采购询价函

**项目名称：** 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目 设备采购

**招 标 人：** 海南省信投启明科技有限公司

**编制时间：** 2024 年 12 月 2 日

**举报渠道告知函**

为维护公平、公正的商业环境，保护双方共同利益，敬请各单位在与我公司各部门业务交往工作中，将我方人员明示或暗示要求宴请、接待，或索取礼金、礼品、礼券、或其他利益，或故意刁难、显失公平现象，向海南省信投启明科技有限公司综合管理部进行投诉。

**我们的承诺：对所有举报信息及时调查处理，对举报来源严格保守秘密，对举报单位或个人因举报所可能遭受的利益损害采取特别措施予以保护！**

海南省信投启明科技有限公司

各被邀请公司：

您好！

海南省信投启明科技有限公司拟就 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目设备采购 开展采购工作，本次采购方式为询比价，在满足采购方商务条款要求的情况下，由报价最低方中标，超出最高限价的报价，按无效报价处理，请贵公司于**2024 年 12月 6 日 18 时 00 分**之前进行邮件报价。

**一、报价形式**

**（一）邮件报价须知：**按要求将需要反馈的询价文件每页加盖公司公章后，用扫描件以电子邮件的形式在规定的时限内将报价发送至指定邮箱：

**（二）报价专用邮箱：hnxtqm-cg@iiivtech.cn**

**（三）注意事项：**

1.每个邮件不要超过20M，如超过分成多个邮件发送。

2.请务必确认邮件发送成功。

3.此邮箱为此次询比价的唯一指定邮箱。发往其他邮箱的报价将视为无效。

**二、其它要求**

**（一）报价时限：**超出规定时限报价的，将被视为无效报价，并且视为自动取消竞标资格。

**（二）特别强调：**在报价时间截止前，我们将贵司提供的最后一次价格视为最终报价。

**（三）纪律强调：**

1.如报价单位需要答疑的，请邮件预约时间，由采购专员统一答疑；

2.严禁供应商与采购专员以外人员进行接触打听项目信息，一经发现，有权取消其项目参与资格。

3.严禁供应商围标、串标等非合规行为，一经发现，将严肃处理。

**（四）答疑联系方式**

            答疑咨询：赵诗宇 13976274994

**三、询报价单（见附件）**

（一）采购需求

|  |  |
| --- | --- |
| **项目名称** | **社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目安全设备采购** |
| **采购需求** | 详见附件四：采购需求清单与内容 |
| **服务采购要求** | 无 |

（二）询价响应代理商的资质要求：（未达到以下资质要求的，将被视为无效询价响应）

1.要求企业获得工商行政部门颁发营业执照的，具有纳税人资格、国家组织机构代码能力。

2.具有独立承担民事责任能力。

3.法律、行政法规规定的其他条件。

4.询价文件的组成：询价响应声明书、报价表、企业工商营业执照复印件（提供三证合一或五证合一的复印件）、法人代表身份证有效复印件、本询价文件其它条款要求提供的相关文件以及各询价响应供应商认为应该提供的其它相关文件，加盖公司公章。（文件格式可参照附件，可自拟）

5.评审原则：在所有的询价文件符合或高于采购文件各项要求的情况下，报价最低者为成交供应商；在此基础上报价若相同，以服务承诺最优者为成交供应商。

6.出现下列情况之一者，响应文件无效，**作废处理**：

（1）询价响应文件字迹模糊不清（包括提交的各类复印件、图纸）；未在在规定的时限内提交等（2）未提供企业工商营业执照复印件（提供三证合一或五证合一的复印件）、报价表、询价响应声明书。

**附件1**

**询价响应声明书**

海南省信投启明科技有限公司：

根据贵方为**（ 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目设备采购 ）** 询价项目及服务的询价邀请，签字代表（姓名、岗位）经正式授权并代表询价响应供应商（公司名、办公地址）提交以下文件。

据此函，签字代表宣布同意如下：

1.询价响应供应商将按询价文件规定履行合同责任和义务。

2.询价响应供应商已详细审查全部询价文件，以及全部参考资料和相关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

3.询价响应供应商同意提供采购方可能要求的与其询价响应文件有关的一切数据或资料。

供应商代表的姓名：

询价响应供应商（加盖公章）

日期： 年 月 日

**附件2**

**报价表**

海南省信投启明科技有限公司：

在研究了询价文件中所有文件后，我公司对 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目设备 采购项目询价响应报价如下：

|  |  |
| --- | --- |
| 供应商名称 |  |
| 项目名称 | 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目安全设备采购 |
| 项目总报价合计 | 小写：¥ 元 （例：123,456.00元）  大写：人民币 （例：壹拾贰万叁仟肆佰伍拾陆元整） |
| 其他 |  |

注：

1、报价可参考此表格的形式。

2、询价响应单位如果需要对报价或其它内容加以说明，可在备注一栏中填写。

3、此表应经法定代表人或询价响应供应商授权代表签名，并盖上公章。

4、超过百万的项目金额，在项目总报价合计处，可以以万元为单位填写。

5、 项目总报价红字举例部分填写完后请删除。

询价响应供应商（加盖公章）：

法定代表人或授权代表：

日 期:

**附件3**

**法定代表人授权书**

海南省信投启明科技有限公司：

　　 法定代表人 ，兹授权我公司 （ 姓名 身份证号码 ） 为我公司全权代表，代表我公司全权负责 社会治理综合信息平台、公共安全视频监控联网应用综治共享分平台等平台整改升级项目设备采购 具体工作，并签署相关的文件、协议、合同和处理项目有关的一切事宜，产生的法律责任由我单位承担。

　　授权委托时间 个月，被授权人签署的文件(在授权书有效期内签署的)不因授权的撤销和到期而失效。

被授权人无转委权。

供应商：

法定代表人签章：\_\_\_\_\_\_\_\_\_\_\_\_

　　被授权人(签字) \_\_\_\_\_\_\_\_\_\_\_\_

　　\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

**附件4 报价清单及内容**

**采购需求清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 品牌 | 型号 | 名称 | 功能描述 | 单位 | 数量 |
| 1 | 绿盟 | NFNX3-HH1600 | 互联网边界防火墙 | 1、1U机型，含交流冗余电源，1个RJ45串口，1个RJ45管理口，2个USB接口，6个GE电口（Bypass）,4个SFP光口，2个接口扩展槽位，256G固态硬盘，4T 机械硬盘，整机吞吐量16G,应用层吞吐量14G,最大并发连接数250万,新建连接数25万。 2、支持一体化防护模块，包含应用管理/IPS/URL过滤/防病毒模块，且含应用管理特征库/IPS特征库/URL分类库/病毒特征库； 3、支持虚拟线，二层透明，三层，混合，旁路监听等接入方式，支持汇聚接口，二层聚合、三层聚合、虚拟线聚合，能够手动绑定接口，聚合方式支持平衡轮询、手动负载分担和LACP； 4、支持基于源/目的地址、接口、基于服务、应用的策略路由，支持反向路由； 5、支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑； 6、支持通过ICMP、TCP、UDP协议，完成对目的IP地址可达性的探测，支持在策略路由、DNAT策略、HA中设置链路探测； 7、支持文件传输限制，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制，支持基于FTP、HTTP、SMTP、POP3、IMAP、SMB、NFS、IECMMS、IEC104协议的病毒检测与阻断，包括邮件正文/附件、网页及下载文件中包含的病毒； 8、支持基于源/目的IP地址、安全区、应用、应用组、协议/端口、时间、安全模板等的精细粒度的安全访问控制，安全策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整； 9、支持针对源地址或者目的地址、网段、IP地址池进行黑名单和白名单的配置名单内容支持IP地址、协议TCP/UDP/ICMP和端口进行设置； 10、支持≥11000种入侵规则过滤，并提供服务器、内网等多种规则模板，支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等检测和防护； 11、支持二层协议（包含BPDU、802.1Q、SLOW、MPLS单播、MPLS多播、pppoe发现控制、pppoe会话控制、QinQ）进行控制，支持非IP协议（包含IPX和AppleTalk）的进行控制； 12、支持URL过滤，支持站点白名单、黑名单，临时删除的黑白名单可以临时存储在回收区，方便下一次恢复使用，无需重新创建，支持DNS检测，支持自定义URL类型过滤。 13、采用国产化芯片，国产化操作系统； 14、提供三年特征库升级，提供三年软硬件维保服务。 | 台 | 1 |
| 2 | 绿盟 | NFNX3-HH1600 | 政务外网边界防火墙 | 1、1U机型，含交流冗余电源，1个RJ45串口，1个RJ45管理口，2个USB接口，6个GE电口（Bypass）,4个SFP光口，2个接口扩展槽位，256G固态硬盘，4T 机械硬盘，整机吞吐量16G,应用层吞吐量14G,最大并发连接数250万,新建连接数25万。 2、支持一体化防护模块，包含应用管理/IPS/URL过滤/防病毒模块，且含应用管理特征库/IPS特征库/URL分类库/病毒特征库； 3、支持虚拟线，二层透明，三层，混合，旁路监听等接入方式，支持汇聚接口，二层聚合、三层聚合、虚拟线聚合，能够手动绑定接口，聚合方式支持平衡轮询、手动负载分担和LACP； 4、支持基于源/目的地址、接口、基于服务、应用的策略路由，支持反向路由； 5、支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑； 6、支持通过ICMP、TCP、UDP协议，完成对目的IP地址可达性的探测，支持在策略路由、DNAT策略、HA中设置链路探测； 7、支持文件传输限制，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制，支持基于FTP、HTTP、SMTP、POP3、IMAP、SMB、NFS、IECMMS、IEC104协议的病毒检测与阻断，包括邮件正文/附件、网页及下载文件中包含的病毒； 8、支持基于源/目的IP地址、安全区、应用、应用组、协议/端口、时间、安全模板等的精细粒度的安全访问控制，安全策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整； 9、支持针对源地址或者目的地址、网段、IP地址池进行黑名单和白名单的配置名单内容支持IP地址、协议TCP/UDP/ICMP和端口进行设置； 10、支持≥11000种入侵规则过滤，并提供服务器、内网等多种规则模板，支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等检测和防护； 11、支持二层协议（包含BPDU、802.1Q、SLOW、MPLS单播、MPLS多播、pppoe发现控制、pppoe会话控制、QinQ）进行控制，支持非IP协议（包含IPX和AppleTalk）的进行控制； 12、支持URL过滤，支持站点白名单、黑名单，临时删除的黑白名单可以临时存储在回收区，方便下一次恢复使用，无需重新创建，支持DNS检测，支持自定义URL类型过滤。 13、采用国产化芯片，国产化操作系统； 14、提供三年特征库升级，提供三年软硬件维保服务。 | 台 | 1 |
| 3 | 绿盟 | NFNX3-HH1200 | 公安网边界防火墙 | 1、1U机型，含交流冗余电源，1个RJ45串口，1个RJ45管理口，2个USB接口，6个GE电口（Bypass）,4个SFP光口，2个接口扩展槽位，256G固态硬盘，4T 机械硬盘，整机吞吐量12G,应用层吞吐量10G,最大并发连接数200万,新建连接数15万。 2、支持一体化防护模块，包含应用管理/IPS/URL过滤/防病毒模块，且含应用管理特征库/IPS特征库/URL分类库/病毒特征库； 3、支持虚拟线，二层透明，三层，混合，旁路监听等接入方式，支持汇聚接口，二层聚合、三层聚合、虚拟线聚合，能够手动绑定接口，聚合方式支持平衡轮询、手动负载分担和LACP； 4、支持基于源/目的地址、接口、基于服务、应用的策略路由，支持反向路由； 5、支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑； 6、支持通过ICMP、TCP、UDP协议，完成对目的IP地址可达性的探测，支持在策略路由、DNAT策略、HA中设置链路探测； 7、支持文件传输限制，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制，支持基于FTP、HTTP、SMTP、POP3、IMAP、SMB、NFS、IECMMS、IEC104协议的病毒检测与阻断，包括邮件正文/附件、网页及下载文件中包含的病毒； 8、支持基于源/目的IP地址、安全区、应用、应用组、协议/端口、时间、安全模板等的精细粒度的安全访问控制，安全策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整； 9、支持针对源地址或者目的地址、网段、IP地址池进行黑名单和白名单的配置名单内容支持IP地址、协议TCP/UDP/ICMP和端口进行设置； 10、支持≥11000种入侵规则过滤，并提供服务器、内网等多种规则模板，支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等检测和防护； 11、支持二层协议（包含BPDU、802.1Q、SLOW、MPLS单播、MPLS多播、pppoe发现控制、pppoe会话控制、QinQ）进行控制，支持非IP协议（包含IPX和AppleTalk）的进行控制； 12、支持URL过滤，支持站点白名单、黑名单，临时删除的黑白名单可以临时存储在回收区，方便下一次恢复使用，无需重新创建，支持DNS检测，支持自定义URL类型过滤。 13、采用国产化芯片，国产化操作系统； 14、提供三年特征库升级，提供三年软硬件维保服务。 | 台 | 1 |
| 4 | 绿盟 | NFNX3-HH1200 | 网络安全管理域边界防火墙 | 1、1U机型，含交流冗余电源，1个RJ45串口，1个RJ45管理口，2个USB接口，6个GE电口（Bypass）,4个SFP光口，2个接口扩展槽位，256G固态硬盘，4T 机械硬盘，整机吞吐量12G,应用层吞吐量10G,最大并发连接数200万,新建连接数15万。 2、支持一体化防护模块，包含应用管理/IPS/URL过滤/防病毒模块，且含应用管理特征库/IPS特征库/URL分类库/病毒特征库； 3、支持虚拟线，二层透明，三层，混合，旁路监听等接入方式，支持汇聚接口，二层聚合、三层聚合、虚拟线聚合，能够手动绑定接口，聚合方式支持平衡轮询、手动负载分担和LACP； 4、支持基于源/目的地址、接口、基于服务、应用的策略路由，支持反向路由； 5、支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑； 6、支持通过ICMP、TCP、UDP协议，完成对目的IP地址可达性的探测，支持在策略路由、DNAT策略、HA中设置链路探测； 7、支持文件传输限制，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制，支持基于FTP、HTTP、SMTP、POP3、IMAP、SMB、NFS、IECMMS、IEC104协议的病毒检测与阻断，包括邮件正文/附件、网页及下载文件中包含的病毒； 8、支持基于源/目的IP地址、安全区、应用、应用组、协议/端口、时间、安全模板等的精细粒度的安全访问控制，安全策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整； 9、支持针对源地址或者目的地址、网段、IP地址池进行黑名单和白名单的配置名单内容支持IP地址、协议TCP/UDP/ICMP和端口进行设置； 10、支持≥11000种入侵规则过滤，并提供服务器、内网等多种规则模板，支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等检测和防护； 11、支持二层协议（包含BPDU、802.1Q、SLOW、MPLS单播、MPLS多播、pppoe发现控制、pppoe会话控制、QinQ）进行控制，支持非IP协议（包含IPX和AppleTalk）的进行控制； 12、支持URL过滤，支持站点白名单、黑名单，临时删除的黑白名单可以临时存储在回收区，方便下一次恢复使用，无需重新创建，支持DNS检测，支持自定义URL类型过滤。 13、采用国产化芯片，国产化操作系统； 14、提供三年特征库升级，提供三年软硬件维保服务。 | 台 | 1 |
| 5 | 绿盟 | OSMSNX3-HFC | 堡垒机 | 1、1U机型，冗余电源，4T硬盘，256G SSD，7个千兆电口，4个千兆光口，2个万兆光口，不含光模块，1个扩展插槽，2个USB，1个串口，字符并发数1800，图形并发数2000，授权管理300台设备，最大可管理设备数无限制； 2、支持基于SDP技术的远程接入，无需额外部署VPN设备，支持服务隐藏功能，开启后，攻击者无法扫描到对应服务端口，支持客户端在开启VPN的情况下，通过SDP技术和该端口建立安全隧道； 3、支持用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户管理，用户角色管理，资产管理，密码管理、策略管理、审计管理，支持不同角色相互组合； 4、支持基于组织机构、角色、属性和账户的静态授权，通过不同授权模型满足运维管控要求； 5、支持RDP、X11、VNC、SSH、TELNET、RLOGIN、SFTP、FTP、SAMBA协议的HTML5运维，无需本地运维客户端，支持通过H5文件运维的方式上传和下载文件； 6、支持静态密码认证，支持配置静态密码的期限、最小长度要求、到期提醒、密码强度限制级禁止使用常用密码； 7、支持堡垒机专用客户端和堡垒机建立加密隧道，隧道加密算法可按需选择是国密或者标密； 8、支持基于IP的DNAT网络环境部署，通过映射后的IP信息能够访问堡垒机； 9、支持终端合规检查策略，包含针对Windows补丁检测、操作系统版本检测、端口检测、进程检测和安装应用检测，可由管理员自定义配置合规策略，自定义范围包括但不限于检查项、告警等级、执行操作等； 10、支持服务端口代理功能，支持可将多个服务端口代理成一个，支持通过堡垒机直接代理HTTP/HTTPS协议，无需前置机。 111、提供三年软件、硬件维保服务。 12、采用国产化芯片，国产化操作系统； 13、产品制造厂商具备中国网络安全审查技术中心与认证中心颁发的信息系统安全运维一级资质证书，提供有效证书的复印件并盖制造厂商公章。 | 台 | 1 |
| 6 | 绿盟 | LASNX3-HH1000 | 日志审计 | 1、1U机型，冗余电源，2个USB接口，1个RJ45串口，1个GE管理口，6个千兆电口，4个千兆SFP插槽，2个接口扩展槽位，4TB SATA硬盘，授权接入40个日志源； 2、支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、JDBC、Net flow、KAFKA、WMI、二进制数据、专用Agent等方式采集日志； 3、支持利用JDBC的方式对数据库表日志进行综合管理与分析，支持采集国产化数据库数据接入，包括但不限于人大金仓、南大通用、达梦数据库，神州通用等； 4、支持界面配置即可完成未识别日志接入，无需编写xml； 5、支持规则自适应日志接入，仅输入IP范围及端口即可自动匹配相应规则，完成日志自动接入； 6、支持范式化日志多级提取，支持正则、KV、CSV、格式串等多种灵活的提取方式； 7、支持对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联,注册表审核监控等； 8、支持对WEB服务器日志展开深度分析，分析内容包括但不限于发起请求的地址及浏览器情况、响应结果、访问趋势、恶意扫描识别等； 9、支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式； 10、支持将产生硬件故障但能WEB访问设备上的数据备机到新设备上，备机数据应包含日志源、事件规则、统计项、枚举值等； 11、提供三年软件、硬件维保服务； 12、采用国产化芯片，国产化操作系统。 | 台 | 1 |
| 7 | 绿盟 | ESSNX1-SNM | 杀毒软件 | 1、含系统中心，实现终端安全系统的集中管理、策略配置、报表查看等功能，Windows客户端授权许可（数量3点），Linux/国产化-服务器/授权许可（数量12点），提供病毒防护、补丁加固、桌面管理、EDR（资产清点、终端行为采集、入侵防御、日志采集）、数据防泄露等功能； 2、支持本地多引擎查杀能力，且引擎可自定义配置，Windows/Linux/国产操作系统均支持多引擎配置，具备人工智能引擎，人工智能引擎支持PE/OFFICE/PDF常见文件类型威胁检测，人工智能引擎支持恶意代码检测多分类，能够区分Virus、Trojan、Ransom、Rootkit、Backdoor、Exploit、Worm等类型； 3、支持ARP欺骗防御，支持网关和DNS绑定，支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截； 4、支持检测挖矿木马通信协议和连接矿池地址，实时阻断挖矿木马挖矿行为； 5、支持检测Linux操作系统（包括但不限于BCLinux、龙蜥、欧拉、debian、redhat、ubuntu等）漏洞，支持检测数据库（包括但不限于MySQL、Redis、Mongodb等）漏洞； 6、具备主机防火墙，支持对终端端口和IP进行进或出单向及任意双向过滤，支持黑白名单机制； 7、具有持续采集浏览器HTTP/HTTPS访问记录的机制，支持Chrome、Edge、Maxthon、FireFox、QQ、UC、2345等常见浏览器； 8、支持操作系统、数据库组件、大数据组件、WEB组件等提供虚拟补丁功能，在不修复漏洞的情况下拦截攻击行为； 9、支持自定义主机名、IP地址、MAC地址、时间作为屏幕内容水印显示，支持设置水印宽度、高度、行间距、倾斜度、水印布局等内容； 10、支持自定义主机名、IP地址、MAC地址、时间作为屏幕内容水印显示，支持设置二维码大小、背景色、前景色等内容； 11、提供三年软件升级服务。 12、产品制造厂商需具备中国网络安全审查技术与认证中心颁发的信息安全应急处理一级服务资质证书，提供有效证书的复印件并盖制造厂商公章； | 台 | 1 |
| 8 | 绿盟 | NIDSNX3-HH3200 | 入侵检测 | 1、标准机架式硬件，1U机型，交流冗余，2个USB接口，1个RJ45串口，2个千兆电口（1个管理，1个热备），6个千兆电口（3路bypass），4个千兆SFP插槽，2个扩展槽位，256G SSD，4T硬盘，整机网络层吞吐量12Gbps，应用层吞吐量3Gbps； 2、支持攻击特征库数量≥10000条，支持检测勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等等，规则支持按CVE、CNNVD、CWE、Bugtraq关联、查询和筛选； 3、支持丰富的响应方式，包括告警、阻断、IP隔离、抓包等，满足用户各种响应需求； 4、支持手动添加非法IP到黑名单的功能，支持基于IP、源地址、目的地址去手动添加全局白名单； 5、支持敏感数据保护功能，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据； 6、支持通过X-Forwarded-For、X-Real-IP、Cdn-Src-IP来识别通过HTTP代理或负载均衡方式连接到Web服务的客户端最原始的IP地址，并可自定义三个字段的识别优先级顺序； 7、支持各检测模块，具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的IP、事件类型等信息，对告警日志执行归并，有效抵御告警风暴； 8、支持基于HTTP、FTP、EMALL等协议传输的敏感数据进行泄露防护； 9、支持过滤器模板功能，可将复杂的查询参数保存为过滤器模板，生成报表时直接调用模板即可，无需重复查询输入参数，以减少日常维护工作量； 10、提供三年软件、硬件维保服务； 11、采用国产化芯片，国产化操作系统。 | 台 | 1 |
| 9 | 新华三 | H3C UniServer R4930 G5 | 杀毒软件服务器 | 1、CPU：海光3号CPU，1颗CPU，每CPU核数16核，主频2.5GHz。 2、内存16G DDR4，频率3200MHz。 3、配置12个3.5寸热插拔硬盘槽位，可扩展至14个3.5寸硬盘槽位，同时可扩展4个2.5寸小盘。全部硬盘可在不打开主机箱盖的情况下热插拔维护。安装2块2.4T 12G SAS 10K硬盘； 4、配置8端口SAS RAID卡，2G缓存，支持RAID0/1/10/5/6/50/60，含掉电保护。 5、配置一块4端口1GE电接口网卡; 6、配置2个550W白金热插拔冗余电源； 7、配置6个热插拔冗余风扇； 8、支持5个USB 3.0接口（前面板1 个，后面板2 个，主板2 个）；1个USB前置2.0接口； 9、标配1个VGA，可选配支持最高2个VGA接口，支持后部独立的管理端口； 10、可配置机箱入侵检测，在外部打开机箱时提供报警功能； 11、提供三年软件、硬件维保服务； 12、采用国产化芯片，国产化操作系统。 | 台 | 1 |

**注：以上报价需含13%增值税**