广州市政府采购合同

一、总　　则

第一条　合同当事人

甲方（采购人）：广州番禺职业技术学院

法定代表人：

地址：广东省广州市番禺区市良路 1342 号

乙方（中标人）：广东名科信息技术有限公司

法定代表人：陈劲

地址：广州市天河区天慧路 16 号 301 房自编之 15

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及广州公共资源交易中心“2022 年广州番禺职业技术学院信息化建设项目（双高）-网络安全防护及学生服务中心大楼网络系统项目子项目 1”（项目编号：CZ2022-3134）招标文件的要求和招标结果，经甲乙双方协商一致，签订本合同。双方共同遵守如下条款（其他有关合同项目的特定信息由合同附件予以说明，合同附件及本项目的招标文件、投标文件、中标通知书、在实施过程中双方共同签署的补充文件等均为本合同不可分割之一部分）。

二、合同标的

第二条　乙方根据甲方要求提供以下货物：

货物品名	规格型号	单位	数量	单价（元）	总价（元）	随机配件
网络入侵防护系统	NIPS NX5-HD4500	台	1	¥478,800.00	¥478,800.00	/
动态应用保护系统	AP-5200 一体机	台	1	¥522,000.00	¥522,000.00	
云安全监测系统	青藤主机自适应安全平台 V3.0	台	1	¥411,600.00	¥411,600.00	
数据备份与恢复管理系统	AB2000	台	1	¥494,400.0	¥494,400.0	

合计人民币（大写） 壹佰玖拾万零陆仟捌佰元整（￥1,906,800.00元）

产品参数详见附件1

三、质　　量

第三条 货物质量

（一） 乙方应提供原装、全新的、符合国家质量标准的设备，并随设备提供有关设备安装、调试、使用、维修和保养所需的足够的中文技术文件（包括但不限于说明书、图纸、手册、技术资料和关键配套件清单等）。

乙方保证其供货渠道合法，在本合同签订之前，乙方应向甲方提供核心产品的生产企业出具的供货确认函原件、售后服务承诺函原件、货物出厂合格证及生产企业有效授权函原件等证明材料，并提供一份复印件交由甲方存档备查。

（二） 本合同涉及纳入《国家强制性产品认证目录》内的产品，乙方须提供3C认证证书。

（三） 货物质量出现问题的，乙方应负责三包（包修、包换、包退），费用由乙方负责。

（四） 货到现场并验收合格后，由于甲方保管不当造成的质量问题，乙方亦应负责修理，但费用由甲方负担。

四、交货与验收

第四条 交货、安装、调试、验收必须在合同签订后 20 个工作日内完成（期间如遇寒、暑假工期顺延）。

第五条 交货地点：广州番禺职业技术学院指定地点。

第六条 甲方及甲方聘请的监理将依据市信息主管部门立项审核意见、市财政局批复文件、招标文件和合同等文件，按照《广州市财政投资信息化建设项目验收规范》及相关标准规定对货物进行验收。货物验收时若乙方不参与现场验收，则视为同意甲方验收结果，验收合格的，甲方按合同要求办理付款手续；验收不合格的，甲方或由甲方聘请的监理单位书面反馈验收情况及处理意见给乙方。产品若有国家标准按照国家标准验收，若无国家标准按行业标准验收，为原制造商制造的全新产品，整体无污染、无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用，同时符合本合同约定的质量要求。产品规格、型号、技术参数、产地须与合同、招标文件规定一致，若出现不符，乙方应及时办理退换货并负责负担全部费用及由此给甲方造成的全部损失。

本项目验收分为校内验收、合同验收两部分：

1、校内验收：由校内外专家组成的专家组负责，项目监理、计划财务处、项目实施部门负责对整个验收过程进行监督。项目承建单位负责准备所有验收所需文档（含电子版），并进行建设汇报和功能演示。专家组验收后必须出具验收意见，对不能通过验收的项目，须出具整改报告。

2、合同验收：在完成校内验收，试运行满三个月后，乙方须完善项目遗留的问题和各项整改工作，通过并提交符合甲方上级相关主管部门终验要求的各类文档，由监理单位审核通过并出具文档审核报告。合同验收具体标准以甲方上级相关主管部门发布的验收规定为准。

第七条 乙方承诺，本项目将按甲方上级相关主管部门要求，在合同验收前通过由学校招标确定的第三方测评机构的验收测评及安全评估，相关验收标准以主管部门要求为准。

上述验收均合格后，视为乙方完成交付。

第八条 乙方应将所提供货物的装箱清单、用户手册、原厂保修卡、随机资料及配件、随机工具等交付给甲方；乙方不能完整交付货物及本合同约定的单证和工具的，视为未按合同约定供货，乙方必须负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。

五、合同金额及付款方式

第九条 合同金额

本合同金额为人民币（大写）壹佰玖拾万零陆仟捌佰元整（￥1,906,800.00元）。该合同总价是货物设计、制造、包装、运输、安装、调试、检测、培训、技术服务及验收合格之前及质保期内服务及备品备件发生的所有含税费用。本合同执行期间合同总价不变。

第十条 付款方式

支付比例100%，

1.签署合同生效且财政资金到位后20个工作日内，甲方支付给乙方合同总价的40%；即人民币（大写）柒拾陆万贰仟柒佰贰拾元整（￥762,720.00元）。

2.货物全部到场齐全，经用户及监理单位现场清点确认合格后，甲方支付给乙方合同总价的40%；即人民币（大写）柒拾陆万贰仟柒佰贰拾元整（￥762,720.00元）

3.货物及系统软件安装调试完毕，试运行期满，且项目通过验收测评和校内验收后，甲方支付给乙方合同总价的15%； 即人民币（大写）贰拾捌万陆仟零贰拾元整

（￥286,020.00元）。

4.项目通过安全评估，且合同验收合格后甲方支付合同总价的5%给乙方。即人民币（大写）玖万伍仟叁佰肆拾元整（￥95,340.00元）。

5.以上款项在乙方提交付款申请（首期款无须申请）及相应发票并由甲方监理单位审核确认后启动办理支付程序，乙方逾期交付发票或所开具的发票不符合约定的，甲方有权延期支付相应费用并不视为违约。。

甲方使用的是财政资金，故甲方向财政主管部门完成支付材料的提交即视为完成支付手续，具体款项支付时间视财局资金到位情况而定。由于财政资金拨款导致付款迟延的，不视为甲方违约。

六、售后服务

第十一条 乙方需提供售后的技术服务支持，保证甲方顺利使用所购货物，具体售后服务包括但不限于提供设备的安装、调试、检验等；根据甲方需求提供不少于2天的技术培训等。乙方需提供原装、全新的、符合国家质量标准的设备、设备使用说明书和关键配套件清单；向甲方提供有关设备的安装、调试、使用、维修和保养所需的足够的中文技术文件（图纸、手册和技术资料）。

第十二条 乙方应为甲方提供货物的质量保证期限（以下简称“质保期”），质保期自甲方完成合同验收之日起计算，硬件设备质量保证期为3年。质保期内系统软件升级、运维和硬件的维护属于免费服务范围，乙方不得另行收费。质保期后的货物维护由双方协商再定。

第十三条 质保期内，乙方负责对其提供的货物实行包修、包换、包退、包维护保养，不再收取任何费用，但不可抗力（如火灾、雷击等）造成的故障除外。

第十四条 乙方所提供的售后服务应及时有效。乙方承诺，在广州市内设有维修服务点并提供电话服务热线，其工作人员在接到维修电话，保证在接到故障电话后5个工作日排除故障如乙方未按照合同约定提供保修等售后服务的，甲方有权自行或聘请第三方服务，并有权要求乙方赔偿因此给甲方造成的一切费用和损失。

第十五条 乙方货物的销售人员需持有相应的培训证书。乙方应设专业的售后服务中心，同时能够提供常用耗材及配件的及时供应，提供维修服务的维修工程师需持有相应产品的维修授权证书。

第十六条 甲方将聘请项目监理单位，协助对本项目建设进行监督。乙方必须接受甲方及甲方聘请的监理对本项目的管理和监督，及时向甲方及监理同时提交各种设计方案、

实施方案、报告等项目文档。对于监理对本项目实施过程中指出的问题，应该积极给与答复并解决。对于监理提出的合理的整改要求，积极限期完成整改。

第十七条 在质保期内，乙方须对所提供的设备做定期检查和保养。乙方人员应遵守甲方的各项规章制度，不得影响甲方的正常管理秩序。乙方人员在甲方范围内发生事故或因乙方、乙方人员过错导致的一切人身损害或财产损失，乙方应妥善处理纠纷并承担全部赔偿责任（包括但不限于赔偿甲方因此支出的赔偿金/和解款、诉讼费/仲裁费、律师费等）。

七、违约责任

第十八条 甲方无正当理由拒收货物的，甲方须向乙方交纳合同总价 5 %的违约金。如甲方无故变更、中止或者终止本合同的，应当对乙方受到的损失予以赔偿或补偿。

第十九条 甲方无故逾期支付货款的，甲方须每日以欠款总额 3 ‰的标准向乙方交纳违约金。

第二十条 乙方逾期交付货物的，乙方须每日以逾期交货部分货款总额 3 ‰的标准向甲方交纳违约金。逾期交货超过30天，视为乙方不能交付货物，须向甲方交纳合同总价1%的违约金。同时甲方有权单方解除本合同，并要求乙方赔偿由此造成的一切损失（包括但不限于直接损失、诉讼费/仲裁费、律师费等）。

第二十一条 如乙方未按照合同约定履行义务，包括但不限于所交付产品的型号、规格、数量和质量不符合甲方要求等，甲方有权拒收；乙方提供的产品若经甲方或甲方聘请的第三方机构检查认定后，如检查认定产品质量不符合合同规定标准，达不到约定技术条件的，则视为乙方没有按时交付而违约，乙方须在规定的时间内无条件更换合格的产品给甲方，若乙方拒不更换或更换后仍不符合甲方要求的，则视为乙方不能交付产品而违约，甲方有权单方解除本合同，不予支付相应费用，并有权要求乙方按照合同总价的 5 %支付违约金及赔偿损失（包括但不限于直接损失、诉讼费/仲裁费、律师费等），并须全额退还甲方已经付给乙方的货款及其利息。

第二十二条 乙方所供货物必须权属清楚，不得侵害他人的知识产权，否则构成对甲方违约。如甲方因此遭受到第三方索赔、诉讼或任何权利请求的，乙方应妥善处理纠纷，并承担全部赔偿责任（包括但不限于赔偿甲方因此支出的赔偿金/和解款、诉讼费/仲裁费、律师费、差旅费等）。

第二十三条 由于政策的变化或不可抗力的原因导致项目停工，使合同无法继续履行的，视为项目终止。项目终止后，乙方应妥善做好已完成项目的保护和移交、质保工作，甲方按合同条款支付已完成工作量的价款。

八、不可抗力

第二十四条 由于不可预见、不可避免、不可克服等不可抗力的原因，一方不能履行合同义务的，应当在不可抗力发生之日起 7 天内以书面形式通知对方，证明不可抗力事件的存在。

第二十五条 不可抗力事件发生后，甲方和乙方应当积极寻求以合理的方式履行本合同。如不可抗力无法消除，致使合同目的无法实现的，双方均有权解除合同，且均不互相索赔。

九、争议解决办法及通知送达

第二十六条 因货物的质量问题发生争议，由广州市市场监督管理局或其指定的质量鉴定单位进行质量鉴定。货物符合质量标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

第二十七条 本合同发生争议，由双方协商或由政府采购监管部门调解解决，协商或调解不成时按以下第 2 种方式解决：

1. 中国广州仲裁委员会仲裁；
2. 向甲方所在地人民法院提起诉讼。

第二十八条 任何一方因履行本合同而相互发出或者提供的所有通知、文件、材料，均以本合同所列明的地址送达，一方迁址或者变更联系方式的，应提前三日书面通知对方。否则，因联系方式错误致使无法送达而造成的不利后果均由未通知方承担。（甲方联络人：钟煜明，13416163808；乙方联络人：张杰，13560315380）

十、其　　他

第二十九条 本合同一式 捌 份，甲方执 伍 份，乙方执 叁 份，具有同等法律效力。合同自双方签字盖章之日起生效。

第三十条 本合同未尽事宜，由双方协商处理。

（以下无正文）

甲方：（盖章）广州番禺职业技术学院	乙方：（盖章）广东名科信息技术有限公司
签约代表：	签约代表：
地　　址：广州市番禺区沙湾市良路 1342 号	地　　址：广州市天河区天慧路 16 号 301 房自编之 15-1
开户银行：	开户银行：长沙银行股份有限公司广州黄埔支行
银行账号：	银行账号：810000297738688888
电　　话：020-84736666	电　　话：020-85577703
传　　真：020-84736785	传　　真：020-62619247
签约日期：2022年 6月 21日	签约日期：2022年 6月 7日

附件清单1

序号	货物名称	规格型号	品牌	产地	制造商名称	单价	数量	单位	总价
1	网络入侵防护系统	型号：NIPS NX5-HD4500 1.系统应为机架式独立IPS硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠。 2.★系统提供1个RJ45串口，2个1000M管理口，4万兆SFPP接口，含2个万兆SFPP模块，1TSATA硬盘，应用层防护吞吐量4Gbps，TCP最大会话数：400万，每秒新增会话：120000，时延小于40us 3.系统提供覆盖广泛的攻击特征库，能够针对9000以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。系统携带的攻击特征库须获得CVE-Compatible兼容性认证，提供入侵规则数量和CVE认证，已提供相关的截图。 4.支持完善的漏洞攻击防御库，应支持定期漏洞收集和挖掘升级能力。 5.系统提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测和阻断。支持基于SCADA等工控协议的相关漏洞攻击检测。 6.支持针对隔离列表进行解除隔离操作。支持对单条或多条被隔离IP执行解除隔离操作；支持隔离列表展示功能。能够展示所有被隔离的IP，和开始隔离时间、结束隔离时间。 7.支持在传输层对攻击进行识别检测，对接收的到的数据进行解码和过滤，得到第二层数据；在应用层对第二数据进行解码，得到第三数据；在应用层对所述第三数据进行会话流重组，得到第四数据；在应用层对所述第四数据进行检测。设备包括：传输层处理模块，应用层解码模块，会话重组模块和检测模块。通过在传输层对数据包进行解码和过滤，在应用	绿盟	北京	绿盟科技集团股份有限公司	¥478,800.00	1	台	¥478,800.00

		层对数据包进行会话流重组，减少额处理的数据量，从而提高了入侵检测的有效性和准确性，已提供国家权威机构（如中国信息安全测评中心、中国网络安全审查技术与认证中心、国家知识产权局）颁发的相关证明截图。 8.系统提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为，系统提供敏感数据外发的防护功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）。 9.系统提供关键文件外发防护功能，能够识别通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，音频视频类如MP3、AVI、MKV、MP4、MPEG、WMV等，脚本类如BAT、CMD、WSF等，程序类如APK、DLL、EXE、JAVA_CLASS等，已提供界面截图。 10.系统提供URL分类库，提供中英文网页过滤数据库，实现高风险、不良网站过滤，支持联动云端威胁情报中心，在日志界面点击威胁IP后，可以直接跳转至云端查看IP的详细信息。 11.系统支持实时获取安全事件攻击源的详细信息，包括host、地理位置、端口开放、历史攻击情况等，支持僵尸网络防护、恶意URL访问防护及文件信誉防护，支持配置文件信誉检测白名单。 12.支持提供恶意软件分析服务，支持联动本地沙箱和云端沙箱，对未知可疑文件文件进行分析，并对高危的文件进行拦截，将分析的结果进行统计展示，已提供相关截图证明。 13.设备界面支持反馈厂商的功能，能够实现将抓包的情况，通过界面一键反馈给厂商的运营中心，实现误报							

		的及时性处理，已提供界面截图证明。 14.支持识别某IP上登录的用户并将用户名关联在该IP触发的安全事件上；用户信息来源包括：邮件用户、文件传输、即时通信用户、远程登录用户、网站登录用户、数据库用户等。已提供界面截图证明。 15.系统提供多种升级方式，提供自动在线升级、离线升级两种方式，系统支持版本恢复功能，可恢复到出厂时自带的软件版本。 16.系统提供基于资产的保护，具备资产识别功能，包括操作系统、浏览器、应用类型等客户资产相关信息的识别能力，系统应能识别主流的应用程序，识别种类不少于2500种，已提供功能界面截图。 17.系统支持“一键巡检”功能，可根据设备运行过程中反馈的数据进行全面分析，并生成图表相结合的安全报告。定时进行巡检可发现异常漏洞与受攻击情况。 18.投标IPS产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，已提供有效证书的复印件。							
2	动态应用保护系统	型号：AP-5200一体机 1.★提供4个千兆电口模块、2个万兆单模模块，CPU：20核，内存：32GB，硬盘：1TB，电源：双冗余电源。 2.★网络吞吐量：3Gbps，并发TCP会话数：500万，每秒新建http请求数：9000，TPS处理性能：6000。 3.保护系统支持Cookie令牌和URL令牌，通过对当前访问页面内的合法请求授予在一定时间内有效的一次性令牌，防止攻击者发出非法请求，有效抵御越权访问、网页后门及重放攻击等恶意行为。已提供功能界面或验证效果截图。 4.对网页中的表单做动态封装，每次封装的内容均不相同，让攻击者无法直接通过查看网页源代码获取表单	瑞数	上海	瑞数信息技术（上海）有限公司	¥522,000.00	1	台	¥522,000.00

		等内容，从而无法预测服务器的行为，大幅提升攻击难度。已提供功能界面或验证效果截图。 5.支持ajax请求内容与响应内容动态混淆，即对ajax请求内容和响应内容进行动态变换，将重要信息从明文的形式转化为毫无规律的乱码。提供功能界面或验证效果截图。 6.可收集客户端浏览器信息，为每个客户端生成唯一的指纹标识，该标识具有一定的稳定性，在清理浏览器cookie、浏览器本地存储、访问记录、更换IP地址时指纹均不变化。提供功能界面或验证效果截图。 7.可防止攻击者重放先前的交易内容，形成虚假交易或破坏后台数据的完整性。 8.支持通过对可攻击点的动态隐藏，自动化工具无法获得攻击入口，可有效防止各类已知与未知漏洞的自动化扫描工具。 9.可以基于客户端的运行时环境特征数据实现拦截，包括：客户端指纹User-Agent、IP、是否为ajax请求、浏览器真实内核，实现针对性拦截。 10.考虑与现有网络环境的兼容性要求，支持处理IPv6或IPv6/v4双栈流量。 11.支持自动删除网页HTML代码中的注释内容，防止攻击者通过注释获取敏感信息，从而发起攻击。已提供功能界面或验证效果截图。 12.支持用户行为拦截：可以基于客户端的真人行为数据实现拦截，包括但不限于：键盘输入的次数、鼠标移动的次数、鼠标点击的次数等。针对这些指标可通过AND OR 的方式任意组合，实现针对性拦截。 13.支持防止攻击者通过自动化程序，暴力破解或猜测敏感数据。 14.可防止攻击者通过爬虫或自动化工具，搜刮服务器上的数据或敏感信息。 15.支持通过混淆技术对中间人攻击							

		进行防护，防止窃听、篡改交易数据等中间人攻击行为。提供功能界面或验证效果截图。 16.支持对水平越权攻击行为的防护。提供功能界面或验证效果截图。 17.支持识别WebDriver自动化工具。提供功能界面或验证效果截图。 18.具备采集业务数据的能力，支持对采集的关键业务数据进行配置。已提供功能界面或验证效果截图。 19.可自动识别被保护网站原站Cookie，对网站下发到客户端的Cookie进行混淆，避免信息泄漏，达到防护的效果。 20.具备业务数据采集能力，可采集用户全部Cookie内容，可提取重点关注的Cookie字段值，并且可在报表中进行查看。 21.Web管理页面支持网络抓包功能，可配置抓包条件并且可在管理页面直接下载抓包文件。已提供功能界面或验证效果截图。 22.为防止攻击者利用浏览器自带的开发者工具，对网页的HTML、JS代码进行调试，达到篡改、伪造数据等其他攻击目的。应具备反调试机制，可以检测并阻止利用浏览器开发者工具的使用。已提供功能界面或验证效果截图。 23.支持APP程序和Web应用统一管理：动态安全防护系统可以实现APP程序（包括微信小程序）和Web网站的统一防护和管理。已提供功能界面或验证效果截图。 24.提供的动态应用保护系统支持采用透明部署、基于NG的插件化部署、反向代理模式部署架构，可有效过滤与防护应用服务器的流量。 25.提供网站访问情况的图表化视图，图表内容包括请求访问流量时间表、响应流量时间表，HTTP响应状态码排名。 26.提供访问客户端的统计图表化视图，图表内容包括客户端的IP地址、								

		访问来源国家和城市、referrer信息、访问路径排名，Host排名，User Agent排名、客户端操作系统类型和浏览器类型。 27.提供网站的攻击工具名称排名、攻击来源、攻击数量、攻击类型、攻击数据详情内容报表。 28.提供集群和高可用性功能，内容包括群集各节点的ID、IP、状态、角色及版本等信息 29.对指定的请求网址不检查动态令牌，通常用于静态资源或指定入口。支持请求白名单配置界面、配置界面包含请求白名单、注释、操作等功能。支持批量编辑功能。 30.对指定请求地址的响应内容不进行动态封装，通常用于静态页面或非关键页面。响应白名单配置界面、配置界面需包含响应白名单、注释、操作等功能。 31.对于指定的来源IP地址进行透传，不进行任何防护，通常用于指定内部漏洞扫描器的地址。支持IP白名单配置界面、配置界面需包含类型、IP、子网掩码、备注等功能。支持批量编辑功能。 32.包含防护日志、操作审计日志及系统日志，包含时间、访问网址、来源IP地址、过滤规则及规则细节等，可通过TCP或UDP协议，将日志输出到指定的Syslog服务器，可自动化对日志进行归档及磁盘空间管理。 33.产品通过国家权威机构（如：公安部或工信部）检测。已提供检测报告关键页复印件 34.产品获得IPv6 Ready Go认证证书。已提供证书复印件。 35.产品具备国家信息安全漏洞库兼容性资质证书（中国信息安全测评中心）。已提供证书复印件。							
3	云安全监测系统	型号：青藤主机自适应安全平台V3.0 1.★系统架构与部署方式：采用Agent-Server架构，支持通过B/S管理方式对每个主机进行集中管理，提	青藤	北京	北京升鑫网络科技	¥411,600.00	1	台	¥411,600.00

		供300个主机授权数。 2.操作系统支持：支持常见windows service操作系统，支持常见Linux操作系统：Oracle：5、6、7；RHEL：5、6、7；CentOS：5-8；Ubuntu：10-19；SUSE：10-15；Debian：6-10；OpenSUSE：11-15；，支持常见国产操作系统：NeoKylin：6、7（中标麒麟）；YHKylin4（银河麒麟）；Redflag9（红旗）；Deepin15（深度）；iSoft4（普华），euler V2（欧拉），bc_linux（大云） 3.★安全性与稳定性：客户端占用内存资源应不超过100MB，CPU单核使用率不超过50%，综合使用率不超过5%，客户端不得修改服务器操作系统内核或驱动，并禁止采用抓包技术，安装时不影响业务正常运行，安装卸载无需重启系统。客户端具有自动降级与自杀机制，来保证业务连续性要求。 4.权限管理：系统具备三权分立，支持根据用户类别划分角色和权限，支持设置每个账户管理不同的主机与功能，账号支持与LDAP和AD进行对接，账号应支持OTP 二次验证。已提供功能截图证明。 5.★客户端安装：应支持通过命令行方式进行安装客户（linux、windows） 6.主机管理：支持批量导入资产等级、负责人、负责人邮箱、机房位置、固定资产编号、标签、备注等主机信息。Agent监控：支持通过平台查看Agent的状态，并可随时调整Agent运行模式，导出Agent运行日志与报表，随时分析解决问题。主机发现：支持通过ARP、PING、NMAP等扫描方式发现网络内没有安装客户端Agent的主机信息，为防止网络扫描拥堵，扫描时应允许控制扫描速率，包括并发扫描数量，每秒最大发包数量，每次下发间隔。 7.支持实时清点主机基础信息，监控主机状态，并提供自定义主机分组、			有限公司				

		操作系统、业务进程、安全插件等各种管理维度的主机统计，提供进程信息快照，展示进程各维度的信息，对root权限，僵尸进程，IO waiting进程，非包安装进程，唯一进程进行分析统计，帮助发现问题进程。提供系统端口快照，以进程+端口展示服务分布情况，并检查是否存在对外的端口。 8.支持自动化清点账号数据，快速分析系统当前正在使用的账号；应清点如下账号信息，账号名，UID，GID，登录方式，账号状态，Home目录，Shel、账号最近登录时间、登录终端，账号到期时间、密码修改时间、密码到期天数、密码到期告警天数、密码锁定天数、是否sudo权限，是否root权限等信息 9.支持系统硬件配置清理，包括系统内核，CPU,内存，网卡，设备型号，硬盘，磁盘使用分布等各类硬件信息。 10.支持清点系统的所有常见应用的使用情况，方便运维人员从业务维度分析使用情况，已覆盖系统架构，Web运维，运维工具，数据库，系统应用，安全应用等绝大部分常见应用。支持清点服务器中运行各类常见Web中间件，包括：Nginx，Apache，Jboss，Tomcat，Weblogic，Jetty等。 11.支持清点服务器中的业务数据库，覆盖多种常用类型及大数据分布式数据库，包括：MySQL，Redis，MongoDB，Oracle、MemCache，PostgreSQL，Hbase、DB2、Sybase、TiDB等。 12.支持自动清点Web服务中运行的Web站点，并域名维度分析系统的Web业务情况，梳理对外，root权限，777权限的站点，提醒运维人员优化站点配置。 13.支持清点Web站点中使用的Web框架，包括java框架语言、python框架语言和php框架语言。已覆盖绝							

		大部分主流的Java框架，例如spring，struct，structs2，hibernate各类框架。 14.支持自动清点Web应用中的插件信息，包括插件名称、版本、描述、插件官网链接等。 15.清点的Web站点信息中包含该站点的所有虚拟目录，以确保所有Web目录被监控，目录应清点如下信息：目录虚拟路径，物理路径，文件所有者，文件所属组，文件权限。 16.支持清点Windows系统中包含的根证书颁发机构、受信任证书信息，当无法确定一个程序是否合法，可查询此处信息辅助参考，至少应包括，签名信息，颁发者，指纹，证书路径，有效期。提供截图证明。 17.支持通过自定义应用指纹，识别自研应用或未支持清点应用。支持自动化采集每台服务器上的计划任务、环境变量等信息。 18.风险扫描任务开始后，支持展示整个扫描过程，即使显示扫描结果，展示风险问题数量，影响的主机数量等各类信息；扫描完成后应展示当前结果的更新时间。 19.支持使用POC验证的方式检测上百余种高危漏洞，同时提供自定义检测功能，并对高危漏洞爆发事件提供快速应急响应支持。支持对安全补丁进行周期性自动检测，并提供详细补丁说明，修复方案及其修复影响，且支持支持自定义填写用户修复建议。 20.支持统计近7天、30天、3个月的补丁修复统计、危险程度分布、平均修复时长、统计补丁总数趋势，可按业务组展示补丁修复情况，可按修复时长展示补丁修复情况。已提供截图证明。 21.支持对linux 、windows 系统账号进行弱密码检测，支持自定义弱密码字典的检测。对linux 上的常用应用进行弱密码检测，例如mysql、redis、vsftpd等，检测弱密码默认							

		应隐藏密码值，支持手动打开，查看明文密码值。 22.支持自定义组合密码，允许按照前缀，中缀，后缀模式分别定义字典，自动组合计算弱密码组合，自定义组合密码，用户名与空字符将自动作为任意部分的组合条件，加入检测。 23.支持检测 linux 上由于系统配置的产生的安全风险，例如检测路由转发功能是否开启、检测网卡是否处于混杂模式、检测 grub 密码设置。 24.支持检测 Linux 的黑客关键攻击路径上常用应用的配置型风险，支持的应用有：SSH、redis、Memcache、MongoDB、Apache 等。 25.支持实时发现暴力破解行为，支持 Linux 和 windows 系统暴力破解，以及 VSFTPD、WINRM 等多种服务，并支持自动封堵。 26.支持实时的对在异常 IP 所属区域，异常时间，异常 IP 等异常登录行为的识别，以及支持检查主机环境中的登录日志配置是否正常，防止部分功能没有生效。 27. 支持实时监控主机上所有利用 Shell 进行反向连接的行为并告警，可单独设置是否上报内网反弹行为。 28. 支持实时监控用户以低权限进入主机，之后通过某种行为获得高权限的事件。支持实时检测服务器存在的系统及应用后门并产生告警。包括 Linux 下的 Rootkit、 Bootkit，还有 Windows 下的可疑进程、可疑线等多种后门。 29.支持对主机 Web 目录或着自定义目录下的文件内容监控，提供实时检测和立即检查的方式来发现后门，并支持多种检测引擎。用户可以查看和处理发现的Web后门,还能够查看Web后门的具体文件信息并下载后门文件。 30.支持记录主机上执行的 shell 命令，实时监控被审计规则判断为危险的操作，并发送邮件通知。用户可以							

		查看操作并对操作进行审核，也可以对审计规则的按自己的需求进行配置。 31.支持对主机实时监控进程的异常命令执行行为，对于符合WebRCE特征的行为进行实时告警，并提供进程执行的详细进程树信息，且支持批量配置白名单规则，批量按照连接进程名、进程命令行、进程树、适用主机范围加入白名单。其中进程命令行应支持正则表达式 32.系统安全基线应覆盖Ubuntu、Debian、CentOS、Oracle Linux、Red Hat Enterprise Linux、Suse Linux、中标麒麟；支持系统安全基线Windows2008/2012/2016/2019，等主流Windows系统 33.支持对Apache、Ngnix、Tomcat、Jboss、Resin、WebSphere、Weblogic等应用等保、CIS基线的检测。 34.支持对Mysql、MongoDB、Oracle、DB2、informix 等数据库等保、CIS基线的检测。							
4	数据备份与恢复管理系统	型号：AB2000 1.硬件模块：2U机箱，12盘位，2颗至强10核CPU,**480GB*2** 企业级SSD，标配**256GB内存**，标配裸容量**80TB** SATA 7200转企业级硬盘，**2个800W双冗余电源，4个板载千兆** GE + **2个 10GE 光口（含光模块）**。 2.支持集群式架构，可实现不限制数量不限制CPU的节点部署，不限Windows和Linux的客户端类型和数量，不限制主流数据库类型和数量，不限制虚拟化平台的类型和数量，如Oracle、MySQL、SQL Server、文件系统、VMware、FusionSphere等。 **3.配置1个永久增量备份代理用于支持对备份数据进行永久增量备份。配置1个CDP持续数据保护场地授权代理，不限制使用此特性的客户端数量。配置32TB定时备份后端容量许可。** **4.包含原厂三年维保服务、三年硬件**	爱数	上海	上海爱数信息技术股份有限公司	¥494,400.00	1	台	¥494,400.00

		质保服务、一年金牌服务。							