## 投标分项报价表

项目编号：YZCG-DL201824号 项目名称：禹州市中医院“网络信息化安全等级保护建设采购”项目 单位：元

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格型号 | 技术参数 | 单位 | 数量 | 单价 | 总价 | 产地及厂家 |
| 1 | 互联网出口综合安全网关 | 深信服AF-1000-D420 | 设备接口：4个千兆电口，2个千兆光口；整机吞吐量：7Gbps；应用层吞吐量：1Gbps并发连接数：2,500,000；每秒新建连接数：15万；尺寸：标准1U架构；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能；访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制；支持NAT64、NAT46 地址转换；支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式；支持双机环境下IPSec VPN组网；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和VLAN；支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；支持对服务器和客户端的漏洞攻击防护；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；支持HTTP协议的安全威胁检测和防护；支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；支持高级威胁关联分析的能力，并展示热点事件详情，推送到运维管理员手机中进行快速处置；设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址； 支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护，支持对所有已被入侵和受控的设备进行风险检测与分析，针对风险可以实现快速响应与处置；支持手动评估功能，自动展示最终的风险； | 台 | 1 | 84300 | 84300 | 广东.深圳深信服科技股份有限公司 |
| 2 | 上网行为管理 | 深信服AC-1000-C600 | 吞吐量5Gbps，并发连接数15万;每秒新建连接数20000，6个千兆电口，1U机架式设备，双电源;3年URL特征库更新；国产非OEM品牌；支持网关、网桥、旁路模式、多路桥接和多主模式；支持部署在IPv6环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持IPv6；支持支持触发式WEB认证，静态用户名密码认证、以USB-Key方式实现双因素身份认证、短信认证、微信认证、访客二维码认证；支持LDAP、Radius、POP3、Proxy等第三方认证； 支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证；设备内置应用识别规则库，支持超过4700条应用规则数，支持超过2100种以上的应用，660种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；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；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；支持给每一种应用列上图标，易于客户了解应用的特征；支持记录QQ、MSN等IM聊天行为和传文件的内容；支持移动APP（IOS和android）审计（如论坛类、微博类、新闻评论类等）支持金融类应用内容审计如：阿里旺旺、万德（Wind）、路透等应用的聊天内容；支持流量父子通道技术，支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；支持通过抑制P2P的下行流量，来减缓P2P的上行流量，从而解决网络出口在做流控后仍然压力较大的问题；支持灵活配置流控单位是IP还是用户名（适用于公共账号：多个IP公用一个账号时，可以对每个IP进行限速，更加灵活准确）针对SSL加密的网站、论坛发帖、web邮箱以及客户端邮箱（如闪电邮）的内容进行审计及关键字过滤；针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）下钻查询 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询； | 台 | 1 | 100520 | 100520 | 广东.深圳深信服科技股份有限公司 |
| 3 | 外联防火墙 | 深信服AF-1000-C600 | 整机吞吐量：8Gbps,应用层吞吐量：1.5Gbps；并发连接数：1,500,000,每秒新建连接数：13万；设备接口：6个千兆电口;尺寸：标准1U架构；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能；访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制；支持NAT64、NAT46 地址转换；支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式；支持双机环境下IPSec VPN组网；支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；支持对服务器和客户端的漏洞攻击防护；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址； | 台 | 1 | 74110 | 74110 | 广东.深圳深信服科技股份有限公司 |
| 4 | Web应用防火墙 | 深信服AF-1000-E420-os | 网桥模式部署，标准1U设备，至少提供4个千兆电口，2个千兆光口；整机吞吐量6Gbps，七层吞吐量1Gbps，并发连接数180万，每秒新建连接数10万，支持故障时Bypass；设备具备独立的WEB应用防护识别库，特征总数在3000条以上；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制；支持NAT64、NAT46 地址转换；支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对HTTP、FTP协议内容检测与病毒查杀； 设备具备独立的WEB应用防护识别库，特征总数在3500条以上；支持HTTP协议的安全威胁检测和防护；支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；支持CC攻击、CSRF攻击、COOKIE攻击等攻击防护功能；设备具备独立的WEB应用防护识别库，特征总数在3500条以上；支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；支持Windows和Linux系统下网页防篡改功能，防篡改支持网站登录后台和FTP登录后台防护，管理员支持IP认证和邮件认证；支持热点威胁实时处理检测与快速响应；支持高级威胁关联分析的能力，并展示热点事件详情，推送到运维管理员手机中进行快速处置；支持安全日志进行分析，识别持续性攻击、黑链、高危僵尸病毒等高级威胁并通过微信进行预警；设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持恶意域名重定向功能，用于DNS代理服务器场景下定位内网感染僵尸网络病毒的真实主机IP地址； | 台 | 1 | 98030 | 98030 | 广东.深圳深信服科技股份有限公司 |
| 5 | 核心防火墙 | 深信服AF-1000-F440 | 整机吞吐量：12Gbps；应用层吞吐量：4Gbps；并发连接数：4,500,000；每秒新建连接数：18万；设备接口：4个千兆电口，4个千兆光口; 尺寸：标准2U架构；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议； 支持根据国家/地区来进行地域访问控制；支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对HTTP、FTP协议内容检测与病毒查杀； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；支持HTTP协议的安全威胁检测和防护；支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址； | 台 | 1 | 154300 | 154300 | 广东.深圳深信服科技股份有限公司 |
| 6 | 入侵防御系统 | 深信服AF-1000-D440-pm | 整机吞吐量：6Gbps；并发连接数：1,800,000；每秒新建连接数：6万设备接口：4个千兆电口，4个千兆光口;入侵防护规则库4000条；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能；设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上；支持对服务器和客户端的漏洞攻击防护；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间；可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； | 台 | 1 | 89510 | 89510 | 广东.深圳深信服科技股份有限公司 |
| 7 | 数据库审计系统 | 深信服DAS-1000-A620 | 性能指标：单向数据库流量800M；硬件指标：标准1U机架式，双电源，6个千兆电口，2个千兆光口，2\*2TB SATA硬盘;性能指标：单向数据库流量800M；硬件指标：标准1U机架式，设备接口：6个千兆电口，2个千兆光口；双电源，配置2\*2TB SATA硬盘；审计方式：旁路交换机镜像 、 Agent抓包多机部署支持集中管理，可集中管理多台采集器审计的事件、分析，实现统一配置、统一报表、统一查询；支持多种虚拟化平台，包括Sangfor-HCI (vma格式)、Kvm (qcow2格式)、Vmware (ova格式)支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库。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，白名单内容包括以下4个维度：SQL模版、业务系统、URL地址、数据库条件；审计SQL模版：产品支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威胁支持联动互联网边界设备（如数据分析平台、上网行为管理）实现数据外发泄密分析；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。支持以时间、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、策略、规则、风险级别、SQL模版为条件的数据库风险查询； | 台 | 1 | 13470 | 13470 | 广东.深圳深信服科技股份有限公司 |
| 8 | 安全探针 | 深信服STA-1000-B420 | 性能指标：2Gbps，硬件指标：1U规格，SSD128G、双电源，标配4电2光；旁路部署方式对全流量信息进行采集；与安全态势感知系统为同一品牌；旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制；能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型;支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式；支持设备内置简单命令行管理窗口，便于基础运维调试；支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；提供安全探针特征库软件著作权证书； | 台 | 1 | 103100 | 103100 | 广东.深圳深信服科技股份有限公司 |
| 9 | 负载均衡 | 深信服AD-1000-D620 | 8个千兆电口；标准1U设备;四层吞吐量5.5G，并发连接数400W，四层新建连接数30W，七层新建连接数15W，SSL新建性能6000TPS；支持串接部署方式和旁路部署方式，支持三角传输模式。国产知名品牌，非OEM产品；单一设备可同时支持包括链路负载均衡、全局负载均衡、服务器负载均衡的功能。以上功能同时处于激活可使用状态，无需额外购买相应授权；支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、优先级等算法。通过某种编程语言（如lua）实现自定义的流量编排，对TCP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。支持静态IP和PPPOE两种线路接入方式。支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得Active-Active运行和的能力。内置完备的IP地址库，无需手动导入并支持自动更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能；行为进行关联分析，帮助用户找到真正存在高风险的安全薄弱环节，并通过报表的方式展现安全风险和解决方法；一台物理设备可从逻辑上划分为多台虚拟设备，各虚拟设备拥有独立的计算资源和网络资源，各虚拟设备可运行不同软件版本，虚拟设备重启或升级时不影响其他虚拟设备的正常运行，虚拟设备宕机可自动重启。 | 台 | 1 | 190800 | 190800 | 广东.深圳深信服科技股份有限公司 |
| 10 | 日志审计系统 | 深信服LAS-1000-A600 | 标准1U机架式，处理性能3000条/秒，提供4个千兆电口，支持3路千兆监听口；可用物理磁盘空间>=1TB；日志存储量至少十亿条；深度定制优化的Linux系统；提供旁路接入模式，设备部署不影响原有网络结构；支持通过页面直接将日志文件导入或以syslog方式接收日志信息；支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问、文件访问、数据库服务、WEB服务、FTP服务；支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、深信服、安氏领信、网神]支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；支持文本型日志原始文件管理，可将系统作为日志服务器使用；支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；支持查询模版创建、修改、删除功能；支持内置归并策略，对HTTP数据进行自动归并处理；支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；审计日志文件方式存储；审计日志加密导出审计系统；支持对所有审计管理员操作审计系统的动作进行审计；审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； | 台 | 1 | 159100 | 159100 | 广东.深圳深信服科技股份有限公司 |
| 11 | 堡垒机 | 深信服OSM-1000-A600 | 提供不少于50个资源授权，1U,标配6个千兆电口，支持扩展接口；标配双电源；提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护二级建设要求;1U机架式，提供50个资源授权，6个千兆电口，支持扩展接口；标配双电源；提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护二级建设要求;支持windows系统、linux/unix系统、网络设备；支持KVM、Vmware、数据库、http/https等支持从windows AD域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式支持windows系统、网络设备、linux/unix系统、数据库等设备账号的收集功能；支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权同时支持本地口令认证、LDAP认证、AD认证、短信认证、Radius、usbkey、动态口令认证支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存；支持双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权；支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人；支持对常见设备运维操作进行记录（至少包括windows主机、linux/unix主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆IP、设备IP、设备名称、设备类型、访问账号、访问协议等信息；全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端。需支持HA，配置信息实时同步，配置过程在web界面完成 | 台 | 1 | 163100 | 163100 | 广东.深圳深信服科技股份有限公司 |
| 12 | 网闸 | 北京安盟SU-GAP3000-XBS0 | 千兆双向隔离网闸，4个千兆网口，2个串口；文件同步、数据库同步、WEB文件传输；邮件交换；视频隔离等；负载均衡；双机热备,带宽：600Mbps，延时10ns，并发连接数30000个；含三年软件升级，硬件质保，远程技术支持；外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置。设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、WINCC模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。支持平台级联及平台点播，支持GB28181视频通信国家标准及相关厂商协议规范；支持的数据库种类包括ORACLE、SQLSERVER、MYSQL、SYBASE等主流数据库支持多种关系型数据库通信。支持SQL语句的白名单；支持TCP应用层数据单向传输的控制，保证TCP应用数据的0 反馈，以满足二次防护对数据传输的安全性需求。系统支持多任务的组播代理功能，可穿透三层交换机网络进行部署，支持PIM协议；支持DCS/SCADA生产网络与办公网络之间的OPC应用数据的传输。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输。支持TCP/IP以上的应用层协议，支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等协议解析方式来解析自定义应用的通信内容。系统提供ping ,traceroute ,TCP端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题； | 台 | 1 | 85100 | 85100 | 北京北京安盟信息技术有限公司 |
| 13 | SSL VPN | 深信服VPN -1000-A400 | SSL加密流量300M，并发连接数40万，4个千兆电口，1U机架式设备，双电源；本次开通20个SSL移动接入授权；用于在外人员通过加密的互联网隧道访问医院内网，保障数据安全；专业VPN设备，同时支持IPSec VPN、SSLVPN两种VPN，支持网关模式、单臂模式、双机模式、集群模式的部署支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用；在windows系统上，能同时安装并运行多个VPN客户端，满足有多套VPN的客户同时登录VPN；支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入IP、接入时间、接入线路IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN。支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；支持与阿里钉钉、企业级微信绑定，实现其内置OA的安全接入，实现动态口令认证，增加认证的多样性。支持随机验证码短信认证，可自定义所发送短信信息格式，支持用户端短信重发功能；设备内部必须支持自建CA中心，便于数字证书认证平台搭建；支持与基于PKI体系的第三方CA进行结合认证。支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议；产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固；产品应该支持企业级“云盘”（又名“网盘”、“文件共享”）功能，即可以通过手机、PC、IPAD的客户端，将数据、文件同步到云端或和分享到终端。也能够能够支持分享给他人。产品必须在Windows和MAC操作系统下支持远程应用发布功能；支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置； | 台 | 1 | 50150 | 50150 | 广东.深圳深信服科技股份有限公司 |
| 14 | 下一代防火墙 | 深信服AF-1000-D420 | 设备接口：4个千兆电口，2个千兆光口；整机吞吐量：8Gbps；应用层吞吐量：1.2Gbps，并发连接数：2,500,000；每秒新建连接数：8万；尺寸：标准1U架构；支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能；访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对HTTP、FTP协议内容检测与病毒查杀； 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测；支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上； | 台 | 1 | 84300 | 84300 | 广东.深圳深信服科技股份有限公司 |
| 15 | 互联网业务监测服务 | 深信服网络安全人工服务 | <http://www.hnyzszyy.com> 互联网业务安全监测；安全威胁分析：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害；安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务；事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径；安全加固建议：根据事件发生的根因、影响范围，针对性给出安全加固方案；按季度输出安全加固方案及安全运营效果汇报。提供实时带宽15Mb/s、防护域名数量5个，为用户网站提供云端的Web应用安全防护、IPS、独享防护、防绕过、失陷监测、安全可视化、动态防护、定向防护、实时对抗、应急对抗；以及安全专家代管服务。支持关键资产系统域名发现，自动发现客户所填入域名相关的所有子域名；支持对Web漏洞进行扫描，覆盖通用漏洞和常规漏洞。支持SQL注入、XSS、安全配置错误、已知漏洞组件包含、敏感信息泄露等常见漏洞的检测；对风险评估报告中的高危漏洞进行专家验证，确保高危事件的准确性，并定期给用户推送云扫描报告。支持高危0day实时检测；出现0DAY漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持微信端实时推送告警信息；支持对目标站点提供7×24小时网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现；支持敏感时期（如重大会议期间）的防篡改，当敏感时期到来，对外显示缓存在服务器中的静态页面，充当网站的安全替身，支持一键开启、一键关闭；支持对常见http应用服务的口令暴力破解防护功能；支持对网站的扫描防护和防止恶意爬虫攻击；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等 ；0Day发布后24小时内进行全面排查，第一时间告知用户是否存在该风险，并针推出针对性防护方案；针对DDOS、CC等恶意流量攻击行为增加专家在线分析环节，并封锁攻击源IP地址；针对境外IP地址做特殊关注，一旦发现恶意行为立即封锁源IP；支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送；平台展示包括web业务系统的风险统计、风险分布、潜在风险篡改TOP5和风险等级统计；风险列表中包括已被篡改风险、潜在篡改风险、非篡改风险；支持每日生成安全运营日报，每月生成安全运营月报，并针对安全事件实时生成安全事件报告； | 年 | 5 | 47200 | 236000 | 广东.深圳深信服科技股份有限公司 |
| 16 | 终端安全防护软件EDR | 深信服端点安全软件V3.0（Windows Server客户端授权） | 端点安全防护软件，提供更全面的主机安全的预防、防御、检测和响应能力。主机安全预防包含主机安全基线合规审查、访问控制微隔离。主机安全防御包含恶意文件实时监控防御、勒索病毒实时防御、WebShell实时防御、僵尸网络实时防御、暴力破解实时防御。主机安全检测包含恶意文件扫描检测、WebShell扫描检测。主机安全响应包含全网威胁定位、一键文件和主机隔离、设备联动响应。产品是软件形态，包含管理平台和终端Agent软件；Agent软件支持32位和64位的Windows系统和64位的Linux系统。产品和国内主流云平台实现解耦和，适用于Vmware、华为云、华三云、阿里云、腾讯云等国内主流云平台的主机；管理平台采用软件包方式提供安装，安装后其中必须具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性。本次开通20个服务器端授权。无需安装任何其他软件和专用设备硬件，采用基于X86服务器或虚拟服务器即可完成平台部署；终端Agent软件可以通过软件安装或虚拟机模板的方式进行安装。支持终端资产盘点管理，平台支持自动区分网内终端为业务终端或用户终端，也支持终端组的新增、修改、删除和终端分组切换；支持自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端Agent版本、病毒库版本、最近登录时间、最近登录的用户名；支持录入终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，做到准确定位。支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、已失陷、高可疑、低可疑，支持下钻到对应的终端列表；支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量、WebShell后门数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表；支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量；支持以安全策略模板方式对指定终端/终端组快速部署安全策略，安全策略支持缺省默认模板和自定义模板等多种格式；支持安全策略一体化配置，通过一条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、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置；支持极速、均衡、低耗三种扫描模式，以控制扫描时对业务系统CPU资源的占用；支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。支持对来自Internet、E-mail或是光盘、移动存储、网络等各种入口渠道病毒进行实时检测；支持单个攻击源和分布式攻击源的暴力破解检测；支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置；支持windows系统永恒之蓝漏洞（MS17-010）的检测；针对Linux系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范； 支持配置WebShell检测开启或关闭；支持配置WebShell定时扫描任务，配置参数包括：扫描周期（每日、每周、每月）、扫描时间精确到分、发现威胁处置方式；支持配置WebShell实时扫描，一旦发现WebShell文件，自动隔离或仅上报不隔离。业务系统详情支持展示流量分布Top5、业务流量排行Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）；服务器详情支持展示服务器的资源状态（CPU占有率、内存占有率和磁盘率）、流量分布Top5、该服务器开发的服务；流量线详情支持展示该流量线对应的微隔离策略；支持图形化显示服务器间流量关系，包括访问详情、流量趋势等；支持将Agent检测出来的恶意文件事件、WebShell事件、暴力破解事件、微隔离事件的日志上报到安全态势感知平台，安全态势感知平台进行分析和展示；支持安全态势感知平台下发禁止指定终端所有目标IP的入站或出站策略；支持策略为自定义设置的目标IP或IP范围、端口或端口范围；可以实现被感染终端IP封锁隔离，防止风险扩展。支持多台防火墙通过配置终端检测响应管理平台IP地址实现与EDR平台的联动，实现端网安全联动；支持管理员在下一代防火墙平台对其下发的查杀任务中查杀出来的病毒进行处置；支持基于威胁情报的病毒md5值的全网终端定位搜索，适用于对变种流行病毒的快速响应，快速确认全网终端是否感染； | 套 | 20 | 4190 | 83800 | 广东.深圳深信服科技股份有限公司 |
| 17 | 安全感知平台 | 深信服SIP-1000-A600 | 硬件指标：1U规格，32G内存，SSD 128G系统盘、SATA 16T存储、双电源，标配6电；基于海量的安全数据，通过机器学习、UEBA、关联分析等智能技术，帮助客户看清业务、感知威胁、及时预警、快速响应。支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势，支持页面跳转到对应态势大屏；支持不同视角展示全网态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势等8个独立的大屏展示功能，并支持大屏轮播；支持感知业务/服务器资产、终端资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。支持安全域维度感知资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP范围、备注等信息，并支持导入导出csv配置文件；支持页面展示业务脆弱性风险分布，不同严重级别业务分布，漏洞类型分布图，漏洞整体态势等，支持7天、30天统计；支持安全域维度展示安全风险，包含安全域列表、安全域评分、事件类型TOP5、IP地址、IP类型、风险等级、关键风险、状态等信息；横向威胁感知展示包含横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包含发起与遭受横向威胁主机TOP5，发起视角包含发起者IP、发起者类型、所属分析、所属业务/终端组、横向威胁类型、遭受者数、遭受者类型、日志数；支持与上网行为管理设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联；支持通过浏览器推送用户提醒或冻结用户上网；支持与数据库审计设备联动，支持同步数据库审计设备的数据库风险日志、管理员操作日志、数据库正常审计日志、web审计，便于统一审计；支持与SSL VPN设备同步用户用户信息，包括用户登录、登出、分配IP、访问资源记录的日志数据，实现远程接入用户与安全事件关联分析，分析出异常用户，以VPN用户为可视化视角，呈现风险问题、风险程度、内网资源访问情况等。支持同步管理员操作日志，满足审计要求。支持与终端安全软件联动响应，禁止攻击流量出站或入站，也可以实现被感染主机IP封锁隔离，防止风险扩展； | 台 | 1 | 275300 | 275300 | 广东.深圳深信服科技股份有限公司 |
| 18 | 安全探针 | 深信服STA-1000-B420 | 性能指标：2Gbps，硬件指标：1U规格，SSD128G、双电源，标配4电2光潜伏威胁探针主要通过旁路部署方式对全流量信息进行采集；与安全态势感知系统为同一品牌；旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力；可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型；支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式；支持设备内置简单命令行管理窗口，便于基础运维调试；支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； | 台 | 1 | 103100 | 103100 | 广东.深圳深信服科技股份有限公司 |
| 19 | 漏洞基线扫描 | 深信服BVT-1000-A620 | 支持并发100台设备的扫描；1U，标配6个千兆电口，支持扩展接口；标配双电源，支持扩展为冗余电源;含配置核查、漏洞扫描、配置变更检查三大引擎。功能包括：任务管理、检测报告、结果对比，告警分析、综合报表、综合仪表板等；支持并发≥100台设备的扫描；≥6个千兆电口，支持扩展接口；标配双电源，支持扩展为冗余电源；标准机架式硬件设备，无需在被扫描目标系统上安装任何软件；产品功能的实现无需额外增加服务器等设备。采用B/S架构操作方式，无需安装客户端软件。通过SSL加密对数据传输等进行处理；加密存储；备份机制；防篡改机制；HTTPS方式；用户密码策略机制基线检查和变更检查支持远程检查，SSH、TELENT、SMB等多种方式基线检查和变更检查支持离线检查；漏洞扫描支持指定登录用户名和口令进行本地漏扫检查基线检查和变更检查支持跳转机跳转；主机类：windows、Unix、solaris、HP-Unix、AIX、 Linux等网络设备：华为、H3C、Cisco、Juniper、中兴等防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等系统支持对IP对象的自动发现功能；并智能识别对象系统类型；内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略支持高级数据分析，可对同一IP的两次扫描结果进行风险对比分析，并可在线查看同一IP的多次历史扫描结果能够扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi违规列表：显示系统内所有的违规信息情况，以列表方式呈现；违规详细查看：在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息。查询：在违规列表中提供查询功能，输入相关查询字段进行查询。支持离线任务：支持用户离线执行任务检查，并支持离线检查结果导入系统分析，与在线任务一样详细展示任务执行结果； | 台 | 1 | 165390 | 165390 | 广东.深圳深信服科技股份有限公司 |
| 20 | 终端安全软件 | 深信服端点安全软件V3.0（智防客户端模块授权） | 产品是软件形态，包含管理平台和终端Agent软件；管理平台要求其操作系统为64位的Centos7或ubuntu操作系统；Agent软件支持32位和64位的Windows系统和64位的Linux系统。管理平台采用软件包方式提供安装，安装后其中必须具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性。本次开通300个电脑端授权。无需安装任何其他软件和专用设备硬件，采用基于X86服务器或虚拟服务器即可完成平台部署；终端Agent软件可以通过软件安装或虚拟机模板的方式进行安装。支持终端资产盘点管理，平台支持自动区分网内终端为业务终端或用户终端，也支持终端组的新增、修改、删除和终端分组切换；支持自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端Agent版本、病毒库版本、最近登录时间、最近登录的用户名；支持录入终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，做到准确定位。支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、已失陷、高可疑、低可疑，支持下钻到对应的终端列表；支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量、WebShell后门数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表；支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量；支持以安全策略模板方式对指定终端/终端组快速部署安全策略，安全策略支持缺省默认模板和自定义模板等多种格式；具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。支持极速、均衡、低耗三种扫描模式，以控制扫描时对业务系统CPU资源的占用；支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。支持客户端安装结束后录入终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，并同步更新到控制中心；支持多种病毒查杀模式，包括：快速查杀、全盘查杀和自定义查杀；支持多种杀毒性能配置，包括：极速模式、均衡模式和低耗模式，以控制杀毒扫描时对业务系统CPU资源的占用；客户端的防退出和防卸载功能：卸载或退出客户端时需要输入管理员在控制中心配置的密码，避免非管理员无故卸载或退出客户端，造成终端安全真空。支持对来自Internet、E-mail或是光盘、移动存储、网络等各种入口渠道病毒进行实时检测；支持单个攻击源和分布式攻击源的暴力破解检测；支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置；支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史；支持对指定终端/终端组进行终端基线合规性检查，对不合规的检查项提供设置建议；针对Windows系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范；支持windows系统永恒之蓝漏洞（MS17-010）的检测；针对Linux系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范；支持对业务系统配置微隔离策略规则；支持安全态势感知平台下发禁止指定终端所有目标IP的入站或出站策略；支持策略为自定义设置的目标IP或IP范围、端口或端口范围；可以实现被感染终端IP封锁隔离，防止风险扩展。支持多台防火墙通过配置终端检测响应管理平台IP地址实现与EDR平台的联动，实现端网安全联动；支持管理员在下一代防火墙平台对其下发的查杀任务中查杀出来的病毒进行处置；支持基于威胁情报的病毒md5值的全网终端定位搜索，适用于对变种流行病毒的快速响应，快速确认全网终端是否感染；需配套提供同品牌不低于20套VDI桌面云授权及瘦终端，满足终端安全软件统一部署； | 套 | 300 | 245 | 73500 | 广东.深圳深信服科技股份有限公司 |
| 21 | 等保一体机 | SdSec-1000-A600 | 产品为软硬一体化形态；支持部署于通用X86服务器平台，无需绑定底层操作系统即可搭建；平台支持旁路引流及网关模式部署平台支持下一代防火墙、SSL VPN、上网行为管理、数据库审计、运维审计、日志审计、主机杀毒等安全功能组件平台支持用户进行安全拓扑的编排，可根据实际业务环境定义业务安全区域，简化运维管理；平台具备业务风险可视化界面，包括业务风险状况、风险事件状态及整体安全态势等，针对单独业务系统可提供业务风险提供业务状态及业务风险分析评估；平台支持关键安全组件双机功能，保障安全组件高可用；对虚拟防火墙分布式策略管控，策略内容可以针对IP、MAC地址或通讯端口，可防护所有基于IP五元组（TCP、 UDP、 ICMP 等）；提供基本的安全防御，包括但不限于4-7层访问控制、入侵防御、病毒过滤、网页防篡改等安全功能；对所有应用系统进行漏洞的攻击防护，包括防跨站、防SQL注入、防篡改、防木马、防黑客攻击等；支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面；支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证；提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作；支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限；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；支持把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽，以及单用户最高带宽属性对外网IP有效；支持基于访问行为的目标IP/IP组实现带宽划分与分配；支持多种事件进行邮件告警，包括攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库；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，白名单内容包括以下4个维度:SQL模板、业务系统、URL地址及数据库条件；支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间；内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色；针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息；系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段；对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义；支持多级系统中心，并能够对每级系统中心及所属客户端进行统一升级、统一管理；支持全网统一自动升级，不需要人为干涉，支持病毒库无缝主动式智能升级，增量升级，以减少升级时带来的网络流量；支持多种病毒报警方式，包括发送到管理控制台、声音报警、发送邮件、显示消息框、报告给上级系统中心等；提供公安部颁发的云安全服务平台销售许可证； | 台 | 1 | 273000 | 273000 | 广东.深圳深信服科技股份有限公司 |
| 22 | 业务系统测评 | 拓尔康集成 | His、lis、pacs主业务系统定级、备案、二级等保测评费用 | 套 | 1 | 330000 | 330000 | 河南.郑州河南拓尔康医药科技有限公司 |
| 合计：大写：贰佰玖拾捌万玖仟玖佰捌拾元整 小写：2989980.00元 |