|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 参数要求 | 单位 | 数量 |
| 一 | 云安全中心综合运营平台 | 　 |
| 1 | 统一身份认证系统 | 1.提供普通用户与管理员提供统一访问登录入口页面，根据访问权限，展示不同的门户功能。包含普通用户的个人工作台、管理员的管理工作台；2.门户框架包含首页、主题设置、全局搜索、站内消息、公告、用户提醒等主要功能；3.支持门户展示组件视图的自定义与编排能力，自定义个人工作台，可以拖拉拽方式自定义工作台上展示的视图组件；4.支持用户自定义常用应用列表、管理员定义应用类别的应用分类视图管理方式；5.支持组织多棵树管理、上下级管理员分级管理，组织机构支持按模板文件的导入功能；6.支持灵活外部身份源管理，支持LDAP、AD、自定义数据库或excel批量导入；7.支持用户信息脱敏显示，信息脱敏策略与开关可配置；8.支持对僵尸账号、过期账号、弱密码、密码过期、账号锁定、离职人员的身份稽核与治理，并提供身份综合视图进行数据比对与展示；9.支持身份账号治理能力，定期分析出风险账号；10.支持认证策略管理与编排，实现单因素及多因素认证；11.支持认证策略与组织、用户、用户组的绑定，实现不同主体的不同认证策略，并支持优先级设置；12.支持从IAM门户登录、应用门户拦截跳转至IAM门户登录、应用调用IAM平台的API认证服务进行登录、应用内嵌IAM登录窗口的四种登录认证集成方式；13.访问控制策略支持按主体、时间、终端检查项（否安装防病毒软件、屏保策略、终端密码策略等）、环境等因素，支持白名单管理；14.支持自定义密码策略，支持各种复杂强度的密码，支持密码过期检查以及自动改密；15.认证策略、金库策略支持优先级设置；16.支持按标准单点登录协议（OAuth2）、代填单点、票据单点的应用资源集成方式；17.支持应用账号与组织由IAM托管与应用自管方式；18.支持B/S架构的应用资源单点登录；19.支持按角色授权，根据主体的用户、用户组、组织、数据管理范围、菜单按钮、角色、岗位、职级、数据角色纬度进行授权；20.支持按访问授权，支持按用户、资源选择被授权对象范围；21.支持属性授权，根据主体属性（组织、用户、用户组）、客体属性（角色、菜单属性、管理资源范围、访问资源范围）、环境属性（时间、客户端环境—操作系统、浏览器类型、IP等）；22.细粒度权限管控，可控制至元数据字段级别，支持菜单、按钮与互斥设置；23.支持用户对其访问权限的在线委托办理，方便了业务中的协助操作，同时将协助明晰到具体操作人；24.支持金库关系人进行预约申请，避免操作人员在紧急情况下不能及时执行运维访问操作；25.支持平台操作过程实现日志记录与日志查询。 | 套 | 1 |
| 2 | 态势感知系统 | 1. 支持与安全数据中台对接，实现常用数据的采集；
2. 支持把规则分析结果生成内部事件，以作为其它关联分析规则的数据源，进行多重关联分析以支持复杂的安全分析；3.支持查看告警规则触发列表和触发详情，包括规则匹配输入数量、规则输出数量、归并后数量、规则运行时间等；4.支持定义黑白名单，对IP进行加白、加黑等操作，支持设置IP加白或加黑的有效期，白名单可以降低告警的误报率，黑名单可以提升告警的覆盖率；5.支持系统推荐常用字段检索日志，常用推荐字段有源IP、目的IP、源端口、目的端口、设备类型、设备名称、原始事件类型、原始威胁名称、雪花ID等，支持多字段组合检索查询；6.支持高级日志检索，基于检索语言生成检索分析模型，可对长周期安全日志数据进行复杂运算，支持输入查询语句检索；7.支持对日志字段进行排序。支持对展示的日志字段进行聚合分析，选择某个日志字段能够统计该字段的值、日志总数、日志占比，支持选择某个字段值添加、排除到检索查询条件中，根据用户需要提高检索效率；8.支持基于IP的可视化关系图谱方式进行威胁狩猎，实现风险钻取分析功能，根据不同的时间维度、攻击方向、威胁类型、ATTCK&CK战术查看攻击者和受害者的风险要素，对整网安全进行可视化逐层分析和逐级追踪，可以从IP进行下钻分析，聚合关联与该IP相关的所有安全告警与日志，支持逐层节点下钻呈现告警上下游关系；9.具备狩猎报告一键快照能力：支持创建、修改、删除狩猎报告，支持将狩猎关系图、通过狩猎下钻检索的日志和告警等元素一键添加到威胁狩猎报告内容中；10.支持从告警或安全事件页面查看与脆弱性的关联性，能够展示告警中相关资产的脆弱性信息；能够从告警TAB页面直接查看影响的资产、以及该资产存在的脆弱性信息，包括脆弱性类型、脆弱性名称、漏洞CVE编号、漏洞CNNVD编号、资产名称、资产IP等；11.处置动作支持：IP封堵、域名封堵、终端隔离、忽略、加白、线下处置。针对封堵、隔离等动作能够调用联动设备插件下发自动执行处置动作；12.可视化方式展示安全事件统计信息，包含事件名称、威胁等级、攻击结果、攻击者IP、受害者IP、事件状态、检测引擎、开始时间、结束时间、来源设备、受害者资产名称等内容；支持自定义展示安全事件字段；13.支持端网融合安全事件深度溯源分析，还原攻击路径，能够通过链路图方式展示攻击者对应的告警名称以及攻击结果。支持在攻击链路图中下钻查看攻击详情，包括查看该攻击相关的告警信息、标准日志信息、关联的资产、关联脆弱性、处置响应信息，支持展示该攻击的告警威胁定性结果；14.支持还原进程树，在进程树能能够溯源进程信息、进程路径、进程运行账号、进程命令等。便于对终端行为进行溯源分析；15.具备10块态势大屏，包括综合态势、安全告警、外部威胁、横向威胁、外连威胁、脆弱性威胁、恶意程序、资产态势、资产画像、重保演练，大屏显示支持3D效果；16.支持大屏轮播，可以指定轮播的大屏和时间；可批量或者单独设置大屏的过滤参数包括是否情报命中、安全域、组织机构；17.支持剧本任务执行，提供边界一键封堵场景、终端一键查杀场景、Web病毒查杀、挖矿检测场景、勒索防护-漏洞库、漏洞攻击场景、应用漏洞补丁、勒索防护-域名封禁、WEB攻击处置场景、威胁情报匹配+阶梯式自动化响应、IP/域名信息查询、资产漏洞扫描管理、定时任务-防火墙在线检查、定时任务-设置日夜运行策略、日常运维-资产脆弱性统计、日常运维—深度研判场景、IP解禁场景、告警处置子剧本、告警处置扩展子剧本、虚拟补丁、终端查杀、告警处置等不少于30种剧本。
 | 套 | 1 |
| 3 | 产品运营系统 | 1.支持查看授权的整体使用情况，同时具备多个维度进行使用情况的统计展示，包括分启用时间统计、分授权对象统计，也可以查看已使用情况的趋势图；2.支持查看授权对象的授权变更的使用情况，包括具体启用时间、授权消耗、组件、用途等信息；3.支持授权的启用、变更、确认单打印等授权变更管理功能；4.支持查看所有云安全资源池的汇总数据、整体情况，同时可选择云安全资源池的名称，查看单个资源池的运营情况；5.支持查看所有资源池关键数据的统计与排名，包括产品开通统计、工单审批情况、订单记录、实例分布概览、实例在线率产品授权数、订单趋势图等；6.支持各级安全资源的级联配置，通过安全资源池认证后，可完成安全资源池的接入，包括账户、产品、工单、订单等给相关数据的同步；7.支持资源池的工单表单,包括工单号、产品规格、所属资源池节点、租户名称、工单创建时间、审批时间、状态；8.支持资源池的订单表单,包括订单号、部署模式、产品名称、产品规格、资源池名称、租户名称、订单创建时间、状态等；9.支持添加产品、发布、下架、查看、查询等，发布并查看安全市场中的安全服务；10.提供内置等保套餐和管理员自定义组合产品注册套餐功能；11.具备对应资源池的运营数据概览、产品管理、套餐管理、资源池组件点数管理、实例管理、订单管理和工单审批功能；12.具备管理安全组件的工作台、安全市场、实例管理、工单和订单管理功能；13.支持与现有云安全管理平台完成对接。 | 套 | 1 |
| 4 | 场景化运营系统 | 场景化运营平台通用功能：1.支持系统管理功能，运营团队接入新客户时的客户管理、根据不同客户形态进行流程制定以及人员分配；2.支持客户管理功能，维护接入客户的信息、联系方式等，用于关联安全事件例如勒索治理时的客户联络方式，方便完成安全事件推送；3.支持专家管理功能，运营团队的分类分级管理；4.支持流程管理功能，根据客户运营需求，专项场景治理规范，配置不同的分析检测流程，保障事件的有效检出和闭环；5.支持项目管理功能，维护运营项目的基本信息，包括服务类型（试用、正式），运营的SLA、服务级别，运营人员的分配等；6.支持安全运营大屏，通过直观的图表和数据，大屏能够提供全面的安全状况概览，让运营人员一目了然地了解网络安全态势。同时，大屏还可以展示运营人员的工作效率概览，包括事件响应时间、任务完成情况等；7.支持审计日志功能，为保障员工行为规范、满足合规要求，记录可溯，提供审计功能；8.支持产品可视化管理，通过直观的可视化面板，实时展示关键安全态势、警报信息和运维状态；9.支持数据接入功能，支持多种安全设备、系统和应用程序的数据接入，确保信息流的顺畅与一致性；10.支持与态势感知系统完成对接。 | 套 | 1 |
| 5 | 场景化功能-勒索治理：1.支持勒索情报管理，通过对接多方勒索情报源，保障对最新勒索样本、行为的检测能力。主要包括情报导入、情报下发和处置动作配置；2.支持自动化编排响应，为保障运营的及时性和准确性，通过内置勒索专项分析模型，对高置信的攻击行为进行自动研判，提供自动封禁、查杀文件、阻断进程等勒索常见处置剧本；3.支持运营工作台，将客户以卡片的形式进行分类展示，动态查看各个客户的勒索风险待处置项，动态进行风险打分；4.支持威胁管理功能，提供威胁清单的统一展现和详情下钻的功能页面，运营人员可以按照客户类别查看和处理不同威胁，并依据约定的研判流程进行威胁的分析、处置和跟踪；5.支持事件管理功能，T2运营人员对T1、智能模型确认的勒索危害行为进行事件上升，此功能提供二次复核、应急策略的一键下发，确保对事件进行全面的审查和及时的处置；6.支持勒索威胁狩猎，运营人员根据自身的勒索治理经验和最新情报热点，结合安全日志数据，创建勒索威胁狩猎模型，并进行勒索狩猎任务派发，挖掘潜在攻击；7.支持勒索工单响应，用于对客户提交的工单进行认领和闭环处理；8.支持报表管理功能，报表管理功能支持按照客户要求定期输出勒索专项风险报告，帮助用户全面了解网络安全状况；9.支持资产管理功能，支持按照项目维度，对资产信息进行导入管理，利用可视化技术，分析资产态势、刻画资产画像，并实现资产勒索风险打分10.具备安全运营知识库，提升平台检测能力和人员安全水平，包含漏洞情报、勒索手法研究、勒索威胁狩猎模型等多个维度的安全知识，为平台使用人员提供知识储备。 | 套 | 1 |
| 二 | 云安全中心数据中台 | 　 |
| 1 | 安全数据中台 | 1.提供数据标准管理，包括数据标签管理、日期管理、字典管理、标准规则管理等等；2.通过界面化形式维护安全数据中心的敏感词库，包括敏感词分类、等级和敏感词；通过界面化形式维护安全数据中心的数据标签，包括服务数据标签类型和数据标签值；3.支持数据建模，包括业务规划、模型管理、数仓规划等等；支持通过图形化界面，查看业务规划及逻辑表数量统计，以及通过数据建模导向图进行快速建模操作；4.支持查看系统默认数仓分层及进行自定义数仓分层维护；通过界面化操作，进行业务规划，包括业务板块、数据域、业务对象及业务过程等的规划；同时支持进行可视化业务对象及业务过程相关关系维护；5.支持存储元数据，包括但不限于ElasticSearch存储、Clickhuse存储、MySQL存储、Kafka存储、HDFS存储等类型；6.支持服务元数据管理，包括服务元数据类型和服务元数据值，支持多层级管理；7.支持安全数据管理，提供安全数据的统一维护，包括数据资产目录、数据资产管理、数据归档管理等功能；8.通过界面化形式维护安全数据中心的数据资产，前台可根据服务元数据对资产进行分类展示，维护数据资产时，需要关联模型元数据和服务元数据信息；9.支持数据集成，具有数据主被动采集能力，数据采集组件包括但不限于JDBC、FTP、SFTP、Kafka、FTP、SFTP、Syslg\_tcp、Syslg\_udp、SNMP、HTTP、HTTPS、TCP)、UDP、File、RabbitMQ、Pulsar、Netflw、Webservice、Interface、win终端Agent、linux终端Agent、自定义脚本；10.提供数据预处理能力，包括但不限于数据解析、数据过滤、数据替换、数据校验、关联补齐、数据标签、数据脱敏等；11.具有数据解析能力，针对采集的数据按照配置的规则进行解析，然后将解析后的数据提供给后续其它预处理环节进行数据的预处理，解析方式包括但不限于正则表达式解析、json解析、xml解析、定长解析、分隔符解析、键值对解析、混合解析等；12.支持用户统一管理，包括用户信息查询、用户信息检索、用户信息维护。 | 套 | 1 |
| 三 | 云安全中心基础设施扩容 | 　 |
| 1 | 万兆交换机 | 1.接口≥48个10G SFP+ 端口（满配光模块），≥6个 40GQSFP+端口（满配光模块），冗余双电源。 | 台 | 6 |
| 2 | 超融合服务器1（HDD） | 1.CPU：配置≥2\*(32 Cores,2.2GHz)；2.内存：配置≥1024GB；3.系统盘：配置≥2×480GB SSD；4.缓存盘：≥2\*6.4TB；5.数据盘：≥12\*10TB SATA盘；6.阵列卡：系统盘控制器接口从CPU直出；7.网卡：≥4×10G网卡（带模块）;8.电源：双电源，冗余配置；9.自带国产正版操作系统。 | 台 | 5 |
| 3 | 超融合服务器2（HDD） | 1.CPU：配置≥2\*(16 Cores,2.2GHz)；2.内存：配置≥192GB；3.系统盘：配置≥2×480GB SSD；4.缓存盘：≥2\*6.4TB；5.数据盘：≥12\*10TB SATA盘；6.阵列卡：系统盘控制器接口从CPU直出；7.网卡：≥4×10G网卡（带模块）;8.电源：双电源，冗余配置；9.自带国产正版操作系统。 | 台 | 8 |
| 4 | 超融合服务器3（SSD） | 1.CPU：配置≥2\*(32 Cores,2.2GHz)；2.内存：配置≥1024GB；3.系统盘：配置≥2×480GB SSD；4.数据盘：≥12×7.68TB U.2 NVMe SSD盘,热插拔；5.阵列卡：系统盘控制器接口从CPU直出；6.网卡：≥4×10G网卡（带模块）;7.电源：双电源，冗余配置；8.自带国产正版操作系统。 | 台 | 4 |
| 5 | 管理服务器 | 1.CPU：配置≥2\*(32 Cores,2.2GHz)；2.内存：配置≥1024GB(64GB×16)；3.系统盘：配置≥2×480GB SSD,热插拔；4.数据盘：配置≥2×16TB HDD SATA；5.缓存盘：配置≥1×6.4TB NVMe SSD U.2 ；6.阵列卡：1块独立RAID卡,2G Cache,端口数≥8,端口速率:12Gb/s,配置电池或者电容;支持RAID0、1、10、50、60以及直通；7.网卡：≥4×10G网卡（包含模块）;8.电源：双电源，冗余配置；9.自带国产正版操作系统。 | 台 | 3 |
| 6 | 云平台 | 云平台要求：1.云平台软件产品支持主流设备厂商提供的X86、ARM服务器，同一套平台可以同时管理调度不同硬件厂商的服务器及其资源；2.云平台软件产品支持定义多个资源池集群，每个资源池集群可以拥有独立的服务器、存储、网络配置和虚拟化类型，形成一个独立的资源池，池内所有服务器对等，可以启用集群高可用及资源调度；3.云平台软件产品具备在同一管理平台同时提供CPU云主机、GPU云主机、弹性裸金属、高性能计算（EHPC）和容器云服务能力；4.云平台软件产品架构支持管理集群（含多个管理节点）和业务资源池集群（含计算、 存储、网络节点）分离部署，云平台管理软件单独部署于管理集群中，保证整体安全性和运行稳定性；5.云平台软件产品应支持业内主流架构CPU，如x86（Intel，海光，兆芯，龙芯），ARM（飞腾，鲲鹏），同一个资源池内同时支持上述几种CPU 架构；6.云平台软件产品支持定义多个资源域，根据资源池所在地理位置（例如地域、可用区）等对资源池进行分类；7.云平台软件产品支持基于跨数据中心的分布式网络功能，用户能够自助创建跨数据中心的VPC和私有虚拟网络，创建VPC时根据需要选择区域、设置VPC类型和安全组，创建私有虚拟网络时，支持单数据中心（单可用区）和跨多数据中心（多可用区）部署方式，创建的VPC和私有网络支持加入到项目；8.云平台软件产品提供图形化的统一门户，具有便捷的操作界面，简洁直观的图形展示界面，用户使用统一单点登录界面即可完成对所有云服务的自助操作；9.云平台软件产品支持自定义监控面板，以业务系统视角，监控某个业务系统内所有云主机资源使用情况，并在同一监控面板进行呈现，支持自定义监控指标，如CPU、内存、磁盘、网络带宽等；10.云平台软件产品应提供自动伸缩功能，可以帮助用户基于资源的监控告警规则动态调节配置或集群规模，比如调整带宽上限，扩容关系型数据库的存储空间，增加或减少负载均衡器后端数量；11.云平台软件产品提供云主机全生命周期管理，在同一界面上同时提供云服务器修改、启动和删除、批量克隆云服务器（对多台运行状态下的云服务器进行批量克隆）、批量绑定指标告警、批量绑定事件告警、重置系统、重置登录密码、更换系统、时间同步、项目管理（支持创建的云服务器加入到项目）。12.分布式存储产品支持对云硬盘IOPS、吞吐量、空间使用率、逻辑空间等指标进行实时监控；13.分布式存储产品提供云硬盘生命周期管理，包括创建、删除、挂载、卸载、快照、备份、扩展、编辑名称、更新状态、重置挂载状态、更改属性功能，支持单块云硬盘容量100TB。 | 套 | 1 |
| 7 | 容器平台要求：1.容器平台需通过 Kubernetes 一致性认证，涵盖 Distribution、Hosted、Installer 三个领域；2.支持多集群资源数量聚合汇总，包括但不限于集群数量、节点数量、namespace 数量、容器组数量、deploy 数量、有状态副本集数量、守护进程级数量、任务数量、定时任务数量、pvc 数量、svc 数量以及应用路由数量；3.支持对接多种日志收集者，将平台中的日志推送到第三方平台，如：elasticsearch、kafka、opensearch等。容器平台软件应包含至少一种日志平台；4.支持数据库应用专属控制台，可进行常规数据库操作如备份、添加数据库用户名、修改数据库用户密码等；5.管理分布在多数据中心、多云平台上的Kubernetes集群，比如：私有云、虚拟化平台、物理机等；6.支持多集群可用性动态感知及动态分配；7.可查看Kubernetes集群中主机的基本信息，包括私有云或物理机资源配置、IP 地址等，可查看主机资源、Pod列表、标签、IP等主要信息；8.为了方便细粒度的对DevOps项目进行管控，容器平台应预置DevOps项目角色，方便用户快速授予用户内置角色，加速应用研发；9.提供在线命令工具，可实现集群命令行化操作以及容器内命令行操作；10.提供应用的全生命周期管理，可实现应用创建、打包上传、应用审核、应用上架、测试部署、版本管理、应用下架等功能，还包括应用仓库管理、一键部署应用等，对应用的生命周期有完整的管理机制。 | 套 | 1 |
| 四 | 云安全服务能力 | 　 |
| 1 | 多方计算平台 | 1.包含基础管理模块、安全求交、隐匿查询、多方计算、联合建模、基础组件库；2.支持基于Python语言的MPC算法编译功能；3.支持基于SQL语言的MPC算法编译功能；4.支持开发可视化IDE，提供图形化操作页面；5.支持提前开发部署匿踪查询编码库，提升查询效率；6.支持用户身份、位置信息等核验；7.支持配置联邦学习算法并配置训练集、测试集、学习率等参数，执行联邦学习模型训练和计算，根据模型评估指标进行迭代优化；8.支持对特征进行分箱操作，计算IV、WOE、VIF完成特征选取；9.支持调用模型API实现模型推理预测，支撑业务应用，支持批量预测；10.支持建模流程可拖拽编辑，提供拖拉拽的编程操作方式；11.支持用任意关键字对所有事件进行高性能全文检索；12.支持可指定多个查询条件进行组合查询；13.根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义。 | 套 | 4 |
| 2 | SaaS安全服务-终端检测与响应 | 1.提供至少6000个终端授权；2.具备资产管理、虚拟补丁、病毒防护、漏洞管理、EDR、基线核查、运维管控、软件商店等全部功能模块； 3.资产登记功能支持与AD域、LDAP域等用户认证系统同步组织结构，终端登记信息支持与AD域中的信息进行校验，错误信息提示终端用户修改；4.按攻击面维度统计并展示已知资产、互联网暴露面资产的攻击点，攻击点包括：未安装的高危补丁、开放的高危端口、存在的弱口令账号、连接的外设资产；5.支持一个管理控制台同时管理Windows,Linux,信创操作系统，同时支持这些操作系统的服务器版和客户端版；6.支持统计单个终端的最近24小时、7天、30天的安全威胁，包括：病毒风险、入侵检测事件、失陷检测事件。并计算相较上一周期的增长环比；7.支持以推荐措施的维度，展示针对系统内所有风险的推荐措施，措施信息包括：风险描述、处置措施步骤、受影响终端的统计与信息展示、受影响策略、推荐时间、所属类别；8.提供基于程序行为的独立恶意行为监控引擎，基于进程的操作行为和序列组合来应对未知威胁；9.具备预测机器学习技术，可检测可疑进程中或来自可移动存储、Web邮件等各渠道的文件中的新兴未知安全风险威胁；10.支持针对不同病毒类型针对性设置处置措施，可设定清除动作前，备份文件；11.具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新；12.支持终端防火墙功能，可依据以下标准设定规则：远程IP，方向（出站\入站），协议（所有协议\ICMP\TCP\UDP\TCP+UDP）,端口；13.基于性能和业务需求，可配置探针记录内容（文件、进程、网络、注册表、系统、脚本、UMH、WMI事件）的详细程度和规则检测范围，支持“低消耗模式”、“均衡模式”和 “高检出模式”；14.支持管理员配置是否分别打开或关闭需记录事件类型（包括文件、进程、网络、注册表、系统、脚本、UMH、WMI事件）与事件记录子类型（包括文件创建、文件打开、文件写入、文件更名、文件删除、进程伪装、动态链接库注入、PE文件注入、脚本注入、线程劫持等）；15.在Windows 操作系统上，对于恶意域名访问检测，可精准定位的发起域名请求的原始进程信息而不是svchost；16.提供远程遏制终端给管理员，仅保留终端与服务器的连接，有效避免威胁蔓延。并支持配置遏制白名单，遏制白名单支持按IP、域名、进程名/进程全路径进行添加白名单；17.支持以终端维度查看终端所有资产信息，包括运行应用，安装软件，硬件，账号详情，启动项，进程，系统服务，计划任务，端口，数据库，Web服务，web站点，web应用，web框架，进程，系统服务，jar包和第三方类库；18.支持从运行进程统计中直接指定进程黑名单；19.支持禁用双网卡连接，禁用后仅支持与服务器连接的网卡通讯，断开其他网卡的网络连接；支持设置移动数据网卡的禁用、启用；支持禁用WIFI连接，同时支持配置允许使用的SSID白名单；支持禁用代理服务器，同时支持配置允许使用的代理服务器白名单，支持以IP或域名的方式添加白名单；支持禁用DNS域名解析服务，同时支持配置允许使用的DNS服务器白名单；20.支持对注册表键值进行保护，不允许被修改；当某个注册表键不存在时，支持管理员配置是否自动创建，则能够根据配置自动创建注册表键值；21.能够按照软件标识识别终端上已安装的软件，并将相同软件的不同版本聚合展示，便于统一管理和维护；22.对于白名单之外的域名访问，能够直接执行阻断动作，禁止访问违规域名；联动EDR能力，对于恶意域名可直接点击进入“调查分析-新建调查”页面，将域名条件带入进行调查。 | 套 | 1 |
| 3 | 网络安全靶场 | 1.支持讲课和实操两种培训模式，讲课模式仅支持操作员查看教员屏幕，实操模式既支持操作员查看教员屏幕也支持操作员登录自身环境实操；2.支持教学管理功能，包含教学班级管理和教学内容管理；3.支持教学内容管理，可基于课程、实验、试卷安排教学；4.支持教学环境自动管理功能，包含自动部署环境、自动分配环境、自动开始课节、自动结束课节以及自动销毁环境；5.支持教员对教学环境进行手动管理，包含一键部署、一键销毁、单个部署、单个业务系统标准指标销毁等；6.支持操作员上传教学报告，并支持教员对报告进行预览、评级；7.支持教员查看操作员学习情况，包括指导书学习统计、答题记录、视频学习统计等；8.实操实验自学支持操作员自主管理实操环境，包括手动部署环境、手动销毁实操环境和手动延长实操环境保留时间，并支持实操环境的定时销毁；9.支持操作员对视频进行锚定，系统自动截取视频的当前播放画面，支持操作员为每个锚点添加文字说明；10.支持自动判定是否已学，包括指导书、视频、文档等学习资源的判定；11.支持集中考试管理，包含设定人员、起止时间、试卷等信息；12.支持个人自测功能，操作员可选择同一份自测试卷多次自测，系统自动判分并记录每一次自测的成绩；13.支持系统自动判定考试成绩，并支持自动检测及记录考试违规行为；14.实操实验包含实操环境、指导书、课件、学习视频、随堂练习5个方面的内容；15.理论学习包含指导书、课件、学习视频、随堂练习4个方面的内容；16.支持实操实验自定义，包含创建、修改、删除、测试、发布等操作；17.支持三种试卷类型，包含定序试卷、随机顺序试卷、不固定题目试卷；18.支持渗透闯关场景管理，可对场景进行导入、导出、编辑、删除等操作，并支持查看指定场景创建人、创建时间等详情信息；19.渗透闯关场景下支持创建空白任务和基于场景创建任务两种创建任务方式，并支持对任务进行编辑、删除以及查看详情等操作；20.渗透闯关场景下支持团队管理，可定义角色的名称、组别等，角色类型包括管理类、设计类、裁决类、操作类等；21.渗透闯关场景下支持设备管理，可实时展示设备运行状态，并支持设备接入以及对设备进行开机、关机、重启、重置、修改密码等操作；22.渗透闯关场景下支持流程事务、临机事务两种事务模式，并可对环境事务、人员事务、判断事务等多种类型事务进行管理与运行状态监控；23.支持红蓝对抗场景管理，可对场景进行导入、导出、编辑、删除等操作，并支持查看指定场景创建人、创建时间等详情信息；24.红蓝对抗场景下支持创建空白任务和基于场景创建任务两种创建任务方式，并支持对任务进行编辑、删除以及查看详情等操作；25.支持使用目标网络模板快速构建目标网络拓扑，包括选择内部模板和导入外部模板两种方式；26.提供虚拟网络的二层VLAN配置能力；并支持VLAN配置在两个交换机间传导的精确控制；27.支持多层次网络配置编辑，通过拖拽并配置子网络的方式实现网络层次化编辑，包括子网络基础信息以及子网络内的网络、节点等相关配置；支持右键展开和关闭子网络的拓扑结构；28.支持查看目标网络中虚拟节点及实物节点的实时运行状态，包括节点运行中、已关机、已挂起、已搁置等多种运行状态的实时查看；29.支持以图表的形式对虚拟节点的CPU、内存、磁盘利用率等信息进行展示，以及磁盘读写吞吐量、网卡出/入流量、网卡出/入丢包率等相关信息监控展示；30.支持系统中虚拟服务器节点、客户端节点、虚拟网络节点、虚拟安全设备节点等不同功能类型节点的生成，支持常见网络和安全设备，包括交换机、路由器、防火墙、IDS、WAF等；31.支持X86架构虚拟机、ARM架构虚拟机、容器的混合生成，同一二层网络中支持三种虚拟化节点；32.支持虚拟机和容器多网卡的仿真，支持对指定虚拟链路的详细特性进行设置，包括链路带宽、延迟和丢包率等，用于模拟相关区域的网络实际情况；33.路由器仿真支持进入路由进行路由配置，虚拟路由支持RIP、OSPF、BGP、等常用协议，支持配置IPsec、OpenVPN等多种VPN协议，支持VXLAN协议，并能够与实物路由互联互通；34.支持根据不同的虚拟节点类型，自动选择KVM域或者Docker域；35.支持部署过程的监控和展示，支持对部署的各类节点总数、各类节点进度、部署错误的类型进行展示，显示进行中、等待中、失败和成功的具体节点和数量，对于部署失败的节点，系统给出失败原因。部署状态支持自动和手动刷新的模式；36.单一拓扑增量部署次数不限，并能记录各次的部署记录。37.支持将异地的设备接入到虚拟网络中，并与虚拟网络中的虚拟机和容器在同一编址空间；38.支持配置公共网络IP地址池，可给不同的试验环境配置不同的公网IP地址池，支持公网IP地址池的管理。39.具备单位配置管理能力，可配置单位名称、单位描述、单位所属系统等信息；支持单位的增、删、改、查等操作40.支持虚拟节点启动配额管理，可定义虚拟节点 CPU、磁盘和内存的大小，支持配额的新增、删除、查询以及将本地配额同步到虚拟化平台;41.系统网络和外部网络之间互相隔离，保证系统免受外部的攻击；42.具备目标网络信息列表展示能力，支持显示目标网络的名称、IP、部署状态、虚拟节点数量、目标网络使用计算域、创建人、所属系统、所属单位、创建时间等信息。 | 套 | 1 |
| 4 | 防火墙 | 1.国产CPU，千兆电口≥6个, 千兆光口≥4个，万兆光口≥4个；硬盘≥1TB；配置双电源；2.吞吐量≥20Gbps，应用层吞吐量≥12Gbps，最大并发连接数≥500万，每秒新建连接数≥50万；3.整机同时具备防火墙、服务器负载均衡、入侵防御、防病毒、应用识别和web应用防护（WAF）等功能；4.可基于每个SSLVPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控；支持IPsecVPN智能选路，根据隧道质量调度流量；支持SSL的版本包括TLS1.0、TLS1.1、TLS1.2、TLS1.3；5.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、内容安全（WAF、IPS、数据过滤、文件过滤AV、URL过滤和APT防御等）统一界面进行安全策略配置；6.支持策略风险调优，支持安全策略优化分析，支持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；7.支持SQL注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库、网页应用等设备的专属特征分类，支持CC攻击防护，可基于检测请求报文头的X-Forwarded-For字段，以获取真正的源IP地址；8.支持至少5000种独立Web特征的攻击检测和防御特征库；9.当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时(比如将原厂商的摄像头换为其他厂商的摄像头)向用户发送日志提示用户；10.设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤;设备支持管理者自定义新的URL地址和URL分类；支持不解密的方式实现HTTPS URL过滤；支持联动云端URL地址库进行全面实施核查；11.僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现；基于应用的数据分析；12.支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单；13.可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表;防病毒本地库数量600万+支持基于文件协议、邮件协议(SMTP/POP3/IMAP)、共享议(NFS/SMB)的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持用户编辑告警内容；14.支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理且代理策略中可同时配置多类过滤条件，具体包括:源安全域目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项；15.支持服务器负载均衡(SLB)，支持基于HTTP、RADIUS、MYSQL等应用类型的匹配，支持基于IP流量特征、ISP、用户入接口、TCP载荷等类型的匹配规则。 | 台 | 6 |
| 5 | 云防火墙 | 1.国产CPU，万兆光口≥16个；硬盘≥480GB；配置双电源；2.吞吐量≥40Gbps，应用层吞吐量≥25Gbps，最大并发连接数≥40000万，每秒新建连接数≥100万；3.整机同时具备防火墙、服务器负载均衡、入侵防御、防病毒、应用识别和web应用防护（WAF）等功能；4.可基于每个SSLVPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控；支持IPsecVPN智能选路，根据隧道质量调度流量；支持SSL的版本包括TLS1.0、TLS1.1、TLS1.2、TLS1.3；5.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、内容安全（WAF、IPS、数据过滤、文件过滤AV、URL过滤和APT防御等）统一界面进行安全策略配置；6.支持策略风险调优，支持安全策略优化分析，支持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；7.支持SQL注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库、网页应用等设备的专属特征分类，支持CC攻击防护，可基于检测请求报文头的X-Forwarded-For字段，以获取真正的源IP地址；8.支持至少5000种独立Web特征的攻击检测和防御特征库；9.当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时(比如将原厂商的摄像头换为其他厂商的摄像头)向用户发送日志提示用户；10.设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤;设备支持管理者自定义新的URL地址和URL分类；支持不解密的方式实现HTTPS URL过滤；支持联动云端URL地址库进行全面实施核查；11.僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现；基于应用的数据分析；12.支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单；13.可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表;防病毒本地库数量600万+支持基于文件协议、邮件协议(SMTP/POP3/IMAP)、共享议(NFS/SMB)的病毒功能（提供界面截图并加盖公司公章）。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持用户编辑告警内容；14.支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理且代理策略中可同时配置多类过滤条件，具体包括:源安全域目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项；15.支持服务器负载均衡(SLB)，支持基于HTTP、RADIUS、MYSQL等应用类型的匹配，支持基于IP流量特征、ISP、用户入接口、TCP载荷等类型的匹配规则。 | 台 | 2 |
| 6 | 管理防火墙 | 1.国产CPU，千兆电口≥6个, 千兆光口≥4个；硬盘≥1TB；配置双电源；2.吞吐量≥10Gbps，应用层吞吐量≥5Gbps，最大并发连接数≥200万，每秒新建连接数≥15万；3.整机同时具备防火墙、服务器负载均衡、入侵防御、防病毒、应用识别和web应用防护（WAF）等功能；4.可基于每个SSLVPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控；支持IPsecVPN智能选路，根据隧道质量调度流量；支持SSL的版本包括TLS1.0、TLS1.1、TLS1.2、TLS1.3；5.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、内容安全（WAF、IPS、数据过滤、文件过滤AV、URL过滤和APT防御等）统一界面进行安全策略配置；6.支持策略风险调优，支持安全策略优化分析，支持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；7.支持SQL注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库、网页应用等设备的专属特征分类，支持CC攻击防护，可基于检测请求报文头的X-Forwarded-For字段，以获取真正的源IP地址；8.支持至少5000种独立Web特征的攻击检测和防御特征库；9.当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时(比如将原厂商的摄像头换为其他厂商的摄像头)向用户发送日志提示用户；10.设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤;设备支持管理者自定义新的URL地址和URL分类；支持不解密的方式实现HTTPS URL过滤；支持联动云端URL地址库进行全面实施核查；11.僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现；基于应用的数据分析；12.支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单；13.可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表;防病毒本地库数量600万+支持基于文件协议、邮件协议(SMTP/POP3/IMAP)、共享议(NFS/SMB)的病毒功能（提供界面截图并加盖公司公章）。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持用户编辑告警内容；14.支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理且代理策略中可同时配置多类过滤条件，具体包括:源安全域目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项；15.支持服务器负载均衡(SLB)，支持基于HTTP、RADIUS、MYSQL等应用类型的匹配，支持基于IP流量特征、ISP、用户入接口、TCP载荷等类型的匹配规则。 | 台 | 2 |
| 7 | 防毒墙 | 1.国产化CPU，千兆电口≥4个，万兆光口≥2个；配置双电源；内存≥32GB，硬盘≥2TB；2.网络层吞吐率≥10Gbps；3.能够对威胁进行可视化展示，展示维度至少包括威胁类型统计（至少包含勒索、挖矿、病毒、APT、漏洞利用威胁事件）、近30天威胁事件趋势、攻击源IP TOP5、受影响主机TOP5、勒索&挖矿事件拦截统计、热门威胁事件TOP5、自定义黑名单TOP5等；4.能够支持超过100种协议的解析, 包括但不限于HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC等；5.能够支持SMBv1/SMBv2/SMBv3文件共享协议的病毒检测与查杀,且针对SMBv3协议，并能对256k以上的文件进行病毒检测和过滤；6.能够支持两个的防病毒引擎同时工作，并能够按需开启；7.能够支持快速扫描模式和深度扫描模式切换，确保在不同网络环境下的查杀效率；8.支持反向代理部署模式，支持该模式下对HTTP/HTTPS流量解析检测，并支持阻断或监控模式；9.能够允许定义被扫描文件的大小范围，最大不小于2G；10.威胁情报IOC检测，支持的威胁类型包括但不限于：远控、钓鱼、僵尸网络、矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、黑客工具、APT攻击事件、流氓推广、其他恶意软件，IOC情报总量达800万以上。IOC检测类型支持域名、URL、IP类型的威胁情报检测，对IP情报可以精确到端口级别的研判；11.支持用户自定义黑/白名单，支持URL/DOMAIN/IP类型 黑/白名单设置、支持邮件收发件人黑/白名单设置、支持基于SHA1的文件黑/白名单设置；12.为保证安全性，防止未授权访问，管理中心应具备密码+动态口令等双因素认证方式，且动态口令有效期不能超过30秒；13.支持自动/手动在线升级，可配置自动升级周期；提供基于策略（源和用户/目标/通讯类型/时段）的流量日志记录/查询/导出；14.提供特征码最新版本检测和提示功能，提升设备的可维护性；15.可对CPU、内存阈值进行设置，当超过该阈值，防毒墙主进程自动清理且不中断业务。 | 台 | 4 |
| 8 | 抗DDoS系统 | 1.国产化CPU，千兆电口≥6个，万兆光口≥4个；配置双电源；内存≥64GB，硬盘≥1TB；2.网络层吞吐率≥10Gbps，最大并发连接数≥6000万，新建连接率≥126万；3.支持流量攻击自动防御：可自动防御 SYN Flood 、SYN-ACK Flood、 ACK Flood、FIN/RST Flood、ICMP Flood、UDP Flood、IP Fragment Flood、Stream flood、Ping of death、Land、Teardrop、Smurf等攻击；4.支持应用型攻击防御：可防御DNS Query Flood、DNS Reply Flood、Connection Flood、HTTP Get Flood、HTTP Post Flood、CC攻击等；5.支持空连接、新建连接攻击防御；支持并发连接TOPN自动过滤，可防御突发攻击导到服务崩溃；支持TCP 连接双向代理；支持TCP连接自动超时；6.支持动、静态IP黑、白名单。动态黑、白名单支持策略自动加入、支持手动添加、批量导入；动态黑名单内IP地址支持访问二次加黑延时；支持静态黑、白名单手动添加、导入/导出；支持全局动、静态黑、白名单，支持针对服务器动、静态黑、白名单；7.支持自定义特征码防御，自定义特征码报文限速、支持特征字符包内出现频率限制，支持特征包大小限制，自动加白、加黑特征源IP、自定义含特征字符数据包关联匹配限制，自定义策略间联动等；8.支持DNS防护：可防御DNS Request Flood、DNS Replay Flood、DNS缓存感染攻击（DNS投毒）、防DNS欺骗攻击、DNS宕机保护、支持DNS域名黑白、名单，DNS静态解析、DNS QOS配置、随机域名防护、域名劫持配置、DNS防护报表等能力；9.支持多元组超级ACL过滤（外部地址、外部端口、内部地址、内部端口、协议、TCP标志位、地区（洲、国家、省）；10.支持攻击时自动抓包功能，当系统检测到攻击时，自动启动抓包，及时保留攻击证据和攻击报文情况，为日后追责，分析攻击情况提供帮助；支持指定接口抓包；集群部署时支持所有设备同时抓包；11.支持在线数据包查看分析、展示所抓取数包内中的 HTTP URL访问信息、连接统计信息；支持针对分析出的指定报文特征自动导入防护规则；12.支持攻击溯源，攻击溯源报表内可显示攻击源IP、攻击次数、攻击类型、攻击源归属地、攻击源ISP线路、统计时段、攻击目标；13.支持对HTTP/HTTPS 的URL分析、HTTP相应分析、HTTP请求分析、User-Agent分析、Referer分析、客户端流量分析、客户端连接分析、其他分析；14.支持防护对象实时连接状态监控，支持协议、源IP、源端口、目地IP、目地端口、五元组实时连接信息查看；支持源IP+目的IP+目的端口三元连接信息统计；支持对三元连接统计信息按条件加黑；16.支持透明串行、单臂旁路、双臂旁路部署、支持集群部署、主备部署；17.支持导出生成安全报告，报告包括统计报表，可自定义报告统计的时间范围，日攻击峰值流量TOP10，服务器峰值流量TOP10， 攻击类型--攻击次数TOP10,攻击类型—攻击包数TOP10,IP流量攻击TOP10,IP攻击次数TOP10，IP攻击包数TOP10,IP攻击时间TOP10。 | 台 | 2 |
| 9 | 堡垒机 | 1.国产化CPU，内存≥32G，硬盘≥8TB，千兆电口≥6个，千兆光口≥4个，接口扩展槽位≥2个；2.资产管理授权≥300个，最大图形并发连接数≥200个，最大字符并发连接数≥700个；3.主机访问工具应支持:SecureCRT、Xshell、Putty、WinscP、Filezila、MSTSC、RDP、mobaXterm、vmwareclient等客户端；4.数据库访问工具应支持:MySQL-Front、PLSaL、sqlplus、ssMs、db2cmd、SqlDbx、Quest Central for DB2、dbaccess、DM数据库工具、Kingbase数据库工具、sQLyog、Toad、dbeaver；5.支持远程应用单点登录的客户端水印，水印信息包括用户信息及运维时间；6.支持可自定义个人运维资产组，便于快速搜索;设置优先展现资产收藏页或运维资产列表页；7.SFTP/FTP协议应支持控制上传文件、下载文件、删除文件、重命名文件、创建文件目录、删除文件目录、支持留痕文件的大小设置；8.支持调用本地数据库客户端工具Navicat、PLSOL、DM6、DM7、Kingbase、dbever访问数据库资产，支持数据库访问通过本地客户端、远程应用发布方式进行单点登录:;支持通过远程工具mobaxterm、securecrt访问主机；9.支持应用资产访问可指定登录资产所使用的浏览器类型，支持可选择本地浏览器或应用发布浏览器访问；10.支持运维人员使用的客户端工具管理，包括工具统一上传、统一下载等；11.支持本地密码认证、动态口令认证;Radius认证、LDAP认证、AD域认证、短信认证、LDAP认证、USBKEK(北京CA/格尔CA)、指纹认证、X.509证书认证、邮箱认证；12.支持用户忘记登录密码时，在登录首页申请密码重置;支持手机短信、令牌口令、邮箱三种方式重置密码；13.支持AD\LDAP账号同步，支持从windows AD域\LDAP抽取用户账号作为主账号，支持自定义选择AD域的组织机构进行导入；14.支持手工、自动方式发现目标资产，自定义配置IP地址段及自定义资产协议端口，精确识别是否在系统中存在，支持一键导入；应支持手工、自动方式采集主机资产上的帐号列表，精确识别是否在系统中存在，支持一键导入；15支持在线会话和历史会话审计，应支持以字符会话回放、图形会话回放、数据库会话回放、发布服务器会话回放四种方式实现会话操作审计；16.支持内置Web安全组件，防护不因网络调整或内网绕行而失效；17.支持SQL注入、XSS攻击的检测与防御能力，支持Web恶意扫描防护的检测与防御能力；18.支持会话复核，登录目标资产时需要经复核人复核后才能登录，会话复核规则可以指定运维人员、资产、资产账号及会话复核人；19.支持高危命令审批，用户执行高危命令时需要经复核人复核后才允许执行，命令复核规则可以指定运维人员、资产、资产账号及命令复核人；支持Linux命令行及SQL命令；20.支持手工重置账号密码并实时推送至目标资产；支持自动识别主机上的修改密码的命令，并将修改后的密码在系统中更新，减少管理员重复录入； | 台 | 1 |
| 10 | 日志审计 | 1.国产化CPU，内存≥64G，硬盘≥16TB，千兆电口≥4个，接口扩展槽位≥1个；2.审计日志源≥220个，日志处理性能≥4000EPS；3.独立完成审计日志采集，不依赖于设备或系统自身的日志系统；4.审计工作不影响被审计对象的性能、稳定性或日常管理流程；5.审计结果存储于独立存储空间；6.自身用户管理与设备或主机的管理、使用、权限无关联；7.提供全中文WEB管理界面，无需安装任意客户端软件或插件；8.支持使用代理(Agent)方式提取日志并收集；9.支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP、Telnet、SSH协议日志收集；10.支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；11.支持对收集到的重复日志进行自动聚合归并，减少日志量；12.支持跨设备进行数据关联分析；13.支持对用户登录事件、攻击威胁事件、web安全事件的专项审计；14.支持SOX合规、ISO27001、WEB安全3类合规项审计；15.支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、地理城市等参数进行过滤查询；16.支持用任意关键字对所有事件进行高性能全文检索；17.支持可指定多个查询条件进行组合查询；18.根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义。 | 台 | 1 |
| 11 | 漏洞扫描 | 1.国产化CPU，内存≥32G，硬盘≥4TB，千兆电口≥4个；配置双电源；2.最大可扫描IP地址无限制，系统漏扫并发任务数为≥10，单任务系统扫描最大并发扫描IP数为≥180，弱口令扫描并发任务数为≥8；3.支持多用户多任务并发扫描，系统漏扫任务，单任务最大IP数量无限制；4.支持智能服务识别、授权登录扫描、多路扫描（可以同时对多个隔离网络进行扫描）等；5.支持20种以上的默认扫描策略，分别针对不同的扫描对象，如Windows、类Unix、数据库、WEB服务、网络设备、云平台、摄像头、大数据、国产化等；6.系统漏洞知识库兼容CVE、CNCVE、CNNVD、CNVD、CVSS、Bugtraq等主流标准；7.WEB漏洞知识库数量大于20000条，所有的漏洞信息都能够在产品中随机进行浏览和多维度检索；8.支持检测的漏洞种类需覆盖：OWASP TOP10、OA系统漏洞、邮箱系统漏洞、集权设备漏洞、CMS漏洞、开发框架漏洞、网络设备漏洞、操作系统漏洞、数据库漏洞、应用服务器漏洞、Web中间件漏洞、智能设备漏洞、移动终端漏洞、工控设备漏洞等；9.支持全自动进行漏洞探测，自动进行IP端口检测、漏洞验证过程。；10.支持采用基于漏洞原理的验证技术来漏洞验证；11.支持盲测技术，可检测和验证需要反连才能确定真实存在的漏洞；12.支持非授权扫描，只需要配置目标数据库的IP地址和端口号；13.数据库漏洞知识库数量大于2500条，所有的漏洞信息都能够在产品中随机进行浏览和多维度检索；14.支持配置核查任务针对不同主机选用不同策略；15.支持对弱验证码逻辑漏洞的扫描策略配置；16.支持扫描进度展示，包括：任务进度、IP进度、扫描目标总数、正在扫描目标数、预计剩余扫描时间、漏洞信息、端口服务信息等；17.支持断网续扫、断电续扫、断点续扫；18.支持漏洞闭环管理流程，可配置管理资产范围、风险等级；19.离线报表格式支持：html,word,excel,pdf,xml,wps等；20.提供对外联动接口，支持第三方安全产品（如防火墙、安管平台）通过接口调用扫描系统进行扫描。 | 台 | 1 |
| 12 | 数据库审计 | 1.国产化CPU，内存≥32G，硬盘≥8TB，千兆电口≥6个，接口扩展槽位≥1个；2.吞吐量≥3Gbps，支持数据库数量不限，支持数据库审计类型≥4种；3.支持旁路部署模式，部署在物理交换机或虚拟交换机旁，通过端口镜像方式捕获数据流量进行审计；4.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；5.支持Oracle、MySQL、SQLServer、DB2、Informix主流数据库协议的解析；6.支持达梦、人大金仓、神通、高斯DB等国产数据库协议的解析；7.支持PostgreSQL、Greenplum、Cache等专用数据库协议的解析；8.支持主流大数据平台数据库/NoSQL库的解析与审计，包括HBase、Hive、MongoDB、Elasticsearch、Redis、HDFS。支持Hive与Kerberos集成，Hive传输加密的解析；9.支持智能识别IPv6、IPv4地址；10.支持对双向数据包的解析，包括数据库操作请求以及数据库系统返回结果的解析审计；支持对返回结果集样例行数和大小进行限制，降低结果集存储资源占用；11.支持将应用访问信息准确关联到对应到数据库的操作，并完整记录日志；12.支持自定义敏感数据模糊化规则。内置至少18种敏感数据模糊化规则，对审计到的敏感数据进行模糊化处理，防止数审产品使用过程中的数据泄密；13.自动识别SQL语句的归类及合并，形成SQL模版库，可将大量、常见的语句设置为安全规则或过滤规则，规则准确度，优化系统识别规则库，形成安全语句和敏感语句管理；14.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；15.内置SQL、Oracle、MySQL等数据库入侵规规则大于800条；16.支持将用户行为模型转化成数据库访问安全基线，实时识别偏离数据库访问安全基线的异常行为并告警。支持对通过学习用户行为模型建流的安全基线进行人为修正；17.支持告警审阅，并可通过设置审阅规则对与被审阅告警有相同服务端IP、数据库实例名、客户端IP、匹配规则、操作对象名、操作命令、客户端工具和SQL模板条件的告警进行同时处理。支持对非法、高危、中危、低危的数据库访问事件进行告警，并按照风险级别进行统计。支持通过FTP、MAIL、SYSLOG和SNMP方式进行告警外发；18.支持对审计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25个维度。支持一键保存多维分析模型，形成自定义报表模版；19.支持不同时期的审计数据不同的空间、时间对各个维度进行自动同比和环比分析，支持对比结果以图表和趋势的方式进行展示；20.产品应具备web安全访问（https）、密码长度复杂度校验、密码错误尝试锁定、动态验证码验证、账号超时登出以及IP限制管理等安全性自定义配置功能。 | 台 | 1 |
| 13 | 国芯流量探针 | 1.国产化CPU，千兆电口≥2个，万兆光口≥2个，应用层吞吐量≥4Gbps；2.提供多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等；3.支持TiDB、GoldenDB、MongoDB数据库协议识别功能；4.具有文件威胁检测能力，能够准确识别300多种文件类型；支持恶意程序分类；针对检测出的恶意文件，能够给区分类型，如木马、勒索病毒等等。能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等，并支持多种高危病毒的侦测；5.提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持winserver2003、win7和win xp镜像；（提供界面截图并加盖公司公章）6.沙箱能够对未知漏洞利用代码和恶意程序的以下行为进行动态分析，包括进程操作行为；文件操作行为，文件删除、下载、共享或者复制；系统配置操作行为，自运行或其他系统配置；网络通信行为，控制与命令 (C&C)违规外联；恶意未知威胁逃逸行为；内存镜像分析，畸形，有瑕疵，或者带有已知威胁特征，劫持、重定向，或数据窃取，进程、服务，或者内存对象被篡改；7.支持HTTP、TELNET、FTP、MYSQL、PGSQL、REDIS、IMAP、POP3、SMTP、RDP、SSH、SMB、DB2、MongoDB、MSSQL等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态；（提供界面截图并加盖公司公章）8.支持自定义启用/禁用暴力破解模型；并支持自定义配置模型统计周期、登录次数、聚合维度、检测机制等参数；9.支持分布式爆破、慢速爆破检测，且界面可配；10.支持包含80种以上的深度检测模块，可支持shiro反序列化、蚁剑、哥斯拉、冰蝎3.0、冰蝎4.0等检测能力，且能识别如shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike等隧道通信工具；11.能够使用统计模型对产生的告警日志进行噪声分析。用户在分析日志时，可以根据噪声级别对日志进行实时过滤。支持对历史数据进行噪声标记。分析模型支持在线更新；12.支持在安全告警筛选与分析层面，能够提供超过60个维度的告警筛选，包括但不限于：攻击方法、攻击结果、威胁描述、攻击阶段、攻击方向、文件SHA1、http返回码、攻击评分、威胁特征、威胁标签、传输协议、应用协议等维度的筛选与展示；13.支持风险主机的智能研判功能：能够追踪到风险主机IP号、最近更新时间、主机风险状态、攻击结果、规则触发次数以及风险因素等信息的能力；能够提供攻击详情分析，包含风险信息概览，攻击链阶段，攻击关系图，风险主机涉及的告警列表详情，入侵检测攻击上下文等；14.支持网络威胁自定义与威胁情报自定义，网络威胁能自主添加规则名称，规则等级与规则类型，语法兼容业界最常用的snort规则的写法。威胁情报自定义包括IP、URL、DOMAIN、文件HASH四种类型，可以根据具体的使用场景进行选择。威胁情报自定义的规则可以支持多个同类对象的集合，比如对多个IP同时进行监控；15.能够以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载；（提供界面截图并加盖公司公章）16.支持pcap回放功能，对导入的pcap进行回放并进行威胁检测，回放产生的告警必须和生产网络流量的告警分页面展示，避免干扰正常安全运营；17.支持自动发现存在弱密码账号的资产，展示相关资产信息、以及存在弱密码的账号、密码、协议和登录端口，能够对密码进行脱敏存储和展示；18.可显示受感染主机的APT攻击阶段，帮助管理者制定响应策略；19.支持实时在线升级、自动在线升级、手工升级多种升级方式。 | 台 | 1 |
| 14 | 主机安全管理 | 1.支持宿主机及虚拟机的防护；2.支持接入外置企业级数据库，防止因数据库异常导致数据丢失，安全策略无法下发，包括且不限于SQL Server， Oracle，Postgresql等；3.支持与VMware vCenter， 新华三CAS、华为 FusionCompute等云平台对接，同步虚拟机相关信息;4.支持Linux、windows客户端在同一页面进行集中管理；5.支持自动分组功能，可配置分组策略，策略包括不限于主机名、操作系统、IP地址、安全策略、物理机/虚拟机/Docker主机分类等；6.具备虚拟机文件缓存扫描配置，提高扫描效率；7.支持网络访问控制功能，自定义防火墙策略，支持IP、MAC地址、端口，支持协议：TCP、 UDP、 ICMP、ICMPv6 、IGMP、IDP等，支持IPv4、IPv6、ARP、RARP等；8.支持检测扫描器、黑客工具对主机的探测侦察，支持扫描IP的阻断周期设置；9.可以对每条防火墙规则根据不同时间段，执行不同的防护策略；10.支持网络入侵攻击的防护，包含支持防护SQL注入,Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell攻击防护等；11.内置入侵防御的规则库，支持关联ATT&CK框架的技术ID，便于了解网络入侵技战术点；12.通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web应用、应用等类型的漏洞；13.支持对恶意流量的报文进行捕获，将 HTTP 流量转化为事件日志，支持下载原报文进行溯源及审查；14.支持不同租户分权分域，包括计算机、终端、事件、安全策略、管理、日志文件相互隔离；15.支持对主机资产价值、防火墙规则、入侵防御规则的严重性进行定义，包括低、中、高、严重等。 | 套 | 1 |
| 15 | 云安全管理平台组件授权 | 1.现有云安全管理平台组件授权扩容，用于兑换云安全管理平台上的各类安全组件；2.组件至少包含防火墙、漏洞扫描、数据库审计、主机安全、日志审计、微隔离、容器安全、堡垒机、WAF等。 | 点 | 300 |
| 16 | 服务器密码机 | 1.接口配置：≥4个10/100/1000M自适应电口；≥1个控制串口，≥4个USB；电源：双电源；2.SM1加解密速率≥880Mbps；SM2签名速率≥60,000Tps；SM2验签速率≥20,000Tps；SM2加密速率≥20,000TPS；SM2解密速率≥30,000TPS；SM3运算速率≥900Mbps；SM4加解密速率≥880Mbps；并发连接数≥10,000;3.支持信创环境，国产化平台及系统;4.支持对称密码算法、非对称密码算法以及杂凑密码算法等多种密码算法运算服务，同时需提供高效、高质量的随机数生成服务；5.具备SM1、SM2、SM3、SM4国家商用密码算法运算功能；SM1/SM2算法应当采用国家密码管理局许可的硬件实现；随机数应当由国家密码管理局批准使用的物理噪声源产生器芯片生成；6.具备销毁产品内所有SSP功能，支持开盖自毁和按钮手动销毁机制；7.需具有安全完善的密钥管理功能，能通过配置管理终端进行灵活配置，提供灵活的性能扩展能力；8.具备多种类型开发语言SDK包，可平滑接入各种业务系统，减少业务系统适配成本。SDK包类型包括Java、C、Golang、Python等；9.具备时钟同步功能，可以在无序的Internet环境中与提供精确和健壮的NTP服务器进行校时操作；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 2 |
| 17 | 签名验签服务器 | 1.接口配置：≥4个10/100/1000M自适应电口；≥1个控制串口，≥4个USB，电源：双电源；2.SM2签名速率≥30,000Tps；SM2验签速率≥10,000Tps；并发连接数≥10,000；3.支持 SM1/SM4对称算法、SM2非对称算法、SM3杂凑算法等国家商用密码算法以及 RSA、3DES、AES、SHA256、SHA1等国际算法；4.具备NTP网络时钟同步功能，可以在无序的Internet环境中与提供精确和健壮的NTP服务器进行校时操作；5.支持基于SM2算法的数字信封封装、解封验证功能，支持PKCS#7格式的数字信封封装、解封验证功能；6.支持SNMP标准协议，方便对设备运行状态进行统一监控；7.具备密钥访问控制功能，每对用户密钥对对应一个授权保护码，以保证不同密码应用系统调用同一台密码设备时的密钥安全性；8.具备对物理接口的端口聚合，提高接口带宽，每个聚合组的端口数不做限制，提高聚合组的配置灵活性；9.具备销毁产品内所有SSP功能，支持开盖自毁和按钮手动销毁机制；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 2 |
| 18 | 时间戳服务器 | 1.接口配置≥4个10/100/1000M自适应电口；电源：双电源；2.时间戳签发速率≥30,000Tps；时间戳验证速率≥10,000Tps；并发连接数≥10,000；3.接收应用系统发来的时间戳签发请求，签发时间戳后将时间戳返回给应用系统，时间戳服务请求遵循国际通用的RFC3161标准； 4.支持算法包括：MD5、SHA1、SHA256、SHA384、SHA512、SM3、SM2、RSA等；5.支持时间戳的精简模式，签发者证书全文将不包含在时间戳的签名结果中，部分应用场景下有效的提高网络传输及业务处理效率；6.支持证书信息返回，时间戳验证成功后将该签名数字证书解析并以XML/Text形式返回给业务应用系统；7.内置时间源模块，实现时间戳签名、验签、时间同步服务；8.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 2 |
| 19 | 密码服务管理平台 | 1.CPU≥32核，主频≥2.4G，内存≥64G，硬盘≥2TB；2.具备七项管理功能，包括：密码功能管理、密码业务管理、密码资源管理、密钥管理、安全审计、安全监控和系统管理，能够为用户提供全面的密码服务管理功能；3.可通过平台对密码设备进行远程管理，可管理密码设备的密钥、网络、访问策略等；4.提供统计平台内的所有密码设备数量；支持按密码设备类型进行分类统计；支持按密码设备状态进行分类统计；支持实时监控各密码设备的状态信息（CPU、内存、磁盘、连接数）；5.支持统计密码功能接口调用总次数、当日密码功能接口调用次数；支持按照密码功能接口分类统计调用次数；支持按天、按月统计密码功能接口的调用趋势；支持按租户统计密码功能调用次数；6.AAPS管控：具备AAPS管控机制，可通过配置AAPS控制阈值实现AAPS管控功能；7.提供平台用户和应用系统进行身份认证和访问控制功能；8.支持监控平台的QPS和服务实时流量；9.业务响应时间≤1s；支持应用数量≥1000个；支持密码设备数量≥50台；支持密码资源分组数量≥50组；支持密钥容量≥100万；支持第三方密码业务服务数量≥50个；10.具备采集密钥的全生命周期使用情况，并能按全生命周期时间节点进行展示分析，以帮助用户进行全方位的审计；11.支持对平台内使用的硬件服务器、虚拟服务器进行监控，包括服务的cpu、内存、磁盘等信息；12.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 1 |
| 20 | 智能密码钥匙 | 1.SM4加/解密速率≥1.00Mbps/1.00Mbps；2.SM2密钥对生成速率≥0.60对/秒，加/解密速率≥655Kbps/562Kbps，签名速率为650≥秒，验签速率≥985次/秒；3.SM3运算速率≥1.60Mbps；4.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 个 | 50 |
| 21 | SSL VPN网关 | 1.网络接口≥2个10/100/1000M自适应RJ45以太网接口；新建链接速率：≥100 个/秒；2.终端并发接入量：≥1000；密文吞吐量：≥600Mbps；3.提供基于SSL的安全通道防护，实现终端用户的远程安全接入，对应用进行强有力的安全防护；4.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 2 |
| 22 | IPSEC VPN | 1.网络接口≥4个10/100/1000M自适应RJ45以太网接口；USB接口≥2个；电源：双电源；2.新建隧道速率：≥20条/秒；最大隧道数：≥10000条；密文吞吐量：≥500Mbps；3.支持标准PKI体系结构，能导入第三方CA签发的SM2的x509 v3格式的证书进行认证；4.具备完善的多样式的审计功能，审计系统可以通过邮件和syslog方式将告警信息上报至指定的邮件服务器和syslog服务器；5.具备匿名认证功能，支持在ASDL网络环境中全动态IP地址间的安全隧道建立；6.具备链路安全防护能力，可以创建VXLAN接口并配置VTEP节点，同时具备IPSec Over VXLAN能力；7.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 2 |
| 23 | 国密门禁系统 | 1.系统包含CPU卡、门禁读卡器、门禁控制器、密钥注入器、门禁发卡器、PCI-E密码卡等硬件设备及安全门禁系统、门禁日志审计系统和密钥管理系统等软件系统；2.支持门禁日志记录完整性保护：使用PCI-E密码卡，采用基于SM3的HMAC技术，实现日志记录的完整性保护；3.支持门禁管理：支持用户管理、卡片管理、人员管理、门禁管理、权限配置、数据同步与配置下发、实时监控、日志查看、反潜、互锁、联动、多卡开门、远程开关门、时间段设置、假日设置等通用门禁管理功能；4.支持日志记录篡改报警提示：支持日志记录篡改报警提示；5.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 套 | 1 |
| 24 | 国密视频监控系统 | 1.至少提供视频监控数据安全与防护系统一体机，桌面式设备；2.支持≥8路1080P视频完整性校验；3.内置视频数据安全与防护系统密码模块，串联于 IPC (网络摄像头)和 NVR(网络视频录像机)之间；支持国密SM2/SM3/SM4算法，具有密钥管理、视频数据加解密、视频数据签名验签功能；符合 GM/T0028《密码模块安全技术要求》安全等级第二级相关要求；4.支持WEB界面对IPC (网络摄像头)、NVR(网络视频录像机)白名单设置；对IPC白名单中视频数据作签名、可单独设置是否加密，对未在IPC白名单中视频数据作透传处理；对NVR白名单中数据作验签，对未在NVR白名单中数据作透传处理；5.支持WEB界面进行完整性抓包分析并显示（至少包含IPC (网络摄像头)数据的签名、IPC加密数据的签名、NVR(网络视频录像机)数据的验签、未在白名单中的IPC及NVR的数据透传）；可直接查看签名值，验签公钥等信息；6.支持WEB界面进行网关设置，可添加多个网关，可以同时接入、处理不同网段视频流数据；支持端口配置，设置端号、端口类型（至少支持RTSP、GB28181）、端口描述；7.支持WEB界面查看或修改设备的配置信息；8.支持流量负载、安全业务统计、设备性能监控等功能，用户可实时查看设备性能；9.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 套 | 1 |
| 25 | 数字证书认证系统服务器 | 1.整机硬件形态，证书签发容量≥5000张，证书签发速度≥100个/秒，支持接入RA的数量≥1个；2.LDAP支持条目≥5000条目，精确查询≥46000次/秒，LDAP并发查询的数量≥4096个；3.证书签发，支持机构证书、签名证书、加密证书等数字证书签发；支持同时签发国密SM2和国际RSA算法证书，支持自定义模板证书签发；4.证书申请与审核，提供单个和批量用户证书申请信息的录入与审核；5.密钥管理，提供密钥申请、撤销、恢复、司法取证、归档等操作；6.证书管理，提供证书的更新、延期、冻结、解冻、撤销、恢复、下载制证等操作，发起的操作均需在注册审核系统中进行审核；7.登录认证，提供数字证书认证方式登录系统，对登录系统的人员依职责进行权限管理；8.监管上报，核心服务支持与监管系统对接，能够实时上报服务状态等信息；9.算法支持，支持国密SM1/SM2/SM3/SM4和国际RSA/SHA1/AES等密码算法；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 1 |
| 26 | 国密浏览器 | 1.支持国密算法，与服务端安全网关构建基于国密算法的安全传输通道；2.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 个 | 50 |
| 27 | 数据融合治理 | 项 | 1 |
| 五 | 重大活动网络安全保障云服务能力 |
| 1 | 云安全管理平台 | 1.提供安全组件的管理功能，包括产品功能描述、产品规格、产品部署模式、产品版本等；2.支持安全组件特征库（包括病毒库、检测规则库、客户端安装包）的定期升级和自定义升级策略，支持立即升级和定时升级，升级策略支持指定特定的租户和资源进行升级，支持查看升级的结果；3.主机安全、日志审计、网页防篡改、微隔离、容器安全、堡垒机、数据库审计、web防火墙（主机板）支持软件化部署，可兼容主流的各种硬件、云平台和操作系统；4.所有组件均支持精细化、全功能、自定义的策略配置，不仅只是接口调用的阉割功能；5.支持与第三方安全组件对接，统一纳管第三方安全组件；6.支持自定义安全套餐,不仅灵活适应用户多样化的安全防护需求，还能精准有效地抵御各类网络攻击，保护用户的数据和业务安全；7.支持运营人员全面监控和管理云上所有应用的安全状态,实时监控安全资源的使用情况,支持可视化展示;支持安全组件的统一管理和配置;8.支持单点登录,租户无需输入账号密码即可从平台跳转进入对应安全组件的控制台;9.支持对安全组件的申请、开通、部署等全业务流程统一管理;10.支持租户申请订购安全服务,并实时监控工单审批,部署进程;11.支持运营人员对工单进行审批,部署;12.支持弹性扩容，支持租户对已购安全组件进行续订,扩容等操作,能够根据租户的需求动态调整安全资源的规模；13.支持虚拟化技术,实现安全资源的池化管理。 | 套 | 1 |
| 2 | USBKEY智能密码钥匙 | 1.SM4加/解密速率≥1.00Mbps/1.00Mbps；2.SM2密钥对生成速率≥0.60对/秒，加/解密速率≥655Kbps/562Kbps，签名速率为650≥秒，验签速率≥985次/秒；3.SM3运算速率≥1.60Mbps；4.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 个 | 45 |
| 3 | 服务器密码机 | 1.接口配置：≥4个10/100/1000M自适应电口；≥1个控制串口，≥4个USB；电源：双电源；2.SM1加解密速率≥880Mbps；SM2签名速率≥60,000Tps；SM2验签速率≥20,000Tps；SM2加密速率≥20,000TPS；SM2解密速率≥30,000TPS；SM3运算速率≥900Mbps；SM4加解密速率≥880Mbps；并发连接数≥10,000;3.支持信创环境，国产化平台及系统;4.支持对称密码算法、非对称密码算法以及杂凑密码算法等多种密码算法运算服务，同时需提供高效、高质量的随机数生成服务；5.具备SM1、SM2、SM3、SM4国家商用密码算法运算功能；SM1/SM2算法应当采用国家密码管理局许可的硬件实现；随机数应当由国家密码管理局批准使用的物理噪声源产生器芯片生成；6.具备销毁产品内所有SSP功能，支持开盖自毁和按钮手动销毁机制；7.需具有安全完善的密钥管理功能，能通过配置管理终端进行灵活配置，提供灵活的性能扩展能力；8.具备多种类型开发语言SDK包，可平滑接入各种业务系统，减少业务系统适配成本。SDK包类型包括Java、C、Golang、Python等；9.具备时钟同步功能，可以在无序的Internet环境中与提供精确和健壮的NTP服务器进行校时操作；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 4 |
| 4 | 签名验签服务器 | 1.接口配置：≥4个10/100/1000M自适应电口；≥1个控制串口，≥4个USB，电源：双电源；2.SM2签名速率≥30,000Tps；SM2验签速率≥10,000Tps；并发连接数≥10,000；3.支持 SM1/SM4对称算法、SM2非对称算法、SM3杂凑算法等国家商用密码算法以及 RSA、3DES、AES、SHA256、SHA1等国际算法；4.具备NTP网络时钟同步功能，可以在无序的Internet环境中与提供精确和健壮的NTP服务器进行校时操作；5.支持基于SM2算法的数字信封封装、解封验证功能，支持PKCS#7格式的数字信封封装、解封验证功能；6.支持SNMP标准协议，方便对设备运行状态进行统一监控；7.具备密钥访问控制功能，每对用户密钥对对应一个授权保护码，以保证不同密码应用系统调用同一台密码设备时的密钥安全性；8.具备对物理接口的端口聚合，提高接口带宽，每个聚合组的端口数不做限制，提高聚合组的配置灵活性；9.具备销毁产品内所有SSP功能，支持开盖自毁和按钮手动销毁机制；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 4 |
| 5 | 数字证书认证系统服务器 | 1.整机硬件形态，证书签发容量≥5000张，证书签发速度≥100个/秒，支持接入RA的数量≥1个；2.LDAP支持条目≥5000条目，精确查询≥46000次/秒，LDAP并发查询的数量≥4096个；3.证书签发，支持机构证书、签名证书、加密证书等数字证书签发；支持同时签发国密SM2和国际RSA算法证书，支持自定义模板证书签发；4.证书申请与审核，提供单个和批量用户证书申请信息的录入与审核；5.密钥管理，提供密钥申请、撤销、恢复、司法取证、归档等操作；6.证书管理，提供证书的更新、延期、冻结、解冻、撤销、恢复、下载制证等操作，发起的操作均需在注册审核系统中进行审核；7.登录认证，提供数字证书认证方式登录系统，对登录系统的人员依职责进行权限管理；8.监管上报，核心服务支持与监管系统对接，能够实时上报服务状态等信息；9.算法支持，支持国密SM1/SM2/SM3/SM4和国际RSA/SHA1/AES等密码算法；10.具备国家密码管理局颁发的《商用密码产品认证证书》。 | 台 | 1 |
| 六 | 安全功能组件服务 |
| 1 | 安全功能组件购置（包含500000个License） | 项 | 1 |
| 2 | 安全组件服务费 | 项 | 1 |