口≥8个； 2.具备丰富资产指纹库及自主研发的识别引擎，对目标资产进行多维度信息探测，支持场景下全资产盘点包括操作系统识别、中间件识别、数据库识别、开启端口与服务识别、网络设备识别、安全设备识别，须具备各类前端设备的识别能力。 3.减轻运维工作量，可基于A段、B段创建下发资产盘点任务，检测任务可发现目标范围内在线的资产，可检测到在线资产的IP地址、MAC地址、操作系统、设备类型、设备、设备型号、软件版本，并在报告中展示设备开放的高危端口； 4.具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测； 5.支持对高危漏洞提供自动化验证功能。自动化验证不需要任何人进行参与，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现； 6.可生成网络场景的专业安全检测报告(支持HTML等格式)，报告内容包括但不限于检测汇总(总体安全评级及安全风险分布、区域资产总体风险分析)、检测结果详情分析(主机资产风险、前端监控设备风险等、漏洞分类分析)、资产漏洞统计(IP、资产类型、漏洞分布、风险评级)、模拟人工渗透详细风险描述等； 7.具备高危事件预警能力，能够对最新安全事件、高危漏洞及时更新推送平台，同时资产异常情况进行实时预警通知； 8.具备边界完整性检测能力，可检测出目标设备连接智能手机热点、通过智能手机USB共享网络等违规双网卡共享外联行为，可检测出违规内联行为。 9.具备安全可视化监测大屏，7×24h监控资产状态及安全风险态势。可展示当前安全评分，前端监控设备统计，最新安全风险包括：时间、资产、风险以及风险级别。 10.集成安全漏洞验证知识库(提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库、安全设计方案知识库)。 11.在系统管理层面支持用户管理设置、可对用户操作日志进行收集、进行邮箱告警

		设置、在线问题反馈等。 12.具备与本次所投安全态势感知平台的联动能力，实现内部网络所有资产的主动脆弱性扫描发现能力，此参数需提供承诺函。
4	可信边界接入网关	1.网络吞吐量≥3Gbps，并发连接数≥100万，每秒新建连接数≥2万，千兆口≥6个； 2.支持IPSecVPN、L2TPVPN等VPN，支持主流的商业加密算法，包括：AES、DES、3DES等； 3.支持静态路由、RIPv1/2、OSPF等，支持二三层混合模式模式，可以与内网交换机进行access、trunkVLAN对接，并能够对二层流量做防火墙等功能； 4.支持隧道内地址转换，不改变原有站点地址规划，解决站点两端地址重叠问题； 5.支持Portal认证、短信(APP)认证、微信认证； 6.可以识别协议数量≥4500个通过告警、干扰、阻断等模式可提供万种以上应用规则，支持根据IP、端口、协议等自定义应用规则； 7.能够识别认证用户在各大论坛、贴吧(不限于天涯、百度等知名网站)的发帖和搜索内容、能够识别认证用户在微博搜索的内容以及下载上传文件的内容，并且可留存≥180天，以便事后溯源； 8.支持远程智能运维功能，通过“一键体检”功能，将设备和网络的指标状态以分值的形式直观展示，可查看设备状态、无线状态、安全策略、带宽策略等是否存在问题；通过“一键修复”功能，能够对体检出的相关问题，及时对网络进行优化； 9.将指定的带宽资源分配给指定服务器，实现对外发布应用的保障；手工添加基于“深度内容检测”技术的新应用协议识别规则，提供无限扩展能力； 10.支持Land、Smurf、IPSpoofing攻击防护、支持SYNFlood、ICMPFlood、UDPFlood、ARPFlood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； 11.基于内网用户流量模型和会话连接、新建连接的异常行为识别攻击，有效防护内网病毒传播、僵尸网络、木马等安全威胁； 12.为提供设备实施上线效率，设备通电之后通过即可完成设备接入，后续配置均可通过web集中管理平台远程下发，对于无专业IT人员的网点可自行上线，提高IT部署效率； 13.支持查看网关设备CPU、内存等信息、设备互联状态、用户接入情况等，能够自动生成网点拓扑，统计设备数量，及时发现用户和设备的异常，精确定位和溯源；
5	安全态势感知平台	1.标准机架式，CPU≥8核，内存≥64G，硬盘≥8T，万兆接口≥2个，千兆接口≥2，冗余电源； 2.支持网络整体安全概况的分析，包括资产等级分布(安全、低风险、中风险、高风险、已攻陷)、资产类型分布(服务器、终端、未知)、新增资产(IP地址、类型、状态、识别时间)、实时会话趋势、会话连接时长、服务端口TOP、流量趋势、攻击事件(攻击趋势、攻击类型、攻击列表)、黑客概览(地理位置分布、高频黑客TOP、攻击手段或类型)；

		3.支持多个图形化大屏实时展示界面，包括综合安全大屏、网络监控大屏、资产监控大屏、内部威胁大屏、外联威胁大屏、外部威胁大屏等； 4.支持多维度的安全威胁分析，能从外到内、内到内、内到外三个方向展开，攻击列表可显示出攻击发起方、地理位置、威胁范围、事件类型及次数等，并可以转化为攻击链分析，攻击链阶段包括：侦查追踪、武器构建、载荷投递、漏洞利用、安装植入、命令和控制、目标达成； 5.支持黑客画像分析，展示包括黑客IP地址、地理位置、威胁资产数量，攻击手段、攻击频率、攻击详情列表等； 6.支持基于深度学习算法的恶意域名/网站检测，可识别出域名地址、访问时间、访问次数、资产IP及安全状态等； 7.支持资产管理，通过流量自动化进行资产识别并生成资产列表，可针对单一资产进行网络维度和安全维度的分析。 8.支持日志检索，通过关键字进行快速查询，可查看会话日志、流量日志、攻击日志； 9.支持报表管理，系统中可进行报表的个性化设置，包括报表类型、生成周期、报表格式、邮件接收人等； 10.支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警。同时平台也支持内置安全知识库供经验沉淀。 11、支持对接同品牌可扩展检测和响应平台，开启数据上报，上报安全事件、安全告警、安全日志、HTTP/DNS数据、资产信息上报给可扩展检测和响应平台用于安全分析。 12.★支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。
6	威胁情报超融合流量探针	标准机架式，千兆口≥4； 1.为保证态势安全系统运行稳定可靠，威胁情报超融合探针需与安全态势感知平台为同一品牌； 2.采集探针吞吐量≥1Gbps； 3.支持采集探针管理，可显示接口状态、设备状态、流量趋势，支持参数配置，包括设置采集接口的分析策略； 4.具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析，能够对网络通信行为进行识别，包括但不限于：FTP行为、SMTP行为、DHCP行为、HTTP行为、DNS行为、SSL通信、SMB协议、Traceroute跟踪、文件传输，SSH行为、远程桌面等； 5.支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击，支持对webshell后门脚本上传的检测，支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露

		攻击等的检测； 6.支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析；
7	内网安全接入模块	1.千兆光口≥8，万兆光口≥2，扩展槽位≥1； 2.支持异常流量监测，支持“肉鸡”检测、支持防 IP 扫描、防 UDP 端口扫描、防 TCP 端口扫描等异常行为检测、支持连接数异常检测； 3.支持对病毒的网络层传播行为进行检测；支持对恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入分析； 4.支持与安全威胁分析平台联动实现识别终端接入 IP、MAC、端口等信息，并关联用户身份支持对病毒的网络层传播行为进行检测分析； 5.支持识别 IPC 等哑终端设备类型，并支持开启终端安全功能，只允许特定类型的设备接入网络； 6.支持与安全态势感知平台联动，实现 L2-L4 的访问控制； 7.支持与智能网络可视化系统联动，实现对横向流量默认阻断、按需放通，纵向流量按需阻断； 8.支持中文管理界面、WEB 管理接口、SNMPv1/v2/v3；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 9.要求支持 Ipv4 和 Ipv6 三层路由功能；
8	内网威胁诊断模块	1.标准机架式，千兆电口≥4 个，千兆光口≥2 个,有扩展槽，有万兆扩展接口，220V 交流电源； 2.吞吐量≥10Gbps，并发连接数≥60 万，每秒新建连接数≥1.4 万； 3.具备 IPv4\IPv6 下的基于源、目的 IP、端口、报文类型的 TCP\UDP\ICMP 攻击检测，并且用户可自定义策略修改检测阈值； 4.具备对 LAND 攻击、死亡之 ping，IP 分片重叠攻击、路由首部、TearDrop 攻击、伪首部等各种畸形包网络攻击的检测能力； 5.内置威胁确诊特征库，特征规则数量不少于 9000 条；具备系统一键修改特征级别的功能，用户可根据自身安全需求将特征内容根据流行度规则高低进行检索，并可一键修改流行度规则级别(警告、一般、严重、致命、废除)； 6.集成第三方专业防病毒的专业病毒库； 7.支持与内网安全接入模块通过智能网络可视化系统联动，针对内网安全接入模块发现的“疑似”病毒传播行为进行确诊、手动阻断； 8.★支持外发审计，可审计内容审计、ToDesk、向日葵、AnyDesk 等远程工具的文件外发行为，可审计内容审计、WinSCP、Xftp、FileZilla 等文件传输工具的文件外发行为。 9.★支持终端外联行为检查，包括：连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、否使用非法网关（可设置合法网关白名单），对不满足检查要求的终端强制断网，支

		持向管理员告警，并弹窗提示用户；
9	智能网络可视化系统	1.要求支持通过图形界面方式规划网络拓扑，并展示设备自动上线过程； 2.支持对安全设备、网络交换等网络通信设备的运行情况进行监控；监控指标应包含设备状态、Ping状态、CPU使用率、内存使用情况、网络流量等； 3.要求提供对全网设备告警的实时监控和统一浏览，提供多种提醒方式，如界面上的告警实时提醒、告警音响提示、短信告警、邮件告警等； 4.要求支持基于用户以及用户组进行网络资源编排，实现用户以及用户组和网络属性VLAN、IP网段、IP地址的绑定。简化底层网络规划； 5.可自动发现网络中的IP摄像头、打印机、一体机等设备终端并提供保护，可识别IP、MAC、接入位置、接入端口等信息； 6.要求支持关联接入策略和接入场景，用户组中的用户在不同的场景下应用相同的接入策略，并可基于时间段进行设置； 7.根据用户IP、Radius账号的上网记录等用户上网信息反查出用户IP在指定时间段内的Radius账号，如果同时存在相应的LDAP用户信息，可根据Radius账号查询出真实用户名信息； 8.提供一次接入，多次使用的无感知认证，只需要输入一次用户名/密码，后续接入无需再输入用户名/密码； 9.要求支持漫游认证，可对漫游用户在线查看和接入明细日志查询；无需终端用户输入用户名和密码； 10.支持对用户的业务异常行为、连接数异常行为等进行实时阻断及告警； 11.要求提供强大的“黑名单”管理，可以将恶意猜测密码的访客加入黑名单，并可按MAC、IP地址跟踪非法行为的来源； 12.支持识别终端类型、IP、MAC、接入端口等信息，防路由器和HUB私接，并限制单端口下接入终端数量； 13.支持基于用户设定新建速率阈值并进行监控，支持对TCP、UDP、ICMP等协议下报文速率的阈值设置，并可根据网络需求自定义防护级别，支持对SYNFlood、UDPFlood、ICMPFlood等攻击设置防护策略，支持防ARP欺骗、防ARP广播攻击； 14.支持对病毒的网络层传播行为进行溯源及阻断，防止内网病毒扩散； 15.支持防IP扫描、防UDP端口扫描、防TCP端口扫描等异常行为，支持“肉鸡”源主机的溯源及阻断，支持IP仿冒、MAC仿冒溯源与阻断； 16.支持安全日志基于时间、事件、攻击源IP、目的IP进行查询和报表导出功能； 17.支持系统日志、操作日志、安全日志收集功能，保证日志≥180天的记录和查询；
10	安全自查工具	1.提供全面的安全保障服务及配套服务工具，满足日常业务连续性保障的需求； 2.业务在面对未知的、潜在的网络安全风险之前提供渗透测试服务，确保在风险事件发生之前尽可能多的封堵安全漏洞； 3.对重要网络及网络安全设备进行专业安全巡检，确保通过频繁的巡检指标对潜在风险做提前预判和评估；

		4.业务系统在日常运行过程中，如遇突发应急故障，可以第一时间进行机动应对，结合用户的业务紧急程度和应急事件处理流程做出快速的、专业的保护工作； 5.能够提供安全检测工具，可以第一时间通过专业的手段进行资产脆弱性、威胁、风险的跟踪分析，并及时输送有效的结果； 6.业务系统上线前，对业务系统进行上线前的安全检测，全面的安全风险评估、漏洞扫描等安全检测，避免信息系统脆弱性被非法利用，增强信息系统安全防范能力，保障业务的可持续性； 7.★针对内/外网或特定业务系统及特定漏洞，基于客户业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹、钓鱼痕迹等，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助客户验证风险并推动发现的问题和隐患进行闭环处理，输出《威胁狩猎报告》。（供应商需承诺威胁狩猎频次不低于每季度一次，并且证明服务平台支持钓鱼狩猎的功能）

3.实施要求

（1）交货期要求

自合同签订之日起2个月内，中标人按照交货期的要求，分阶段制定合理的工作进度，应至少细化到周，并且应根据建设方要求进行调整和细化，要求给出时间具体安排及交货期。

投标人应就本项目提供详细的实施计划及日程安排。

（2）组织实施要求

投标人应详细说明实施本项目拟采用的团队组织方法和具体组织机构，保证在此项目实施期间足够的人力投入，并提交与项目相符的项目组人员名单、核心团队人员相关证书。

投标人实行项目负责人制，在项目验收前，不得随意更换，如需更换，须事先征得采购人同意。

中标人在进场前，在项目实施前要制定详细的项目工作方案，要对工作阶段和流程进行描述，严格按工期、参与人数、时间，制定出详尽工作方案。

（3）项目控制要求

投标人应就本项目提出明确的实施过程及其控制方法，并以此作为项目建设过程管理依据。投标人应按照质量保证体系，提出具体措施，确保项目质量。

投标人应充分认识到项目风险管理的重要性，在投标文件中必须分析识别项目中的各类风险因素，并采取相应的对策。

投标人中标后须提供相关证明材料，确保所提供产品或服务已符合招标文件、需求说明书的预定要求，系统运行正常。

（4）项目验收要求

项目验收合格需要达到以下条件：

1）按照合同约定，已完成全部软硬件安装部署、调试、培训和试运行，且试运行过程中相关问题已全部解决；

2）监理已完成对建设材料清单和内容审核，郑州市智慧气象项目网络安全系统项目建设无遗留问题。

3）已向用户提供了双方约定的全部郑州市智慧气象项目网络安全系统项目文档。

（5）项目培训要求

投标人应根据项目实际需要，向用户提供全面的网络安全培训，确保用户能够正确熟练地运用网络安全系统。培训对象包括项目建设单位信息部门人员和业务部门有关人员等。投标人应选派有实际工作和教学经验的专业人员来完成教学和辅导，根据用户实际要求，提供完整的培训计划，包括培训方式、课程内容、人数、时间、地点。

（6）项目运维要求

中标供应商应为本项目提供3年免费质保服务，自本项目竣工验收合格之日起。投标人应充分为本项目建设的运行维护措施，提供7×24小时远程服务，全年7×24小时技术支持热线服务，中标人在任何时间接到用户通知后30分钟内应做出响应，2个小时内到达现场。

（7）项目其他要求

对于招标文件没有列举的内容，但对于郑州市智慧气象项目网络安全系统必不可少的内容，投标人有责任予以补充，所需投资须包含于投标报价总价中。

本项目采购需求相关产品参数与要求，为满足采购人最低要求，投标人可以进行优化，允许投标人以不低于招标文件要求的产品或服务参与投标，允许投标人提出满足采购人实际需求更优的产品。

投标人应当在投标文件中列出完成本项目并通过验收所需的所有各项服务等全部费用。中标人必须确保整体通过采购人验收，所发生的验收费用由中标人承担。

投标人如需更详细的表述，可单项另作说明。

中标人须严格落实和遵守相关保密制度，服务过程中如出现资料、信息外泄或泄密，将追究中标人法律责任。