第四章　采购需求

一、商务要求

1.1. 服务期限

自签订合同之日起一年

1.2. 磋商范围

计算资源、网络资源、数据库资源、存储资源、安全资源、数据加密服务、运维服务等。

1.3. 付款条件

于合同签订后 15 个工作日内，一次性支付合同总价款。

1.4. 售后服务

1）保障公有云资源的正常运行，提供的运维服务：

基本服务支持提供 7x24 小时热线电话支持

2）国密改造涉及的数据加密服务、SSL VPN、动态令牌系统等资源的搭建与维护

3）提供 7x24 小时云产品工单支持

4）提供 IM 企业群支持

5）提供 API 与 SDK 支持、帮助文档支持、云社区/消息订阅支持、在线培训课程支持

6）应急预案

1.5. 项目团队要求

项目团队成员至少 5 人以上，具有安全、运维等类似项目经验，提供证书复印件。

1.6　项目验收

需求提供方应及时足量依照需求提供云资源；

需求提供方依照服务方案的相关承诺，完整提供云资源维护与支持服务。

需求提供方应在项目完成后 15 日内按照采购方要求提交项目验收材料。

验收材料应包括但不限于如下内容：项目实施情况、 云服务资源数量，月度使用报告，资源占用量，年度用户满意度，项目总结报告等。

采购方根据合同约定的服务内容及要求对需求提供方实际完成工作质量进行验收确认，并组织专家验收评审。

二、技术要求

本次公有云服务的采购，云服务厂商需具备全面的产品体系，包括云计算（弹性计算、网络、存储、数据库、视频与 CDN、中间件、云通信、研发协同、运维管理、企业服务等）、云安全（主机安全、安全运营中心、WEB 应用防火墙、网站威胁扫描等）、大数据计算、人工智能等全面的产品能力。

1.1. 产品需求

采购内容：本次采购内容包括公有云服务一年租用。

供应商需报价内容见下表：

资源	配置	数量
普通云主机	计算优化 标准 8C16G 40G 系统盘（SSD）	90
	通用 标准 8C32G 40G 系统盘（SSD）	40
	内存优化 标准型 8C64 40G 系统盘（SSD）	30
	通用标准 16C64G 40G 系统盘(SSD)	20
云硬盘	通用 SSD 300G	100
	通用 SSD 500G	80
快照备份	快照容量 500G	20
负载均衡	负载均衡，实例流量每月 1000G，不包含公网 IP 带宽	15
NAT 网关	NAT 网关，小型 100 万连接数，不包含公网 IP 带宽	15
弹性公网 IP	支持挂载到主机、负载均衡、NAT 网关等产品，多个弹性公网 IP，BGP，总固定带宽 500M	1
对象存储	存储 50T，外网下行流量 500GB，请求次数每月 200 万次读请求或写请求)	2
云文件服务	通用型云文件 60T	2
数据库 MySQL	规格：8 核 32GB 存储空间：600GB	10
数据库 MongoDB	规格：8C32G 3 节点 存储空间：1500GB	6
云缓存 Redis	规格：8G，标准版	8
云缓存 Memcached	规格：1C4G，集群版，2 节点	6
消息队列 Kafka	4C16G，存储：500G	8
云搜索 Elasticsearch	8C16G，存储：200G	6
DDoS 基础防护	提供最少 2G 的基础防护服务或 DDoS 防护包，根据需求选择不同保底带宽和弹性防护。	180
IP 高防	DDoS IP： 线路类型 BGP IP 类型 IPv4 IP 个数 1 个	3

	保底防护峰值　10 Gbps CC 防护峰值　30,000 Qps 弹性防护峰值　50 Gbps 业务带宽　100 M 端口数　60 个 防护域名数　60 个 （不包含弹性防护计费，实际的防护峰值为 60Gbps，超出 10Gbps 后的攻击会产生费用，最高收取 6400 元/天的费用。）	
web 应用防火墙	低配要求如下： 业务带宽: 30Mbps 正常业务请求 QPS: 3000 一级域名个数: 1 防护域名总数: 10 OWASP TOP 10 检测与防御 0Day 漏洞防护、规则更新 HTTP、HTTPS 端口的业务防护 支持部分指定的非标端口 报表统计分析 黑名单规则：20 条/域名 HTTP 流量管理规则：20 条/域名 自定义规则/地域封禁：20 条/域名 流量限速：10 条/域名	15
	高配要求如下： 支持 Web 威胁检测，具有检测各类应用层攻击行为的能力，如 SQL 注入、XSS 攻击、远程溢出攻击、漏洞扫描、Bash 漏洞攻击、远程命令执行、敏感文件访问等 支持 OWASP TOP 10 安全检测和防御 0Day 漏洞防护、规则更新 HTTP、HTTPS 端口的业务防护 报表统计分析、全量日志查询 防爬虫、恶意 IP 自动封禁、全量日志下载 支持设置黑名单规则，50 条/域名 支持 HTTP 流量管理规则，50 条/域名 支持自定义规则/地域封禁，50 条/域名 支持流量限速，20 条/域名 支持网页防篡改，20 条/域名 支持业务风控，10 条/域名 支持 BOT 高级，10 条/域名 支持 IPv6 防护 支持自定义 CC 防护规则，20 条/域名 正常业务请求 QPS: 5000 业务带宽: 50Mbps 支持一级域名个数: 2 支持防护域名总数: 20	2

	地域：双地域可选	
主机安全	提供主机层面基础数据采集，资产统一管理，风险发现，漏洞扫描，检查，入侵检测，病毒木马查杀，容器运行时安全，调查分析能力	180
安全运营中心	提供统一资产管理，安全可视化、安全大屏，安全防范、威胁检测、调查响应，全量日志分析、未知威胁取证、黑客攻击溯源，安全托管，安全报表能力	180
网站威胁扫描	提供各类资产进行威胁扫描检测能力，包括 Web 漏洞扫描、端口漏洞扫描、弱密码扫描、API 接口扫描、容器镜像扫描，覆盖 VPC 内网资产、提供互联网服务的 IP/域名资产、IDC 机房内网资产 支持 1 个一级域名，不限制该域名对应的子域名和 IP 数量。	50
数据库审计	提供的实时监控数据库安全的审计产品，通过旁路模式，实时记录用户访问数据库的行为，形成细粒度的审计报告，并对风险行为进行实时告警： 吞吐量：3000 条 SQL/秒 支持数据库数：3 个 入库速率：200 万/小时 在线存储量：100 亿条 SQL 语句	6
堡垒机	提供具备权限管控、安全审计、自动化运维能力的运维平台，旨在帮助企业在云端构建统一、高效、安全运维通道，保障云端运维工作遵循法律法规要求、降低人为安全风险，提高运维效率，支持 50 资产	15
SSL 证书	提供一站式安全证书服务，可在线快速签发多种品牌数字证书。帮助您的网站、APP、小程序，从 HTTP 明文协议升级至 HTTPS 加密协议，提高网站可信度，防范劫持、篡改和监听等网络攻击，满足安全合规要求，并提升 SEO 排名。 GeoTrust 品牌，企业型 OV 泛域名	15
国密证书	国密证书	8
监控服务	提供自定义上报监控指标数据的功能，支持聚合维度查询监控图和配置告警	1
日志服务	提供云产品日志数据实时采集，提供日志检索、日志转存、日志监控等功能	1
漏洞扫描服务	提供对用户指定的操作系统等提供全面的漏洞扫描服务，由安全专家对扫描结果进行解读，并提供专业的漏洞扫描报告和修复指导建议。每次 20 个主机资产或 2 个二级域名。	3
云防火墙	4 核 8G 硬盘 40G 可防护 VPC 数：2 每秒新建连接数：10w 防火墙吞吐量：2Gbps 最大并发连接数：400w 支持以下能力： 安全策略、ALG、基于全局配置 NAT、网络攻击防范、加密流量检测、深度包解析等能力	3

	网络入侵防御：包含 IPS、IPS 特征库升级 链路负载均衡：包含智能 DNS、Inbound、Outbound 链路负载均衡等能力 IPv6：包含 2、3 层运行模式，各类路由协议和 ipv6 攻击防范 威胁监控：包含运行监控、流量监控、应用分析中心、统计和趋势、僵尸网络分析、用户信息中心等能力 VPN 特性：包含 IPSecVPN、SSLVPN（含 15 个用户授权）等基础 VPN 功能特性	
安全托管服务	提供对主机、网络、应用及数据多维度安全风险事件的智能化分析，利用安全编排自动化响应处置技术与安全专家相结合的高效运营处置，提供全天候的安全保障服务。 1. 协助客户方进行安全产品接入 2. 提供安全产品日常托管运营服务 3. 对云上安全产品进行简单的可用性监测和处置支持 4. 帮助用户构建基础安全告警运营能力 基础版，50 资产	3
数据加密服务	提供应用系统数据的签名/验证、加密/解密等密码运算，保证信息的机密性、完整性和真实性，同时提供安全、完善的密钥生命周期管理机制。	5
SSL VPN	提供集成 SSL VPN 和身份认证功能，内置轻量级 CA 中心和防火墙，可为用户提供可信认证服务和传输加密服务。	1
动态令牌系统	提供基于动态口令技术的身份鉴别服务，具备手机、硬件令牌的分发管理、挑战应答动态口令的生成与验证、交易签名的实现与验证、认证服务器身份的验证、用户与系统之间的双向认证等身份认证功能。	1

1.2. 技术要求

本次采购公有云产品需满足以下技术参数要求，供应商需要对各项指标逐条应答，#号项目（一共 10 项）除了应答之外，还需要提供截图证明并加盖公章，应答需要详实，禁止简单答复“满足”，“支持”等短回复。

指标项	**参数要求**
总体要求	#1、本项目要求针对中国大陆地区，公有云厂商在全国范围需提供跨城域的异地可用区，提供截图证明，需加盖公章 2、支持包括中国联通、中国电信、中国移动在内的至少 3 线的 BGP 网络接入 3、支持用户自服务门户、命令行和 openAPI，并向用户提供统一门户、统一服务
云主机	1、提供生命周期管理：支持实例增删改查、重启、停止、启动、自定义数据（启动脚本）、动态调配（CPU、内存、带宽、存储）、重置系统、重置密码、支持控制台 VNC 及远程 SSH 两种方式登录等 2、存储支持挂载多块云硬盘、支持云硬盘做系统盘、支持快照；

	#3、SLA 承诺：对于单实例单可用区维度，云主机的服务可用性不低于 99.99%；单地域多可用区维度，云主机的服务可用性不低于 99.995%，提供截图证明，需加盖公章 4、云主机信息导出：支持通过控制台导出实例列表，可选择的导出信息包括：名称、镜像、可用区、主 IP 地址、私有网络、状态、规格类型、配置、标签、计费信息、资源组等。单次支持最多 2000 条数据的导出。 5、云主机组支持高可用，支持冗余组，每个组内的云主机数量可调，可以跨 AZ 均匀分布，且在每个 AZ 内支持至少 5 个故障域分布来保障多重高可用 6、镜像支持官方/私有/共享镜像，支持导入、导出、共享/取消共享、整机镜像、自动镜像策略 7、自动镜像策略支持使用自动镜像策略为云主机设置周期性的主机备份任务。能够根据用户指定的规则定期定时为用户备份云主机数据，制作镜像。可免去用户定期手动为云主机制作镜像的工作。 #8、镜像类型转换：基于当前镜像生成一个新的镜像，两种镜像类型分别为本地盘系统盘和云硬盘系统盘，提供截图证明，需加盖公章 9、镜像导出支持私有镜像导出，在云环境下制作的私有镜像，导出至同地域下的对象存储空间中。导出之后，可随时下载镜像文件用作其他环境下的部署。提供镜像导出 OpenAPI 文档链接和 CLI 命令。 10、支持安全组、SSH 安全密钥、硬盘加密、IAM 访问权限控制、实时监控报警、节点故障自动恢复
云硬盘	1、提供 SSD 云硬盘、HDD 云硬盘类型 2、云硬盘系统盘需支持云硬盘形式的系统盘卸载和挂载 3、支持多个云实例并发读写访问的数据块级存储设备，具备多挂载点、高并发性、高可靠性等特点。单个多点挂载盘最多可同时挂载给 16 个云实例，多点挂载只适用于数据盘，不支持系统盘。 4、提供生命周期管理：支持创建、挂载、卸载、删除、多点挂载、在线扩容 5、支持三副本、云硬盘加密、快照数据备份、自定义快照策略
对象存储	1、提供多种权限控制方式，包括私有读写，公有读私有写，公有读写和自定义权限等方式支持服务器横向扩展，扩容过程中不影响对外服务 2、支持最大文件不小于 48TB，控制台/单个文件或者分片大小：5GB；支持图片处理服务: 获取图片信息、图片缩放、裁剪、旋转，图片格式转换。支持 Bucket 创建/删除/列举，静态网站托管，防盗链，访问日志，跨域访问。 3、支持跨域复制能力，对象存储支持存储桶之间数据同步，跨区域数据复制，具备区域级别的容灾备份能力
文件存储	1、提供两种规格后端存储：通用型文件系统后端采用 SSD 硬盘；容量型文件系统后端采用 HDD 硬盘。 2、提供按需扩展的高性能文件存储，可为云上多个弹性云服务器/容器、裸金属服务器提供共享访问。 #3、在云文件服务中创建文件存储时，无需预先配置容量大小。文件存储可根据您添加或删除文件的操作，弹性伸缩容量。提供截图证明，需加盖公章 4、云文件服务支持 NFS v4.1 协议、 NFS v4.0 协议和 NFS v3 版本协议
私有网络（VPC）	#1、支持子网跨 AZ，在创建子网时无需选择 AZ 区，子网内的资源可以仅基于某一个 AZ 区创建使用，也可以分布到多个 AZ 区进行创建使用。跨 AZ 子网的设计为业务规划部署。提供截图证明，需加盖公章

	2、VPC 支持增删改查、创建 VPC 时支持预设和不预设 CIDR 两种方式 3、支持路由表增删改查、路由策略、边界网关路由传播 4、支持无状态网络访问控制，入站规则、出站规则，支持允许和拒绝规则、支持绑定多个子网 5、VPC Peering 支持 VPC 互通，且对等连接互通性不传递 6、提供 VPC 隔离、子网级安全组一级防护、实例级 ACL 二级防护、支持高可用路由
负载均衡	1、支持分布式网络负载均衡，基于 SDN 技术实现，无负载均衡实体存在，提供软件定义的全可用区四层分布式负载均衡服务。 2、应用负载均衡支持 TCP/TLS/HTTPS 等多种协议的不同端口侦听服务，以支持丰富多样的客户端服务接入和流量分发。
NAT 网关	1、支持单可用区集群部署，可以通过双机热备、自动容灾等高可用设计，实现不低于 99.95% 的服务可用性。 2、支持最大 1000 万并发连接数和 4Gbps 的吞吐量。 3、提供多维度的监控数据，利用图表直观展现，实时掌握 NAT 网关的流量健康状况，对故障设定预警。
弹性公网 IP	1、支持增删改查、绑定和解绑资源、调整带宽 2、支持在不同可用区云主机之间动态迁移。提供无可用区属性弹性网卡，支持弹性网卡在不同可用区云主机间动态迁移，实现可用区级的高可用方案，缩短故障时间，提升系统可靠性
DDOS 基础服务	1、免费提供最高 2G 的防护能力 2、支持根据业务需求设置清洗触发值，保护常见的 DDoS 攻击的威胁 3、支持对所有流量进行实时检测，第一时间发现其中的攻击流量，秒级应对攻击，清洗迅速，保障业务的正常运行。
IP 高防	1、提供对各类不同 DDoS 攻击类型的防护，包括：网络层攻击 ICMP flood、UDP flood、TCP syn flood、TCP ACK flood、NTP flood、http flood、TCP 慢速攻击等，应用协议层 DDoS 攻击 HTTP Flood，HTTP 慢速攻击，CC 攻击等 2、支持 BGP 线路，单机房防护能力超过 1T 3、支持单实例多防护 IP，支持防护 IP 黑洞后自动轮换可用 IP 4、支持多种协议和非标端口的转发，包括 TCP/UDP 的 4 层转发及 HTTP/HTTPS 应用层七层转发。 5、支持 websocket，http2.0。 6、支持 SSL 加密套件选择，包括 SSLv2，SSLv3，TLSv1.0，TLSv1.1，TLSv1.2，TLSv1.3，国密 SM2。支持选择加密套件。 7、支持回源长连接，被动健康检查，请求头下划线 8、支持轮询、IP Hash、加权轮询、按地域回源 9、支持 https 证书卸载和 HTTPS->HTTP 协议转换。支持 HTTPS 强制跳转定制化功能，支持基于 IP、地域、URI、Cookie、Headers 的黑/白名单，支持地域封禁 10、支持联动防护，非攻击状态下不防护，攻击状态下自动切换防护 Web 应用防火墙，云主机等云资源 11、支持回源模式和防护模式切换 12、支持开关虚假源与空连接防护、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度过滤

	13、支持 CC 防护自定义规则，支持设置基于 URI，访问频率，阻断规则（封禁/人机识别），返回自定义页面，阻断时长参数的自定义规则 14、支持抗 D 安全态势大屏功能（展示机房、IP 维度的攻击统计数据） 15、管理和告警，提供管理平台，方便运维管理人员及时查看流量和攻击情况，支持自助配置和管理功能。 16、支持批量导入导出转发规则 17、支持异常状态码告警，支持自定义异常状态码返回页面 支持攻击防护、业务流量、新建连接、CC 防护、状态码报表展示，支持保留 180 天防护日志 管理平台支持攻击实时监测和告警（邮件、短信等），包括攻击类型、攻击大小、攻击时长、攻击流量曲线等。
Web 应用防火墙	1、支持 SQL 注入攻击、XSS 攻击防护、Web 应用扫描防护、文件读取/包含攻击、命令/代码执行攻击、敏感文件探测、恶意扫描攻击、恶意/后门文件攻击、XML 注入攻击、目录遍历攻击、Web 插件漏洞防护。支持正常、宽松、严格三种规则等级。2、支持配置防护动作。 3、支持对请求智能语义检测，支持观察动作。 4、支持字符串、正则、地域、长度、IP、SQL 注入、XSS 条件的自定义规则。 5、支持白名单、黑名单配置，可匹配 URI、IP、Cookie、Geo、Header，匹配方式以及后续执行动作。 6、支持规则名称配置，匹配逻辑（精确匹配、包含、前缀匹配），匹配类型（身份证、信用卡，手机号），匹配动作（告警，过滤），URI 7、支持配置 URL 匹配、设置限速 IP/IP 段、限制 QPS 大小及配置动作，包括 302 跳转和拦截（可返回自定义页面）。
云防火墙	1、支持策略风险调优，策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。 2、支持支持源地址转换 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。 3、支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组进行安全策略配置 4、支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御，支持挖矿行为检测和勒索病毒检测。发现病毒发送的告警信息，支持用户编辑告警内容。 5、支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。 6、支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证。 7、支持 IPsec VPN 智能选路，根据隧道质量调度流量。
云安全运营中心	1、支持安全能力统一管理、大屏呈现整体/网络/主机/纵深防御态势等数据信息、支持大屏告警及自定义 logo 与标题 2、支持分类统计各类资产（云主机、容器、物理服务器、网站）在线数量统计，通过进行资产扫描，对外暴露的端口和应用进行看板可视化呈现，可以直

	观呈现当前资产，存活公网 IP 数量、开放端口数量、暴露端口及应用类型数量，并可以支持自定义违规端口和应用，并将端口和应用按照 TOP10 进行分类统计； 3、支持进行攻击源 IP 统计分析，包括攻击总次数，攻击 IP 总数，并支持按照攻击源检测引擎进行分类统计分析，支持自定义规则制定聚合攻击网段排名，呈现攻击源 IP 地址位置分布（国家-省份-城市） 4、支持实时分析漏洞功能，漏洞分析类型包含 web 常见漏洞、弱密码漏洞、端口漏洞、API 漏洞等，支持呈现漏洞类型分析、漏洞态势与危害和处置建议，并支持导出漏洞报告 5、支持安全调查响应：围绕企业用户日志集中管理和搜索分析核心需求，全量日志分析可对现有的基础日志、告警日志、安全日志进行管理。同时支持用户自定义威胁检索，另存为威胁告警，日志导出，自定义报表分析，日志状态管理等功能。查询方式分为：检索模式，实时模式。检索模式：检索模式实际上是周期性查询底层数据，所以需要指定查询周期。 5、支持安全日志实时分析、关联、聚合，支持查看系统遭受的攻击详情和遭受的各类攻击信息，如暴力破解，有效溯源出攻击 IP 和入侵弱点 6、支持基于不同类型安全检测引擎进行安全威胁检测分析，包括但不限于终端安全检测引擎、Web 攻击检测引擎、DDoS 攻击检测引擎、应用安全检测引擎、网络入侵检测引擎、威胁诱捕检测引擎、威胁情报检测引擎、文件沙箱检测引擎、AI 异常检测引擎等； 7、支持多个厂家安全产品日志接入，包括但不限于长亭科技（洞鉴 X-ray）、华顺信安（Fofa）、青藤云安全（主机安全）、腾讯云安全（御界）、火绒安全（终端杀毒）、谷歌云（入侵检测）、Cloudflare（SCDN）、网神防火墙、深信服防火墙、华为云防火墙、京东云安全产品等。 8、支持安全剧本编排能力，包括：1）支持自定义安全剧本，包括安全剧本的创建、删除、修改、查看等操作；2）支持可视化的安全剧本画布功能，包括支持通过模块化、拖拉拽的方式在画布中编辑安全剧本；3）剧本内支持聚合节点和判断节点设置；4）支持多种数据接入方式（包括但不限于告警、kafka 消息、工单状态通知等）；5）支持数据调查功能，能通过 API 联动其他业务系统；6）支持触发式流程驱动，支持多种触发方式（至少包括告警触发、定时器触发、资产变更触发、kafka 消息触发、扫描结果触发）；7）支持子剧本的配置管理和引用；8）支持剧本执行过程中的状态统计与查看，包括每个流程的执行实例、节点执行状态和执行输入输出结果；9）支持剧本执行的实时效果展示。 9、支持安全工单系统：致力于为用户提供企业安全告警事件处置的凭据。负责公司内业务系统安全人员，可以通过安全工单服务快速将发现的已知系统漏洞、被攻击资产、当前的告警事件，及时流转对应业务归属部门及业务归属人，同时监控业务团队进行漏洞修复、资产加固、事件处置的状态。可以帮助用户实现告警处置闭环，及时发单到人、追踪跟进解决。 10、支持用户行为分析能力，包括：1）支持 NAT 日志行为分析：至少包括源目的 IP/端口、会话连接状态、协议类型、IP 地理位置信息（包括国家-省份-城市）；支持图表展示，包括 NAT 会话状态统计，TCP/UDP 会话数统计等。2）支持数据库审计日志行为分析：至少包括客户端 IP、匹配命中规则、风险级别、执行结果、SQL 语句等；支持图表展示，包括操作行为统计，风险级别分布统

	计等。3）运维操作审计日志行为分析：至少包括：a) 堡垒机审计日志，包括操作日志、登录日志、修改密码日志等；b) 终端审计日志，包括终端操作日志、终端会话日志、终端修改秘密日志等；c) 支持图表展示，包括行为分析统计，动作行为类型统计等。
网站威胁扫描	1、支持资产风险评估，资产漏洞统计，风险资产统计，漏洞变化分析，TOP N 的风险资产与漏洞类型等功能。 2、支持多种类型添加扫描资产，资产自动关联发现，资产认证与管理，资产登录态管理，URI 白名单设置自定义，模糊匹配查询资产，资产管理可视化等功能。 3、支持快速添加扫描目标资产，按需选择多种扫描模式，灵活选择多种扫描方式，自定义选择扫描速度与选择端口配置，支持 UDP 高级扫描模式，自定义 web 扫描配置以及模糊匹配查询扫描任务等功能。 #4、支持针对安全漏洞风险、IP 资产风险、域名资产风险进行管理，具备海量漏洞检测类型，数百种 PoC 插件检测，以及资产指纹扫描关联能力。提供截图证明，需加盖公章。 5、支持提供评估报告摘要，详细的资产指纹信息，完善的资产漏洞信息，包括：系统存在的 Web 安全漏洞、应用系统安全漏洞，系统存在的弱口令等及修复建议，引导并帮助用户修补漏洞等信息。 5、可以与安全运营中心联动能力，支持通过安全运营中心下发扫描策略。
主机安全	1、支持主机安全功能，支持病毒木马查杀，网页木马查杀，系统后门检测，敏感文件篡改，可疑操作（包含挖矿进程检测，密码文件修改恶意文件下载，代理软件滥用，篡改系统日志，篡改 SSH 秘钥，运行黑客程序）； 2、支持主机漏洞检测，账号口令进行检测，异常登录，暴力破解和合规基线等功能。 3、支持容器安全与宿主机安全在同一管控端，支持联动配置策略与资产管控关联。 4、支持容器资产指纹，包含容器 ID、宿主 ID、容器名称、容器 IP、地域、保护状态，告警详情，基线详情，关联主机。 容器网络拓扑展示，支持通过对集群连接进行分析，识别 IP 五元组对应的资源信息，构建出更高维度的连接拓扑，帮助用户更好地进行网络规划和隔离管理，有效识别出异常连接。阡陌 5、支持从 Pod、Service、App 视角进行流量拓扑连接展示。支持识别 helm3 部署的 kubernetes 应用，能够自动分析每个应用下的 Service、Pod、容器、进程、Node 信息，并构建相互之间的关联关系，使整个应用结构一目了然。 6、支持暴力破解检测，包括：1）检测范围至少包括：SSH、RDP、FTP、中间件（至少包括 MYSQL、SQLSERVER、redis、mongdb、postgresql）；2）支持告警及阻断；支持用户自定义暴破阻断规则，包括判断条件规则、阻断时长等；3）支持暴力破解成功检测及告警，包括但不限于：SSH、RDP、sqlserver、redis、mongdb、postgresq 等。 7、支持防勒索能力，支持主机数据自定义备份及随时按版本和时间恢复功能，自定义范围包含：备份时间，备份文件类型图片，视频，文件，备份地址。 合规基线，支持等保 2.0 二级、三级、CIS、弱口令、中间件基线检测，提供修复方案。中间件基线需支持 redis，nginx，CIS nginx，tomcat，ElasticSearch，Apache，mysql，MongoDB，CIS 等 MongoDB。

	8、支持云+端的查杀机制，上报到云端控制中心进行病毒样本检测，无需本地存放引擎数据，占用主机资源。必须支持多引擎查杀，并提供商业杀毒引擎证明。支持云沙箱以及威胁情报检测能力。支持 AI 杀毒引擎对未知病毒检测进行精准识别，检测率不低于 95%。支持检测勒索病毒、 DDoS 木马、远程控制、挖矿类软件等，并告警用户。 9、支持一键批量及分组下发止损策略，支持根据安全事件级别上传止损策略脚本文件，支持自动触发邮件审批流程。
数据库审计	1、支持数据库访问记录，应至少包括发生时间、业务用户名、操作终端主机名及 IP 地址、终端工具名称、服务器端主机名及 IP 地址、数据库名、表名、SQL 语句、响应时间、返回结果等关键信息。 2、支持对日志进行细粒度解析，支持审计数据库操作(DML)、对象管理(DDL)、控制(DCL)等操作语句的审计，至少包括访问发生时间、操作终端主机名及 IP 地址、客户端 MAC、终端程序名称、访问账号、服务器端主机名及 IP 地址、访问数据库名、操作表名、SQL 语句、数据库响应时间以及返回结果等关键信息。 3、支持以操作类型、时间、IP 地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、敏感数据等作为事件识别规则。
SSL 证书	1、提供多种安全级别的证书产品，包括免费的 DV（单域名）证书和收费的 OV/EV （单/多/泛域名）证书，可选收费的 DV（多/泛域名）证书
堡垒机	1、支持多种用户维护及配置操作，包括创建/删除用户、导入用户、启用/停用用户、编辑用户基本信息及角色、搜索用户等。 2、主机管理支持添加、导入、编辑主机功能；可以将多个主机加入到一个主机组，并对这些主机进行批量授权。 3、支持实时会话，在堡垒机实例上随时切入某个运维会话查看现场操作，管理正在运维主机的会话，对于危险会话可以进行 阻断会话操作。 4、支持会话审计，记录运维人员对主机操作过程中产生的所有会话日志。管理员可通过审计会话定位故障及追溯故障根源。 会话支持在线播放以及下载离线播放两种查看方式。 会话审计支持通过时间段、主机 IP、来源 IP、协议类型等条件进行筛选。支持命令查询，可回放执行过程。 5、支持操作日志记录：包括登录日志、改密日志、操作日志以及会话日志，用来审计用户操作及配置堡垒机所产生的日志。 6、支持基于 SDP 模型实现针对访问主体的身份、网络环境、终端状 态的安全审计。支持 Windows 安装包、Mac 版安装包、Chrome 浏览器插件包，通过安装浏览器扩展插件的方式进行终端绑定，将运维的堡 垒机地址及用户的 AccessKey 及 SecretKey 配置到扩展插件，启用后只能通过该唯一入口访问。
云数据库 MySQL	1、支持高可用架构：主从热备架构，故障可自动转移，实现数据库的持续访问，并支持同城多可用区部署及跨城灾备。 2、支持 SQL 审计功能，记录数据库的全部操作，方便在数据库发生故障时及时追溯。同时支持通过 SSL 加密、 TDE 透明数据加密，进行数据保护。自动备份功能，支持自定义，可在指定时间全量自动备份，支持一键恢复至当

	前实例，并对过去七天的变更进行实时增量备份。
云数据库 MongoDB	1、提供副本集和分片集群两种部署方式，均采用高可用架构，支持自动容灾切换。 2、支持多可用区部署，您可指定主从节点与隐藏节点部署的可用区，可以提供跨机房的高可用。 3、支持自动备份、手动备份和备份恢复 4、支持用户自定义 IP 白名单，从访问源进行安全控制。
云搜索 Elasticsearch	1、提供高可用架构，节点故障自动发现、容灾切换自动完成，确保业务连续性；多可用区部署，数据具有对可用区的感知能力，自动分布到多个可用区，具备跨机房级的容灾能力。 2、支持弹性扩缩容，根据业务需求，灵活调整数据节点的规格和数量， 以及增删专有主节点和协调节点，应对业务波动的同时提高资源使用率，降低冗余成本，升级过程不影响业务运行。 3、100% 兼容 ELK 产品体系，开放大量简单易用的 RestfulAPI，支持 Kibana 等周边生态；默认提供 IK 分词、pinyin 拼音、S3、ICU 分析器等多种插件，支持 SQL 查询，降低使用门槛。 4、支持全托管服务，无需部署维护软硬件设施；提供完善的集群管理、监控、告警服务，您可轻松应对集群中数据的搜索和统计分析工作。 5、可自动、手动均生成集群的健康诊断报告，通过对集群、节点、 索引等十多个诊断项执行健康检查，主动探测集群潜在风险并给出处理建议。
云缓存 Redis	1、支持全托管模式，对实例的生命周期管理、性能分析、备份管理、监控告警、参数配置等服务。 2、支持双机热备架构，主节点故障时，自动完成秒级切换，避免业务受到故障影响，全程无需做任何操作。 3 提供数据指标监控，包括 CPU 负载、QPS、实例使用量、连接数、出入网流量等。
消息队列 Kafka	1、需兼容开源 Apache Kafka，无需部署维护软硬件设施，分钟级即可成功创建出 Kafka 实例。 2、支持多副本机制，通过多副本机制实现故障自动转移，部分 Broker 节点失效时仍然保证服务可用 3、可根据资源使用情况按需扩容，不影响现有业务的同时以满足业务增长需求。 4、支持每秒百万级别的吞吐量和数千个客户端同时读写，实时监控实例、Topic、broker、consumerGroup 状态、设置告警规则，及时发现问题。
访问控制	1、身份&权限管理：支持主账号（租户账号）、子账号、群组、角色（用户角色、服务角色、联合身份角色）、策略管理（控制台登录或者 Open API）。
云监控	1、支持原始采样数据实时上报，对云服务进行实时监控，当云服务的状态变化达到报警规则设置的阈值时，自动发送邮件和短信通知。 2、自持报警则支持自定义报警级别，当资源的监控指标达到阈值时，会自动匹配报警级别。同时报警方式支持报警回调。 3、Dashboard 支持跨地域跨产品管理监控图表。提供汇总、明细、TOPN 图三类视图展现类型，支持放大、数据对比、数据导出等多种的操作方式，满足各种场景下可视化及问题排障需求。
操作审计	1、操作记录：支持账号登录操作、资源变更记录、操作审计查询、 合规性审

	计、安全分析
漏洞扫描服务	1、提供对用户指定的操作系统等提供全面的漏洞扫描服务，由安全专家 对扫描结果进行解读，并提供专业的漏洞扫描报告和修复指导建议。 20 个主机资产或 2 个二级域名。
数据加密服务	#1、提供应用系统数据的签名/验证、加密/解密等密码运算，保证信息的机密性、完整性和真实性，同时提供安全、完善的密钥生命周期管理机制。提供截图证明，需加盖公章 #2、使用符合国家密码管理局（ GM/T 0029-2014 ）和中国人民银行（ PBOC 1.0/2.0/3.0 ）要求的密码机设备，符合国家密码监管部门的监管规范和使用要求。提供截图证明，需加盖公章 #3、数据加密服务使用通过国家密码管理局检测认证的密码机，让用户可以安全地生成、存储和管理密钥，满足合规需求。提供截图证明，需加盖公章 #4、支持国产及国际的加密算法。提供截图证明，需加盖公章
SSL VPN	提供集成 SSL VPN 和身份认证功能，内置轻量级 CA 中心和防火墙，可为用户提供可信认证服务和传输加密服务。
动态令牌系统	提供基于动态口令技术的身份鉴别服务，具备手机、硬件令牌的分发管理、挑战应答动态口令的生成与验证、交易签名的实现与验证、认证服务器身份的验证、用户与系统之间的双向认证等身份认证功能。