# 上海“数字法院”（一期）——综合安全管理子系统建设项目采购需求

# 项目概况

上海法院已初步建立了覆盖云、网、端、应用的信息安全保障体系，形成了以安全通信网络、安全区域边界、安全计算环境、安全管理中心组成的法院系统安全保护环境。在安全区域边界方面，已具备区域边界访问控制、入侵防范、恶意代码防范、网络及数据库审计能力。在安全通信网络方面，已具备通信网络数据传输的保密性和完整性保护能力。在安全计算环境方面，已具备用户身份鉴别、访问控制、防病毒等能力。在安全管理中心方面，已具备系统管理、安全管理、审计管理能力。随着数字法院的快速推进落实，提出了基于分析联动的主动防御和对安全事件的风险防范、应急响应、处置恢复能力的要求。上海法院综合安全管理子系统是构建“数字法院”主动安全防御体系的关键组成部分，是上海“数字法院”的支撑保障体系，是上海法院依法依规持续满足安全合规并在数字化转型过程中不断提升综合安全管控能力的背景下提出的建设需求。

是否按信创要求建设：是

# 建设目标

从上海法院综合安全管理子系统架构层面，通过汇集全网各类安全事件，采集、汇总和分析网络流量、安全日志、安全告警信息，实现对上海法院专网中部署的安全设备的集中统一监管，形成安全态势感知、预警告警、应急处置，起到提升综合安全管控能力，逐步形成基于安全态势分析研判的主动防御能力，全面支撑法院安全运营的作用；同时通过主机及终端安全、移动安全，运维终端数据防泄漏建设，实现提升主机及终端安全防护水平，补强移动安全防护能力，落实运维终端数据保护要求，起到持续加强等级保护合规，构建支撑新时代数字法院建设的信息安全保障体系的作用。

以下是本项目拟实现的技术指标和绩效目标：

## 1.技术指标

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目  绩效  目标 | 项目总目标 （2024年-2027年） | | | 年度总体目标  （2024年） |
| 一、建设上海法院专网安全监管中心，包括两个本地数据中心和两个云数据中心的全流量采集探针；政务云虚拟化服务器流量分析；形成覆盖高院、法官培训中心两个本地数据中心和两个政务云数据中心的态势感知分析平台及其日志集中分析平台。  二、主机和终端安全  针对上海高院法院专网和互联网本地及云端服务器，在服务器身份鉴别、访问控制、入侵防范、恶意代码防范、安全审计等方面达到等级保护三级标准，最终完成上海高院法院专网和互联网本地及云端服务器的安全加固。针对全市法院专网本地办公终端，完成全市法院专网本地办公终端的终端安全管理系统（控制台）的国产化替代与升级，以及终端安全管理系统统一管理平台建设（终端安全管理系统客户端已完成国产化替代与升级）。  三、移动安全防护  针对上海高院移动端业务，在安全通信网络、安全计算环境方面达到等级保护三级标准。实现边界控制、身份认证、隔离交换、移动设备管理、移动应用管理和移动数据防泄露等功能，建设移动办公的网络通信链路以及建立移动办公终端安全管理平台。  四、运维终端数据防泄漏  针对上海高院法院专网和互联网本地运维终端，实现运维终端数据防泄露功能。 | | | 项目建设周期：合同签署后半年。 |
| 绩效指标 | 一级指标 | 二级指标 | 三级指标 | 年度指标值 |
| 产出指标 | 数量指标 | 系统建设数量 | 4 |
| 覆盖法院数量 | 23 |
| 质量指标 | 等级保护安全管理中心要求符合度 | 实现法院专网高院、法官培训中心、政务云法院VPC等4个节点的集中管控要求合规。 |
| 等级保护安全计算环境要求服务度 | 实现高院法院专网本地数据中心和政务云法院VPC服务器的入侵防范要求合规。  实现高院互联网和政务云互联网区法院VPC服务器的入侵防范要求合规。  实现上海法院专网全部办公终端的身份鉴别、安全审计要求合规。 |
| 移动互联等级保护要求符合度 | 实现移动办公办案安全通信网络要求合规。  实现移动办公办案移动互联安全扩展要求中安全计算环境要求合规。 |
| 时效指标 | 项目进度安排 | 合同签订后半年内完成项目建设 |
| 成本指标 | 建设成本 | 建设成本不超过预算 |
| 效益指标 | 经济效益指标 | 全市法院使用覆盖率 | 安全监管中心覆盖高院、法官培训中心、政务云XC区和X86区法院VPC。  主机安全防护覆盖上海法院专网350台服务器，上海法院互联网150台服务器。  终端安全覆盖上海法院专网100%终端。  移动办公办案覆盖所有移动终端访问通信链路安全、后台服务交互链路安全和隔离交换通道的扩容、高院600台办公手机防护。  运维终端数据防泄漏覆盖高院法院专网本地200台和互联网本地25台运维终端。 |
|  | 满意度指标 | 服务对象满意度指标 | 用户满意度 | ≥90% |

## 2.绩效目标

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 绩效目标 | 目标值 | |
| 产出目标 | | | 项目效果 |
| 1 | 建设上海法院专网安全监管中心 | 两个本地数据中心和两个云数据中心的全流量采集探针；政务云虚拟化服务器流量分析；形成覆盖高院、法官培训中心两个本地数据中心和两个政务云数据中心的态势感知分析平台及其日志集中分析平台。 | 上海法院专网达到等保三级要求 |
|
|
|
|
| 2 | 完成主机安全建设 | 针对上海高院法院专网和互联网本地及云端服务器，在服务器身份鉴别、访问控制、入侵防范、恶意代码防范、安全审计等方面达到等级保护三级标准，最终完成上海高院法院专网和互联网本地及云端服务器的安全加固。 | 加强主机层安全防护措施 |
|
|
| 3 | 完成终端安全建设 | 针对全市法院专网本地办公终端，完成全市法院专网本地办公终端的终端安全管理系统（控制台）的国产化替代与升级，以及终端安全管理系统统一管理平台建设（终端安全管理系统客户端已完成国产化替代与升级）。 | 实现上海法院专网全市XC终端统一管理 |
| 4 | 完成移动安全防护建设 | 针对上海高院移动端业务（目前运行在高院互联网链路中），在安全通信网络、安全计算环境方面达到等级保护三级标准。实现边界控制、身份认证、隔离交换、移动设备管理、移动应用管理和移动数据防泄露等功能，建设支持全市法院移动办公的网络通信链路以及建立全市法院移动办公终端安全管理平台（各中基层法院按需接入），为全市法院移动办公办案提供安全合规运行环境。 | 健全补强移动通信安全和安全计算环境 |
| 5 | 完成运维终端数据防泄漏建设 | 针对上海高院法院专网和互联网本地运维终端，实现运维终端数据防泄露功能，最终完成上海高院法院专网和互联网本地运维终端数据安全能力提升。 | 加强运维终端数据防泄露能力 |

# 项目建设内容

# （一）建设内容

本期项目建立法院安全监管中心，初步形成覆盖法院专网本地和政务云4个数据中心等节点的云网安全态势感知能力，实现集中安全风险管控，集中安全事件处理，集中安全审计；通过主机及终端安全建设，提升法院专网、互联网服务器的安全防护能力，完成法院专网XC终端安全管理系统的替换，并实现终端监控与审计功能；建设移动互联安全通信链路，扩充法院专网到互联网的隔离交换通道和后台服务通道VPN性能，实现移动终端与法院专网内部数据和服务的安全通信和交换能力。建立高院互联网和法院专网的运维终端的数据防泄露系统，落实运维数据安全要求。具体内容如下：

### 1.安全监管中心

1.1安全监管运营平台

实现安全态势分析，形成安全态势的可视化能力，可以协助进行安全状况的全局性掌控、安全概览，提供安全态势展示。实现资产安全风险评估与管理，通过对接资产管理系统或主动采集建立资产数据库，对资产的来源、风险状态、安全事件进行持续地跟踪和管理，并通过资产识别、脆弱性识别和威胁识别得出安全现状分析。实现安全威胁分析，通过收集和加工从主机、网络、安全设备采集上来的流量、安全日志，采用关联分析引擎的流式分析能力，将资产指纹信息、资产脆弱性、网络流量、安全日志等的信息关联起来，发现更复杂的、更具价值的威胁事件。实现安全告警响应处置，为安全运营人员提供的处置闭环的能力。利用自动化编排技术通过整合联动现有安全防护系统，实现事件自动化处置的目标。

1.2网络流量采集及分析

实现法院专网流量采集、还原及检测，基于探针的安全检测能力进行安全检测、反病毒、漏洞防护、防间谍软件、IOC情报检测等威胁分析，并将基于流量被动发现的资产信息数据、威胁分析产生的威胁日志等数据，上传至安全监管运营平台。流量采集包括：法院专网高院数据中心、法官培训基地第二数据中心、政务云XC区、政务云X86区四个核心节点及一级网接入区域，高院信访办法院专网入口的网络流量采集。

1.3日志集中收集与分析

实现法院专网日志集中收集与分析，对高院所属专网节点的网络设备、安全设备、主机系统的日志进行集中收集，并对所收集的日志进行自动解析、过滤、富化、范式化预处理，方便对日志数据进行实时关联分析和数据分析。

建立高院互联网本地+云的日志集中收集和分析系统，将来自不同厂商的安全设备、网络设备、主机系统的日志信息进行汇集和集中存储，满足基于日志的安全审计需求。

1.4威胁情报中心

安全监管运营平台配置并集成本地威胁情报库，将威胁情报样本作为数据分析来源，可以在多数据关联分析和威胁溯源中，快速补充攻击者上下文信息，提升威胁分析、溯源效率；也可以使用不同日志数据检测内部主机连接远程C&C服务器，发现失陷主机，从而迅速做出响应，防止由于失陷带来的数据泄密、系统破坏等关键风险。

### 2.主机及终端安全

2.1主机安全

为上海高院法院专网和互联网（含本地与云端）主机部署主机安全管控系统，实现主机资产管理、入侵检测、访问控制、安全加固等功能；

2.2终端安全

建设全市法院专网终端安全管理系统统一管理平台，对终端安全管理系统进行统一管理，实现全网终端、设备数据集中汇总、分析与展示，感知系统运行状态，对系统进行统一策略下发。

实现各法院终端安全管理系统升级，将当前网络安全终端安全产品的载体替换为XC服务器，实现全市法院专网本地办公终端终端安全管理系统的国产化替代与升级，以及终端管理业务系统的平滑迁移。

### 3.移动安全

3.1移动通信链路安全

建立移动办公工作人员与移动办公办案应用的网络通信链路：采购零信任网关和零信任控制中心，为全市法院工作人员访问上海高院移动办公办案云端应用建立安全通信信道，为移动终端接入提供安全防护。主要针对工作人员使用移动设备，借助互联网络，实现基于国家商用密码算法体系，为法院干警移动办公提供涵盖网络连接、信道加密、认证接入、访问控制等多重安全措施的移动安全接入服务。

3.2隔离交互通道安全

实现上海高院移动办公办案互联网本地与云端（上海市大数据中心）的安全通信信道，建立移动办公办案互联网应用区与移动办公办案本地应用区之间的网络通信链路；扩建跨网隔离交换安全平台，为上海高院移动办公办案的跨网数据交互建立安全的数据交换平台。

3.3移动终端安全管理

建立支持全市法院移动办公安全防护的移动终端安全管理系统，实现移动设备管理、移动应用管理和移动数据防泄露等功能，为上海法院移动办公办案应用提供安全合规运行环境。

### 4.运维终端数据防泄漏

为上海高院法院专网本地和互联网本地运维终端部署数据防泄露系统，实现运维终端数据防泄露功能。

# （二）采购清单

### 1.产品软件购置清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **软件名称** | **功能说明/配置要求** | **数量** | **单位** | **备注** |
| 1 | 安全监管中心 |  |  |  |  |
| 1.1 | 安全监管运营平台 | 包括安全态势、资产发现、资产指纹、风险评估、数据采集、威胁分析、响应处置功能模块 | 1 | 套 | 中心平台 |
| 1.2 | 日志分析管理 | 包括日志集中收集、处理、关联分析、检索查询、可视化运营功能模块 | 1 | 套 |
| 1.3 | 自动化编排与响应 | 包括编排与自动化管理、高级告警分析、案例管理、工单管理、平台支撑管理功能模块 | 1 | 套 |
| 1.4 | 虚拟流量分析 | 云内虚拟机之间流量采集，基于流量的应用识别、对入侵、漏洞利用、web入侵和病毒等检测 | 6 | 套 |
| 1.5 | 威胁情报 | 威胁情报许可，一年 | 3 | 套 |
| 1.6 | 硬件日志源的数据分析授权 | 满足100个日志数据源（硬件）的数据分析授权 | 1 | 套 |
| 1.7 | 互联网云日志审计 | 互联网云日志审计,对政务云互联网区法院VPC的设备日志进行统一收集与分析 | 1 | 套 |  |
| 1.8 | 系统对接及定制 | 安全设备告警日志格式解析适配、威胁响应处理流程定制、安全策略下发接口对接、跨光闸数据传输格式定制。 | 1 | 套 |  |
| 2 | 主机及终端安全 |  |  |  |  |
| 2.1 | 互联网主机安全管控系统控制台（云端） | 提供主机安全统一管控，功能包括：主机管理、实时监控、告警通知、系统审计、策略配置等。 | 1 | 套 |  |
| 2.2 | 互联网主机安全管控系统客户端（本地+云） | 主机自适应安全Agent授权：部署客户端，提供资产清点、风险评估、入侵检测、合规基线、主机隔离等。 | 150 | 套 |  |
| 2.3 | 法院专网主机安全管控系统控制台（云端） | 提供主机安全统一管控，功能包括：主机管理、实时监控、告警通知、系统审计、策略配置等。 | 1 | 套 |  |
| 2.4 | 法院专网主机安全管控系统客户端（本地+云） | 主机自适应安全Agent授权：部署客户端，提供资产清点、风险评估、入侵检测、合规基线、主机隔离等。 | 350 | 套 |  |
| 2.5 | XC网络终端安全管理系统统一管理平台-分级权限管理 | XC网络终端安全管理系统统一管理平台-分级权限管理,  分级分权限管理：采用三全分立，支持高院、分院两级管理模式分权。  1）后台支持配置管理员不同的管理范围权限和不同的功能权限。  2）市级法院系统管理员集中管理，可以集中管理所有区县法院机器情况、管理策略。区法院管理员分级自治，界面只显示在管理范围内的机器情况，管理策略等等。 | 1 | 套 |  |
| 2.6 | XC网络终端安全管理系统统一管理平台-系统监控管理 | XC网络终端安全管理系统统一管理平台-系统监控管理,系统监控：各分院终端安全管理系统运行状态监控，异常状态报警及输出。  1）系统运行状态监控：监测终端安全管理系统运行是否正常，如异常则报警；  2）资源使用状态监控：监测终端安全管理系统CPU、内存、系统空间、备份空间，如超过80%则报警；  3）系统服务状态监控：监测终端安全管理系统服务运行状态，如异常则报警；  4）异常报警展示及输出：报警通过首页展示，采用SYSLOG及短信输出 | 1 | 套 |  |
| 2.7 | XC网络终端安全管理系统统一管理平台-终端汇总管理 | XC网络终端安全管理系统统一管理平台-终端汇总管理,终端数据汇总：采集各分院终端信息，汇总统一报表。  1）采集各分院的终端基本信息，包括不限于IP、MAC、使用人、部门等，集中到统一管理平台汇总；  2）采集各分院的终端硬件信息，集中到统一管理平台汇；  3）采集各分院的终端软件信息，集中到统一管理平台汇；  4）采集各分院的终端的违规情况，集中到统一管理平台汇； | 1 | 套 |  |
| 2.8 | XC网络终端安全管理系统统一管理平台-策略统一管理 | XC网络终端安全管理系统统一管理平台-策略统一管理,策略汇总：建立策略统一下发机制，高院对各分院进行统一策略下发。  1）支持以树状结构对部门信息进行层级展示；  2）支持策略执行结果的统一汇总；  3）支持策略告警的统一展示； | 1 | 套 |  |
| 2.9 | XC网络终端安全管理系统统一管理平台-日志审计管理 | XC网络终端安全管理系统统一管理平台-日志审计管理,审计汇总管理：对分院终端的文件操作行为进行审计汇总，包括但不限于以下操作如新建、修改、移动、改名、彻底删除、放入回收站、还原、清空；  1）支持汇总常用软件产生的文件变动行为审计；  2）支持汇总用户访问的网站进行审计记录，汇总各分院网站审计列表，包括：设备名称、远程IP、远程端口、域名、进程路径、标题、网址、设备IP；  3）汇总各分院终端系统上当前运行的进程及状态进行监控和审计。  4）汇总各分院终端用户的文档打印行为、光盘刻录行为用于审计、记录；  5）汇总各分院终端系统上相关服务及启用、停止等状态进行监控和审计。  6）汇总各分院终端系统上的共享目录进行监控和审计。  7）汇总各分院终端上的用户账户进行监控和审计  8）汇总各分院终端上的开机启动项进行监控和审计，监控的内容包括启动项的添加、删除和修改等操作。  9）汇总各分院指定目录下的注册表项，监控的内容包括注册表项的添加、删除和修改等操作。  10）汇总各分院网络流量使用情况 | 1 | 套 |  |
| 2.10 | XC网络终端安全管理系统统一管理平台-数据展示管理 | XC网络终端安全管理系统统一管理平台-数据展示管理,整体展示管理：对于高院及下属各区县的终端统一管理要求，进行数据统一管理和分析  1）展示各分院违规情况，以地图形式在后台直观展示  2）违规地区以标志性亮点，显示违规情况，可以点击查看分院更多违规详  3）对于高院及下属各区县分院之间实时链路、流量状况，以及终端在线率，终端设备合规率排行、安检项通过率、文档操作等报表信息通过投射大屏的方式进行实时、直观展现 | 1 | 套 |  |
| 2.11 | XC网络终端安全管理系统统一管理平台-系统报警管理 | XC网络终端安全管理系统统一管理平台-系统报警管理,系统报警：多采用多种类型告警方式，以方便管理员快捷、及时、准确的了解每个终端以及平台自身的运行状况。  1）支持不同的类别的告警自动分级，便于管理员及时迅速的了解这些系统意外状况；  2）支持syslog输出报警  3）支持EMAIL、手机短信等更为及时告警方式，以帮助管理员能够在第一时间发现问题； | 1 | 套 |  |
| 3 | 移动安全 |  |  |  |  |
| 3.1 | 移动终端安全管理平台 | 移动终端安全管理平台,包含移动设备管理、移动应用管理、移动内容管理和移动数据防泄露（沙箱） | 1 | 套 |  |
| 4 | 运维终端数据防泄漏 |  |  |  |  |
| 4.1 | 互联网数据防泄露控制台 | 互联网数据防泄露控制台,DLP系统的管理中心，进行安全策略设置、事件管理、用户、日志等管理 | 1 | 套 |  |
| 4.2 | 互联网数据防泄露客户端 | 互联网数据防泄露客户端,发现、识别、监控终端中的敏感数据，对终端数据资产分布、终端敏感数据的违规存储进行展现；对终端敏感数据的违规使用、扩散等敏感行为进行策略响应控制。 | 25 | 套 |  |
| 4.3 | 法院专网数据防泄露控制台 | 法院专网数据防泄露控制台,DLP系统的管理中心，进行安全策略设置、事件管理、用户、日志等管理 | 1 | 套 |  |
| 4.4 | 法院专网数据防泄露客户端 | 法院专网数据防泄露客户端,发现、识别、监控终端中的敏感数据，对终端数据资产分布、终端敏感数据的违规存储进行展现；对终端敏感数据的违规使用、扩散等敏感行为进行策略响应控制。 | 200 | 套 |  |

### 2.安全产品购置清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **类别** | **功能说明/配置要求** | **数量** | **单位** |
| 1 | 安全监管中心 |  |  |  |  |
| 1.1 | 核心节点网络流量采集探针 | 安全管理平台产品 | 同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量3Gbps，HTTP并发连接数400万，HTTP新建连接速率15万/秒,6个10/100/1000M自适应千兆电口，两个万兆光口（含短波长光纤模块） | 5 | 台 |
| 1.2 | 信访办网络流量采集探针 | 安全管理平台产品 | 同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量1Gbps，HTTP并发连接数300万，HTTP新建连接速率10万/秒，6个10/100/1000M自适应千兆电口 | 1 | 台 |
| 1.3 | 互联网本地日志审计 | 安全审计产品 | 互联网本地日志审计,对高院本地互联网的设备日志进行统一收集与分析 | 1 | 台 |
| 2 | 主机及终端安全 |  |  |  |  |
| 2.1 | XC网络终端安全管理系统 | 安全管理平台产品 | XC网络终端安全管理系统,产品CPU:龙芯3A3000（1.4GHz，4核）；操作系统：中标麒麟 V7.0（服务器版）；内存：8GB；硬盘：240GB；网络接口:1个管理口、4个千兆电口和4个千兆光口；整机规格：1U机箱。  产品包含服务端和客户端程序，支持通过客户端代理对受控主机状态、系统资源、软件情况、运行进程、网络端口、文件打印情况、非授权外联情况和文件操作行为等进行监测，支持对受控主机进行控制，包括进程开启/关闭、移动存储介质的使用和USB接口的使用等。默认包含50个点的终端管控授权 | 23 | 台 |
| 3 | 移动安全 |  |  |  |  |
| 3.1 | 零信任控制中心 | 安全产品 | 零信任控制中心,性能参数：最大并发用户数（个）10000。  硬件参数：内存大小：16G，硬盘容量：480G SSD，电源：冗余电源，接口：6千兆电口+4千兆光口SFP+2万兆光口SFP+。  功能描述：采用国家密码管理局颁布的SM1、SM2、SM3、SM4密码算法及其协议，支持多种身份认证方式、访问权限控制等主要功能，保证远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全  包含加密传输、接入、认证、日志审计等功能。 | 1 | 台 |
| 3.2 | 零信任网关 | 安全产品 | 零信任网关,性能参数：最大理论加密流量：2.1Gbps，最大理论并发用户数（个）：20000。  硬件参数：内存大小：32G，硬盘容量：480G SSD，电源：冗余电源，接口：4千兆电口+4千兆光口SFP+4万兆光口SFP+。  功能描述：采用国家密码管理局颁布的SM1、SM2、SM3、SM4密码算法及其协议，支持多种身份认证方式、访问权限控制等主要功能，保证远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全  负责建立、监视及切断零信任客户端和业务应用之间的隧道连接，并对经过代理网关转发的流量进行加密。支持三层、四层、七层等多种访问协议代理，可以满足多种类型应用的发布。 | 2 | 台 |
| 3.3 | IPSec VPN网关 | VPN | 网络层吞吐量：40Gbps，应用层吞吐量：30Gbps，并发连接数：4000万，新建连接数（CPS）：23万。IPSEC吞吐量：2Gbps | 2 | 台 |
| 3.4 | 服务调用交换平台 | 安全隔离与信息交换产品 | 最大吞吐量≥8Gbps数据库交换数量（100Kb/条）≥3000条/秒；数据库交换最大并发数无限制；文件数据处理数量（100Kb/个）≥5000个/秒； | 1 | 台 |
| 3.5 | 单向光闸 | 安全隔离与信息交换产品 | 应用层单向UDP吞吐≥5Gbps；支持国产芯片及操作系统，产品包含数据库单向导入、文件单向导入、单向协议导入、异常告警等 | 2 | 台 |

# （三）技术指标要求

### 1、安全监管中心

#### 1.1中心平台

##### 1.1.1功能要求

1.安全运营管理

安全运营管理功能模块，通过事前的资产梳理、资产风险识别，事中的高级威胁检测，发现内部的安全风险和高级威胁入侵行为；通过事后的追踪溯源，形成安全运营的闭环，提升安全运营效率。

安全运营管理功能模块应实现：安全态势、资产管理、资产指纹、风险评估、数据采集、威胁分析和响应处置等功能。

（1）**安全态势**

该项功能需提供态势的可视化和安全态势展示，协助安全运营人员对安全状况进行全局性掌控、安全概览。具备以下安全态势大屏展示：

安全威胁大屏：可展示全局安全威胁场景，从攻击者、攻击方式、被攻击者、攻击结果角度完整呈现了现网中的安全风险、安全趋势等信息。

安全流量大屏：可展示全局流量访问关系，从被访问资产、外联资产、正常业务流量、可疑流量进行区分，绘制访问趋势。

安全脆弱性大屏：可展示安全整体脆弱性情况，从全局资产、已防护资产、未防护资产，整体风险评分等方面展示资产风险等级的分布情况。

（2）**资产管理**

该项功能需与法院现有资产管理平台进行对接，以接口API的方式，接收资产管理平台的已登记的主机资产信息，对同步的主机资产建立资产数据库，对资产的来源、风险状态、安全事件进行持续地跟踪和管理，直到资产最终下线。并结合网络实体威胁情报进行安全态势分析，扩大安全可见性。

（3）**资产指纹**

该项功能需与主机（服务器）安全管控系统进行对接，通过API接口等方式，定时获取主机资产信息，包括主机资产内安装的软件包、进程、服务等详细信息，建立资产指的纹信息和档案，通过定期收集指纹信息，监听稳定的指纹数据，分析是否有异常行为并进一步的排查分析。

（4）**风险评估**

该项功能需与主机安全管控系统进行对接，通过API接口、syslog等方式，定时获取主机风险信息进行全面风险评估（包括漏洞、暴露端口、弱口令、告警、资产属性、重要性等），通过资产识别、脆弱性识别和威胁识别结果得出安全现状分析和评估结果。

（5）**数据采集**

该项功能需负责采集汇聚接收本地及云内的资产信息、流量数据和安全日志数据，并对采集的数据进行数据清洗、数据转换、数据抽取、数据融合等预处理操作，形成符合要求的统一数据，为安全运营管理后续的检测、评估及态势分析呈现提供基础数据支撑。

数据采集：需完成资产指纹、安全日志采集、网络流量等采集工作，将其送到数据预处理部分进行下一步的处理。

数据预处理：需对采集的数据进行数据清洗、数据转换和数据抽取，完成对数据的去重和去噪，过滤不符合要求的安全信息数据，转换成主题库要求的形式，抽取相关数据要素。

数据融合：需将各种信息的互补冗余进行最优化计算，进行完整度处理，将进行信息归类，做到标签、结构和内容三个层面的深度融合。

（6）**威胁分析**

该项功能需采用大数据分析引擎和关联分析引擎，对从主机、安全设备采集来的流量、日志和安全告警进行处理，结合资产指纹信息、资产脆弱性、网络流量、安全日志等的信息进行关联分析，发现更复杂的、更具价值的威胁事件。

（7）**响应处置**

该项功能需通过对安全事件、日志以及网络流量进行检测，分析出网络攻击、异常流量等威胁，产生安全告警，在平台安全告警处理页面展示相关告警列表信息。检测出安全告警事件后，可以对告警及时性处置，可以阻断所有访问到目的IP、网段，从而达到检测响应闭环的效果。

2.日志分析管理

日志分析管理可以对高院专网本地网络设备、安全设备、主机系统，以及政务云法院VPC内的主机的日志、告警等数据进行统一的采集和汇集，对采集到的安全日志和告警进行标准化（范式化）处理，从而进一步地对日志数据流进行实时关联分析和离线分析。

（1）**日志集中收集**

日志分析管理需具备全面的采集能力，可以采集本地及云内主机的系统行为日志、网络设备日志、安全设备的日志。

（2）**日志集中处理**

日志分析管理需对所采集到的日志进行标准化转换和富化加工后，存入到安全监管运营平台的分布式集群数据存储。

（3）**日志关联分析**

日志分析管理需对从本地及云内主机、网络设备、安全设备的安全日志，进行关联分析和归并，根据安全事件的类型、所处攻击阶段、攻击目标资产进行归并后，减少安全运营人员需要处理的告警数量，提高人工可分析处理效率，发现更复杂的、更具价值的威胁事件。

（4）**日志检索查询**

日志分析管理需对所采集的日志提供高性能的分布式集群数据存储，需具备分布式搜索引擎，并提供分布式的日志全文检索、结构化搜索的查询能力，能够处理PB级别以上的结构化或非结构化数据，达到百亿条数据秒级检索，提供安全事件调查取证的支撑。

（5）**可视化运营**

日志分析管理需提供可视化的视图管理，提供日志的查看和检索能力，支持交互式选择需要查询的字段并提供智能联想降低使用的门槛，同时支持面向专业人员的高级的SQL搜索语句，方便安全运营人员开展安全运营工作。

（6）**日志审计**

通过集中收集的日志进行自动化和交互式关联分析，提供综合全面的安全审计能力，发现来自组织内部和外部的多种安全事件，为管理员集中提供必须的日志文件以方便分析和排查故障，生成各类合规报表和报告，满足《网络安全法》对日志保存180天的要求和等级保护2.0中的安全审计要求。

3.自动化编排与响应

需要将安全运营人员和技术能力编入安全运营业务流程中，通过编排将安全事件分析过程中各种复杂性分析流程和处理平台进行组合，将繁杂的安全运营（尤其是安全响应）过程梳理为任务和剧本，将分散的安全工具与功能转化为可编程的应用和动作，依靠网络安全监管平台所汇聚的告警数据，进行自动化的事件分析、安全能力编排及自动化的响应处理。

自动化编排与响应实现包括编排与自动化管理、高级告警分析、案例管理、工单管理和平台支撑管理等功能。

**（1）编排与自动化管理**

该项功能需实现安全运营流程的剧本化和安全应用的编排化，并通过编排器实现了剧本和应用的自动化执行。需具备以下功能：

剧本管理：安全运营人员可对所有剧本进行统一管理，支持剧本的增删改查、导入、导出、版本管理、发布和草稿管理。能够监控所有正在执行的剧本的情况，查看剧本执行的详情。

脚本管理：安全运营人员可以对脚本进行管理，通过内嵌的Python脚本编辑器创建、编辑和调试脚本。

响应编排器：安全运营人员可以通过响应编排器，从剧本库中加载所有激活的剧本，并依照不同的触发条件执行相应的剧本实例。

**（2）高级告警分析**

该项功能需对安全运营管理模块提供的各类告警信息进行过滤、归并、聚合等加工处理，对告警信息进行增强，将不同来源的告警信息进行交叉比对，提取出精度和确定性更高的告警，提升安全响应的准确度与有效性。

**（3）案例管理**

该项功能需帮助安全运营人员对一组相关的告警按照既定的行动方案进行流程化、持续化、协作化、全周期的调查分析与响应处置，以及行动方案自身的持续改进。需具备以下功能：

案例清单：以列表的形式展示所有案例清单，可以展示每个案例概况，安全运营人员可以进行案例的查看、创建和编辑修订。

案例处理：可以查看案例相关的告警信息；安全运营人员可以持续地对案例信息进行处理。

行动方案管理：按照行业标准或者最佳实践来设置预案，预案可分为多个不同阶段，每个阶段可进一步分解为多个任务，并分配给不同成员。

可视化处理：以案例处理过程生成一个全周期的时间线，可按照时间顺序展示该案例处理过程中的信息。

**（4）工单管理**

安全运营人员可以通过工单管理对告警信息进行快速简单地响应，或者分配周期性地工作任务。可以手工添加工单，或者在告警调查的时候触发产生工单，并对工单的生命周期进行管理。

**（5）支撑管理**

用户权限管理：具备基于角色的权限管理机制，可对角色授权访问的资源进行细粒度的权限划分，赋予不同的功能。

平台管理：需具备自身操作审计能力，能够对使用平台的各种操作进行记录留存和审计。

开放接口：具备开放式API接口，可以将自身能力集成到其它第三方系统中（北向接口）。

4.虚拟流量分析

实现对云环境中主机之间东西向流量的采集，提供基于流量的应用识别、病毒检测、入侵检测、风险发现、追踪溯源等功能，有效检测相关网络攻击和威胁。

流量采集：通过在云内主机上部署流量采集插件，将云内主机的全流量采集并发送至虚拟流量分析系统，不少于500台主机流量采集。

威胁检测：虚拟流量分析系统对主机的网络流量进行威胁检测分析，发现可疑威胁（恶意扫描、暴力破解、后门检测、WebShell等），生成网络日志和威胁日志，并将网络日志和威胁日志上传到安全监管运营平台。

5.威胁情报

威胁情报采集：通过离线导入方式获取威胁情报数据，进行威胁情报采集和累积。

威胁情报应用：利用威胁情报数据对采集的数据进行实时比对分析，发现可疑的连接行为，对发现的可疑的IP、域名、URL进行深入的情报判定。在发现攻击行为后，安全运营人员可对事件进行溯源分析，找到攻击行为背后的攻击者，了解攻击者的攻击企图、常用工具、技术和攻击手法等，以评估来自特定攻击者的安全风险，有针对性地采取防范措施，搜集攻击相关证据。

##### 1.1.2技术指标

| **指标项** | | **功能要求** |
| --- | --- | --- |
| 安全运营管理 | 安全态势 | 1.安全威胁大屏 |
| 支持查看失陷主机； |
| 支持展示受攻击资产排行、威胁类型、攻击源排行、告警趋势、安全告警、攻击地图等安全信息； |
| 2.安全流量大屏 |
| 支持查看当前最新攻击告警事件及攻击结果信息； |
| 支持查看资产统计、失陷资产统计、告警统计、外联统计，对攻击流量可查看攻击源IP、目的IP、攻击事件、结果信息； |
| 支持查看被访问资产、受攻击、外联资产、流量、访问趋势等信息； |
| 3.脆弱性大屏 |
| 支持展示全局资产风险值态势，包括资产漏洞、弱口令等； |
| 支持展示所有高危风险资产，按照风险值排序； |
| 资产管理 | 支持与现有高院运维管理平台进行对接，以接口API的方式，接收平台管理的资产信息； |
| 支持收集和展示主机、网站、数据库资产相关信息； |
| 支持展示接入的资产数量信息及占比情况，包括资产类型分布； |
| 支持展示、查看所有主机的资产指纹信息，支持资产指纹详情展示，包含：进程名、进程路径、PID、启动用户、启动时间、运行时间、命令行、父进程PID等； |
| 资产指纹 | 支持与主机安全管控系统进行对接，通过API接口等方式，定时获取主机资产信息，建立资产指纹信息和档案； |
| 支持对端口、计划任务、账号、启动项的异常指纹分析，提供判定结果等异常结果，进行异常指纹判断； |
| 风险评估 | 支持漏洞的分类管理和统计； |
| 支持展示资产漏洞分布情况，包括漏洞的严重性、漏洞名称、CVE编号、受影响的资产等； |
| 支持主机漏洞展示所在路径、受影响版本、服务、协议、端口等信息； |
| 支持单个、多个漏洞的验证和批量验证； |
| 支持展示存在弱口令的资产总数； |
| 支持单个、多个主机弱口令验证； |
| 支持查看已经检测出弱口令的资产列表，包括资产名称、存在风险的账号； |
| 数据采集 | 支持以agent或插件的方式部署，对虚机全流量或指定流量进行采集转发，并支持限制转发速率； |
| 支持VXLAN转发协议； |
| 威胁分析 | 支持统计近7天趋势、等级分布、告警类型数量分布； |
| 支持告警信息的展示，包括等级、告警名称、攻击源、目的IP、告警类型、ATT&CK、攻击结果、所属租户、最近发生时间、告警状态等； |
| 支持针对计划任务可疑新增、启动项可疑新增、账号可疑新增模型异常告警设置； |
| 支持设置学习周期、对比频率、告警阈值； |
| 支持行为分析列表，告警信息包括：告警名称、异常类型、资产信息、所属租户、模型类型、学习周期、对比频率、告警阈值、异常计数、首次发生时间、最新发生时间、处置状态等； |
| 支持自定义检测规则，类VISIO的图形化连线拖拽交互，灵活组合规则建模中的计算单元以应对不同威胁场景建模； |
| 响应处置 | 支持阻断IP入站、出站访问能力； |
| 支持对告警事件的恶意IP进行阻断动作； |
| 支持联动主机端安全能力批量下发阻断策略，生成主机黑名单； |
| 支持对处置记录进行查询、新增、删除； |
| 日志分析管理 | 日志集中收集 | 支持对网络设备、安全设备、操作系统的日志的采集； |
| 支持对采集策略管理、采集任务管理和数据采集状态的监控等； |
| 日志集中处理 | 支持对所采集的日志进行范式化处理； |
| 支持对所采集的数据进行数据清洗、数据转换、数据抽取、数据标记等预处理，形成符合要求的统一数据； |
| 支持对采集到的日志数据进行数据补全、冗余处理、数据融合、数据富化等； |
| 日志关联分析 | 支持对所采集的流量、安全日志，进行关联分析和归并，通过事件之间存在的相似关系、因果关系等对事件进行聚合处理； |
| 支持安全事件的关联分析，综合各类安全事件间的内在联系，对安全事件进行关联分析，实现安全攻击检测； |
| 日志检索查询 | 支持多种检索模式，能够实现复杂搜索语句的构造； |
| 支持提供类SQL语法搜索，支持语法辅助提示，提供“语法帮助”功能；提供“语法帮助”功能； |
| 支持按照日志分类进行日志筛选和检索； |
| 支持对字段进行快速统计，支持对字段统计结果进行下载和快速过滤； |
| 支持通过日志关键字段进行追加搜索，从上一次的搜索结果中重新按照新的规则搜索日志； |
| 可视化运营 | 支持检索字段展示，提供可检索字段的列表展示； |
| 支持对检索结果的展现，包含全文展示和结构化展示（Key-Value格式）； |
| 支持日志的时间分布展示，并提供按照时间分布图进行下钻检索； |
| 自动化编排与响应 | 编排与自动化管理 | 管理员可以通过可视化剧本编辑器自定义剧本。在编辑剧本的时候，可以选择的元素包括动作、API、子剧本、任务、审批、脚本、轮询、分支、聚合。管理员可以将这些元素通过鼠标拖拽的方式加入到编辑器中，构成一个图形化的剧本图。针对每个元素，管理员都可以进行详细的设置；【需提供截图】 |
| 支持剧本新增、删除、移动、修改、查询、锁定、导入、导出功能。 |
| API节点支持在剧本执行过程中在案例模块创建案例、添加标注到案例、添加痕迹到案例；支持编辑活动列表、查询活动列表、添加到活动列表、是否在活动列表中、事件和告警查询/统计、创建工单等。 |
| 支持手动输入剧本参数后执行； |
| 支持添加调度任务执行一个或多个App动作和剧本，调度任务支持单次调度和周期调度，周期调度可按分钟，小时，天和周执行；支持按任务执行时间查看调度任务执行记录； |
| 支持列表查看正在运行的剧本，包括剧本对应告警Id，剧本名称、执行对象、剧本执行状态、开始时间、运行时长等【需提供截图】 |
| 支持查看剧本执行结果，查看每个流程节点的执行状态； |
| 子剧本节点执行结果面板支持显示输入参数、输出参数、执行状态、执行时间； |
| 支持打开新标签页显示子剧本详情； |
| 支持通过点击剧本名称打开新标签页查看剧本执行结果详情； |
| 支持脚本锁定，创建人锁定脚本后，其它用户只能引用不能修改脚本内容。 |
| 高级告警分析 | 告警采集速率高于2000条/s； |
| 支持接收第三方系统/设备通过syslog发出的告警信息；支持通过Kafka、REST API接口接收第三方的告警信息； |
| 支持对接收到的告警日志进行范化，实现对异构告警日志格式的统一描述。系统内置针对常见告警日志的范化策略，并支持用户手工编辑范化策略。用户可以修改现有的告警日志数据模型，也可以自定义告警数据模型。 |
| 支持多个事件或告警通过不同属性关联成一条关联事件； |
| 支持源IP、目标IP、事件名称、攻击类型等所有事件属性中任务多个属性的关联合并与分析； |
| 支持以列表方式，按照告警所处的不同状态显示所有告警信息，以及每种状态的告警数量； |
| 支持以时间轴方式展示告警触发的App动作和剧本，钻取查看App动作和剧本的执行结果； |
| 支持基于告警响应规则的自动化响应，告警响应规则包含告警条件、告警响应动作，支持一次响应多个剧本或动作；【需提供截图】 |
| 支持将符合条件的告警生成案例，并将响应中的过程数据自动或人工地加入到痕迹清单中； |
| 支持对多个不同类型不同来源的告警事件信息进行综合关联分析，支持与或非筛选事件信息，多事件具备实时关联和历史关联能力分析； |
| 支持关联规则嵌套和引用，通过多规则联合，可精确识别复杂安全事件和场景；【需提供截图】 |
| 关联分析支持可视化配置，支持单字段的筛选过滤，也支持引用活动列表，可将一个规则匹配后事件的某个或某些属性添加到活动列表内，并可在另一个规则内引用活动列表，实现两个规则的联动，进而实现对复杂长周期的攻击行为的描述和刻画； |
| 案例管理 | 支持管理员对案例增删改查，案例的属性包括案例名称、类型、严重程度、标签、预案、责任人、成员、计划完成时间和描述； |
| 支持痕迹管理、标注管理和附件管理功能； |
| 支持在案例中添加痕迹信息、编辑标注、上传附件； |
| 支持对每个案例分配一个或者多个标签； |
| 支持对案例激活预置的编排剧本，并将相关操作和结果记录到活动记录； |
| 支持针对案例痕迹激活预置响应动作清单； |
| 支持选择并执行某个响应动作； |
| 支持自动记录动作执行操作及结果并展示； |
| 支持案例的报告生成； |
| 支持按照行业标准或者最佳实践来设置预案应对措施，可以将应对措施分为多个不同阶段，每个阶段进一步分解为多个任务，并分配给不同成员； |
| 工单管理 | 支持手工添加工单，或者在告警调查的时候触发产生工单；【需提供截图】 |
| 支持用户查看自己创建的工单以及被分配的工单； |
| 支持显示当前指派的任务数； |
| 平台支撑管理 | 具备自身操作审计能力； |
| 支持系统管理员、安全操作管理员和审计管理员三权分立； |
| 支持基于角色的权限管理机制，可对角色授权访问的资源进行细粒度的权限划分，赋予不同的功能； |
| 支持对系统自身的CPU、内存、磁盘等运行状态和性能等设置告警阈值； |
| 支持开放式API接口，允许其它系统调用该接口，提供详细文档支持；【需提供截图】 |
| 虚拟流量分析 | | 支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发； |
| 支持对采集对象进行网络流量数据采集和威胁检测数据采集； |
| 支持将威胁检测数据还原成威胁样本； |
| 支持对流量数据和威胁检测数据灵活配置外发对象，包括态势感知平台、大数据分析平台等；【需提供截图】 |
| 支持解析、生成及外发流量日志、Web访问日志、域名解析日志、文件传输日志、登陆动作日志、数据库操作等日志； |
| 支持多种类型、协议的漏洞检测； |
| 支持多种类型的间谍软件检查； |
| 支持Web威胁检测； |
| 支持全面、强劲的恶意文件检测和发现能力，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB协议进行恶意文件检测；【需提供截图】 |
| 支持自定义恶意文件，可以通过MD5码定义恶意文件特征； |
| 支持实现基于威胁情报的失陷主机检测及日志外发； |
| 支持失陷主机、恶意文件检测、漏洞攻击检测的数量统计； |
| 威胁情报 | | 支持并提供威胁情报能力； |
| 支持从云端或离线导入等方式获取威胁情报数据； |
| 支持通过威胁情报数据对采集的数据进行实时比对分析，发现可疑的连接行为； |
| 硬件日志源的数据分析授权 | | 满足100个日志数据源的数据分析授权 |

#### 1.2核心节点网络流量采集探针

|  |  |
| --- | --- |
| **指标项** | **技术指标** |
| 性能参数 | 吞吐量≥3Gbps，并发连接数≥400万，新建连接数≥15万/秒； |
| 网络接口 | 配置6个10/100/1000M自适应千兆电口 |
| 硬件规格 | 产品应为标准机架式设备； |
| 部署模式 | 支持旁路部署，可同时接入多个镜像口，每个镜像口相互独立； |
| 流量采集 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现； |
| 支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备； |
| 支持常见数据库协议的识别或还原； |
| 支持TCP/UDP会话记录、异常流量会话记录、web访问记录、域名解析、SQL访问记录、邮件行为、登录情况、文件传输、FTP控制通道、SSL加密协商、telnet行为、IM通信等行为描述； |
| 支持自定义协议和端口，满足特殊场景下的流量抓取； |
| 支持离线流量采集，可通过手动PCAP导入方式对离线流量进行采集； |
| 威胁检测 | 支持基于流量实时IOC匹配功能，设备具备主流的IOC； |
| 支持检测针对WEB应用的攻击，支持跨站请求伪造CSRF攻击检测；支持其他类型的WEB攻击； |
| ▲支持基于工具特征的WEBSHELL检测，通过系统调用、系统配置、文件操作来及时发现威胁；支持基于webshell函数的攻击检测；（提供产品功能截图） |
| 支持基于代理程序的攻击检测，如TCP代理程序、HTTP代理程序等； |
| 支持多种攻击检测，能更全面的从流量中发现威胁； |
| 行为分析 | 支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为 |
| 持基于网络请求的语义分析检测，提升对未知威胁检测能力； |
| 具备AI隧道检测、非TCP完整流、畸形包检测、数据包完整性检测、碎片重组检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力； |
| 支持门罗币、莱特币、以太坊、比特币等币种的检测，区分挖矿行为阶段：恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额； |
| 策略配置 | 支持对HTTP、FTP\_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS等类型协议的流量进行文件还原； |
| 支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP地址、端口或协议类型； |
| 支持基于网络请求的语义分析检测，详细展示请求内容，并能提升对未知威胁检测能力； |
| 支持基于IP地址的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断；支持基于URL的旁路阻断，并能将URL请求进行重定向； |
| ▲支持自定义弱口令字典，支持HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP等协议的自定义弱口令检测；支持自定义弱口令规则，可正则表达式方式自定义弱口令强度、复杂度规则；（提供产品功能截图） |
| 支持旁路HTTPS解密、威胁检测； |
| 支持对告警进行加白； |
| 系统管理 | 支持AES256、SM4数据传输加密，确保数据传输的安全性； |
| 支持威胁告警信息发送给syslog服务器，支持将威胁告警、网络日志、攻击结果、威胁类型等日志传输给威胁分析平台； |
| 支持将威胁告警外发集中管理平台，支持与集中管理平台进行联动，统一进行情报、规则的升级； |

#### 1.3信访办网络流量采集探针

|  |  |
| --- | --- |
| **指标项** | **技术指标** |
| 性能参数 | 吞吐量≥1Gbps，并发连接数≥200万，新建连接数≥10万/秒； |
| 网络接口 | 配置6个10/100/1000M自适应千兆电口 |
| 硬件规格 | 产品应为标准机架式设备； |
| 部署模式 | 支持旁路部署，可同时接入多个镜像口，每个镜像口相互独立； |
| 流量采集 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现； |
| 支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备； |
| 支持常见数据库协议的识别或还原； |
| 支持TCP/UDP会话记录、异常流量会话记录、web访问记录、域名解析、SQL访问记录、邮件行为、登录情况、文件传输、FTP控制通道、SSL加密协商、telnet行为、IM通信等行为描述； |
| 支持自定义协议和端口，满足特殊场景下的流量抓取； |
| 支持离线流量采集，可通过手动PCAP导入方式对离线流量进行采集； |
| 威胁检测 | 支持基于流量实时IOC匹配功能，设备具备主流的IOC； |
| 支持检测针对WEB应用的攻击，支持跨站请求伪造CSRF攻击检测；支持其他类型的WEB攻击； |
| ▲支持基于工具特征的WEBSHELL检测，通过系统调用、系统配置、文件操作来及时发现威胁；支持基于webshell函数的攻击检测；【需提供截图】 |
| 支持基于代理程序的攻击检测，如TCP代理程序、HTTP代理程序等； |
| 支持多种攻击检测，能更全面的从流量中发现威胁； |
| 行为分析 | 支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为 |
| 持基于网络请求的语义分析检测，提升对未知威胁检测能力； |
| 具备AI隧道检测、非TCP完整流、畸形包检测、数据包完整性检测、碎片重组检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力； |
| 支持门罗币、莱特币、以太坊、比特币等币种的检测，区分挖矿行为阶段：恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额； |
| 策略配置 | 支持对HTTP、FTP\_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS等类型协议的流量进行文件还原； |
| 支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP地址、端口或协议类型； |
| 支持基于网络请求的语义分析检测，详细展示请求内容，并能提升对未知威胁检测能力； |
| 支持基于IP地址的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断；支持基于URL的旁路阻断，并能将URL请求进行重定向； |
| ▲支持自定义弱口令字典，支持HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP等协议的自定义弱口令检测；支持自定义弱口令规则，可正则表达式方式自定义弱口令强度、复杂度规则；【需提供截图】 |
| 支持旁路HTTPS解密、威胁检测； |
| 支持对告警进行加白； |
| 系统管理 | 支持AES256、SM4数据传输加密，确保数据传输的安全性； |
| 支持威胁告警信息发送给syslog服务器，支持将威胁告警、网络日志、攻击结果、威胁类型等日志传输给威胁分析平台； |
| 支持将威胁告警外发集中管理平台，支持与集中管理平台进行联动，统一进行情报、规则的升级； |

#### 1.4互联网本地日志审计

| **指标项** | **技术指标** |
| --- | --- |
| 性能参数 | 产品应支持综合日志处理能力≥3000EPS； |
| 日志授权 | 产品应具备100个日志授权； |
| 网络接口 | 产品应具备千兆电口≥4个、千兆光口≥4个；接口板卡扩展插槽≥2个； |
| 硬件规格 | 产品应配置≥4TB硬盘存储； |
| 产品应为标准机架式设备，具备冗余电源； |
| 部署模式 | 支持单一部署、分布式集群部署、级联部署 |
| 级联管理 | ▲支持系统级联管理，可对下级系统的IP地址、系统信息、运行状态和性能进行集中监测，支持对下级系统的注册与注销； |
| 审计对象 | 支持审计各种网络设备（路由器、交换机等）的配置日志、运行日志、告警日志等；  支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关、网闸、防DDOS攻击、Web应用防火墙等）配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400等）配置日志、运行日志、告警日志等；  支持审计各种数据库（ Oracle、Sqlserver、Mysql、DB2、Sybase、Informix、达梦数据库、MongoDB等）配置日志、运行日志、告警日志等；  支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic等）配置日志、运行日志、告警日志等；  支持审计各种应用系统（邮件，Web，FTP等）配置日志、运行日志、告警日志等；  支持审计各种业务系统的日志、事件、告警等安全信息； |
| 日志采集  与转发 | 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent日志代理、WMI、(S)FTP、NetBIOS、文件\目录读取、Kafka、WebService等方式完成各种日志的收集； |
| 支持TCP、UDP协议转发，支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址； |
| 资产管理 | 支持资产按多种维度进行分组、分域管理； |
| 支持对资产IP地址（含内网IP）的地理信息进行管理，支持地图显示；(提供产品功能截图) |
| 支持自定义资产类型及资产属性；支持对资产自定义标签，对标签内容进行查询和管理； |
| 日志归一化 | 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； |
| 支持提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略；(提供产品功能截图) |
| 支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化； |
| 支持自动识别收集的日志并自动选择范化策略，针对匹配的多条范化策略，支持用户手工设置策略匹配优先级，保证最佳范化策略匹配；(提供产品功能截图) |
| 日志交互式分析 | 支持全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，快速搜索分析各类安全事件； |
| 支持采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)； |
| 支持图形化展示日志属性之间的聚合关系，支持手动选择日志属性，显示多维事件分析图；(提供产品功能截图) |
| 关联分析 | 支持基于规则的关联分析引擎，可提供逻辑关联、统计关联和递归关联的关联分析能力； |
| 支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； |
| 支持对关联规则进行监控，了解规则命中情况；(提供产品功能截图) |
| 日志统计分析 | 支持自定义统计场景，可设定统计的字段和时间段等； |
| 支持将统计结果保存为仪表板、报表和策略； |
| 日志综合展现 | 支持可编辑的自定义仪表板；支持自定义创建框架，可在框架内添加不同的仪表板组件； |
| 支持随时调整已创建的仪表板，编辑仪表板展示条件，调整位置、新增组件等，可对仪表板的任一元素进行下钻，查看原始日志；(提供产品功能截图) |
| 支持展示日志源数量、原始日志数、关联事件数、告警总数、已保存日志天数、平均每天日志存储量、存储空间情况等； |
| 告警管理 | 支持告警规则自定义，告警可查询，支持列表和统计展示；支持告警归并； |
| 报表管理 | 提供丰富的报表管理功能，根据时间、数据类型等生成报表，为管理员提供决策和分析的数据基础； |
| 支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告；(提供产品功能截图) |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；支持以FTP/SFTP方式将日志数据备份至外部存储空间，支持数据恢复 |
| 国产化要求 | 须为国产化设备，配备国产芯片及操作系统； |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |
| 产品具备信息技术产品安全测评证书（EAL3+及以上） |

#### 1.5互联网云日志审计

| **指标项** | **技术指标** |
| --- | --- |
| 部署模式 | 支持软件化部署，支持云平台部署； |
| 日志授权 | 产品应具备150个日志授权； |
| 级联管理 | ▲支持系统级联管理，可对下级系统的IP地址、系统信息、运行状态和性能进行集中监测，支持对下级系统的注册与注销； |
| 审计对象 | 支持审计各种网络设备（路由器、交换机等）的配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400等）配置日志、运行日志、告警日志等；  支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix、达梦数据库、MongoDB等）配置日志、运行日志、告警日志等；  支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic等）配置日志、运行日志、告警日志等；  支持审计各种应用系统（邮件，Web，FTP等）配置日志、运行日志、告警日志等；  支持审计各种业务系统的日志、事件、告警等安全信息； |
| 日志采集  与转发 | 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent日志代理、WMI、(S)FTP、NetBIOS、文件\目录读取、Kafka、WebService等方式完成各种日志的收集； (提供产品功能截图) |
| 支持TCP、UDP协议转发，支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址； |
| 资产管理 | 支持资产按多种维度进行分组、分域管理； |
| 支持对资产IP地址（含内网IP）的地理信息进行管理，支持地图显示；(提供产品功能截图) |
| 支持自定义资产类型及资产属性；支持对资产自定义标签，对标签内容进行查询和管理； |
| 日志归一化 | 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； |
| 支持提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略；(提供产品功能截图) |
| 支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化； |
| 支持自动识别收集的日志并自动选择范化策略，针对匹配的多条范化策略，支持用户手工设置策略匹配优先级，保证最佳范化策略匹配；(提供产品功能截图) |
| 日志交互式分析 | 支持全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，快速搜索分析各类安全事件； |
| 支持采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)； |
| 支持图形化展示日志属性之间的聚合关系，支持手动选择日志属性，显示多维事件分析图；(提供产品功能截图) |
| 关联分析 | 支持基于规则的关联分析引擎，可提供逻辑关联、统计关联和递归关联的关联分析能力； |
| 支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； |
| 支持对关联规则进行监控，了解规则命中情况；(提供产品功能截图) |
| 日志统计分析 | 支持自定义统计场景，可设定统计的字段和时间段等； |
| 支持将统计结果保存为仪表板、报表和策略； |
| 日志综合展现 | 支持可编辑的自定义仪表板；支持自定义创建框架，可在框架内添加不同的仪表板组件； |
| 支持随时调整已创建的仪表板，编辑仪表板展示条件，调整位置、新增组件等，可对仪表板的任一元素进行下钻，查看原始日志；(提供产品功能截图) |
| 支持展示日志源数量、原始日志数、关联事件数、告警总数、已保存日志天数、平均每天日志存储量、存储空间情况等； |
| 告警管理 | 支持告警规则自定义，告警可查询，支持列表和统计展示；支持告警归并； |
| 报表管理 | 提供丰富的报表管理功能，根据时间、数据类型等生成报表，为管理员提供决策和分析的数据基础； |
| 支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告；(提供产品功能截图) |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；支持以FTP/SFTP方式将日志数据备份至外部存储空间，支持数据恢复 |
| 国产化要求 | 须支持国产化环境，支持国产芯片及操作系统； |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |
| 产品具备信息技术产品安全测评证书（EAL3+及以上） |

### 2、主机及终端安全

#### 2.1互联网主机安全管控系统

本系统包含控制台和客户端两部分，控制台和客户端的技术规格参数分别如下。

控制台技术规格参数：

| **指标项** | **技术指标** |
| --- | --- |
| 主机管理 | 客户端安装方式：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。常见操作系统至少包括：支持如下操作系统：Windows（包括windows Server 2008、2012、2016、2019、2022；）、Linux（包括CentOS 6、7、8；RHEL 6、7、8、9；Ubuntu 14、16、18、20；麒麟；统信；欧拉）、Unix （包括Solaris(X86) 10）  支持主流国产化环境：中标麒麟、华为鲲鹏、统信、海光、飞腾（需提供兼容互认证证书） |
| 客户端安全性：客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制。 |
| 服务端国产化适配：服务端部署需支持国产化环境。 |
| 以列表形式查看所有的访问关系，可对各来源IP、目的IP、目的端口、协议、进程名、连接状态、首次时间、最近连接时间等字段进行检索； |
| 第三方对接：支持通过标准API和syslog接口的方式与第三方平台进行数据对接。 |
| 实时监控 | 应支持对主机异常行为，至少包括异常登录、暴力破解、反弹shell、web后门检测、系统后门检测、远程命令执行检测、可疑操作检测、本地提权检测等实时检测功能。 |
| 告警通知 | 系统应提供邮件、站内信等告警方式，告警支持统一管理，在系统中未被打开的通知应标识为未读，提供一键批量标记所有通知已读，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。 |
| 系统审计 | 支持对本安全系统所有行为进行审计记录。 |
| 策略配置 | 支持资产标签自动更新，方便资产运维管理。 |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |

客户端技术规格参数：

| **指标项** | **技术指标** |
| --- | --- |
| 资产清点 | 基本资产：支持清点主机各类基础资产，包括硬件、CPU、内存、磁盘、网卡IP、操作系统等信息。 |
| 系统层资产清点：支持清点主机系统层相关资产，包括进程、端口、账号、启动项、计划任务、环境变量、内核模块等信息。 |
| 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、web站点、web框架、web应用、web服务等信息。数据库和中间件至少包括达梦数据库、人大金仓、神州通用数据库、宝兰德应用服务器。 |
| Windows资产支持：清点Windows系统注册表项值，选择清点其中与安全相关的重要表项值，至少包括：路径、名称、类型、数据、风险描述等。  ▲至少清点Windows域账号，清点域账号服务器管理的账号与域账号被使用登录的信息，至少包括：所属域名，帐号最近登录时间，帐号状态，账号类型，home目录，最近登录主机名，最近登录ip等。  支持清点Windows进程数字证书签名，帮助初步推断进程安全性；具体包括，是否包含数字签名，签名者，有效期，证书路径等。 |
| 风险评估 | 风险分析：支持对漏洞补丁、弱口令和配置风险进行整体脆弱性分析，以评级评分体系的方式简要直观评价当前安全态势，并统计近7天、近1月风险评分的变化，并展示单个主机的风险评分最低TOP5。 |
| 漏洞扫描：支持检测各类常见系统与应用漏洞，漏洞详细信息至少包括：漏洞等级，漏洞名称、漏洞说明、漏洞类型、影响应用与版本、漏洞exp链接、修复建议、CVE编号、CVSS评分与详情、参考链接、引用链接、并提供各维度的补丁风险特征：内核风险、是否存在exp、远程利用、本地提权。 |
| 弱口令管理：支持检查Linux/Windows系统账号弱密码；应用进行弱密码检测，至少包括：InfluxDB、MySQL、Redis；中间件弱密码检测，至少包括：Weblogic、Jenkins、Tomcat；支持应用弱密码检测，应至少包括：OpenLDAP、ProFTPD、SVN、PPTP、VNC、SSH、OpenVPN、rsync、vsftpd。支持弱密码隐藏密码值，根据权限控制是否明文显示，保证安全性。 |
| 入侵检测 | 异常登录：支持配置正常登录规则，实时检测在非法登录来源IP、非法账号、非合法登录时间的登录行为。  支持对发现的告警事件进行手动处置，支持手动封禁和解封IP。 |
| 暴力破解：支持实时检测针对Linux系统账号和Windows系统账号的暴力破解行为，并支持配置自动封停，也可在告警界面进行手动封禁和解封。 |
| 反弹shell：支持实时检测Linux和Windows下的反弹shell行为并产生告警，告警信息能看到事件基本信息如受害主机IP、目标主机IP、目标端口、发现时间等，可看到事件说明，以及以攻击链方式展示的反弹详细过程。  可按照进程、目标主机等维度选择特定业务组范围的主机进行白名单策略配置。 |
| 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，文件修改时间，域名，受感染主机，发现时间等信息；支持对文件进行下载查看。 |
| 系统后门检测：支持系统后门实时检测，对后门进行隔离、加白、确认已修复等操作。后门告警信息包括：告警类型、告警说明、IP、发现时间等。 |
| 远程命令执行检测：支持对特定主机或者全部主机进行web远程命令执行检测，同时可查看详细的进程树信息，包括进程名，PID，所属用户，所属用户组，文件路径，文件执行权限，进程命令行等； |
| 合规基线 | 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。 |
| 主机隔离 | 客户端配置：实时监控网络连接，对不符合策略的访问产生告警，在列表中展示；相同告警聚合为同一条计数，并更新告警时间 |
| 微蜜罐 | 端口蜜罐：支持伪造任意系统端口，实时检测对设置蜜罐端口的尝试连接行为，并提供告警，监控已设置规则的端口，一旦尝试访问端口，即上报告警，其中端口应支持输入多个。 |
| 内存后门检测 | 内存webshell检测：支持实时检测在内存中加载网站恶意文件，无任何本地文件、恶意代码注入的检测。需要展示内存对应的类名、父类名、所属类加载器、内存对应大小、MD5信息等。 |
| 文件完整性 | 支持对文件的新增、修改、删除、权限变更等变化行为进行告警。 |
| 病毒查杀 | 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。 |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |

#### 2.2法院专网主机安全管控系统

本系统包含控制台和客户端两部分，控制台和客户端的技术规格参数分别如下。

控制台技术规格参数：

| **指标项** | **技术指标** |
| --- | --- |
| 主机管理 | 客户端安装方式：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。常见操作系统至少包括：支持如下操作系统：Windows（包括windows Server 2008、2012、2016、2019、2022；）、Linux（包括CentOS 6、7、8；RHEL 6、7、8、9；Ubuntu 14、16、18、20；麒麟；统信；欧拉）、Unix （包括Solaris(X86) 10 ）  支持主流国产化环境：中标麒麟、华为鲲鹏、统信、海光、飞腾（需提供兼容互认证证书） |
| 客户端安全性：客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制。 |
| 服务端国产化适配：服务端部署需支持国产化环境。 |
| 以列表形式查看所有的访问关系，可对各来源IP、目的IP、目的端口、协议、进程名、连接状态、首次时间、最近连接时间等字段进行检索； |
| 第三方对接：支持通过标准API和syslog接口的方式与第三方平台进行数据对接。 |
| 实时监控 | 应支持对主机异常行为，至少包括异常登录、暴力破解、反弹shell、web后门检测、系统后门检测、远程命令执行检测、可疑操作检测、本地提权检测等实时检测功能。 |
| 告警通知 | 系统应提供邮件、站内信等告警方式，告警支持统一管理，在系统中未被打开的通知应标识为未读，提供一键批量标记所有通知已读，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。 |
| 系统审计 | 支持对本安全系统所有行为进行审计记录。 |
| 策略配置 | 支持资产标签自动更新，方便资产运维管理。 |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |

客户端技术规格参数：

| **指标项** | **技术指标** |
| --- | --- |
| 资产清点 | 基本资产：支持清点主机各类基础资产，包括硬件、CPU、内存、磁盘、网卡IP、操作系统等信息。 |
| 系统层资产清点：支持清点主机系统层相关资产，包括进程、端口、账号、启动项、计划任务、环境变量、内核模块等信息。 |
| 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、web站点、web框架、web应用、web服务等信息。数据库和中间件至少包括达梦数据库、人大金仓、神州通用数据库、宝兰德应用服务器。 |
| Windows资产支持：清点Windows系统注册表项值，选择清点其中与安全相关的重要表项值，至少包括：路径、名称、类型、数据、风险描述等。  ▲至少清点Windows域账号，清点域账号服务器管理的账号与域账号被使用登录的信息，至少包括：所属域名，帐号最近登录时间，帐号状态，账号类型，home目录，最近登录主机名，最近登录ip等。  支持清点Windows进程数字证书签名，帮助初步推断进程安全性；具体包括，是否包含数字签名，签名者，有效期，证书路径等。 |
| 风险评估 | 风险分析：支持对漏洞补丁、弱口令和配置风险进行整体脆弱性分析，以评级评分体系的方式简要直观评价当前安全态势，并统计近7天、近1月风险评分的变化，并展示单个主机的风险评分最低TOP5。 |
| 漏洞扫描：支持检测各类常见系统与应用漏洞，漏洞详细信息至少包括：漏洞等级，漏洞名称、漏洞说明、漏洞类型、影响应用与版本、漏洞exp链接、修复建议、CVE编号、CVSS评分与详情、参考链接、引用链接、并提供各维度的补丁风险特征：内核风险、是否存在exp、远程利用、本地提权。 |
| 弱口令管理：支持检查Linux/Windows系统账号弱密码；应用进行弱密码检测，至少包括：InfluxDB、MySQL、Redis；中间件弱密码检测，至少包括：Weblogic、Jenkins、Tomcat；支持应用弱密码检测，应至少包括：OpenLDAP、ProFTPD、SVN、PPTP、VNC、SSH、OpenVPN、rsync、vsftpd。支持弱密码隐藏密码值，根据权限控制是否明文显示，保证安全性。 |
| 入侵检测 | 异常登录：支持配置正常登录规则，实时检测在非法登录来源IP、非法账号、非合法登录时间的登录行为。  支持对发现的告警事件进行手动处置，支持手动封禁和解封IP。 |
| 暴力破解：支持实时检测针对Linux系统账号和Windows系统账号的暴力破解行为，并支持配置自动封停，也可在告警界面进行手动封禁和解封。 |
| 反弹shell：支持实时检测Linux和Windows下的反弹shell行为并产生告警，告警信息能看到事件基本信息如受害主机IP、目标主机IP、目标端口、发现时间等，可看到事件说明，以及以攻击链方式展示的反弹详细过程。  可按照进程、目标主机等维度选择特定业务组范围的主机进行白名单策略配置。 |
| 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，文件修改时间，域名，受感染主机，发现时间等信息；支持对文件进行下载查看。 |
| 系统后门检测：支持系统后门实时检测，对后门进行隔离、加白、确认已修复等操作。后门告警信息包括：告警类型、告警说明、IP、发现时间等。 |
| 远程命令执行检测：支持对特定主机或者全部主机进行web远程命令执行检测，同时可查看详细的进程树信息，包括进程名，PID，所属用户，所属用户组，文件路径，文件执行权限，进程命令行等； |
| 合规基线 | 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。 |
| 主机隔离 | 客户端配置：实时监控网络连接，对不符合策略的访问产生告警，在列表中展示；相同告警聚合为同一条计数，并更新告警时间 |
| 微蜜罐 | 端口蜜罐：支持伪造任意系统端口，实时检测对设置蜜罐端口的尝试连接行为，并提供告警。监控已设置规则的端口，一旦尝试访问端口，即上报告警，其中端口应支持输入多个。 |
| 内存后门检测 | 内存webshell检测：支持实时检测在内存中加载网站恶意文件，无任何本地文件、恶意代码注入的检测。需要展示内存对应的类名、父类名、所属类加载器、内存对应大小、MD5信息等。 |
| 文件完整性 | 支持对文件的新增、修改、删除、权限变更等变化行为进行告警。 |
| 病毒查杀 | 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. |
| 产品资质 | 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |

#### 2.3 XC网络终端安全管理系统统一管理平台

本系统包含分级权限管理、系统监控管理、终端汇总管理、策略统一管理、日志审计管理、数据展示管理和系统报警管理共7个模块。具体技术规格参数如下：

| **指标项** | **技术指标** |
| --- | --- |
| 分级权限管理 | 分级分权限管理：采用三全分立，支持高院、分院两级管理模式分权。  1）后台支持配置管理员不同的管理范围权限和不同的功能权限；  2）市级法院系统管理员集中管理，可以集中管理所有区县法院机器情况、管理策略。区法院管理员分级自治，界面只显示在管理范围内的机器情况，管理策略等等。 |
| 系统监控管理 | 系统监控：各分院终端安全管理系统运行状态监控，异常状态报警及输出。  1）系统运行状态监控：监测终端安全管理系统运行是否正常，如异常则报警；  2）资源使用状态监控：监测终端安全管理系统CPU、内存、系统空间、备份空间，如超过80%则报警；  3）系统服务状态监控：监测终端安全管理系统服务运行状态，如异常则报警；  4）异常报警展示及输出：报警通过首页展示，采用SYSLOG及短信输出。 |
| 终端汇总管理 | 终端数据汇总：采集各分院终端信息，汇总统一报表。  1）采集各分院的终端基本信息，包括不限于IP、MAC、使用人、部门等，集中到统一管理平台汇总；  2）采集各分院的终端硬件信息，集中到统一管理平台汇总；  3）采集各分院的终端软件信息，集中到统一管理平台汇总；  4）采集各分院的终端的违规情况，集中到统一管理平台汇总。 |
| 策略统一管理 | 策略汇总：建立策略统一下发机制，高院对各分院进行统一策略下发。  1）支持以树状结构对部门信息进行层级展示；  2）支持策略执行结果的统一汇总；  3）支持策略告警的统一展示。 |
| 日志审计管理 | 审计汇总管理：对分院终端的文件操作行为进行审计汇总，包括但不限于以下操作如新建、修改、移动、改名、彻底删除、放入回收站、还原、清空；  1）支持汇总常用软件产生的文件变动行为审计；  2）支持汇总用户访问的网站进行审计记录，汇总各分院网站审计列表，包括：设备名称、远程IP、远程端口、域名、进程路径、标题、网址、设备IP；  3）汇总各分院终端系统上当前运行的进程及状态进行监控和审计；  4）汇总各分院终端用户的文档打印行为、光盘刻录行为用于审计、记录；  5）汇总各分院终端系统上相关服务及启用、停止等状态进行监控和审计；  6）汇总各分院终端系统上的共享目录进行监控和审计；  7）汇总各分院终端上的用户账户进行监控和审计；  8）汇总各分院终端上的开机启动项进行监控和审计，监控的内容包括启动项的添加、删除和修改等操作；  9）汇总各分院指定目录下的注册表项，监控的内容包括注册表项的添加、删除和修改等操作；  10）汇总各分院网络流量使用情况。 |
| 数据展示管理 | 整体展示管理：对于高院及下属各区县的终端统一管理要求，进行数据统一管理和分析  1）展示各分院违规情况，以地图形式在后台直观展示  2）违规地区以标志性亮点，显示违规情况，可以点击查看分院更多违规详情  3）对于高院及下属各区县分院之间实时链路、流量状况，以及终端在线率，终端设备合规率排行、安检项通过率、文档操作等报表信息通过投射大屏的方式进行实时、直观展现 |
| 系统报警管理 | 系统报警：多采用多种类型告警方式，以方便管理员快捷、及时、准确的了解每个终端以及平台自身的运行状况。  1）支持不同的类别的告警自动分级，便于管理员及时迅速的了解这些系统意外状况；  2）支持syslog输出报警；  3）支持EMAIL、手机短信等更为及时告警方式，以帮助管理员能够在第一时间发现问题。 |

#### 2.4 XC网络终端安全管理系统

| **指标项** | **技术指标** |
| --- | --- |
| ▲基础要求 | 1、产品具备主流系统和主流架构的兼容性互认资质，包括但不限于银河麒麟（飞腾版、鲲鹏版、龙芯版、兆芯版、海光版）和统信（飞腾版、鲲鹏版、龙芯版、兆芯版、海光版）（提供证明文件）  2、支持兼容现有终端管理系统客户端。（提供证明文件） |
| 硬件指标 | 产品CPU性能不低于龙芯3A3000（1.4GHz，4核）；  国产化操作系统，如中标麒麟 V7.0（服务器版）等  内存≥8GB；硬盘≥240GB；网络接口:不少于1个管理口、4个千兆电口和4个千兆光口；  设备为标准机架式设备。 |
| ▲准入技术 | 支持镜像准入技术，能通过浏览器完成身份认证、客户端安装、设备注册、安全检查、检查结果展现等全流程引导管理。（提供截图） |
| 日志记录 | 支持按事件类型、时间进行查询，查询结果以列表展示，包括时间、事件类型、描述、结果等。可按操作类型、时间、操作人，查询所有管理员的操作日志 |
| 策略管理 | 1、支持策略组的管理，以策略组的形式下发组策略。  2、支持策略执行时间范围控制。  3、支持已下发策略的启用、禁用。  4、支持安全策略部署情况查询，展示查询用户端的策略下发情况。  5、支持终端IP查询已下发策略，策略以列表形式展示 |
| 未关机统计 | 支持设置终端定时关机统计 |
| 终端信息查询 | 支持以设备为维度，展示设备名称、IP、MAC地址、所属用户、所属部门、是否安装客户端、设备是否在线、设备位置、操作系统版本、系统安装时间等； |
| 设备硬件信息 | 支持汇总终端硬件信息，包括但不限于硬盘信息、主板信息、CPU信息、内存信息等 |
| 支持以终端维度和硬件维度进行统计和导出。（提供截图） |
| 设备软件信息 | 支持汇总终端上安装的软件信息，包括但不限于操作系统名称、版本、安装时间和软件名称、版本、类型、厂商、安装日期 |
| 支持以终端维度和软件维度进行统计和导出。（提供截图） |
| 软件分发 | 支持RMP和DEP等格式的软件分发，并支持后台静默安装 |
| 支持针对终端、IP段、部门等模式的分发对象。 |
| ▲能够自动统计分发成功率及软件安装成功率，支持进程、安装路径等多种参数判断方式。（提供截图） |
| 支持根据操作系统不同分发不同升级包，提高软件分发功能对操作系统系统的适应性。（提供截图） |
| 软硬件变动记录 | 支持软硬件资产管理，可对软硬件资产变动提供报警 |
| 文件分发 | 支持分发指定文件到终端指定的文件夹中，并支持脚本的运行。 |
| 消息分发 | 支持向终端推送消息，并支持消息标题、内容、皮肤、关闭时间等配置。支持针对终端、IP段、部门等模式的分发对象。 |
| 在线状态监控 | 支持通过客户端代理对受控主机状态进行监控 |
| 终端资源监控 | 对终端上的CPU、内存、硬盘的使用情况进行实时监控 |
| 进程审计 | 支持对进程的开启、关闭行为进行记录 |
| 端口监控 | 支持对恶意端口进行及时关闭 |
| 打印审计 | 支持对打印行为进行记录，包括网络打印机和直连打印机 |
| 违规外联 | 支持对终端上出现的违规外联行为进行阻断和告警 |
| 文件审计 | 支持对终端上的文件操作行为进行记录，包括新建、复制、删除等 |
| 进程控制 | 支持对非法进程进行控制，及时关闭恶意进程 |
| 移动介质使用审计 | 支持对移动介质进行全流程管理管理，包括注册和审批，杜绝外部U盘未经审批接入内网终端 |
| USB接口控制 | 支持对USB接口的使用进行控制 |
| 授权管理 | 支持按终端点数进行授权计算，系统初始化时默认包含50个点的终端管控授权 |
| 资质要求 | 所投产品必须具备公安部《信息安全产品检测报告-内网主机检测》（提供证明文件） |
| 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。  国家版权局《计算机软件著作权登记证书》  国家保密局《涉密信息系统产品检测证书》 |

### 3、移动安全

#### 3.1移动终端安全管理平台

| **指标项** | **技术指标** |
| --- | --- |
| 移动设备管理要求 | 禁止使用摄像头/禁止发送短信/禁止使用WiFi网络/禁止开启WiFi网络/强制开启WiFi网络/禁止开启移动数据网络/强制开启移动数据网络/禁止使用外置存储（TF卡）/禁止开启网络共享热点/禁止使用系统原生浏览器/禁止使用麦克风/禁止修改系统时间和日期/禁止使用定位服务/禁止开启开发者选项、USB调试及数据传输/禁止使用蓝牙/禁止恢复出厂设置/禁止使用移动数据网络（2G/3G/4G）/禁止使用第二张SIM卡/禁止使用设备分身、应用分身、访客/禁止使用下拉通知栏/禁止使用APN设置/禁止截屏/禁止开启飞行模式/禁止使用设备备份/强制开启GPS/强制关闭GPS/禁止安装外部来源应用/禁止使用NFC/禁止MTP数据传输/禁止使用设备卡槽二/禁用侧边栏/禁止使用安全模式  黑白名单：应用黑白名单、WiFi黑白名单、蓝牙黑白名单、通讯黑白名单、上网黑白名单  配置项：锁屏密码、WiFi配置、APN配置、设备轨迹、安全工作区、客户端行为配置  支持时间围栏，可配置策略的生效时间、排除时间及时间段、支持保活唤醒  支持地理围栏，可配置策略生效的地理范围  支持电子围栏，通过扫码方式进入或离开围栏  支持WLAN围栏，可配置策略生效WLAN，支持配置WIFI SSID和MAC地址  支持对设备批量推送消息，同时消息支持上传附文本 |
| 移动应用管理要求 | 支持应用发布、包括Android原生应用、远程H5应用、本地H5应用。支持应用定时发布机制  支持后台同时多任务上传机制  支持应用上架/下架、删除、更新等维护管理  支持发布应用版本管理  支持应用基础信息配置、排序管理和分类管理  支持查看推荐应用和必装应用安装详情  支持应用DLP安全防护。针对不同用户分发不同的DLP策略，并对应用进行授权  支持应用分发例外范围设置，针对部分用户/部门/用户组不生效  支持应用强制升级  支持应用禁止个人桌面启动  支持设置推荐应用设置，推荐应用消息通知，安全空间自动添加图标。  支持设置必装应用设置，必装应用自动下载安装。  支持为应用开启/关闭消息推送通知  支持应用级零信任安全网关  支持第三方接口开放，应用管理、应用分发、默认策略配置和应用管理员设置  支持JS桥接、应用传参和sdk集成等方式为应用提供sso能力  支持应用分类管理，应用商店分类展示  支持设置应用默认策略模板，策略模板支持启用/禁用  支持配置容器化应用引导安装、登录客户端，支持提示语自定义 |
| 移动数据防泄露（沙箱）要求 | ▲支持配置应用数据安全：应用明/暗水印、截屏/录屏保护、复制粘贴保护、应用数据加密、安全文件、安全键盘、安全相机相册  支持配置应用行为保护：应用锁、应用调用安全、系统权限限制、应用运行安全、应用更新控制、应用无痕使用  支持配置设备环境保护：应用网络安全控制、允许环境保护 |
| 移动内容管理要求 | 支持查看、新建、编辑、删除文件夹  支持文件上传、重命名、移动、下载和删除  支持下发文件/文件夹到用户/部门/用户组  支持对文件有效期、文件分发通知、文件下载、文件自动下载进行设置  支持加密后的文件使用指定的Android封装后的应用打开  支持文档在阅读多长时间后，在本地删除文件  支持在根目录文件夹配置密码  支持以文件/文件夹关键字进行搜索  支持根据管理员根目录筛选查看文件 |
| 移动设备合规管理要求 | 支持Android设备出现系统版本过低时能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备SIM卡违规后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备被破解后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备SD卡变更后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备不在线时间超过一定时间后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备电量低于一定比例后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备可用存储空间低于一定比例后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备关闭移动数据网络（2G/3G/4G/5G）后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间，但仅针对高权限设备生效  支持Android设备开启飞行模式（2G/3G/4G/5G）后能够告警通知，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间，但仅针对高权限设备生效  支持Android设备MDM策略应该生效，但是未生效时能够告警，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间  支持Android设备要求安装应用未安装时能够告警，告警信息发送方式支持周期通知和实时通知。出现告警后，能够对违规设备进行实时或者定时处罚。处罚方式包括：锁定设备、擦除企业数据、恢复出厂、禁用应用商店、禁用摄像头、禁用SD卡、禁用使用工作空间 |
| 资质要求 | 成熟度：供应商提供的应用软件必须是先进、成熟、安全可靠的商业化软件产品，其技术路线和实现方式清晰，符合网络安全、移动信息化的发展趋势，可进行弹性扩展，强内聚松耦合，适应未来业务发展战略和方向。原厂商拥有自主知识产权，能够提供自主知识产权证书。 |
| 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |
| 提供原厂商质量提议体系ISO9001认证证书 |
| 提供原厂商信息技术服务管理体系ISO20000认证证书 |
| 提供原厂商信息安全管理体系ISO27001认证证书 |
| 提供原厂商信息安全服务资质认证证书（安全集成三级） |
| 为保障软件开发质量，要求厂商具有CMMI3级认证。 |
| 提供国家版权局颁发的《计算机软件著作权登记证书》。 |

#### 3.2零信任控制中心

| **指标项** | **技术指标** |
| --- | --- |
| 硬件要求 | 内存大小≥16G，硬盘容量≥480G SSD，电源：冗余电源，接口：6千兆电口+4千兆光口SFP+2万兆光口SFP+ |
| 性能要求 | 最大并发用户数（个）10000。 |
| 功能要求 | 采用国家密码管理局颁布的SM1、SM2、SM3、SM4密码算法及其协议，支持多种身份认证方式、访问权限控制等主要功能，保证远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全  包含加密传输、接入、认证、日志审计等功能。 |
| 资质要求 | 成熟度：供应商提供的应用软件必须是先进、成熟、安全可靠的商业化软件产品，其技术路线和实现方式清晰，符合网络安全、移动信息化的发展趋势，可进行弹性扩展，强内聚松耦合，适应未来业务发展战略和方向。原厂商拥有自主知识产权，能够提供自主知识产权证书。 |
| 提供原厂商质量提议体系ISO9001认证证书 |
| 提供原厂商信息技术服务管理体系ISO20000认证证书 |
| 提供原厂商信息安全管理体系ISO27001认证证书 |
| 提供原厂商信息安全服务资质认证证书（安全集成三级） |
| 为保障软件开发质量，要求厂商具有CMMI3级认证。 |
| 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |
| 提供国家版权局颁发的《计算机软件著作权登记证书》。 |

#### 3.3零信任网关

| **指标项** | **技术指标** |
| --- | --- |
| 硬件要求 | 内存大小≥32G，硬盘容量≥480G SSD，电源：冗余电源，接口：4千兆电口+4千兆光口SFP+4万兆光口SFP+。 |
| 性能要求 | 最大理论加密流量：2.1Gbps，最大理论并发用户数（个）：20000。 |
| 功能要求 | 采用国家密码管理局颁布的SM1、SM2、SM3、SM4密码算法及其协议，支持多种身份认证方式、访问权限控制等主要功能，保证远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全  负责建立、监视及切断零信任客户端和业务应用之间的隧道连接，并对经过代理网关转发的流量进行加密。支持三层、四层、七层等多种访问协议代理，可以满足多种类型应用的发布。 |
| ▲安全架构需符合CSA定义的SDP规范，采用客户端+控制器+网关的SDP安全架构，控制流和数据流分离。 |
| 支持移动端Android设备安全接入功能，可通过互联网安全访问内网业务系统。 |
| 使用SPA单包授权技术，仅通过认证的用户才能通过网关正常访问业务，减少互联网暴露面，降低恶意攻击和入侵风险 |
| SPA消息通过UDP协议敲门，控制器仅需开放一个UDP端口，避免开放TCP端口容易被扫描和攻击的问题。 |
| 支持移动端接入限制，例如单设备绑定：用户仅登录绑定一个移动端/PC端设备；自动踢除：用户新登录移动端/PC端设备踢除上一个设备下线 |
| 当登录的设备不是上次使用的设备时，需使用短信验证码等方式进行身份二次认证 |
| 支持应用级接入，仅允许终端的上的指定APP通过SDP隧道访问业务服务，且认证阶段是采用的是临时密钥机制 |
| 可根据用户状态、时间、位置、网络、设备类型、IP地址等信息综合评估定义访问权限，根据评估结果可基于虚拟组、组织架构、用户做最小化授权。 |
| 对访客等外部用户，可以设置临时访问的时间段，如配置6月1日～6月3日期间可以访问，到期权限自动失效。 |
| 即使网关处于连接状态，但不访问数据时，隧道自身应不占用带宽、处理器等资源。 |
| 为了保证spa的兼容性，不能在网络协议中附加option字段，如ip option、tcp option等，需保证敲门信息不被防火墙、路由器等设备过滤掉。 |
| 支持异常和攻击行为的IP统一展示和管理，可查看IP的攻击行为记录，可对IP进行解锁管理 |
| 高性能隧道：SDP隧道处于连接状态，但不访问数据时，隧道自身应不占用带宽、处理器等资源 |
| 多类型业务系统支持：支持发布TCP及UDP协议的资源，包括但不限于HTTP/HTTPS、FTP、TELNET、RDP、SMTP/POP3邮箱等，支持各类B/S、C/S架构应用通过安全隧道访问业务应用 |
| 针对风险接入可以追加二次验证，风险接入包括：新设备登录、非常用的登录、非指定IP的登录、非连续性登录、非指定时间登录等 |
| 支持在同一后台管理多地数据中心的网关，并支持多地网关工作状态的直观展示 |
| 支持指定网关接入功能，在控制器集群部署或异地部署的情况下，支持为不同控制器分配不同的网关。 |
| 平台需支持多种域名解析方式，支持自带私有域名解析、通过第三方DNS解析以及混合使用场景。 |
| 安全隧道支持将客户端的虚拟IP透传给业务系统，业务系统可以使用虚拟IP进行溯源和审计 |
| 即使网关处于连接状态，但不访问数据时，隧道自身应不占用带宽、处理器等资源 |
| 展示SDP系统攻击、接入、流量的统计和分析信息，动态显示攻击走向和流量走向 |
| 通信隧道密钥加密采用高安全的加密算法，临时密钥机制，周期性更新认证/隧道临时密钥，保证通信密钥的安全性。报文使用临时密钥签名，无法在传输过程篡改，数据检验有误将丢弃异常的数据包，也避免防重放攻击。 |
| 支持私有化域名解析，无需配置互联网域名解析的前提下，可为内网用户提供私有化域名解析访问内网应用，不改变用户之前的使用习惯。 |
| 支持管理员密码复杂度设置、管理页面会话有效期设置、管理后台接入白名单等，保证管理后台的安全性。 |
| 可提供安全接入和移动应用安全防护SDK包并做集成 |
| 资质要求 | 成熟度：供应商提供的应用软件必须是先进、成熟、安全可靠的商业化软件产品，其技术路线和实现方式清晰，符合网络安全、移动信息化的发展趋势，可进行弹性扩展，强内聚松耦合，适应未来业务发展战略和方向。原厂商拥有自主知识产权，能够提供自主知识产权证书。 |
| 提供原厂商质量提议体系ISO9001认证证书 |
| 提供原厂商信息技术服务管理体系ISO20000认证证书 |
| 提供原厂商信息安全管理体系ISO27001认证证书 |
| 提供原厂商信息安全服务资质认证证书（安全集成三级） |
| 为保障软件开发质量，要求厂商具有CMMI3级认证。 |
| 产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |
| 提供国家版权局颁发的《计算机软件著作权登记证书》。 |

#### 3.4 IPSec VPN网关

| **指标项** | **技术指标** |
| --- | --- |
| 硬件与性能要求 | 硬件参数：产品不少于4个千兆电口，4个千兆光口，4个万兆光口；规格：内存≥16G，硬盘容量≥128GB SSD，冗余电源。  网络层吞吐量≥40 Gbps，应用层吞吐量≥30Gbps，并发连接数≥4000万，每秒新建连接数≥23万，IPSEC吞吐量≥2 Gbps。 |
| 链路状态探测 | 产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。 |
| 功能要求 | 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。 |
| 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等。 |
| 产品支持多对一、一对多和一对一等多种地址转换方式。 |
| 产品支持NAT44 、NAT64、NAT66地址转换方式。 |
| 支持NAT穿透技术ALG，支持FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323等协议。 |
| 产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 产品支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制 |
| ▲为满足组网兼容性，IPSec VPN需支持信息安全技术 IPSec VPN技术规范（GB/T 36968-2018 ），IKEv1和IKEv2协议，支持基于主模式和野蛮模式建立加密隧道，支持国密算法SM2-SM4。 |
| 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。 |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 安全策略管理 | 产品支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |
| 产品资质 | 提供《计算机信息系统安全专用产品销售许可证》，《商用密码产品认证证书》 |

#### 3.5服务调用交换平台

| **指标项** | **技术指标** |
| --- | --- |
| 产品架构 | 双主机架构，包含可信端和非可信端；搭配隔离交换产品，承载数据处理平面相关工作，隔离交换产品承载数据转发平台相关工作 |
| 网络接口 | 产品应具备≥6个千兆电口；2个扩展卡槽； |
| 硬件规格 | 产品应为标准机架式设备，冗余电源； |
| 系统管理 | 具备多种认证方式：支持用户名/口令、Radius、LDAP、密码+证书、密码+U-key认证； |
| 产品应支持管理员账户密码可灵活设置密码长度，密码强度，同时可制定哪些特殊字符可以包含在密码中 |
| 支持带内管理，具备web、SSH方式，同时可直接在系统选择带内管理IP地址以及端口 |
| 便捷运维 | 支持配置管理，能够对单独模块及全部模块配置进行配置的导入导出； |
| 产品应具备配置智能备份功能，可灵活设置备份周期、备份个数，当配置无变化时，不进行重复备份 |
| 产品应具备可视化流量监控，可直观展现数据交换平台接口秒级业务流量情况，同时可灵活查看最近7天内历史流量情况 |
| 文件交换 | 产品支持无客户端模式，有客户端模式，服务端模式； |
| 文件同步支持FTP、SFTP、SMB、NFS等协议，同时可设置服务器加密方式，服务器编码方式等； |
| 文件交换可灵活设置文件传输方向，工作模式支持源端移动、源端删除、增量更新、完全复制等多种模式； |
| 支持文件重构技术，可自动剔除文件中夹带的危险程序，可执行代码等； |
| 产品支持重名策略，支持对重名文件的控制策略； |
| 产品应具备文件断点续传，同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源 |
| 数据库同步 | 数据库同步支持无客户端方式同步； |
| 产品应支持无客户端方式同步由数据交换平台主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件，可以在数据交换平台系统上完成数据库同步配置）(提供证明截图) |
| 产品应支持数据库同步可指定资源使用情况，按任务优先级进行资源分配，可灵活设置一个或一组任务所使用最小内存、最大内容等资源情况（提供功能截图） |
| 支持数据库同步线程数配置，提升数据库同步性能； |
| 邮件访问 | 所投产品应支持邮件发送地址策略、接受地址策略、关键字过滤、主题内容过滤； |
| 所投产品应支持对附件及其附件类型进行过滤控制，邮件内容过滤、文档重建、病毒过滤； |
| 数据库访问 | 支持数据库访问用户名过滤、数据库名、表控制等策略 |
| 支持数据库命令控制，可对数据库语句进行过滤； |
| 产品应支持数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤 |
| 产品应支持数据通道配置，任务运行时间控制； |
| 安全FTP | 产品应支持安全FTP支持最大并发连接数、单个IP最大并发数设置，灵活限制数据通道是否在1024以下端口使用 |
| 产品应支持安全FTP模块支持病毒扫描文件大小限制、文件类型大小限制、关键字过滤文件大小限制 |
| TCP/UDP访问 | 所投产品应支持TCP、UDP业务数据统计，可按照秒、分钟展示发送速率、接受速率、连接数，并且可按照图表进行展示； |
| 安全浏览 | 产品应支持安全浏览支持域名控制、源端控制、URL过滤、命令过滤、文件大小限制、用户认证 |
| 产品应支持安全浏览支持用户认证配置，具备本地认证、LDAP认证、RADUIUS认证 |
| 日志审计 | 产品应支持FTP、SFTP、SMB、NFS等协议进行日志导出到指定服务器目录下 |
| 产品应支持安全审计能力，可通过自定义时间、任务名称 、文件名称、文件类型、文件大小类型、源目的文件路径、源目IP等详细字段追溯业务数据流向，可自定义配置查询条件，查询条件策略可以自定义设置； |
| 告警中心 | 持按照功能模块，灵活开启告警功能，支持邮件告警、日志告警、SNMP等告警方式； |
| 支持多种告警类型：病毒告警、攻击告警、硬件异常、系统异常、资源异常、配置变化、日志告警，支持状态日志配置； |
| 病毒防护 | 产品应支持云查杀模式，可联动云端文件鉴定中心，预判文件安全风险，防止恶意文件通过数据交换平台进入内网，提供高中低不同级别阻断策略； |
| 兼容性 | ▲与现有隔离交换平台中服务调用产品（奇安信网神品牌）相兼容，可以互换部署和使用。（需提供设备原厂承诺，并加盖原厂公章） |

#### 3.6单向光闸

| **指标项** | **技术指标** |
| --- | --- |
| 产品架构 | 采用2+1模式，即系统由A网主机模块、B网主机模块和交换模块组成； |
| 设备性能 | 系统吞吐量≥5Gbps； |
| 网络接口 | 内网侧标配千兆电口≥4个，千兆光口≥4个，接口板卡扩展插槽≥2个；外网侧标配千兆电口≥4个，千兆光口≥4个，接口板卡扩展插槽≥2个； |
| 硬件规格 | 产品应为标准机架式设备，冗余电源； |
| 适配平台 | 支持信创CPU芯片和操作系统； |
| 文件导入 | 支持内嵌模式、客户端模式、服务端模式文件导入； |
| 支持无客户端模式，不需要安装任何客户端软件；无客户端模式下，支持FTP、SMB、NFS、SFTP方式的文件单向导入； |
| 支持多种同步模式： 源端移动、源端删除、源端保留等模式； |
| 支持服务器数据传输编码形式； |
| 支持客户端服务模式，当服务器异常重启，客户端可自行启动，无需人员干预； |
| 支持病毒检测功能，支持通过文件大小控制病毒查杀；支持文件名及后缀名过滤，同时支持文件类型识别过滤，即不基于后缀名的过滤； |
| 支持文件安全策略细分到任务，可按需配置全局策略或细分任务策略； |
| 数据库导入 | 支持Oracle、SQL Server、人大金仓、达梦等主流国产数据库同步； |
| 支持无客户端多种部署方式实现数据库同步，同步由网闸主动发起并完成，不需要第三方软件支持； |
| 支持一对一、一对多、多对一数据库同步，支持设定同步时间和同步周期； |
| 支持两台单向设备实现数据库的双向同步； |
| 支持数据库同步进度监控，支持数据库连接状态检测； |
| 邮件导入 | 支持发件人、收件人过滤、邮件主题过滤、邮件正文过滤、附件类型过滤、邮件传输大小设置； |
| 支持黑、白名单邮件导入控制； |
| 支持每秒最大并发数、每秒新建连接数、单链接最大吞吐量、每秒最大吞吐量设置； |
| 分发访问 | 支持两台单向设备实现标准TCP访问，由光闸自身完成，不需要第三方软件或服务器支持； |
| 单向TCP | 支持单向TCP定制服务； |
| 支持源地址绑定、网络接口地址绑定功能；支持源地址、源端口、目的地址、目的端口过滤功能； |
| 单向UDP | 支持单向UDP定制服务； |
| 支持源地址绑定、网络接口地址绑定功能；支持源地址、源端口、目的地址、目的端口过滤功能； |
| 单向JMS | 支持JAVA平台上的信息单向通信，支持JMS监听队列配置； |
| 单向探针 | 支持KAFKA、ZMQ方式发送、接收消息； |
| 防护设置 | 支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎； |
| 支持抗Dos攻击功能设置； |
| 安全管理 | 支持内、外网分别具有独立的管理接口，而不是通过内/外网一个管理接口完成全部管理； |
| 支持基于https的图形化安全管理；支持用户名/密码+U-KEY、用户名/密码+数字证书等双因子认证方式； |
| 支持带内管理，可通过业务口进行管理工作；用户可自行选择是否启用带内管理功能； |
| 支持跨网段管理，实现管理终端IP地址和端口的访问控制；管理员及审计员区分并独立，支持分权管理；具有独立审计用户，提供完善的日志审计功能 |
| 运维管理 | 支持设备运行状态检测、系统资源监控；支持通过界面能够查看到多核CPU使用率，进行设备的远程关闭及重启功能； |
| 支持提供调制工具，包括trace、ping、telnet、arp等 |
| 集中监控 | 支持集中监管平台，可对多台光闸进行统一监控，记录每台设备的系统资源运行情况； |
| 兼容性 | ▲与现有隔离交换平台中的单向光闸产品（奇安信网神品牌）相兼容，可以互换部署和使用。（需提供设备原厂承诺，并加盖原厂公章） |

### 4、运维终端数据防泄漏

#### 4.1互联网数据防泄露

本系统包含控制台和客户端两部分。控制台是系统的管理中心，进行安全策略设置、事件管理、用户、日志等管理；客户端功能包含发现、识别、监控终端中的敏感数据，对终端数据资产分布、终端敏感数据的违规存储进行展现；对终端敏感数据的违规使用、扩散等敏感行为进行策略响应控制。

产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。

控制台和客户端的技术规格参数分别如下：

##### 4.1.1控制台技术规格参数

| **配置要求** | **技术规范** |
| --- | --- |
| 安全策略设置 | 具有统一、可视化的管理平台 |
| 系统支持中英文界面，根据登录用户的设置自动进行显示 |
| 通过 DLP 内容检测，实现分类分级的落地执行和数据流动的可追溯性 |
| 支持正则表达式检测内容。要求应提供常见的正则表达式，如手机号码、固话号码、姓名、地址等 |
| 支持脚本方式定义，预置身份证、信用卡等常用脚本检测数据 |
| 支持对常用文件系统进行非结构化指纹、支持对常用数据库系统进行结构化指纹 |
| 支持对有规范的模板类文件进行智能学习定义 |
| 支持文件格式识别支持（pdf，office 文件，压缩文件，图片文件，加壳文件等），并提供具体可识别文件类型列表 |
| 支持数据自动标签功能，对 URL 站点下载到本地的文件内容自动标记，可基于文件类型，关键字词等不同规则自动标签，针对包含关键词或带标签的文件 DLP 可以审计/阻断 |
| 支持数据分级分类定义，可策略调用 |
| 支持数据聚类功能，辅助数据梳理和策略定义 |
| 支持识别多种图像格式文档中的敏感信息 |
| 系统预置多种模板，如：政治言论、高管信息、非法言论、技术方案、会议纪要、采购计划、网络安全、投资信息、GDPR、简历等 |
| 事件管理 | 提供预置及定制趋势分析的报告，包括：支持显示一周内的事件趋势图、支持显示安全等级事件趋势图、支持显示策略事件趋势图、来源事件 TOPN、目标事件 TOPN、来源总匹配 TOP20 |
| 能够设置定制报告模板的样式及条件 |
| 支持定制数据统计分析，如多种 TOP 排名能力（可定制）的报表展示能力 |
| 支持多种报告模板，详见各模块报告功能参数 |
| 提供设置定时事件报告发送给特定的管理人员 |
| 可定制的图表报告，用直观的图表同时显示多个报告，至少提供 10 个图表。可点击报告，向下展开额外的事件细节。 |
| 产品监控的数据均可以按照每小时、每天、每周显示，并均可以下载或导出至 PDF 和 XLS 文件 |
| 系统邮件记录的统计、分析、报表等支持 IPv6 相关的内容输出 |
| 用户管理 | 支持通过管理平台后台配置启用三权分立，提供多权分立角色管理，各角色之间的功能没有交叉，每一种角色类型都有预置的管理员，包括系统管理员、事件管理员、审计管理员、安全管理员等 |
| 支持基于实际需要的权限分配，结合用户分组和分级进行灵活定义 |
| 支持定期及手动方式从第三方同步用户信息 |
| 支持集成的第三方系统：AD、Generic Ldap、Domino、ADAM、CSV |
| 支持用户目录设置高级对应同步，同时也支持过滤用户属性同步 |
| 支持自定义组织架构及导入导出功能，包括自定义用户、用户主管、部门、部门主管、计算机组织架构信息 |
| 支持基于用户目录及自定义组织架构定义用户目录组，实现已有系统用户信息及自定义用户的重新分组，用于策略通知、事件审批及告警通知 |
| 分级对象应支持三级管理，上级可管理本级和下级用户的日志、策略以及设备 |
| 可根据分级架构，为不同分支机构管理员实现不同的角色权限控制 |
| 支持继承上级对象的用户管理范围，此种方式下，下级与上级对象管理的用户事件日志范围一致 |
| 支持指定用户范围的分级管理，可根据组织架构或者自定义用户组，对事件日志进行用户分级管理 |
| 支持指定设备的用户分级管理，即只要该用户通过该设备即可管理该用户产生的事件日志信息 |
| 产品应支持不同分支机构具备管理自己分支设备权限，上级机构可查看管理下级设备，下级只能对上级分配的设备进行监控管理 |
| 产品应支持根据分级对象设置不同分级的策略，上级策略对下级策略生效，也可根据策略优先级设置上级策略对下级生效的优先程度 |
| 产品应支持上级查看管理本级和下级策略，同时下级也能查看上级策略 |
| 产品应支持根据用户分级架构，不同分级管理员查看管理各自分级的事件日志和报告 |
| 日志管理 | 能够以 SNMP 的方式向外部系统实时对接设别信息，支持主动和被动方式，支持 TCP 和 UDP 连接 |
| 能够向第三方日志系统实时传输后台日志，包括但不限于：系统日志、网络日志、审计日志、邮件日志、风险事件。 |
| 其他功能 | 在线下载或上传升级包进行升级，升级失败自动回退 |
| 升级成功以后可以进行版本回退 |
| 在线检查最新补丁，在线下载或上传补丁包打补丁 |
| ▲数据防泄露系统需支持国产化硬件环境，软件产品为国内自主研发，符合国家自主可控要求 |
| ▲数据防泄露系统须覆盖终端、网络和邮件通道数据泄漏的审计和阻止功能，统一集中管理平台要求，进行策略、日志报告等统一管理 |
| 产品品牌要求国际主流机构（Gartner）连续 3 年推荐 DLP 厂商、数据与分析机构（IDC）连续多年 2 年数据防泄漏市场份额 TOP3，并具备中国本地原厂技术服务研发能力 |
| 投标方持有制造商出具的项目授权函及售后服务承诺函 |
| 终端 DLP 支持windows操作系统，支持DLP 检测和阻止功能。  支持 Ubuntu、麒麟（中标&银河）及 UOS 通信平台等操作系统，支持DLP 检测和阻止功能 |
| 与使用的终端安全产品兼容（桌管及防病毒等），在不影响现有终端管理的模式下，实现终端数据防泄密的管理需求。 |
| 产品必须支持 6 个月本地日志存量 |

##### 4.1.2客户端技术规格参数

| **配置要求** | **技术规范** |
| --- | --- |
| 敏感数据发现与识别 | 支持终端敏感内容发现。 |
| 支持终端发现任务计划定期扫描，支持增量与全量扫描 |
| 支持终端离线时所有终端 DLP 防护策略依然有效  （离线可控） |
| 支持用户端分级分类标签定义功能，支持终端 DLP 用户手动方式右键属性标记分类标签，支持终端 DLP 用户手动方式右键属性标记指纹标签 |
| 支持终端日志多种多种收集途径：本地手动收集、管理平台在线自动收集 |
| 支持终端发现任务计划定期、增量扫描与全量扫描  支持终端发现指定计算机、指定扫描目标、指定策略、文件属性过滤器、扫描时间计划、增量扫描、手动数据发现、手动数据发现报告 |
| 敏感数据分布及展示 | 提供预置及定制趋势分析的报告，包括：支持显示一周内的事件趋势 图、支持显示安全等级事件趋势图、支持显示策略事件趋势图、来源事件 TOPN、目标事件 TOPN、来源总匹配 TOP20 |
| 能够设置定制报告模板的样式及条件 |
| 支持定制数据统计分析，如多种 TOP 排名能力（可定制）的报表展示能力 |
| 支持多种报告模板，详见各模块报告功能参数 |
| 提供设置定时事件报告发送给特定的管理人员 |
| 可定制的图表报告，用直观的图表同时显示多个报告，至少提供 10 个图表。可点击报告，向下展开额外的事件细节。 |
| 产品监控的数据均可以按照每小时、每天、每周显示，并均可以下载或导出至 PDF 和 XLS 文件 |
| 系统邮件记录的统计、分析、报表等支持 IPv6 相关的内容输出 |
| 用户管理敏感数据监控及违规使用控制 | 支持终端应用控制，粘贴复制，截屏、文件访问控制 |
| 支持屏幕水印，应用水印，打印水印。 |
| 支持终端 DLP 用户在保存未分类 Office 文档时，强制弹处分类弹窗标记文档（属性标签） |
| 支持对打印的文件进行内容分析，并支持放行、阻断、确认动作 |
| 支持信创环境屏幕水印支持屏幕水印 |
| 支持基于源/目标 IP、源/目标 IP 段、域名、域名通配符、发件人、发件人邮箱通配符、路径的终端白名单设置 |
| 敏感数据防扩散 | 支持终端协议（如HTTP、HTTPS、FTP、SMTP、SMB）内容审计和阻断 |
| 支持终端通道（应用程序、USB 存储、蓝牙、光盘、打印、截屏等）管理、审计和阻断 |
| 支持在终端离开办公网络的环境下可以控制终端访问特定的 Web 网站类别 |
| 支持安全 URL 过滤功能，恶意 URL 识别率超过 95% |
| 支持终端部署在 VDI 系统，并审计 VDI 系统里的数据流转 |
| 支持 IM 应用的消息和文件内容审计和阻断,及证据截屏 |
| 支持 Ubuntu、NeoKylin 7 、UOS （X86\_64 & ARM64）、KylinV10 SP1  （ X86\_64 & ARM64 & la64）等信创操作系统。 |
| 支持企业级深度内容识别技术，对外发文档做敏感内容检测和阻断 |
| 支持 信创终端上 HTTP/HTTPS/FTP/SMB/NFS/SAMBA/WEBDAV 等网络数据传输控制，必须可以对敏感数据的外发进行阻断 |
| 支持应用程序管理（剪切板/文件访问/截屏/应用程序水印）审计和阻断 |
| 其他功能 | 支持 32/64bit Windows XP/7/8/10/11、Windows server2003 R2 至 Windows Server2022 主流操作系统终端 DLP 部署 |
| 支持信创环境麒麟、统信等主流操作系统 |
| 支持终端 CPU 占用、带宽、日志存储大小控制，避免过度占用操作系统主机资源 |
| 终端服务器支持分布式管理 |
| 支持终端卸载密码保护控制，密码校验正确才可以卸载。包括全局密码和临时密码 |
| 支持管理端远程在线卸载与禁用 |
| 支持终端邮件 SMTP、内外部邮件域功能设置 |

#### 4.2法院专网数据防泄露

本系统包含控制台和客户端两部分。控制台是系统的管理中心，进行安全策略设置、事件管理、用户、日志等管理；客户端功能包含发现、识别、监控终端中的敏感数据，对终端数据资产分布、终端敏感数据的违规存储进行展现；对终端敏感数据的违规使用、扩散等敏感行为进行策略响应控制。

产品若是列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应至少符合以下条件之一，方可提供：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。

控制台和客户端的技术规格参数分别如下：

##### 4.2.1控制台技术规格参数

| **配置要求** | **技术规范** |
| --- | --- |
| 安全策略设置 | 具有统一、可视化的管理平台 |
| 系统支持中英文界面，根据登录用户的设置自动进行显示 |
| 通过 DLP 内容检测，实现分类分级的落地执行和数据流动的可追溯性 |
| 支持正则表达式检测内容。要求应提供常见的正则表达式，如手机号码、固话号码、姓名、地址等 |
| 支持脚本方式定义，预置身份证、信用卡等常用脚本检测数据 |
| 支持对常用文件系统进行非结构化指纹、支持对常用数据库系统进行结构化指纹 |
| 支持对有规范的模板类文件进行智能学习定义 |
| 支持文件格式识别支持（pdf，office 文件，压缩文件，图片文件，加壳文件等），并提供具体可识别文件类型列表 |
| 支持数据自动标签功能，对 URL 站点下载到本地的文件内容自动标记，可基于文件类型，关键字词等不同规则自动标签，针对包含关键词或带标签的文件 DLP 可以审计/阻断 |
| 支持数据分级分类定义，可策略调用 |
| 支持数据聚类功能，辅助数据梳理和策略定义 |
| 支持识别多种图像格式文档中的敏感信息 |
| 系统预置多种模板，如：政治言论、高管信息、非法言 论、技术方案、会议纪要、采购计划、网络安全、投资信息、GDPR、简历等 |
| 事件管理 | 提供预置及定制趋势分析的报告，包括：支持显示一周内的事件趋势 图、支持显示安全等级事件趋势图、支持显示策略事件趋势图、来源事件 TOPN、目标事件 TOPN、来源总匹配 TOP20 |
| 能够设置定制报告模板的样式及条件 |
| 支持定制数据统计分析，如多种 TOP 排名能力（可定制）的报表展示能力 |
| 支持多种报告模板，详见各模块报告功能参数 |
| 提供设置定时事件报告发送给特定的管理人员 |
| 可定制的图表报告，用直观的图表同时显示多个报告，至少提供 10 个图表。可点击报告，向下展开额外的事件细节。 |
| 产品监控的数据均可以按照每小时、每天、每周显示，并均可以下载或导出至 PDF 和 XLS 文件 |
| 系统邮件记录的统计、分析、报表等支持 IPv6 相关的内容输出 |
| 用户管理 | 支持通过管理平台后台配置启用三权分立，提供多权分立角色管理，各角色之间的功能没有交叉，每一种角色类型都有预置的管理员，包括系统管理员、事件管理员、审计管理员、安全管理员等 |
| 支持基于实际需要的权限分配，结合用户分组和分级进行灵活定义 |
| 支持定期及手动方式从第三方同步用户信息 |
| 支持集成的第三方系统：AD、Generic Ldap、Domino、ADAM、CSV |
| 支持用户目录设置高级对应同步，同时也支持过滤用户属性同步 |
| 支持自定义组织架构及导入导出功能，包括自定义用户、用户主管、部门、部门主管、计算机组织架构信息 |
| 支持基于用户目录及自定义组织架构定义用户目录组，实现已有系统用户信息及自定义用户的重新分组，用于策略通知、事件审批及告警通知 |
| 分级对象应支持三级管理，上级可管理本级和下级用户的日志、策略以及设备 |
| 可根据分级架构，为不同分支机构管理员实现不同的角色权限控制 |
| 支持继承上级对象的用户管理范围，此种方式下，下级与上级对象管理的用户事件日志范围一致 |
| 支持指定用户范围的分级管理，可根据组织架构或者自定义用户组，对事件日志进行用户分级管理 |
| 支持指定设备的用户分级管理，即只要该用户通过该设备即可管理该用户产生的事件日志信息 |
| 产品应支持不同分支机构具备管理自己分支设备权限，上级机构可查看管理下级设备，下级只能对上级分配的设备进行监控管理 |
| 产品应支持根据分级对象设置不同分级的策略，上级策略对下级策略生效，也可根据策略优先级设置上级策略对下级生效的优先程度 |
| 产品应支持上级查看管理本级和下级策略，同时下级也能查看上级策略 |
| 产品应支持根据用户分级架构，不同分级管理员查看管理各自分级的事件日志和报告 |
| 日志管理 | 能够以 SNMP 的方式向外部系统实时对接设别信息，支持主动和被动方式，支持 TCP 和 UDP 连接 |
| 能够向第三方日志系统实时传输后台日志，包括但不限于：系统日志、网络日志、审计日志、邮件日志、风险事件。 |
| 其他功能 | 在线下载或上传升级包进行升级，升级失败自动回退 |
| 升级成功以后可以进行版本回退 |
| 在线检查最新补丁，在线下载或上传补丁包打补丁 |
| ▲数据防泄露系统需支持国产化硬件环境，软件产品为国内自主研发，符合国家自主可控要求 |
| ▲数据防泄露系统须覆盖终端、网络和邮件通道数据泄漏的审计和阻止功能，统一集中管理平台要求，进行策略、日志报告等统一管理 |
| 产品品牌要求国际主流机构（Gartner）连续 3 年推荐 DLP 厂商、数据与分析机构（IDC）连续多年 2 年数据防泄漏市场份额 TOP3，并具备中国本地原厂技术服务研发能力 |
| 投标方持有制造商出具的项目授权函及售后服务承诺函 |
| 终端 DLP 支持windows操作系统，支持DLP 检测和阻止功能。  支持 Ubuntu、麒麟（中标&银河）及 UOS 通信平台等操作系统，支持DLP 检测和阻止功能 |
| 与使用的终端安全产品兼容（桌管及防病毒等），在不影响现有终端管理的模式下，实现终端数据防泄密的管理需求。 |
| 产品必须支持 6 个月本地日志存量 |

##### 4.2.2客户端技术规格参数

| **配置要求** | **技术规范** |
| --- | --- |
| 敏感数据发现与识别 | 支持终端敏感内容发现。 |
| 支持终端发现任务计划定期扫描，支持增量与全量扫描 |
| 支持终端离线时所有终端 DLP 防护策略依然有效  （离线可控） |
| 支持用户端分级分类标签定义功能，支持终端 DLP 用户手动方式右键属性标记分类标签，支持终端 DLP 用户手动方式右键属性标记指纹标签 |
| 支持终端日志多种多种收集途径：本地手动收集、管理平台在线自动收集 |
| 支持终端发现任务计划定期、增量扫描与全量扫描  支持终端发现指定计算机、指定扫描目标、指定策略、文件属性过滤器、扫描时间计划、增量扫描、手动数据发现、手动数据发现报告 |
| 敏感数据分布及展示 | 提供预置及定制趋势分析的报告，包括：支持显示一周内的事件趋势 图、支持显示安全等级事件趋势图、支持显示策略事件趋势图、来源事件 TOPN、目标事件 TOPN、来源总匹配 TOP20 |
| 能够设置定制报告模板的样式及条件 |
| 支持定制数据统计分析，如多种 TOP 排名能力（可定制）的报表展示能力 |
| 支持多种报告模板，详见各模块报告功能参数 |
| 提供设置定时事件报告发送给特定的管理人员 |
| 可定制的图表报告，用直观的图表同时显示多个报告，至少提供 10 个图表。可点击报告，向下展开额外的事件细节。 |
| 产品监控的数据均可以按照每小时、每天、每周显示，并均可以下载或导出至 PDF 和 XLS 文件 |
| 系统邮件记录的统计、分析、报表等支持 IPv6 相关的内容输出 |
| 用户管理敏感数据监控及违规使用控制 | 支持终端应用控制，粘贴复制，截屏、文件访问控制 |
| 支持屏幕水印，应用水印，打印水印。 |
| 支持终端 DLP 用户在保存未分类 Office 文档时，强制弹处分类弹窗标记文档（属性标签） |
| 支持对打印的文件进行内容分析，并支持放行、阻断、确认动作 |
| 支持 信创环境屏幕水印支持屏幕水印 |
| 支持基于源/目标 IP、源/目标 IP 段、域名、域名通配符、发件人、发件人邮箱通配符、路径的终端白名单设置 |
| 敏感数据防扩散 | 支持终端协议（如HTTP、HTTPS、FTP、SMTP、SMB）内容审计和阻断 |
| 支持终端通道（应用程序、USB 存储、蓝牙、光盘、打印、截屏等）管理、审计和阻断 |
| 支持在终端离开办公网络的环境下可以控制终端访问特定的 Web 网站类别 |
| 支持安全 URL 过滤功能，恶意 URL 识别率超过 95% |
| 支持终端部署在 VDI 系统，并审计 VDI 系统里的数据流转 |
| 支持 IM 应用的消息和文件内容审计和阻断,及证据截屏 |
| 支持 Ubuntu、NeoKylin 7 、UOS （X86\_64 & ARM64）、KylinV10 SP1  （ X86\_64 & ARM64 & la64）等信创操作系统。 |
| 支持企业级深度内容识别技术，对外发文档做敏感内容检测和阻断 |
| 支持 信创终端上 HTTP/HTTPS/FTP/SMB/NFS/SAMBA/WEBDAV 等网络数据传输控制，必须可以对敏感数据的外发进行阻断 |
| 支持应用程序管理（剪切板/文件访问/截屏/应用程序水印）审计和阻断 |
| 其他功能 | 支持 32/64bit Windows XP/7/8/10/11、Windows server2003 R2 至 Windows Server2022 主流操作系统终端 DLP 部署 |
| 支持信创环境麒麟、统信等主流操作系统 |
| 支持终端 CPU 占用、带宽、日志存储大小控制，避免过度占用操作系统主机资源 |
| 终端服务器支持分布式管理 |
| 支持终端卸载密码保护控制，密码校验正确才可以卸载。包括全局密码和临时密码 |
| 支持管理端远程在线卸载与禁用 |
| 支持终端邮件 SMTP、内外部邮件域功能设置 |

# 电子政务云资源需求

根据项目前期资源现状，本次建设根据估算拟向电子政务云申请24台服务器资源CPU228核 、内存656G、存储88.5T，其中虚拟机24台，物理机0台。

申请国产化操作系统10套、国产化应用中间件服务器软件3套、国产化数据库软件7套。

# 其他工作要求

## 售后服务要求

本项目从系统验收通过之日起3年内提供7\*24小时免费技术支持和售后服务，3年后进入有偿维护期。

在质量保证期内，供应商将按照售后服务的承诺提供保修和运行维护服务，如果厂商对信息系统中软、硬件设备等产品中的部分保修期超过上述期限的，则按照厂商的规定进行免费保修。

在质量保证期内，供应商负责信息系统的运行维护工作，确保信息系统安全、稳定、可靠地运行。本项目涉及的运行维护工作范围为：

（1）本项目要求提供项目整体（含所有软硬件）自竣工验收之日起不少于3年的质保期；

（2）提供所有软件的三年免费服务，包括软件升级、电话技术支持；

（3）提供2人每周5天、每天9小时驻场运维服务，负责安全平台监测及安全事件响应；服务地点：上海市高级人民法院

（4）各投标单位在方案中应针对项目的特点制定的质保期承诺和售后服务承诺及措施、突发情况下的应急措施和承诺、人员培训计划、备品备件的供应计划等。

（5）质保期内需根据甲方要求提供全年重大敏感时期及节假日保障服务，重大保障工作期间，提供临时增加巡检、增加运行监测、系统加固、策略优化、值守保障等服务，并在紧急安全事件发生时提供应急响应支持。

投标方需具有按等级保护要求开展安全运维的能力。

## 应急响应要求

供应商对系统故障应能够实时响应，若系统发生故障，接到通知后15分钟之内响应，专业工程师半小时内到达现场。特殊故障与客户沟通协商后，按照协商的方式制定解决方案并进行处理。

具体故障级别及对应的应急响应要求如下：

一级故障：在1小时内确诊，总故障解决时间不超过4小时。

二级故障：在2小时内确诊，并在4小时内由专家到达现场确诊并解决，总故障解决时间不超过8小时；

1. 四级故障：在4小时内确诊故障，总故障解决时间不超过16小时。

若属于硬件故障，应在24小时内修复，不能立即修复的应提供备品备件应急使用。

## 培训要求

对系统使用单位提供业务操作培训，应提供详细培训方案。

(1)在质量保证期内，至少提供3次与项目相关的必要培训。

(2)供应商需要开展分层次的人员培训工作，每次培训后应对参加培训人员进行测试，确保用户对象能够掌握对应的操作技能。

## 进度要求

投标单位应根据建设内容，分阶段制定合理的时间进度，并且应根据招标方要求进行调整和细化。

本项目建设周期为6个月。要求项目合同签订后，第1个月内完成项目系统深化设计、需求调研、设备到货。第2-5个月内完成系统部署、设备安装调试，并具备上线运行条件。第6个月系统试运行，期间应能够按照建设单位需求进行优化。

采购人有权监督和管理投标项目的测试、安装、集成、验收等各项工作，投标方必须接受并服从采购人的监督、管理要求。

投标单位中标后必须提交正式的系统集成工作方案，明确系统集成方式、方法、过程步骤、需协调的事项等，并经采购人审核、同意。

中标人在实施过程中必须按周、月提交进度报告，对项目问题等进行说明，制定合理的解决措施。

## 项目团队及驻场人员要求

（1）投标人须具有稳定的在职技术保障力量，能够提供及时的技术支援或服务，应针对本项目提供不少于6人的项目服务团队（包括项目负责人、实施工程师等），投标单位的相关服务人员需具备相应的服务能力，需提供相关证明。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目负责人 | 负责项目质量和进度控制 | 1人 | 项目负责人具有本科或以上学历，具有计算机类高级技术职称，5年及以上类似项目实施经验的优先考虑。 | 驻场 |
| 实施工程师 | 负责项目实施工作 | 5人 |  | 不驻场 |

（2）投标人应针对本项目提供不少于2人的质保期间支撑团队（其中技术工程师不少于2人）；投标人的相关服务人员需具备相应的服务能力，需提供相关证明（最近一个季度依法缴纳社保费的证明）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 技术工程师 | 负责项目运行维护 | 2人 | 专职技术工程师，提供的5\*9驻场运维服务，负责安全平台监测及安全事件响应；  服务商委派的工程师须经过高院检查认可方可入驻，一经认可后，人员调动需经高院同意。 | 驻场 |

## 等级保护要求

本项目按照GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中第三级安全要求建设本项目的安全保障系统。

## 商业密码应用需求

本项目不涉及。

## 技术文件要求

投标人提供的书面技术资料应能确保系统正常运行所需的管理、运营及维护有关的全套文件。技术文件应该全面、完整、详细。技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

## 系统集成要求

### 系统对接

（1）安全监管运营平台需与高院现有ITIL平台进行对接，以API接口方式，接收ITIL平台的资产信息。

（2）安全监管运营平台需与高院主机安全管控系统进行对接，通过API接口等方式，定时获取主机资产信息，包括主机资产内安装的软件包、进程、服务等详细信息，建立资产的指纹信息和档案。

（3）安全监管运营平台需要与高院现有防病毒系统、终端安全管理系统对接，获得安全事件告警信息。

（4）安全监管运营平台需与高院互联网现有网络流量采集探针对接，通过隔离交换平台实现对高院互联网安全态势的统一管理。

（5）投标人所提供的XC网络终端安全管理系统统一管理平台和XC网络终端安全管理系统需与上海法院现有终端安全管理系统对接，确保本次安全建设不影响上海法院现有终端的平稳运行。

（6）上海高院现有一套移动业务系统和身份认证系统，投标人所提供的移动终端安全管理平台、零信任控制中心、零信任网关需与该移动业务系统和身份认证系统进行对接，确保本次安全建设不影响上海高院现有移动业务的平稳运行。

### 安全剧本制定

基于安全专家经验积累，结合高院的网络环境、业务流程和安全运营流程，编制安全识别、检测、响应和恢复的安全运维剧本，用于自动联动各类网络安全设备执行网络安全任务，提高安全事件处置的效率。

### 接口定制开发

为满足安全监管运营平台的使用需要，需提供安全设备告警日志格式解析适配、跨光闸数据传输格式定制开发。

### 数据的初始化服务

平台部署完成后，与高院现有ITIL平台进行对接以获取资产信息，对资产属性进行配置，完成资产信息初始化；与高院主机安全管控系统进行对接，获取主机资产的漏洞和脆弱性信息，完成脆弱性信息初始化；配置接入主机流量日志和安全设备的日志，完成安全数据接入初始化。

根据场景需要，完成系统管理相关的用户、角色、权限、告警策略等初始化配置工作。基于安全运营的场景，开展告警降噪和优化服务，对分析模型进行优化，提升告警准确率。

## 系统验收要求

（1）中标单位应当完成招标要求及合同规定的全部工程建设内容；

（2）系统经过总体功能测试，并提交测试报告；

（3）系统经过约定时间期限的试运行，并提交试运行报告；

（4）工程项目的所有技术文档、图纸已整理完成并经过审核，符合规范要求；

（5）测试完成后，提请甲方验收。

## 知识产权要求

（1）投标人应保证在本项目中使用的投标货物、技术、工程、服务或其任何一部分，均不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，若有纠纷，由投标人承担全部责任。如投标人不拥有相应的知识产权，则在投标价中应包括合法获取该知识产权的相关费用。

（2）除了投标方在投标书中明确知识产权权属的产品外，所有应用软件开发，包括二次开发的成果应归用户单位所有，其知识产权由用户单位和开发商共同享有。

## 安全保密要求

（1）投标人在参与本项目投标以及中标后的实施过程中，均应遵守国家保密法律、法规和规章制度。

（2）投标人应妥善保管本项目投标以及中标建设过程中的所有技术文档，保证不被不应获取者获取，保证未经用户方同意不以任何方式泄露其内容

## 项目管理要求

（1）投标方应当提供实施本项目的完整的项目管理方案，并在项目建设过程中严格执行；

（2）项目计划的制定和执行要与用户进行协调；

（3）应当提供完善、规范的各类项目文档，建立中间环节和文档的审核发布；

## 投标单位资质要求

具备ISO9001质量管理体系认证证书、ISO20000管理体系认证证书、ITSS信息技术服务标准符合性证书、ISO27001信息安全管理体系认证、信息系统建设和服务能力三级（CS3）及以上的优先考虑。