开标一览表

项目编号：JZFCG-G2021053号

项目名称：许昌市东城区科技和工业信息化局东城区电子政务外网等保测评整改项目(不见面开标)　　单位：元（人民币）

包号	项目名称	投标报价	交付日期	备注
第一包	许昌市东城区科技和工业信息化局东城区电子政务外网等保测评整改项目(不见面开标)	大写：捌拾伍万柒仟陆佰叁拾元整　　小写：857630	合同签订后45日历天	/
…				

投标人名称：许昌锐迈电子技术有限公司（公章）：

日期：　2021年　11　月　11　日

注：1、交付日期指完成该项目的最终时间（日历天）。

2、如招标公告明确项目交付日期以年为单位，本表应填写完成该项目的年限。

四、符合性审查证明材料

4.1 投标分项报价表

项目编号：JZFCG-G2021053 号

项目名称：许昌市东城区科技和工业信息化局东城区电子政务外网等保测评整改项目(不见面开标)

序号	名称	品牌、规格型号	技术参数	单位	数量	单价	总价	厂家
1	防病毒网关	深信服 AF-1000-B1510	所投产品涵盖以下功能： 性能参数：网络层吞吐量：6G，应用层吞吐量：2G，并发连接数：180 万，新建连接数：6 万，SSL VPN 用户数（单独购买）：20，SSL VPN 最大用户数（单独购买）：80，SSL VPN 最大理论加密流量（单独购买）：300M，IPSec VPN 最大接入数：1000，IPSec VPN 吞吐量：160M。含防火墙软件基础级、网关杀毒升级许可、网关杀毒模块。 硬件参数：规格：1U，内存大小：4G，硬盘容量：64G SSD，电源：单电源，接口：6 个电口+4 个光口 SFP。 提供 IPS、L7 层多类威胁的检测和防护，有效应对系统漏洞攻击和未知威胁攻击。 产品支持旁路部署、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 产品支持链路聚合功能，可以将多个物理链路组合	台	1	60610	60610	深信服科技股份有限公司

			成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。 产品支持支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能，支持一对一、一对多、多对一等形式的 NAT。 产品支持 IPSec VPN 智能选路功能，根据线路质量实现自动链路切换。 产品支持对不少于 9880 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 产品支持异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、Smurf、Land、WinNuke 等攻击类型。 产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。 产品支持僵尸主机检测功能，产品预定义特征库超过 110 万种，可识别主机的异常外联行为。 产品支持对请求报文头的 X-Forwarded-For 字段检测，并对非法源 IP 进行日志记录和临时封锁。 产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理。 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险					

			等内容，提供安全策略优化建议。					
2	全网行为管理	深信服 AC-1000-B1200	所投产品涵盖以下功能： 性能参数：网络层吞吐量：3G，应用层吞吐量：300Mb，带宽性能：200Mb，IPSEC VPN 加密性能：50Mb，支持用户数：800，准入终端数：500，包转发率：27Kpps，每秒新建连接数：1600，最大并发连接数：80000。 硬件参数：规格：1U，内存大小：4G，硬盘容量：128G SSD，电源：单电源，接口：4千兆电口；含全网行为管理系统软件、终端接入安全软件。 实现全网资产、身份、行为可视可控，智能感知内部威胁风险，帮助用户构建有效防御体系。 支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能； 支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6； 支持 DNS 透明代理，能够基于用户、域名、目标 DNS，指定代理策略生效，代理策略可以设置为：重定向至 DNS 服务器、解析为 IP、丢弃、重定向至制定线路； 支持首页分析显示接入用户人数、终端类型、认证方式、资产类型分布、所设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况； 支持针对内网用户的 web	台	1	50070	50070	深信服科技股份有限公司

			访问质量进行检测，对整体网络提供清晰的整体网络质量评级； 支持认证前使用某个组织结构的上网权限，保障未认证用户可使用开放网络资源； 支持 radius、AD、POP3、Proxy 、 PPPOE 、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户，指定 IP 段的用户必须使用单点登录； 支持哑终端通过 MAC 认证的方式接入网络，必须支持在终端管理列表批量绑定设备IP/MAC快捷放通入网； 支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护IP表的工作量； 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别，至少识别不少于 10 种移动终端型号； 支持检查终端是否更新 Windows 重要补丁、指定补丁，对不满足检查要求的终端可弹窗提示； 支持检查终端是否超级管理员账号上线，对不满足检查要求的终端禁止上网； 支持灵活调用管理员编写脚本或程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网； 支持检查终端是否使用双网卡，对不满足检查要求的终端强制断网，支持向					

			管理员告警，并弹窗提示用户； 支持对终端上U盘和移动硬盘接入设置可读写、拒绝、可读、告警；					
3	OSM-堡垒机	启明星辰 天玥运维安全网关 OSM V6.0	所投产品涵盖以下功能： 1U 机架式软硬一体设备，专用硬件平台和安全操作系统，6 个千兆电口，1 个 Console 管理口，存储容量 1TB，单电源，2 个扩展槽。包含 50 个授权对象.最大可扩展资产数：1500，图形运维最大并发数：200，字符运维最大并发数：800。 支持设定周期性改密计划，批量修改资源密码。 支持手动改密，修改指定资源的账号密码。 ★具备对数据库进行改密包括 Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE 、Mssql(2005,2008,2012)。 实现数据库命令级审计，支持的数据库类型包括：Oracle（支持 ORACLE RAC）、SQL Server、IBM DB2,Sybase,IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担。 支持扫描本地运维工具并进行配置检查，简化运维人员使用配置过程 支持运维人员在苹果（MacBook、iPad、iPhone 上和安卓终端以 SSH/RDP 客户菜单模式登录堡垒机并进行运维操作，运维时支设置运维命令，在 Linux 类主机自动执行并返回结果，供用户查看、下载。提供功能界面并加盖印章证明。 支持改密结果自动发送到	台	1	80500	80500	北京启明星辰信息安全技术有限公司

			指定改密计划的管理员邮箱或发送到 FTP 服务器；密码文件加密保存，需要专用查看工具查看，以保证安全性。提供功能界面并加盖印章证明。 运维用户可以设置自动运维操作定时/周期执行，实现网络设备（华为、思科、h3c）配置的自动备份、供用户查看、下载。 支持 web 页面或数据库防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址。 支持管理员通过 WEB 界面自定义上传用户手册，保证使用手册及时更新 功能描述：运维安全管理系统（堡垒机 OSM），将运维人员离散维护主机及网络设备的行为统一到该平台进行，加强对系统安全以及运维的控制力。一方面通过集中运维，减少因离散操作导致的失误，提高工作效率，如新的安全策略在主机上的统一应用等；另一方面通过对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作行为，便于进行事后的审查与取证。包含运维安全管理系统软件、堡垒主机内控管理平台。					
4	安全态势感知	深信服 SIP-1000-F600	所投产品涵盖以下功能： 性能参数：存储容量：14.4T，在带宽性能 1Gbps 时存储时长：900 天/1Gbps。 硬件参数：内存：4*16GB，系统盘：1*128GB，数据盘：4*4TB，标配盘位数：8，电源：单电源，接口：4 千兆电口；含安全感知平	台	1	203850	203850	深信服科技股份有

			台软件、安全感知系统平台特征库软件。 集检测、可视、响应处置于一体的大数据安全分析平台，让安全可感知、易运营。产品以大数据分析为核心，结合威胁情报、UEBA、机器学习、失陷主机检测、大数据关联分析、NTA流量分析、可视化等技术，对全网安全进行可视。 核心能力：（1）海量多源异构的数据分析（2）全网资产与脆弱性精细管控（3）AI精细发现高级威胁（4）全过程溯源分析举证（5）事件自动化闭环处置（6）安全态势全方位感知（7）量化安全运营工作绩效 支持不同安全视角展示16个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等。 支持对安全事件、外部攻击者等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。 支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息并具备完整的功能展示。 支持基于多维度分支管理，最多可至15层嵌套，支持资产全生命周期自动管理，包括资产自动发现、多级资产[illegible]审核、资产离线风险识别、资产退库、资产数据更新、责任人管理机制等。 弱密码检测技术基于UEBA学习技术（无监督自我学					限公司

			习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，可实时自动生成学习到的登陆成功规则。 弱密码检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，可实时自动生成学习到的登陆成功规则。 支持230+情报源，DNS信誉库总量超过2000万，其中黑名单100万，URL信誉库总量超过1亿，其中URL分类库3000万，文件样本库总量超过10亿，每日新增200万。拥有国内领先的企业级域名信誉库，拥有国内最全最准确的URL分类库。支持威胁情报关联分析，内置威胁情报数量不少于170W。 支持SIEM日志关联分析结果的可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供每一台设备专项分析的页面。如防火墙外部攻击告警分析、VPN账号异常登录分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 支持安全检测日志、审计					

			日志、第三方日志存储：日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS 攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet 等。 支持利用 EBA 技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。共含有 27 种异常行为学习模型；并支持用户对 EBA 基线进行自定义调整，优化模型。 支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击 IP、攻击地址、攻击目标和目标手法。 支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。 可快速生成月度、季度、年度 PPT 报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，帮助用户高效汇报，体现安全工作价值。 告警方式支持邮件告警、短信、微信告警方式。					
5	威胁检测探针	深信服 STA-100-B1500	所投产品需具备以下功能： 本次采购的安全态势感知平台的配套组件，必须与本次采购的安全态势感知平台同品牌。 吞吐性能：0.5Gbps。规格：1U，内存：4G，硬盘：64G SSD，电源：单电源，接口：6 千兆电口；含潜伏威胁探针系统软件、安全感知系统探针特征库软件；提供	台	2	42550	85100	深信服科技股份有

			三年规则库升级及硬件质保。 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 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。 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击,Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测。 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等。 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接,IRC通信等僵尸网络行为检测。 支持5种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 支持终端访问检测日志，包括正常访问、风险访问、违规访问。 内置URL库,IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。					限公司

			支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。					
6	操作电脑	主机：H3C X5-020t 1096 显示器：H3C M4-241F	所投产品涵盖以下功能： i7 10700/16GB/512GB/集显/23.8英寸	台	2	5600	11200	新华三技术有限公司
7	安全网关三年授权	H3C LIS-M9000-IPS-3Y LIS-M9000-AV-3Y LIS-M9000-ACG-3Y	所投产品涵盖以下功能： IPS，AV，ACG三年授权（M9006）	套	1	201300	201300	新华三技术有限公司
8	终端杀毒	深信服 EDR	所投产品涵盖以下功能： 产品可以纯软件交付，包含PC端授权。 单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器的客户端软件；采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能 。 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危	个	500	290	145000	深信服科技股份有限公司

			漏洞及其各自影响的终端数量。 支持按“最近 7 天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数 。 支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组。 支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示 支持对zip，rar，jar，cab，7z等常见压缩文件的扫描检测，支持压缩文件层级进行策略配置，最大可配置检查10层压缩文件。 支持客户端防卸载，客户端卸载需要输入密码才能卸载，避免非管理员卸载终端，造成终端安全真空 。 支持展示终端检测到的WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型,文件名,文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描下载、发现WebShell文件，可自动隔离或保留报不隔离 支持基于IP（网）、服务器角色维度进行配置和设置，并且支持对配置项的备份以及恢复操作。 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） 流量线详情支持展示该流					

			量线对应的控制策略：图形化显示服务器间流量关系，包括访问详情、流量趋势等 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置。 支持基于 IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作。 支持管理员在同厂商的网络防火墙管理界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散					
9	系统集成	锐远实施	所投产品涵盖以下功能： 设备整体安装、调试服务。	次	1	20000	20000	许昌锐远电子技术有限公司
合　计		大写：贰拾伍万柒仟陆佰叁拾元整 小写：257630元						

投标人名称（并加盖公章）：许昌锐远电子技术有限公司