招标项目技术、商务及其它要求

一、建设背景

为全面贯彻落实党的二十大和省委十二届二次全会决策部署,深入贯彻落实习近平总书记对科协“四服务”重要指示和省委“深化天府科技云服务”重要部署，四川省科协系统倾力打造了“统一开放、公平竞争、安全有序、智能便捷”的互联网科技交易市场——天府科技云平台。平台通过手机APP、网站等形式让每个科技工作者（团队）都可自主、便捷向“天府科技云”平台上传其“科技服务”，每个组织机构用户都可自主、便捷上传其“科技所需”，每个城乡群众都可自主、便捷上传其“科普所需”，实现科技（科普）供需智能匹配、精准对接、精准服务。为更好的服务于全省科技工作者、企事业单位和人民群众，省科协搭建了基于“公有云+政务云”的混合云，增加了更多云资源和带宽资源投入，并实现了多地数据点容灾，提升天府科技云平台业务连续性。同时，平台系统有实名认证和交易支付过程，其中包含敏感个人信息和移动支付安全，其信息安全问题不容忽视。

二、采购需求概况

通过采购方式引入专业安全技术服务，评估平台系统风险，制定防范策略，配置安全设备，定期总结报告，全面负责平台信息安全防范，包括规范后台管理操作、防止黑客入侵、排除网络故障、修补安全漏洞等。确保平台用户数据、交易数据、网络通信数据等重要数据的信息安全，保障2023年度“天府科技云”平台信息系统稳定对外服务不中断，避免出现信息安全事故。

三、服务内容及要求

采购标的名称	数量	单位
2023年度天府科技云平台安全技术服务	1	项

（一）服务内容

1.云安全防护。必须提供满足国家信息系统安全等级保护三级要求的软硬件服务，提供公有云部分的云安全服务，包含：云堡垒机服务、Web应用防火墙服

务（WAF）、数据库审计服务、日志审计服务、云防火墙（防病毒）服务、网页防篡改服务、防 DDos 攻击服务（流量清洗）、主机安全监测平台、VPN 专线等软硬件服务。

2.移动应用安全防护服务：

（1）安全加固服务：在移动应用发布前进行高强度安全加固保护，有效防止反编译、二次打包、内存注入、动态调试、数据窃取等恶意攻击行为，全面提升移动应用安全防护等级。

（2）信息合规检测服务：根据监管单位的相关要求和管理规范，进行合规检测评估服务，提供问题详情报告及修复建议，并完成问题修复，避免因不合规造成通报、下架风险。同时提供应急响应支撑服务。

（3）安全监测服务：对移动应用进行安全监测，及时发现针对应用的恶意攻击行为；在重点时段（攻防演练、重点节假日等）能进行攻击发现，并输出分析报告。

3.等保测评服务。根据《中华人民共和国网络安全法》等法律法规及相关文件要求，提供 2023 年度天府科技云平台（公有云及政务云环境）等级保护测评服务（三级）。

4.技术运维服务。提供日常服务器运维、安全运维巡检包括：相关网络实施设备规划、配置、调整、维护、升级、培训、技术咨询等服务，并提供巡检日志和报告，按照本单位信息安全管理制度处置防止重大信息安全事故发生。提供本年度重点时段（攻防演练、重点节假日等活动）安全防护服务、信息安全应急安全演练、数据灾备演练。服务内安排 1 名信息安全专业技术人员驻场，提供维护、修改、升级、巡防、培训、技术咨询、技术支持等服务，并及时排除故障。

（二）功能和技术要求

1.云安全防护

（1）云堡垒机

功能模块	功能描述
身份认证	采用多因子认证和远程认证技术，加强用户身份认证管理。 1、引用多因子认证技术，包括手机短信、手机令牌、USBKey、动态令牌等方式，安全认证登录用户身份，降低用户帐号密码风险。 2、对接第三方认证服务或平台，包括 AD 域、RADIUS、LDAP、Azure AD 远程认证，支持远程认证用户身份，防止身份泄露。并支持一键同步 AD 域服务器用户，复用原有用户部署结构。

用户帐号管理	系统用户帐号全生命周期管理，用户使用唯一帐号登录系统，解决共享帐号、临时帐号、滥用权限等问题。 1、批量导入 通过同步第三方服务器用户，以及批量导入用户，支持一键同步并导入已有用户信息，无需重复创建用户。 2、用户组 用户帐号按属性分组管理，可实现对同类型用户按用户组赋予权限。 3、批量管理 支持批量管理用户帐号，包括删除、启用、禁用、重置密码、修改用户基本配置等。
资源账户管理	集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。
系统访问权限	从单个用户帐号属性出发，控制用户登录和访问系统权限。 1、用户角色；2、组织部门；3、登录限制
资源访问权限	按照用户、用户组与资源账户、账户组之间的关联关系，建立用户对资源的控制权限。 1、访问控制 通过设置访问控制权限，从访问有效期、登录时间、IP 限制、上传/下载、文件传输、剪切板、显示水印等维度，赋予用户访问资源的权限。 2、双人授权 通过设置双人或多人授权审核，需要授权人实时授权才能访问资源，保障敏感核心资源绝对安全。 3、命令拦截 通过设置命令控制策略或数据库控制策略，对服务器或数据库中敏感、高危操作，强制阻断、告警及二次复核，加强对关键操作的管控。 4、批量授权 通过用户组和账户组形式，支持同时授权多个用户以多个资源的控制权限。
系统行为审计	系统操作行为全纪录，针对操作失误、恶意操作、越权操作等行为告警通知。 包括：系统登录日志、系统操作日志、系统报表、告警通知。
资源运维审计	全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。
Web 浏览器运维	堡垒机支持 HTML5 远程登录资源，无需安装客户端，一键登录运维资源
第三方客户端运维	在不改变用户使用原来客户端习惯的前提下，支持一键接入多种运维工具，提升运维效率。
自动化运维	线上多步骤复杂操作自动化执行，告别枯燥的重复工作，提高工作效率。
工单申请	系统运维用户在运维过程中，遇到需运维资源而无权限情况，可提交系统工单申请资源控制权限，寻求管理人员授权审批。

（2）web 应用防火墙

功能模块	功能描述
HTTP/HTTPS 业务防护	WAF 可以防护 HTTP/HTTPS 业务，通过对 HTTP/HTTPS 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。
支持 WebSocket/WebSockets 协议	WAF 支持 WebSocket/WebSockets 协议，且默认为开启状态。
域名备案检查	WAF 云模式支持域名备案检查，添加防护域名时，WAF 会检查域名备案情况，未备案域名将无法添加到 WAF。
PCI DSS/PCI 3DS 合规认证和 TLS	1、TLS 支持 TLS v1.0、TLS v1.1 和 TLS v1.2 三个版本和五种加密套件，可以满足各种行业客户的安全需求。 2、WAF 支持 PCI DSS 和 PCI 3DS 合规认证功能。
Web 基础防护	所提供的 WEB 应用防火墙覆盖 OWASP 最重要的 10 种常见安全威胁（具体为：SQL 注入、XSS 跨站脚本、远程溢出攻击、文件包含、Bash 漏洞攻击、远程命令执行、目录（路径）遍历、敏感文件访问、命令/代码注入、可以针对国外部分国家和国内省份的来源 IP 进行自定义访问控制），支持通过预置信誉库，对以上 10 种常见安全威胁进行检测和拦截
IPv6 防护	Web 应用防火墙支持防护 IPv6 环境下发起的攻击，实现对 IPv6 流量的安全防护，构建安全防护体系。
CC 攻击防护	CC 攻击防护规则支持通过限制单个 IP/Cookie/Referer 访问者对防护网站上特定路径（URL）的访问频率，精准识别 CC 攻击以及有效缓解 CC 攻击。支持人机验证、阻断、动态阻断和仅记录防护动作。 1、策略配置灵活 可以根据 IP、Cookie 或者 Referer 字段名设置灵活的限速策略。 2、阻断页面可定制 阻断页面可自定义内容和类型，满足业务多样化需要。
安全可视化	提供控制界面，实时查看攻击信息和事件日志。 1、策略事件集中配置 在 Web 应用防火墙服务的控制台集中配置适用于多个防护域名的策略,快速下发，快速生效。 2、流量及事件统计信息 实时查看访问次数、安全事件的数量与类型、详细的日志信息。
隐私屏蔽	支持屏蔽攻击日志中的敏感数据，避免信息泄漏
策略共享	允许用户把 IP 地址组和策略共享给其它子账号、企业项目和主账号使用，共享发起方一次修改，全局生效，大幅提升运维管理效率

（3）数据库审计

功能模块	功能描述
用户行为发现审计	1.关联应用层和数据库层的访问操作。 2.提供内置或自定义隐私数据保护规则，防止审计日志中的隐私数据（例如，帐号密码）在控制台上以明文显示。
多维度线索分析	1. 行为线索 支持审计时长、语句总量、风险总量、风险分布、会话统计、SQL 分布等多维度的快速分析。 2.会话线索 支持根据时间、数据库用户、客户端等多角度进行分析。 3.语句线索 提供时间、风险等级、数据用户、客户端 IP、数据库 IP、操作类型、规则等多种语句搜索条件。
风险操作、SQL 注入实时告警	1.风险操作 支持通过操作类型、操作对象、风险等级等多种元素细粒度定义要求监控的风险操作行为。 2.SQL 注入 数据库安全审计提供 SQL 注入库，可以基于 SQL 命令特征或风险等级，发现数据库异常行为立即告警。 3.系统资源 当系统资源（CPU、内存和磁盘）占用率达到设置的告警阈值时立即告警。
针对各种异常行为提供精细化报表	1.会话行为 提供客户端和数据库用户会话分析报表。 2.风险操作 提供风险分布情况分析报表。 3.合规报表 提供满足数据安全标准（例如 Sarbanes-Oxley）的合规报告。

（4）日志审计

功能模块	功能描述
日志采集	支持云主机日志采集、容器日志采集
	支持日志结构化解析：将原始日志解析成 key:value 的形式（分隔符/JSON/正则等）
	支持采集 VPC/ELB/CTS/APIG/DDS/RDS 等云服务租户面日志
	主机管理：基于自定义标识的主机组
	支持基于 IP 地址的主机组
日志查询	关键词查询语法（精确匹配，比较运算符，括号，in 范围查询，and or not 逻辑）
	支持*或?在关键词中间或者结尾的模糊查询
	日志时间-条数统计图
	支持查看日志上下文
	支持实时查看日志
	支持快速分析（快速统计字段的取值占比）

	支持按照日志流设置老化时间
监控与告警	日志资源统计（使用量统计）支持流量/存储/索引指标监控
	支持使用关键词查询配置告警
	通知方式：短信、邮件、钉钉、企业微信、电话、http
	告警通知内容支持自定义
日志开放性	支持客户使用 API 访问日志服务
日志查看	用户可以通过关键字查询日志
	用户可以作实时查看当前时间点之后上报至云日志服务的日志
	当用户需要重复使用某一关键字搜索日志的时，可以将其设置为快速查询语句
过滤器	每个日志流允许创建 5 个过滤器。用户按需配置需要过滤的关键指标，并且可以对过滤的指标进行监控及告警
日志转储	对于需要长期存储的日志数据，提供转储功能，可以将日志转储至对象存储服务中长期保存

（5）云防火墙

功能模块	功能描述
知识产权证书	提供软件的自主知识产权证书
信息技术产品安全测试证书	提供国家网络与信息系统安全产品质量监督检验中心出具的信息技术产品安全测试证书，证书需有虚拟化或云安全字样
授权管理	支持迁移，重装时，不更换授权文件
	授权可批量自动下发，自动回收
	支持公网授权验证方式
	支持内网授权验证方式
应用识别	支持多达几千种的应用特征库，并支持网络实时更新
	支持基于加密流量的应用识别
监控统计	支持 QoS 管道策略实际流量情况监控，支持子管道叠加情况监控
	所提供的下一代防火墙具备监控统计功能，支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析
访问控制	支持基于深度应用识别的访问控制
	支持对 4000+ 种应用的控制，包括 200+移动应用
	支持基于应用/角色的安全策略
	支持主机操作系统、浏览器识别，支持主机活动状态识别
	支持应用过滤器便于配置和维护，至少支持 6 个维度进行过滤，包括：名称、类别、子类别、应用技术、风险等级、特征；其中应用技术至少包括：基于浏览器、客户端服务器、网络协议、点对点；风险等级包括：1、2、3、4、5 总共 5 个等级；特征包括：能够传输文件、已被大规模使用、大量消耗带宽、易逃逸、易被滥用、被其它应用使用、存在已知漏洞、被恶意软件利用
	支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip、P2P 下载、视频、网络游戏等）限制新建连接、

	并发连接
用户认证	支持本地用户认证
	支持外部服务器用户认证(RADIUS、LDAP、MS AD)
	支持 AD/LDAP 用户/组织结构同步
	支持 Web 认证
地址转换	支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换。
	为解决公网 IP 地址资源问题，支持 NAT 的端口扩展技术，实现单个公网 IP 的无限地址转换
	支持 NAT 地址可用性探测，支持 NAT 公网地址池中 IP 有效性检测，避免因 NAT 地址无法使用导致业务中断
安全策略	支持防火墙策略命中数统计功能，便于管理员维护防火墙策略
	支持策略冗余检测，对策略重复检查
路由	支持静态路由、等价路由、策略路由，以及 RIPv1/v2 等动态 IPv4 路由协议（非透传）
QOS 流量管理	支持两层八级管道嵌套，能够同时做到两个维度的流量控制
	对多层级管道进行最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证
防病毒	基于流、低延时、高并发、高性能的病毒过滤
	支持加密流量开启病毒过滤功能
	支持大病毒文件的扫描
	实时病毒连接阻断，病毒事件记录
	支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描
	超过 1000 多万的病毒特征库，病毒库可以在线更新、本地更新
	支持对压缩文件类型的病毒检测，必须支持 RAR、ZIP、GZIP、BZIP2、TAR 等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于 5 层压缩，支持对超出行为自定义处理方式
未知威胁监测	支持 SMTP、POP3、IMAP4、FTP 等协议类型的检测。
	支持对 PE 文件在上传云沙箱前进行文件可信证书检测
僵尸网络 C2 防御	支持通过监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏，并定期升级更新僵尸网络服务器地址
	支持 C&C IP 和域名两种方式检测
	支持 TCP、HTTP、DNS 协议检测
IP 信誉库	支持对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤
入侵防御	支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御
	支持加密流量开启入侵防御功能
	支持抵御所列所有攻击类型，包括：PortScan、DOS Flood、Sockstress、反射攻击、SSL 攻击、应用层攻击等，动作支持记录、阻断两种模式。支持对不同安全域设定不同阈值和处理模式
	具备 9000 种以上攻击特征库规则列表，至少支持基于协议类型、操作系

	统、攻击类型、流行程度、严重程度、特征 ID 等方式的查询，并支持网络实时更新
	内置知识库，详细描述攻击特征及解决方案
	支持 SQL 注入、XSS 防护及自动抓包，支持 HTTP 头域中的 URL、Cookie、Referer、POST 检查点配置防护策略
	支持外链检查防护及自动抓包，支持自定义外链特性，类型支持 HTTP、HTTPS、FTP
	支持 CC 攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到 CC 攻击时支持 JS Cookie、重定向、访问确认、验证码四种认证方法
页面访问控制	支持基于角色、时间、优先级、页面类型等条件的 Web 网页访问控制
	支持自定义 URL 类别
	支持千万级别的 URL 特征库，URL 库支持网络实时更新
安全管理	至少内置三种管理角色，包括系统管理员、系统操作员、系统审计员
	支持对管理员登录方式设定，包括 Telnet、SSH、HTTP、HTTPS 等
带宽管理	所提供的下一代防火墙支持带宽管理，能够针对 IP 和应用进行流量控制，并相互嵌套；能够根据不同需求信息（例如安全域、接口、地址、用户/ 用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息）划分管道
高可靠性	支持主 / 备模式（A/P）
	支持配置、会话同步
	支持修改虚拟 MAC 地址
	支持接口使用真实 MAC
	支持 HA 同步协商使用单播模式
	支持 HA 协议号修改
IPv6	设备支持双栈，支持 NAT64、DNS64、NAT66、NAT46
	支持 4to6 6to4 隧道

（6）网页防篡改

功能模块	**功能描述**
网页防篡改	使用第三代网页防篡改技术，内核级事件触发技术，锁定用户目录下的文件后，有效阻止非法篡改行为。
	篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当企业主机安全服务检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。

（7）防 DDos 攻击服务

功能模块	功能描述
Web 服务器类攻击	SYN Flood 攻击、HTTP Flood 攻击、CC（Challenge Collapsar）攻击、慢速连接类攻击等。
游戏类攻击	UDP（User Datagram Protocol ） Flood 攻击、SYN Flood、TCP（TransmissionControl Protocol ）类攻击、分片攻击等。
HTTPS 服务器的攻击	SSL DoS/DDoS 类攻击等。

监控和报告	1、为单个公网 IP 地址提供监控记录，包括当前防护状态、当前防护配置参数、24 小时内流量情况、24 小时内异常事件。 2、为用户所有进行防护的公网 IP 地址提供拦截报告，支持查询攻击统计数据，包括清洗次数、清洗流量，以及公网 IP 被攻击次数 Top10 和共拦截攻击次数等。
DDos 高防	1、DDOS 高防支持对 IP 地址（段）黑洞路由服务，实现丢弃来自网络特定方向的包括攻击流量在内的所有去往该 IP 地址(段)的流量。 2、DDOS 高防支持 IPV6，支持 IPV6/IPV4 翻译，支持现有 ipv4 网站或者 ipv4 数据中心无需改造接入后即可被 ipv6 用户访问，支持平滑过渡到 ipv6 网络。可提供云端 ipv6 改造方案无需改动源站内容。 3、DDOS 高防支持 IPV6 外链改造，满足 IPV6 检测浓度要求，解决 IPV6 天窗问题。

（8）主机安全监测平台

功能模块	功能描述
客户端安装	支持常见的 Linux 和 Windows 操作系统，客户端安装支持一条命令以代理或直连方式直接安装，不需要重启服务或系统。
客户端运行安全性	客户端支持使用非 root 账号运行。
客户端安装资源占用限制	支持对客户端设置降级和自杀阈值。
客户端升级性能限制	支持限制推送客户端升级的速度。
客户端升级回滚	支持客户端回滚至任意指定版本。
控制台要求	提供系统消息队列状态监控，防止系统数据拥塞。
告警显示	告警支持统一管理。每条通知告警应包括，告警发送时间，告警消息类型，告警标题，告警内容，且支持筛选搜索。
管理要求	支持登录采用 OTP 双因子认证的方式，增强账号的安全性； 支持代理方式与直连方式安装 Agent，支持 IPV6 与 IPV4 通信的主机，Windows 支持 PowerShell 命令方式，安装包方式安装。 支持一个控制台即能实现主机安全、病毒查杀等模块的统一管理。
主机基本信息清点★	支持清点主机各类基础资产，包括硬件、CPU、内存、磁盘、操作系统等信息。
应用层资产清点	支持清点主机应用层相关资产，包括安装包、jar 包、应用、数据库、中间件等信息；
	支持国产化数据库和中间件清点，至少包括达梦数据库、人大金仓数据库、神舟通用数据库、宝兰德应用服务器。
业务层资产清点	支持清点业务层相关资产，包括 web 站点、web 框架、web 应用、web 服务等信息；
	支持自动统计高权限运行和目录为 777 权限的 WEB 站点信息。

风险扫描统计	支持自动化对主机进行全面的安全扫描，支持分组或指定 ip 风险扫描；
	支持以评级评分体系的方式简要直观评价当前安全态势。
安全补丁	支持自动化定时扫描主机中未安装的安全补丁，提供补丁的权威解释、扫描验证信息及命令级的修复建议，提供精细化的补丁风险特征标识；
	支持统计补丁的修复工时、已修复补丁数量；
	支持 windows 补丁替换关系梳理，逐级查询补丁替代关系。
漏洞检测	支持从漏洞视角对主机存在的高危安全漏洞进行扫描检测，提供漏洞的风险描述，影响范围，验证信息，修复建议及互联网的 EXP 公开信息等；
	漏洞检测支持可以选择配置检测方式，包括版本比和 poc 的方式进行扫描，poc 校验能够提供校验返回结果。
弱口令检测	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；
	支持以时间顺序展示弱密码的修复历史；
	支持对弱密码的明文显示进行脱敏，密文显示密码值。
入侵总览	支持实时显示最新发现的入侵信息与告警，实时刷新，可提供多维度的入侵信息统计，包括时间维度，主机维度。
反弹行为检测	支持对内网反弹行为是否上报，进行单独配置。
Web 后门检测	支持实时监控并检测网站目录下文件变化行为，对 webshell 文件进行上报告警，事件信息至少包含事件的危险程度、后门类型、文件名、受感染主机、发现时间等信息，并支持对文件进行下载查看；
	支持配置开启 NFS 挂载的网站目录识别；
	支持根据告警级别、IP、时间段来配置 web 后门自动隔离策略。
自定义检测规则	支持对指定的系统配置文件内容进行检测。
	支持自定义恶意进程名与进程参数检测，实时监控服务器的恶意进程启动行为。
可疑脚本执行	检测事件的上报数据应支持展示脚本文件内容，并标识出命中检测规则的代码段。
可疑操作检测	支持配置堡垒机的环境变量信息以获取真实 IP 信息；
	支持实时监控危险的操作命令，并发送邮件通知用户，系统默认的审计规则不少于 100 条。可自定义危险操作命令。可对所有发现恶意的命令执行操作进行审核，方便用户标记事件。
web 命令执行监控	支持根据进程的执行链和进程执行的命令作为特征来添加监控规则，其中进程执行链可按顺序设置，也可设置首尾进程，对属于异常或者不合规的进程执行行为可进行针对性的检测；

	提供对监控规则的管理能力，系统默认 WebRCE 规则大于 100 项，支持自定义检测规则，且能够对每个规则进行开启或关闭设置。
暴力破解行为	支持对发现的暴力破解事件进行处置，应支持对 IP 进行封停，禁止其登录主机；如果确认事件没有问题，应支持解封 IP。
基线支持	支持按照国际 CIS 检测标准（Level1、Level2）和国内等级保护检测标准（等保二级、三级）对操作系统和应用进行基线检测，内容至少应包含检查项，检查结果，通过率、修复方法等
	支持数据库的等保基线检测，支持录入数据库的用户名、密码和端口检查凭证，管理凭证需要管理员权限密码。
病毒检测	支持挖矿软件检测、支持恶意攻击木马检测、支持勒索病毒检测等其他常见病毒检测。
病毒引擎设置	支持至少包含 5 个杀毒引擎，并可自定义配置每个杀毒引擎的开启与关闭。
静态文件扫描	支持主动发起或定时发起对主机上的静态文件进行扫描的任务。
进程实时监控	可实时监控进程，对其进行病毒查杀。
防病毒能力	防病毒功能需具备国家计算机病毒应急处理中心计算机病毒防治产品检验实验室出具的检验报告。
Agent 管理	支持主动阻断 Agent 进程被恶意关闭的行为；
	客户端在安装前后，Linux 服务器内核模块无变化；
	支持采用配置 ping 或 nmap 的方式对离线的主机进行探测，用以辅助分析主机离线原因。支持手动探测和定时自动探测,并提供离线原因说明；
	支持主机标签，进行分类；支持批量移动主机到其他分组、批量添加标签给主机；支持设置资产等级，自定义备注等，便于管理员区分管理；
	支持批量手动修改 agent 状态，包括停用、降级、启动等。

（9）VPN 专线

提供 VPN 专线服务。

2.应用安全防护

（1）安全加固

Android 应用加固:

要求项	子项	具体要求
Android 应	DEX 加壳保护★	支持对 DEX 文件进行整体加壳保护

用防代码逆向要求	DEX 字符串加密	支持对 DEX 内的明文字符串进行加密保护
	DEX 类动态保护技术	支持对 DEX 内的代码进行动态抽取加密，并且在类被执行时不解密类内全部代码，只对被执行到的方法函数进行解密
	DEX 虚拟化保护技术	支持 DEX 虚拟化技术（VMP），能够将 DEX 代码转换为自定义的虚拟机指令，并以自定义虚拟机进行解释运行
	DEX 全量虚拟化保护技术	支持 DEX 全量虚拟化技术（ALL-VMP），能够将 DEX 代码的通过 DEX 虚拟化技术进行全量保护
	SO 文件加密	支持对 SO 文件加密
	防查看伪代码	支持对 SO 代码进行加密混淆,防止 IDA 的查看伪代码功能（IDA F5 功能）
	导入/导出函数隐藏	支持对 SO 内的函数表信息进行加密
	SO 动态清除	支持 SO 动态清除技术，能够在 SO 执行过程中动态清除内存中的函数符号
	u3d DLL 文件加密	支持 u3d DLL 文件加密
	SO 防盗用绑定	支持将 SO 文件同应用进行绑定，防止 SO 文件被非法盗用
Android 应用防二次打包要求	完整性保护	支持 APK 完整性验证，防止被非法篡改、二次打包
	资源文件加密	支持对应用内的资源文件、配置文件进行完整性保护，防止被篡改
	签名验证	支持对 APP 的开发者签名进行验证，防止被篡改签名、非法发布
Android 应用防数据泄露要求	数据加密	支持对本次存储的数据库文件、JS 文件、证书文件、配置文件等进行透明加密保护，防止查看和修改
Android 应用防调试要求	防动态调试保护	支持防动态调试，防止利用调试技术或工具对应用进行内存动态调试
	防内存注入	支持防内存注入，防止利用内存注入技术对应用进行恶意代码注入
	防内存 dump	支持防内存 dump，防止通过内存 dump 的方式分析内存数据
	防 xposed hook 攻击	支持防止利用 Xposed 工具进行 Hook 攻击
	防 Frida hook 攻击	支持防止利用 Frida 工具进行 Hook 攻击
Android 应用环境风险检测与防护要求要求	防截屏录屏	支持防止在应用运行过程中通过截屏非法窃取、捕获敏感数据，保护用户隐私数据安全、交易安全
	防界面劫持	支持防止界面劫持
	防日志泄露	支持防止攻击者通过分析应用日志信息获取敏感信息

	防设备 root	支持设备 Root 检测，对应用运行环境进行检测，判断设备是否已经 Root 进，确认后能够阻止应用运行
	防模拟器	支持防止模拟器运行，对应用运行环境进行检测，判断是否运行在模拟器上，确认后能够阻止应用运行
	防应用多开	支持防 APP 多开，对应用运行环境进行检测，判断是否通过 VirtualApp 等工具双开、多开应用，确认后能够阻止应用运行
服务形式要求	交付形式	支持 SaaS 在线云交付、支持私有云软件交付、支持本地一体机交付
	使用方式	支持基于 Web 浏览器加固、支持 API 自动化集成工具加固、桌面客户端软件加固
	多语言系统	支持简体、繁体、英语、韩语系统语言。
	配置界面	配置界面支持上传*.apk 和*.aab 文件进行加固,且支持勾选自动生成多渠道加固包。

iOS 应用加固:

要求项	子项	具体要求
iOS 应用加固支持语言要求	Object-C/Object-C++	支持对 Object-C/Object-C++代码的源到源加固
	Swift	支持对 Swift 代码的源到源加固
	C/C++	持对 C/C++代码的源到源加固
iOS 防代码逆向要求	控制流平坦化	支持在不改变语义的前提下，通过控制流平坦化将控制流进行混淆处理
	不透明谓词	支持对跳转逻辑的判断值进行隐藏，增加攻击者逆向分析的难度
	符号混淆	支持对代码内的类名、方法名、函数名进行加密混淆
	字符串加密	支持对字符串进行加密
	虚假控制流	支持增加新的虚假控制分支，加大破解和分析原始控制流的难度
	多样性混淆	支持随机化混淆，每次混淆代码不一样
iOS 应用防调试要求	静态防调试	在源代码内添加防调试校验代码，在函数执行时触发该保护功能，防止继续调试
	静态防 Inline Hook	在源代码内添加防 Inline Hook 校验代码，在函数执行时触发该保护功能，防止 Inline Hook 攻击
	静态防 Swizzling Hook	在源代码内添加防 Swizzling Hook 校验代码，在函数执行时触发该保护功能，防止 Swizzling Hook 攻击
	静态防 Frida hook 攻击	在源代码内添加防 Frida hook 校验代码，在函数执行时触发该保护功能，防止 Frida hook 攻击

	静态防 Cycript 注入	在源代码内添加防 Cycript 校验代码，在函数执行时触发该保护功能，防止 Cycript 攻击
	静态防 Reveal 注入	在源代码内添加防 Reveal 校验代码，在函数执行时触发该保护功能，防止 Reveal 攻击
	静态代码完整性保护	在源代码内添加防代码篡改校验代码，在函数执行时触发该保护功能，防止代码完整性被破坏
	动态防调试	在 APP 运行时开启自动守护功能，随时对调试行为进行监测和阻断
	动态防 hook	在 APP 运行时开启自动守护功能，随时对 hook 行为进行监测和阻断 支持防 Inline Hook 支持防 Swizzling Hook 支持防 fishhook
	动态完整性保护	在 APP 运行时开启自动守护功能，对代码段进行完整性
iOS 应用防二次打包	绑定 App 包名	支持绑定 app 包名，篡改 App 包名将会导致应用运行闪退
	绑定 App 签名	支持绑定 app 签名，篡改 App 签名将会导致应用运行闪退
iOS 应用环境风险检测与防护要求要求	防设备越狱	支持自动检测设备是否越狱，在已越狱的设备上自动阻止 App 运行
	防 Frida Hook 增强	防 Frida Hook 增强
	防 AirPlay 投屏	支持对 iOS 程序的 AirPlay 投屏行为进行检测，当存在 AirPlay 投屏行为时阻断 App 的运行，防止用户被进行远程诱导性欺诈。
	防日志泄露	支持对代码内的系统日志输出进行阻断，防止敏感信息泄漏
	APP 模糊化保护	支持 App 后台切换过程的屏幕模糊化，防止信息泄漏
	FishHook 关键函数防护	支持 FishHook 关键函数防护
	https 证书校验	校验 https 证书的合法性，防止中间人攻击
iOS 应用加固后审计与定位要求	加固结果可视化	支持加固后输出的是混淆加密的源代码，能够直观查看加固后的代码。
	代码逐行定位问题	支持代码逐行调试代码，准确、快速定位问题
	SourceMap 源代码溯源功能	加固后支持查看出问题的加固代码所对应的原始代码行号
服务形式要求	交付形式	支持 SaaS 在线云交付、支持私有云软件交付、支持本地一体机交付
	使用方式	支持基于桌面软件加固、支持命令行自动化加固
	多语言系统	支持简体、英语系统语言。

H5 应用加固:

要求项	子项	具体要求
H5 防逆向要求	代码紧凑	支持自动删除*.html、*.js 文件文件内的代码注释，降低敏感注释信息被恶意利用风险。
	防格式化	支持阻止 JavaScript 代码格式化工具还原易阅读格式。
	加壳保护	支持对 JavaScript 文件进行整体加壳保护，防止整体代码结构暴露。
	伪造控制流	支持在 JS 代码内添加无效、无意义的虚假代码、死代码，包括虚假的控制流代码等，增加代码分析复杂度，并让攻击者分析和调试进入无意义的陷阱内。
	字符串加密	支持对源代码的明文字符串进行加密保护，防止攻击者使用它来快速定位程序核心代码的位置。
	常量混淆	支持对 JS 代码内的常量数字进行混淆加密，防止攻击者使用它来分析代码逻辑。
	函数混淆	支持对 JS 代码内的函数名称、变量名称进行混淆加密，防止攻击者阅读分析、调试定位，增加破解难度。
	控制流平坦化★	支持对 JS 代码内的控制流代码进行扁平化混淆（如循环和条件转移语句等），使 JavaScript 代码可读性差，攻击者无法理解。
	表达式混淆	支持将 JS 代码内的二元表达式转换成等价函数调用形式，增大破解者分析难度，有效隐藏、保护核心算法的原始逻辑。
	虚拟化保护(VMP)	支持将 JS 代码转换为自定义的 JS 指令代码，并且只有通过自定义的解释器才能执行，让攻击者无从破解，保护核心代码安全。
	多样性混淆	支持使用随机化混淆技术，确保每次混淆后得到的代码（函数名、变量名）都不相同，提高攻击者分析的难度。
H5 防调试要求	防调试保护	支持对 JavaScript 源代码进行防调试保护，防止攻击者调试分析。
	防控制台输出	支持屏蔽浏览器控制台的打印函数信息输出功能，从而隐藏输出内容，增加攻击者分析难度。
H5 防盗用要求	域名绑定	支持将 JS 文件同域名绑定，防止 JS 代码运行在非授权的网络域名。要支持绑定多个域名。
	应用绑定	支持将 JS 文件同应用绑定，防止 JS 代码运行在非授权的应用上。要支持绑定多个应用。
体积优化	HTML 文件压缩	支持对 html 文件进行代码压缩，缩减代码体积，提高下载、执行效率
	图片压缩	支持对 png、jpeg 等类型图片进行压缩，缩减代码体积，提高下载、执行效率
服务形式要求	交付形式	支持 SaaS 在线云交付、支持私有云软件交付、支持本地一体机交付

	使用方式	支持基于 Web 浏览器加固、支持 API 自动化集成工具加固
	多语言系统	支持简体、繁体、英语、韩语系统语言。

（2）信息合规检测

依据《个人信息保护法》、《App 违法违规收集使用个人信息行为认定方法》、《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》等标准，提供个人信息保护合规评估服务。服务应包括以下内容：

① APP 个人信息快速访谈或调研：从隐私政策文本、APP 收集使用个人信息行为、用户权利保障三个方面快速评估 APP 针对个人信息保护的现状。

② APP 个人信息合规差距分析：基于法规要求以及 APP 现状，对 APP 进行合规差距分析，评估当前 APP 与法规现状的差距项。

③ APP 个人信息保护现状评估报告：基于快速访谈结果，以及差距分析结果，形成 APP 在个人信息保护方面的现状评估报告，报告中应提出 APP 存在的问题，并提供相应的整改建议。

④ 整改过程中提供指导：基于现状评估报告中提出的问题及整改意见，协助完成 APP 的隐私合规整改并再评估。

（3）安全监测

要求项	子项	具体要求
监测对象要求	Android	支持 Android 应用监测
	iOS	支持 iOS 应用监测
	鸿蒙	支持鸿蒙应用监测
攻击监测要求	Https 劫持	支持监测应用的 Https 加密传输功能是否被劫持
	应用破解	支持监测应用是否被二次打包，加固应用是否被破解攻击；
	根证书库异常	支持监测系统根证书是否存在非可信证书；
	模拟器	支持监测应用终端是否运行在模拟器环境，属于何种模拟器；
	位置欺诈	支持监测短时间之内时空漂移过大的终端设备，或 GPS 坐标被篡改；
	域名欺诈	支持监测本地域名 DNS 遭篡改；
	多开器	支持监测使用多开器在同一设备打开多个应用；
	设备伪造	支持监测使用修改器篡改手机硬件参数信息，伪造新设备；

	注入攻击	支持监测应用遭注入攻击；
	调试行为	支持监测应用遭调试；
	程序外挂	支持监测终端外挂攻击程序；
	内存篡改	支持监测应用程序运行内存被非法篡改；
	Http 代理	支持监测使用 HTTP 代理；
	系统加速	支持监测系统时钟加速行为；
	人脸绕过	支持监测移动端摄像头在拍摄人脸信息时被绕过的行为；
	云手机	支持监测操作者在手机上通过云手机管理 APP 发送操作指令行为
风险监测要求	Root/越狱	支持监测系统是否 Root 或越狱；
	框架软件	支持监测系统是否安装了 Xposed、Cydia_Substrate、Frida、magisk 等框架软件；
	风险应用	支持监测系统上是否安装了自定义的风险应用；
	风险进程	支持监测系统上面是否运行有自定义的风险进程；
	敏感配置	支持监测系统是否存在敏感配置项被打开，如 USB 调试、无线 ADB 调试等；
	界面劫持	支持监测应用是否被切换至后台，支持监测到切换至后台后用户可以定制提醒功能；
	VPN 通讯	支持监测使用 VPN 软件进行通讯；
	定制 ROM	支持监测系统是否存在定制 ROM 的手机环境。
	macOS	支持监测应用是否在 macOS 环境中运行
	虚拟攻击环境	支持监测应用是否运行在 VirtualXposed、太极 APP 等虚拟环境中的能力
	屏幕共享	支持监测在使用 APP 过程中进行手机屏幕共享的场景
	Win11	支持监测应用是否运行在 Win11 的环境中
	运营商异常	监测运营商信息是否与真实信息不一致
	手机虚拟机	监测识别手机虚拟机，例如 VMOS
异常行为监测	高频更换设备	支持监测高频更换设备的异常行为；

	高频更换 IP	支持监测高频更换 IP 的异常行为；
	高频更换地域	支持监测高频更换地域的异常行为；
	高频更换账号	支持监测高频更换账号的异常行为；
可视化展示分析要求	大屏展示要求	能够提供全局监控页面，包含整体的安全事件、威胁、启动趋势；威胁、风险分布统计、威胁实时监测，支持图形化的展现； 能够提供整体的安全统计，包括统计封禁设备数、安全事件数、风险总数、威胁总数；展现整体运行统计，包括统计设备总数、活跃设备数、启动次数、崩溃次数； 能够提供态势地图，支持中国、世界地图切换，地图支持放大、缩小；平台首页能够自动刷新，加载最新数据； 支持自定义筛选今天、昨天、最近 7 天、最近 30 天等；
	实时监控要求	提供实时监控大屏页面，可以监控启动信息、安全威胁、环境风险、崩溃信息、安全事件等类别；支持自定义列表详情信息的呈现方式； 支持的监控过滤条件包括：监控类型、设备类型、地域、系统版本、应用版本、监控条数；
	数据看板	能够提供全局移动风险（安全事件）及移动风险处置的监控页面； 支持自定义筛选今天、最近 7 天、最近 30 天等
安全运营服务	移动端攻击发现及溯源服务	采用远程人工服务方式，基于移动应用安全监测平台和报告模板，提供数据分析服务，通过深度数据分析和专家研判，协助进行移动端攻击发现和威胁溯源，输出安全分析报告及溯源报告，提供安全防护及安全监测策略调优建议。 围绕报告提供整改建议说明、报告解读和答疑。

3.等保测评服务

按照等级保护相关标准对系统从技术、管理等方面进行安全等级测评和密码测评工作并编制测评报告。制定并提交《天府科技云平台网络安全等级保护测评报告》。投标人应提供等保测评的具体方案，描述本次项目整体实施方案，包括项目概述、等保测评服务方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

投标人应描述服务人员的组成、资质及各自职责的划分。投标人应配置有经验的测评人员进行本次等级保护测评工作。安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由投标人推荐，经采购人确认后由投标人提供并在测评中使用。投标人根据采购人现有场地和网络环境提出相应的运行环境的具体要求。

协助采购方与相关监管部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。投标人对整改后的内容进行最终确认，并汇总信息系统等级保护测评阶段性文档（不限于信息系统拓扑图、定级备案材料、测评记录、检测表、差距分析报告、整改实施方案、测评报告、备案证明等）。

★4.技术运维服务

提供日常服务器运维、安全运维巡检包括本合同约定之网络设备的网络实施设备规划、配置、调整、维护、升级、培训、技术咨询等服务，并提供巡检日志和报告，按照本单位信息安全管理制度处置防止重大信息安全事故发生。提供本年度重点时段（攻防演练、重点节假日等活动）安全防护服务、信息安全应急安全演练、数据灾备演练。提供服务器管理、平台安全、数据备份、产品发版、管理平台迭代档案服务。服务期内安排 1 名信息安全专业技术人员（该人员所学专业应为相关专业、至少两年以上相关经验）驻场，提供维护、修改、升级、巡防、培训、技术咨询、技术支持等服务，并及时排除故障。

（提供承诺函，格式自拟）

（三）其他要求

1.投标人须提供售后服务，能够提供 7 天×24 小时远程支持服务。

2.为本项目配备专业团队人员，包括 1 位项目经理和其他专职人员。

（四）绩效要求

1、促进平台安全防护升级，达到信息系统安全等级保护测评（三级）要求，测评分数不少于 80 分。

2、确保平台 2023 年度（尤其重点时段）的信息安全零事故。

3、每月提供业务安全产品运维报告。

4、及时排除故障，在半小时内做出明确响应和安排，故障解决时间不超过 12 小时，并协助采购人处理后续事宜。

★四、商务要求

1、服务期限：自合同签订之日起一年。因成交投标人原因提前终止服务的，根据法律法规和合同条款追究违约责任和法律责任。

2、付款方式及时间：

2.1 签订合同之日起 30 日内支付合同款项的 60%。项目建设完成，驻场人员到位后，投标人提出初验申请并提供相关证明，经采购人组织验收合格后支付合同款项的 30%。在项目服务完成（合同期满）后，经采购人组织对成交投标人开展最终履约验收合格后支付剩余 10%合同款项。

2.2 合同价款的支付采取银行转账方式，每次付款前，成交投标人应提供合法有效完整的完税正式发票及凭证资料，否则采购人有权拒绝付款，由此造成的损失由成交投标人自行承担。

3、验收标准：

3.1 按国家有关规定以及招标文件的服务要求和技术指标、中标人的投标文件及承诺与本项目合同约定标准进行验收；双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，按招标文件与投标文件中质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收；

3.2 本项目采购人及其委托的采购代理机构将严格按照政府采购相关法律法规以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）的要求进行验收。

①验收组织方式:采购人自行组织

②是否邀请本项目的其他供应商:否

③是否邀请专家:否

④是否邀请第三方检测机构:否

⑤履约验收程序:分期验收

⑥履约验收时间:供应商提出验收申请之日起 30 日内组织验收

⑦验收组织的其他事项:项目建设完成，驻场人员到位后，投标人提出初验申请并提供相关证明后，采购人组织初步验收。在项目服务完成（合同期满）后，采购人组织对成交投标人开展最终履约验收。

⑧技术履约验收内容:招标文件要求及投标文件响应等内容进行技术验收。

⑨商务履约验收内容:按投标文件响应商务内容验收。

⑩履约验收标准:(1)严格按照政府采购相关法律法规要求进行验收；(2)按国家有关规定以及招标文件的要求、投标人的投标文件及承诺与本项目合同

约定标准进行验收。

⑪履约验收其他事项:履约验收各条款间有不一致时，按较高标准进行。

注：本章节★要求为实质性要求条款，不满足作无效投标文件处理