**附件3：**

**内网核心交换机参数：交换容量≥76.8Tbps/336 Tbps 、转发能力≥8640Mpps/57600Mpps**

**外网核心交换机参数：交换容量≥76.8Tbps/336 Tbps 、转发能力≥8640Mpps/57600Mpps**

**客户端点位：700+，服务器：150+，交换机：160+，AC:300+**

**网络安全产品需求：**

|  |  |  |  |
| --- | --- | --- | --- |
| **设备** | **产品说明** | **数量** | **单位** |
| 态势感知平台 | 1、性能参数：在带宽性能1Gbps时存储时长：900天/1Gbps。 2、支持大屏展示网络安全态势，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等； 3、内置云沙箱，支持将文件手动上传云沙箱进行验证和补充举证，支持展示云沙箱报告列表，可以看到云沙箱的结果，点击查看报告详情，支持导出报告。； 4、支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题； 5、支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告； 6、支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法； 7、具有检测HTTP/FTP/LDAP/VMWARE/ORACLE/VNC等协议弱密码的功能，弱密码检测列表支持显示账号、密码、服务器、所属分支和业务、弱密码类型、最近发生时间等信息； 8、支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略； 9、支持多种告警方式，包括邮件告警、短信告警、微信告警等； 10、具备元数据行为分析引擎：httpflow、dnsflow、smbflow、maillflow等, 通过异常行为分析完成非法行为的检测告警。支持对暴力破解、隧道和HTTPS恶意流量的检测功能 11、具备资产主动扫描和被动发现功能，主动扫描支持自动入库、手动入库、扫描目标、定时扫描等功能。包括逻辑拓扑和物理拓扑识别及可视化展示。 12、支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、比特币欺诈、垃圾邮件等恶意邮件。 | 1 | 台 |
| 日志审计系统 | 1、性能参数：本次配置主机审计许可证书数量：200，最大可扩展审计主机许可数：≥500。 2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于720种日志对象的日志数据采集； 3、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、文件\文件夹读取、Kafka等多种方式完成日志收集； 4、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 5、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； 6、支持日志文件备份到外置存储节点，支持NFS、NAS、ISCSI三种存储方式，并可查看外置存储容量、状态等信息； 7、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。 8、支持预置审计策略模板，包括：Windows主机类审计策略模板、Linux/Unix主机类审计策略模板、数据库系统类审计策略模板等。 9、支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，支持自定义关联分析规则 10、提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；用于管理账号权限，满足用户三权分立的需求；支持usb-key认证 11、支持POC测试工具一键生成数据。 | 1 | 台 |
| 边界防火墙 | 1、性能参数：网络层吞吐量：≥10G，应用层吞吐量：≥4G，防病毒吞吐量：≥1G，IPS吞吐量：≥1G，全威胁吞吐量：800M，并发连接数：≥400万，HTTP新建连接数：≥10万 2、具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议； 3、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 4、产品支持对不少于10000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。  5、设备安全日志支持本机存储、Syslog服务器存储、态势感知平台存储等不同形式存储方式。 6、产品支持用户账号安全保护功能，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。 7、产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过3320种；  8、产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 9、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。 10、产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。 11、产品支持多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。 | 1 | 台 |
| 数据中心防火墙 | 1、性能参数：网络层吞吐量：≥20G，应用层吞吐量：≥18G，防病毒吞吐量：≥4G，IPS吞吐量：≥4G，全威胁吞吐量：≥2G，并发连接数：≥800万，HTTP新建连接数：≥16万  2、具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议； 3、产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换。 4、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 5、产品支持对不少于10000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。  6、设备安全日志支持本机存储、Syslog服务器存储、态势感知平台存储等不同形式存储方式。 7、产品支持用户账号安全保护功能，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。 8、产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过3320种；  9、产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 10、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。 11、产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。 12、产品支持多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。 | 2 | 台 |
| 流量探针 | 1、性能参数：网络层吞吐量：≤1Gbps，应用层吞吐量：≤500Mbps。 2、硬件参数：规格：1U，使用国产化主流cpu和国产操作系统；内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口+4千兆光口SFP。 3、支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响 4、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 5、支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤 6、支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测 7、支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等。 8、支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求 9、支持传输访问检测日志，包括正常访问、风险访问、违规访问 10、支持将流量还原的文件发送至沙盒分析；支持将流量还原的文件发送至沙盒分析 11、支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式含： 12、安全感知系统探针特征库(\*3年);软件升级(\*3年);产品质保（标准版）(\*3年); | 2 | 台 |
| 堡垒机 | 1、性能参数：运维授权数：≥200，最大可扩展资产数：≥1000，图形运维最大并发数：≥200，字符运维最大并发数：≥550。 2、系统各模块支持以B/S方式管理，采用https加密方式访问； 3、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入； 4、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。 5、用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证； 6、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； 7、全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计；  8、支持登陆控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话； 9、支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别。 10、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； 支持日志数据的外置存储，支持NFS、ISCSI和Windows文件共享协议。 11、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 12、支持运维日志审计，可以进行运维录像回放。 | 1 | 台 |
| 端点安全 | 1、本次需配置服务器授权≥150个；客户端≥600个，提供3年病毒库升级； 2、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； 3、支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量； 4、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数  5、支持按“最近7天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数 6、支持跳转链接至云端安全威胁响应中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、处置建议、影响分析（客户情况、影响行业、区域分布）等。 7、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； 8、具备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； 9、支持对zip， rar， jar， cab， 7z等常见压缩文件的扫描检测，支持压缩文件层级进行策略配置，最大可配置检查10层压缩文件； 10、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。 11、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。 | 1 | 套 |
| 数据库审计 | 1、性能参数：最大硬件吞吐量：2Gbps，最大数据库纯SQL流量：400Mb/s，数据库实例个数：30个，SQL处理性能：30000条SQL/s，日志检索性能：400000条/秒，国产化配置：KX-U6780A/银河麒麟系统。 2、硬件参数：规格：2U，使用国产化主流cpu和国产操作系统；内存大小：8G，硬盘容量：128G SSD+4T SATA，电源：单电源，接口：6千兆电口。 3、支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、IRIS、达梦、人大金仓、南大通用、其中MongDB、K-DB； 4、支持精细化日志秒级查询，通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快； 5、支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。 6、TB级日志秒级查询、支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询； 7、支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索； 8、深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间；  9、支持吞吐量分析，包括SQL语句吞吐量排行、SQL语句吞吐量趋势、SQL操作类型吞吐量排行、SQL操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势； 10、内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等； 11、支持数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源；  12、提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 | 1 | 台 |
| 零信任网关 | 1、IPSEC性能参数：加密最大流量（Mbps）：100，理论并发隧道数（Tunnel）：1000；SSL性能参数：最大理论加密流量（Mbps）：300Mbps，最大理论建议并发用户数：600；此次配置≥50个用户接入授权。 2、为了不改变员工原有使用习惯，保障单位员工的使用体验，需支持通过IE8+、CHROME 69+、edge、Firefox、Opera、Safari浏览器、国产操作系统的浏览器、企业微信/钉钉等H5应用内置浏览器、ANDROID、IOS各大手机厂商的自带浏览器接入访问WEB资源，不需采用专属或指定浏览器才能访问。 3、支持以隧道应用方式发布域名资源，日志审计可以记录到URL级别，支持为隧道域名应用添加WEB水印，支持隧道域名应用单点登录功能 4、为了减少客户端运维工作，快速定位基础问题，需至少支持Windows客户端进行日志收集，方便运维排查； 5、为满足单位多样化安全便捷认证需求，控制中心在不需要额外搭建认证平台、认证组件的情况下便可支持以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、证书认证、HTTP(S)短信认证； 6、为了保障认证安全与便捷性的平衡，支持开启在授信终端环境下/域控环境下/特定网络区域下（即可信的终端或网络环境下），免二次认证； 7、支持本地用户、用户组可直接关联个人应用进行授权，避免需要为部门中的个别特殊人员建立大量角色，简化权限管理； 8、支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复，便于员工自行排查修复终端问题，减少IT运维人员工作； 9、为了尽可能简化员工登录操作难度，支持在客户端登录时内置登录地址； 10、支持站点智能梳理，支持使用自动改写采集的方式梳理依赖站点，支持依赖站点一键启用，自动采集。便于业务快速上线，简化运维工作； | 1 | 台 |
| 全网行为管理 | 1、准入终端数：≥1500 2、支持网关模式、网桥模式、旁路模式等多种部署模式 3、支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6； 4、支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行； 5、支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略 6、支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略； 7、支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录； 8、支持OA认证，支持通过OAuth认证协议对接，支持阿里钉钉，企业微信第三方账号授权认证； 9、设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制； 10、支持超过900种主流Saas应用，对Saas应用有默认分类标签，帮助客户统一配置策略； 11、支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝 12、支持禁止使用代理，不允许使用外部HTTP代理，不允许使用外部Sock4/5代理，不允许在HTTP,SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等） | 1 | 台 |
| 终端准入 | 1. 准入终端数：≥1500   2.支持阻断终端用户使用外设，防止终端用户从内网拷贝信息，支持管理外设类型：存储设备、网络设备、蓝牙设备、摄像头、打印机； 3.能够对百度网盘、百度文库等网络应用的上传动作进行细分控制； 4.支持流控黑名单，可疑基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中；  5.支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； 6.支持不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放； 7.设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别，至少识别不少于8种移动终端型号； 8.支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； 9.支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网； | 1 | 台 |
| 网络安全服务 | 1、安全现状评估 策略检查：上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。 脆弱性评估：对操作系统、数据库、常见应用/协议、系统与Web漏洞进行漏洞扫描，弱口令扫描可实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。 资产暴露面梳理：安全专家在上线前使用扫描组件对资产开展暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行协助处置，实现对暴露面资产可管可控，降低暴露面资产的风险。 2、安全问题处置 策略调优：安全专家根据安全威胁/事件分析的结果以及处置方式，对安全组件上的安全策略进行调整工作。 脆弱性问题修复指导：针对内网脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建议。 3、资产管理 资产指纹探测：持续服务过程中安全专家每季度对资产进行指纹（操作系统、中间件、软件厂商等信息）探测，并对指纹信息进行确认与更新，确保资产指纹信息的准确性和全面性。 资产变更管理：持续服务过程中安全专家每季度对资产进行存活性探测，当发现未存活资产或资产发生变更时，安全专家对变更信息进行确认与更新，确保资产信息的准确性和全面性。 4、脆弱性管理 漏洞扫描与验证：每季度针对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的WEB漏洞进行验证，验证WEB漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。 漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户。 漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。 漏洞复测与状态追踪阿：对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。 弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。 高可利用漏洞防，支持一键防护扫描组件发现的高可利用漏洞。 （本项服务根据客户实际业务情况按需提供） 5、专属服务经理：为用户配置一名经验丰富的安全专家作为专属服务经理。 实时专家咨询：安全专家对用户咨询或上报的安全问题进行及时响应并给出建议，如主机加固建议咨询、安全事件处置建议咨询等。 节假日值守：安全值守专家进行7\*24小时安全监测，对发生的安全事件进行及时响应并在节假日期间每日进行值守总结，在服务群发送值守总结快报。 6、运营成果可视 安全运营周报：安全专家每周对服务资产进行安全运营情况的分析总结并输出《安全运营周报》。 安全运营月报：安全专家每月对服务资产及整体安全状况进行分析总结并输出《安全运营月报》。 安全运营半年度汇报：安全专家每半年总结阶段性安全运营情况并输出《半年度总结报告》发送给用户，向用户进行远程总结汇报。 安全运营年度汇报：安全专家总结年度安全运营情况并输出《年度总结报告》发送给用户，向用户进行总结汇报。 用户Portal：可视化portal支持随时查看服务范围内业务资产安全状态。支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果支持用户在线对服务SLA进行查阅和监督。 | 1 | 年 |
| 离线备份一体机 | 1. 备份存储≥80TB，大容量数据传输速度≥200MB\秒。 2. 支持全量备份和增量备份。 3. 支持多种操作系统，如 Windows、Linux、统信OS等。 4. 数据库系统，如 Oracle、MySQL、SQL Server、Cache、IRIS 等，还能对虚拟化环境中的数据，如 VMware、超融合虚拟机等进行备份。 5. 支持短时间内将备份数据恢复到指定的位置或系统中，支持从全量备份、增量备份或差分备份中快速提取所需数据进行恢复，确保业务的快速恢复和连续性，在数据恢复完成后，能够对恢复的数据进行验证，确保数据的准确性和完整性。 |  |  |

**备注：**

**1、以上设备均包含3年升级、授权等。**

1. **以上安全设备均可支持在线、离线漏洞补丁修复。**
2. **不同的安全厂家可根据自己的产品线制定符合以上需求的报价方案。**