询比价函

各报价单位：

为保证[POWERCHINA-0403-240033]中国电建北京华科软科技有限公司顺德区水智慧管控工程数据机房（安全资源池）项目的真实性、防止围标、串标行为的发生，降低投标、履约过程中风险的需要，我司拟采用公开询比价采购方式进行下列产品的采购。现以公开询比价采购方式对项目中涉及的云安全管理平台（信创版）-平台模块、管理模块、基础运行环境模块、运营模块、安全组件通用授权许可模块、日志审计、堡垒机、数据库审计-实例 1、数据库审计-实例 2、防火墙、WAF、漏洞扫描、主机安全（EDR）以及对应的开发及实施服务进行正式询比价。

一．供应商资格要求

本次招标要求投标人的资质、业绩、项目主要负责人须满足下述要求，并在人员、业绩、设备、资金等方面须具有相应能力。

1.供应商具有订立合同的权利,且通过 ISO14001 环境管理体系认证、ISO45001 职业健康安全管理体系认证、 ISO9001 质量管理体系认证。

2.资质要求:供应商应具有 ISO 20000 信息技术服务管理体系认证证书;CMMI3 级或以上资质；系统集成相关资质。

3. 业绩要求：对供应商的业绩要求：近五年须完成至少 2 个金额 500 万元及以上的系统集成类相关案例，须提供业绩合同关键页扫描件。

4.供应商应具有质量控制、经营管理能力，能够独力承担项目的实施能力，具备良好的售后服 务体系，不接受联合体投标，不允许分包转包。

5.供应商近三年没有处于被责令停业、财产被接管、冻结、破产状态，无采取非法手段谋取不 正当利益的违法、违纪不良记录。未被列入政府采购失信名单，未被“信用中国”网站列入失信 被执行人、重大税收违法案件当事人。

5.本次 不接受 (接受或不接受)联合体投标。

6.供应商不为中国电力建设集团(股份) 有限公司的禁入供应商。

二．货物清单及技术要求

1.采购范围（货物清单）

序号	设备名称	对应设备维保技术支持服务内容描述	数量

1	云安全管理平台（信创版）-平台模块	云安全管理平台（信创版）-基础平台模块	1 套
2	管理模块	管理模块，按照平台管理员及云租户两大视角提供租户管理、安全组件管理等	1 个
3	基础运行环境模块	云安全管理平台基础运行环境模块（ARM 分布式存储版），适用于底层服务器为鲲鹏、飞腾的场景	1 个
4	运营模块	安全运营分析等管理功能	1 个
5	系统授权模块	云安全管理平台（信创版）-银河麒麟 V10 操作系统授权模块	28 套
6	安全组件通用授权许可模块	云安全管理平台（信创版）-安全组件通用授权许可模块，支持激活云内所有类别的安全组件，具体包括： 本地 SaaS 类：CNWAF、网站监测、漏洞扫描、主机安全、网页防篡改、堡垒机 专享镜像类：日志审计、数据库审计、堡垒机、WAF、综合漏洞扫描、主机安全、网页防篡改、APT、防火墙	1 个
7	日志审计	支持 20 个日志源	3 个
8	堡垒机	支持 20 资产管理，20 并发字符	3 个
9	数据库审计-实例 1	支持 4 个数据库实例，4000TPS（2 套每套用 3 个许可）	6 个

10	数据库审计-实例 2	支持 8 数据库实例，16000TPS（1 套每套 4 个许可）	4 个
11	防火墙	500M 吞吐量，包含 FW/IPS/AV 模块；	3 个
12	WAF	防护流量 50Mbps，HTTP 最大并发连接数 50000，HTTP 最大新建数 5000（3 个许可）	3 个
13	漏洞扫描	支持网站、系统、数据库、基线扫描，每个模块支持 20 个 IP 地址	3 个
14	主机安全（EDR）	33 个服务器 EDR（预计占用 3 个许可）	3 个

15	开发服务	通过云管理平台单点登录后，点击安全菜单链接会请求云平台的接口，云平台请求云资源安全管控平台接口获取URL，重定向进入云资源安全管控平台管理平台，云资源安全管控平台admin账户登录创建安全实例分配给租户，然后租户在云资源安全管控平台分配给子用户，初始，云平台侧机房需要划分IP段和VLAN ID给云资源安全管控平台，云资源安全管控平台自己内部实现通过不同的IP段去给租户创建安全实例。具体对接开发包含： 1.用户同步 云平台在创建(删除，更新)用户后，会调用云平台接口，云平台再调用云资源安全管控平台的接口去创建(删除，更新)用户，租户下，有租管和子用户角色。 2.单点登录 使用标准的单点登录方案，通过云平台单点登录到云资源安全管控平台页面。 4.注销 云平台登出后，会调用云管平台的注销，云平台调用云资源安全管控平台的注销接口。 *5.网络 云平台机房侧提前分配租户网	1项

		段和 VLAN ID 给云资源安全管控平台，云资源安全管控平台使用该网段和 VLAN ID，人为约定使用方式，比如默认*.1 的网络是网关，云资源安全管控平台内部完成安全实例网络参数配置(包含 IP,VLAN ID 等)。	
16	安全平台实施服务	提供云安全管理平台实施服务，包括规划设计服务、系统部署与调测服务、验收测试服务等。	1 套

2. 技术要求

云安全服务平台要求

标功能	规格要求
	必须与云平台松耦合，便于适应多厂商云平台，不能在云平台内部以虚

署方式	拟机的方式安装安全产品，不能采用网络设备硬件一虚多的方式，降低扩展性。
	必须支持在主流 ARM 架构的芯片上运行，包括华为鲲鹏 920 系列等，支持在主流的国产化麒麟操作系统上运行；
件规格	组件数量：本次共提供 7 个安全组件的授权，组件内容包括安全组件包含:日志审计、堡垒机、数据库审计、防火墙、WAF、漏洞扫描、主机安全(EDR)。
务方式	租户侧界面必须支持安全组件自运维功能；支持在首页整体展示全部业务系统的风险状态，包括业务风险分布、风险业务 TOP5、安全事件列表（包括失陷事件、攻击事件和漏洞事件）等。
	平台侧界面支持安全组件分配功能，管理员可直接为各个租户分配安全资源，同时完成关键安全资源的策略初始化。
统管理	支持租户安全资源的服务链配置，通过灵活选择源、安全服务节点和目的，完成安全路径的自定义，安全服务节点的先后顺序可灵活调整。（需提供产品界面截图，并加盖厂商公章）
	★支持展示模式和排障模式两种形态的安全架构页面，方便运维人员在全局展示和故障排查之间快速切换。（需提供产品界面截图，并加盖厂商公章）
全运营	★支持基于云平台整体视角的安全运营中心，能够统一监测和收集各租户的安全事件，从租户维度实现安全风险统一管理，并且能够通过大屏进行投放，展示安全资源池的运营情况，及租户的安全建设情况。（需提供产品界面截图，并加盖厂商公章）
	支持以月、周为单位定期生成租户的 PDF 安全报表，包括业务的风险情况，及运维人员的服务情况，提升租户的服务感知。
靠性	★支持对云安全服务平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。（需提供产品功能截图，并加盖厂商公章）

安全组件功能要求

防火墙

功能指标	指标要求
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。
链路状态检测	产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式。
路由功能	产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议。
NAT 功能	产品支持多对一、一对多和一对一等多种地址转换方式。
认证方式	产品支持 3 种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。
流量控制	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。
会话控制	产品支持基于 IP 对象的会话控制策略，实现并发和新建连接数的合理限制。
访问控制策略	产品支持基于网络区域、网络对象、MAC 地址、服务、应用、域名等维度进行访问控制策略设置。
DDoS 防护	产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
	产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护、Land 攻击防护、WinNuke 攻击防护等攻击类型。
URL 分类过滤	产品支持管控非法、违规网站的访问行为，具备海量的 URL 分类库。
文件过滤	产品支持基于文件传输方式、文件类型等维度的管控策略配置。
防病毒	产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等

	协议进行病毒防御。
	产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。
	产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。
	★产品支持勒索病毒检测与防御功能，需提供产品功能截图证明。（需提供产品功能截图证明并提供官方检测机构出具关于“勒索病毒”的证书或检测报告证明功能有效性，并加盖厂商公章）。
入侵攻击防御	产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。
	产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。
	产品支持僵尸主机检测功能，产品内置僵尸网络特征库，可识别主机的异常外联行为。
账号安全	产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。

Web应用防火墙（8.0.85）

功能指标	**指标要求**
源地址识别	支持识别X-Forwarded-For、Cdn-Src-Ip、Clientip字段从而获取请求访问源地址，并支持填写受信任的代理服务器IP，用于日志记录。
HTTP异常检测	支持识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测、Content-Type头部字段异常检测。

Web 应用防护	支持超过 4900 种 Web 应用防护规则，和超过 1200 种 Web 漏洞攻击特征识别规则。
	支持防护 SQL 注入、XSS 攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 漏洞攻击等。
	支持 WEB 登录弱口令检测。
	支持自定义 Web 应用防护规则，通过正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。
语义分析	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。
业务学习	支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题。
机器人流量防护	★产品原生支持 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，并支持用户自定义保护阈值。（需提供产品功能截图证明，并加盖厂商公章）
防扫描和信息保护	支持 HTTP 应用隐藏，支持过滤如 Server、X-powered-by 类型的 HTTP 响应报文头
	支持数据泄密防护，可自定义文件下载类型过滤；
威胁情报	支持每 2 小时自动获取云端黑客 IP，并能在界面上一键进行访问拦截封堵云端黑客 IP。
服务器权限控制	支持 Web 权限控制，支持自定义文件上传类型过滤，防止通过修改文件后缀名绕过检测。
	支持 URL 防护，可自定义允许访问的地址和拒绝访问的地址。
	支持受限 URL 防护，仅允许从自定义的起始页面开始访问网站。
界面展示	支持针对业务风险汇总，支持展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务。

策略模板	支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种方式。
系统管理	产品支持系统配置自动备份功能，可通过备份文件快速恢复产品系统配置，降低管理员误操作引入的风险。
	安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。

漏洞扫描

功能指标	指标要求
风险统计	支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。
	支持全局风险统计时段自定义，展示最近 24 小时、最近 1 周、最近 30 天或自定义统计区间的风险分布和详情，时间跨度不限制。
	支持从漏洞视角分类型呈现风险概览和详情信息，支持在线查看展示“系统漏洞”、“WEB 漏洞”、“弱口令”和“基线风险”的名称、风险等级、漏洞数、最近发现时间，并可关联漏洞详情。漏洞详情可支持展示漏洞名称、漏洞类型、发现时间、影响资产、漏洞描述、漏洞影响、修复建议、CVE 编号、CNNVD 编号和举证信息。
任务类型	★支持快速扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。（需提供产品功能截图证明，并加盖厂商公章）
资产发现	支持资产发现功能，可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入。
	资产发现支持并发扫描数量自定义，最大并发扫描 IP 数为 1024。
	资产发现支持存活探测、服务和端口探测、操作系统识别、应用识别、和设备指纹识别等功能，其中服务和端口探测支持常用端口、全量端口和自定义端口三种探测方式。
	支持操作系统、网络设备、数据库、中间件等漏洞扫描。
	支持多种系统漏洞检测技术，如：基于漏洞原理的原理扫描

	技术、基于 banner 信息的漏洞扫描技术等。
	支持采用 SMB、RDP、Telnet、SSH 等协议对系统进行登录扫描。
	系统漏洞扫描支持高级配置功能，可支持存活性探测配置、端口扫描策略配置、UDP 扫描启用、低可信度漏洞扫描、web 应用扫描启用等配置功能。
WEB 漏洞扫描	支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等。
	持信息泄漏类漏洞检测，如：mail 地址、敏感目录暴露、内部 ip 地址、会话令牌、源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄漏等。
弱口令扫描	支持对多种服务协议的弱口令猜解，包括 FTP、IMAP、LDAP、Microsoft SQL、MongoDB、MySQL、Oracle、POP3、RDP、Redis、Rysnc、SMB、SMTP、SNMP、SSH、SVN、Telnet 等。
基线配置核查	支持对 Windows、Linux 等操作系统按照等保二级、等保三级要求实施基线配置核查。
	支持对 Oracel、MySQL、DB2、SQL Server、MySQL 等数据库按照等保二级、等保三级要求实施基线配置核查。
报告管理	产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。
	支持报表比对功能，可对任意两次同类型的报表进行比对，输出比对报表，并支持以 EXCEL 格式导出。比对报告包含对前后两次扫描结果中漏洞风险等级分布、未修复漏洞、已修复漏洞和新增漏洞信息进行展示。

日志审计

指标项	详细要求
日志采	支持安全设备、网络设备、中间件、服务器、数据库、操作

集	系统、业务系统等不少于800种日志对象的日志数据采集
	支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据,支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka等多种方式完成日志收集
	内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到200种
	支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。
	支持自动识别采集设备、支持设备异常告警、设备异常告警发送邮件或第三方接口
日志传输与存储转发	支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志
	支持日志文件备份到外置存储节点，支持ISCSI存储方式，并可查看外置存储容量、状态等信息。
日志检索	★支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；（需提供截图证明并加盖原厂商公章）
	支持日志检索数据的投屏；支持日志查询结果的统计与导出，支持历史备份文件导入查询；
	支持自定义过滤条件检索，支持对模糊ip、多个ip、ip地址段、应用、协议、MAC地址等其他字段精准检索，至少支持AND、OR、NOT三种运算符；
日志告警	支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。
	日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量
资产管理	支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义

	资产标签、属性、
	支持拓扑管理，能够基于拓扑图的资产相关数据信息快速查看资产评分、安全事件分布、告警分布等，支持通过拓扑下钻查看对应资产的关联事件、审计事件、日志数量。
	支持对 IPv4/ipv6 对象的自动发现功能，对自动发现的设备可以修改、删除或转为资产。
报表	内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持自定义时间导出报表。
	支持灵活的自定义报表，可以选择模板、数据类型等生成导出报表。
知识库	支持内置日志接入配置指导、典型日志事件介绍、安全经验等，并支持自定义创建增加知识库内容。
首页可视	支持自定义首页卡片，支持实时监控系统日志传输量和日志留存的合规情况。

数据库审计

功能指标	指标要求
部署方式	支持旁路部署模式，部署在核心交换中，通过端口镜像方式捕获数据流量进行审计
	支持在访问的数据库服务器上部署审计插件，获取数据库访问的数据流量进行审计
兼容性	支持 Oracle、MySQL、SQL Server、DB2、Sybase、Informix 等主流数据库协议的解析。
	支持 SQLServer2005 及以上版本的加密数据库账号的解析。
	支持达梦、人大金仓、神通、高斯 DB 等国产数据库协议的解析。
	支持 PostgreSQL、Greenplum、Cache 等专用数据库协议的解析。
审计结果	支持实时展示当前活跃会话详情信息。包括：会话开始时间、持续时长、访问来源 IP、目标服务端 IP、数据库协议类型、数据库账户、SQL 请求总数等。
	通过对双向数据包的解析，不仅对数据库操作请求进行审计，而且还可以对数据库系统返回结果进行完整的还原和审计，包括数据库命令执行时长、执行状态、返回行数、执行的结果集等内容。
	支持对超长 SQL 操作语句审计，可以正常记录单条长度最长 3M 字节的 SQL 语句内容。
	支持自动将 SQL 语句分为 login、logout、DDL、DML、DCL、privilege 等操作类型。
审计分析	支持对告警日志进行多维下钻分析、自定义选择图类型（饼图、柱状图），展示分析结果，支持自定义选择下级维度。
	支持一键保存多维分析模型，形成自定义报表模版。

	支持自动生成可视化的用户行为模型，支持自由切换模型中基线节点，显示模型中的其他基线。
统计报表	内置丰富的统计报表模板，至少包括：综合报表，等保报表、PCI 报表、SOX-法案报表等类型。
	报表支持导出为 PDF、CSV 等报表格式。
	支持报表预览，查看报表统计结果。
安全策略	支持自定义黑白名单策略，匹配条件至少包括数据库账号、策略周期、来源 IP、客户端工具、SQL 命令、操作对象名、SQL 语句等条件。白名单命中后识别为信任行为，黑名单命中后可识别为非法行为。
	支持根据来源 IP 设定审计范围。包括：设定不审计指定来源 IP 的所有访问记录，其他 IP 均审计；设定仅审计指定来源 IP 的访问记录，其他 IP 均不审计。
资产管理	支持自动发现镜像流量中的活跃数据库。支持基于端口，自定义发现范围，包括数据库类型、IP 地址、端口范围。
	支持通过手动配置的方式进行数据库资产添加，配置包括资产名称、资产分组、资产类型、资产地址和端口、编码方式等必要参数以及版本、数据库账号密码、服务名等其他参数。
	内置敏感数据标签，用于静态扫描方式对数据库资产进行扫描并打标
	支持敏感数据模糊化，对审计结果中的敏感数据进行脱敏模糊化处理，避免产品运维过程中的数据泄漏
系统管理	支持手动设置系统时间，支持从 NTP 服务器进行时间同步
	支持将网口设置成管理接口，并配置接口 IP、网关和 DNS
	支持系统登录账号的添加、删除和账号密码重置，支持通过导入方式进行账号添加
	支持三权分立，默认提供系统管理员、安全管理员、审计管理员三个角色账户。
	支持对新添加的系统账号进行审核，支持根据操作员账号进

	行自动审核

堡垒机

功能指标	指标要求
支持协议	字符协议：SSHv1、SSHv2、TELNET
	图形协议：RDP、VNC
	文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板
	支持通过协议前置机进行协议扩展，至少支持扩展 KVM、Vmware、数据库、http/https、CS 应用等
用户管理	支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期
	内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴
	支持对用户指定限制登录 IP、登录时间段（可循环，如每周一到周五 9：00-17：00 时）等规则，以确保可信用户登陆系统
	支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求
资源管理	支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源
	支持网络设备 enable 和 unix 主机 su 等身份切换的单点登录功能
运维授权	支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权
	支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息
	支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作

	★支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（需提供截图证明并加盖原厂商公章）
口令策略	可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性；口令策略还可以配置禁止包含的关键字
改密计划	支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式
访问控制	支持命令黑命单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等
	支持对文件传输类协议进行传输控制，如 RDP 剪切板、mstsc 磁盘映射、FTP/SFTP 等的上行、下行控制
审计日志	支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断
	支持对常见设备运维操作进行记录（至少包括 windows 主机、linux/unix 主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆 IP、设备 IP、设备名称、设备类型、访问账号、访问协议等信息
	对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放
管理能力	支持 NTP 系统时间同步配置，保证系统拥有可靠的时间戳
	支持日志数据的外置存储，支持 NFS、ISCSI 和 Windows 文件共享协议

主机安全(EDR)

功能指标	指标要求
一体化管控	单一管理控制中心可统一管理分别部署在 WindowsPC、Windows 服务器、Linux 服务器以及国产化服务器的客户端软件。
管理可视化	采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能
多维度威胁展示	支持全网风险展示，包括但不限于未处理的勒索事件数量、高级威胁、Web 入侵、待处置漏洞、钓鱼攻击及其各自影响的终端数量
策略管理	支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录
资产管理	支持系统信息的清点，包括操作系统及其版本、环境变量、内核模块、运行服务、启动项、计划任务、注册表、网络连接、开放共享以及国产化终端替代率（真替真用）
	支持按 Web 站点、服务、应用、框架等多层次来清点主机上的 Web 应用的资产信息
	支持基于单个终端视角的运行状态的监控，包括但不限于进程、服务、网络连接、计划任务和开放共享信息
	★支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、半夜登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户（需提供产品截图证明并加盖原厂商公章）
威胁检测	支持非常用登录 IP、非常用登录时间的异常登录检测；支持终端扫描端口的异常扫描检测
	具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效

	应对恶意代码及其变种
	可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率
	★支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出 100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情。（需提供产品截图证明并加盖原厂商公章）
业务零侵害	支持开启 agent 自动降级机制，可设置主机资源如 CPU 利用率、剩余内存、等待任务长度、磁盘列队长度达到的阈值
文件实时监控	可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别
Webshell 事件处理	支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离
暴力破解检测	统计单个攻击源及分布式攻击源的暴力破解检测，支持按照 SMB、SSH 和 MSSQL 类型进行封堵并自定义爆破阈值，可对封停时间进行自设置
威胁处置	构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置。
漏洞防护	支持对 Windows 终端的漏洞情况进行扫描，并查看漏洞具体情况及 KB 号，并显示具体修复情况。
	支持流行 Windows 高危漏洞的轻补丁免疫防御，支持 Windows 补丁批量一键修复。
	支持对 Linux 终端扫描系统漏洞、提供漏洞分析详情和修复建议。
入	支持不同攻击阶段的主要攻击手法检测，对包括但不仅限于以下攻

侵攻击行为检测	击手法精准检测，执行、持久化、权限提升、防御逃逸、凭证窃取、横向移动等攻击手法检测记录。显示事件详情，展示攻击手法对应的高危操作和威胁实体

3. 交货时间：（合同生效后 25 个工作日内。），交货地点：佛山市顺德区。

4.质量标准或要求：

投标人建立严格的质量保证体系，保证到货、调试、试运行与验收等各个阶段工作满足用户对质量的要求。根据整个系统建设实施的工作计划，对阶段性工作成果进行审查和测试，并向招标人提交里程碑式工作成果。通过保证各阶段性成果的质量，最终实施质量。

1）质量管理计划：

确定质量管理的需求、目标和规范；明确项目质量管理的组织、主要任务、项目的主要预期工作成果、质量标准和质量审查制度等。

2）实施过程质量监控：

按照质量管理计划建立的质量管理体系，面向项目中实施的全过程实行有效的质量控制；

质量监测：收集、记录和汇报有关项目质量的数据信息；

质量控制：使用质量监测提供的数据，进行控制，确保项目质量与计划保持一致，根据实际情况及时加以调整；在质量控制过程中，应严格执行质量审查制度。结合里程碑评审，对于关键项目成果的质量进行审查；质量监测分析时，对于已发现的不合格或潜在不合格，制定相应的纠正措施或预防措施，以消除不合格或潜在不合格的原因，防止不合格的发生。纠正措施或预防措施制定后，应对质量计划进行相应的调整，保证项目的顺利实施。

5.质保要求：合同设备整体质量保证期为验收合格之日起 36 个月。

6.资质要求：请填写《基础信息表》（详见附件 2），并在表后附相关资质证明文件（加盖公章的原件扫描件）。

7.业绩要求：请填写《近年完成的类似项目情况表》（详见附件 3），并在表后附相关资质证明文件（加盖公章的原件扫描件）。

8.售后服务要求：

在服务期内，供应商应提供专业的项目团队，确保项目顺利实施，供应商应提供客服邮箱、电话，及时解决项目执行过程中的数据问题及相关咨询，并支持7*24小时在线技术支持。若系统出现故障，能够及时根据故障等级提出解决方案，供应商应在收到买方通知后2小时内做出响应、24小时内解决，并根据故障情况支持相应人员现场解决。

9. 成交确定原则：完全满足采购函的供应商资格要求、货物清单及技术要求实质性条款（即标注★号条款）无负偏离，报价最低的为成交供应商。

10.其他要求：

10.1. 此项目支付条件：

10.2.报价方式：请投标人或其代表于2024年8月23日14:00前，在集采平台线上报价。

10.3.报价截止时间：报价文件递交的截止时间为2024年8月23日14时00分整。

10.4.邮箱地址：zhaobiao_hkr@powerchina.cn

10.5.联系人：甘海艳

10.6.联系电话：010-58383916

三．注意事项

1. 本次询比价为整体采购，询比价响应供应商报价时须写明单价及总价、产品的详细配置参数，报价包含清单中所提到的所有服务内容及交付采购人使用前所有可能发生的费用，报价为含税价，税率为6%或13%，确定成交供应商后不再增补任何费用。

附件一 ：《报价单》模板

附件二：《基础信息表》

附件三：《近年完成的类似项目情况表》

采购方：北京华科软科技有限公司

2024年8月16日

附件一：《报价单》模板

报 价 单

项目名称：顺德区水智慧管控工程数据机房（安全资源池）

供应商名称（务必填写全称）：

号	设 备 名称	设备技术参数及支持服务内容	数量	单价	总价	税率	备注
合计							

报价日期：202__年___月___日，报价有效期 6 个月。

联系人姓名：

联系人职务：

联系电话：

电子邮箱：

报价单位（盖章）：

附件二：《基础信息表》

<table>
<tr><td>供应商名称</td><td colspan="4"></td></tr>
<tr><td>注册资金</td><td colspan="2"></td><td>成立时间</td><td></td></tr>
<tr><td>注册地址</td><td colspan="4"></td></tr>
<tr><td>邮政编码</td><td colspan="2"></td><td>员工总数</td><td></td></tr>
<tr><td rowspan="2">联系方式</td><td>联系人</td><td></td><td>电话</td><td></td></tr>
<tr><td>网址</td><td></td><td>传真</td><td></td></tr>
<tr><td>法定代表人（单位负责人）</td><td>姓名</td><td></td><td>电话</td><td></td></tr>
<tr><td>资质证书</td><td colspan="4">类型：　　等级：　　证书号：</td></tr>
<tr><td>其他证书</td><td colspan="4"></td></tr>
<tr><td>基本账户开户银行</td><td colspan="4"></td></tr>
<tr><td>基本账户银行账号</td><td colspan="4"></td></tr>
<tr><td>近三年营业额（以财务报表为准）</td><td colspan="4">2023 年度营业收入_____万元；
2022 年度营业收入_____万元；
2021 年度营业收入_____万元。</td></tr>
<tr><td>备注</td><td colspan="4"></td></tr>
</table>

1） 请提供有效的企业营业执照和组织机构代码证复印件（按照“三证合一”或“五证合一”登记制度进行登记的，可仅提供营业执照复印件。）；

2） 请提供有效的质量管理体系认证证书（如有）；

注：以上《基础信息表》和资质证明文件须为加盖公章的原件扫描件。

附件三：《近年完成的类似项目情况表》

设备名称	
规格和型号	
项目名称	
买方名称	
买方联系人及电话	
合同价格	
项目概况及供应商履约情况	

备注	

注：

1.“近年完成的类似项目情况表”应附中标通知书和（或）合同协议书、设备进场验收单等复印件，具体时间要求见供应商须知前附表。每张表格只填写一个项目，并标明序号。

附件四：各类证明材料

投标人认为需提供的其他资料。

北京华科软科技有限公司

（电子章）

2024 年 08 月 16 日