**宁波市江北区财政局亚信防病墙网络版软件**

**与网络安全设备规则库升级服务询价项目**

本项目询价采购内容主要由“亚信防病墙网络版软件”与“网络安全设备规则库”升级服务费2部分组成，就以下内容进行询价，请各供应商予以报价：

1. 亚信防毒墙网络版软件主要报价内容：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **产品名称** | **型号/规格** | **版本** | **产品描述/支持平台** | **用户数** | **单价** | **续保费用/年** | **备注** |
| 亚信安全防毒墙网络版软件 V16.0 | 客户机防护 | V16.0 | 防病毒软件（客户机版）解决方案。抵御病毒、间谍软件、网络钓鱼和其它灰色软件的攻击。同时提供集中的管理、监控、更新和部署等功能，并具备主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护等能力。支持平台：Windows XP/7/8/8.1/10/11 | 135 | 　 | 　 | 续费 |
|
|
|
|
| 亚信安全防毒墙网络版软件 V16.0 | 服务器防护  | V16.0 | 防病毒软件服务器版解决方案。抵御病毒、间谍软件、网络钓鱼和其它灰色软件的攻击。提供集中的管理、监控、更新和部署等功能，并具备主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护等能力。**支持：**Windows Server 2008/2012/2016/2019 | 20 | 　 | 　 | 续费 |
| **产品名称** | **型号/规格** | **版本** | **功能描述**  | **用户数** | **单价** | **续保费用/年** | **备注** |
|  |  |  |  |  |  |  |  |
| 亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0 | 安全防护系统管理平台 | 管理中心必选 | 提供服务器、虚拟机、私有云、公有云的统一安全防护，实现集中的管理、监控、更新和部署等能力，集中管理客户端防病毒、入侵检测、虚拟补丁、防火墙、Web信誉、资产管理、日志审计等功能 ，帮助实现企业混合云、跨云的安全管理；资产管理可记录主机信息、进程信息、已安装软件信息、账号信息等，支持主流windows和Linux，须有代理部署；日志审计可集中服务器日志，并对日志进行智能分析、依据系统事件与配置规则比对报警，须有代理部署； | 1 | 　 | 　 | 续费 |
| 亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0 | 虚拟补丁包 | 组合包 | 有代理防病毒模块+有代理深度包检测模块，不含管理中心，防病毒模块：具备防病毒保护, Web 信誉度检测功能，须有代理部署；深度包检测模块：具备入侵检测与防御、虚拟补丁、防火墙功能，须有代理部署； | 10 | 　 | 　 | 续费 |
| 亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0 | 有代理深度包检测模块 | 可选模块  | 入侵检测、虚拟补丁、防火墙功能 | 10 | 　 | 　 | 新购 |

以上模块均包括3年规则库升级服务费用。

二、网络安全设备规则库升级服务，报价投标响应内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **指标** | **指标项** | **投标响应** | **报价** |
| 安全设备原厂硬件及规则库维保 | 1. 入侵防御系统(IPS) 天融信TopIDP2000(TI-2230-IDP) 1台

提供一年原厂硬件维保及规则库升级服务； |  |  |
| 2. 天融信政务外网防火墙 天融信NGFW4000-UF(TG-51003) 1台提供一年原厂硬件维保及规则库升级服务； |  |  |
| 3. 天融信政务外网防火墙备天融信NGFW4000-UF(TG-5130) 1台 提供一年原厂硬件维保及规则库升级服务； |  |  |
| 4.思福迪日志审计系统 LogBase-A1600 2台 提供一年原厂硬件维保及规则库升级服务； |  |  |
| 5. 上网行为管理设备 AC12.0.41.115 Build20200116 1台 提供一年原厂硬件维保及规则库升级服务； |  |  |
| 6. 安恒明御WEB防火墙 1台 提供一年原厂硬件维保及规则库升级服务； |  |  |
| 7. 内网核心交换机 H3C LS-7506E 1台 提供一年硬件维保服务； |  |  |
| 8. 内网核心交换机 H3C LS-7506E-S 1台 提供一年硬件维保服务； |  |  |
| 9. 服务器汇聚交换机华为S5700-52C-EI 1台 提供一年硬件维保服务； |  |  |
| 10. 内网楼层汇聚交换机 H3C S5120-28C-EI 1台 提供一年硬件维保服务。 |  |  |
| 合 计 |  |

三、亚信防毒墙网络版软件主要技术指标参数如下：

1. 亚信防毒墙网络版软件详细参数（标有“▲”的为必须满足项）：

|  |  |
| --- | --- |
| **指标项** | **亚信防毒墙网络版软件参数** |
| 基本参数 | 防病毒软件,提供抵御病毒、间谍软件、网络钓鱼和其它灰色软件的功能，同时提供集中的管理、监控、更新和部署等功能，并具备主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护等能力。客户机版支持平台：Windows XP/7/8/8.1/10/11，服务器版支持平台：Windows Server 2008/2012/2016/2019。其中客户机防护授权≥130个，服务器防护授权≥20个 |
| 管理 | 产品管理端需要提供工具集，针对管理端、客户端提供用于自身配置的工具。同时WEB界面，需要提供有关如何使用工具的帮助信息 |
| ▲产品需要支持根据IP地址（包含IPv6）、操作系统、在线状态、处理器结构、病毒码版本、防火墙状态、爆发阻止状态等条件的组合搜索出符合条件的终端进行管理； |
| 产品支持管理用户角色，支持用户权限的灵活设定，可以让不同用户访问在管理界面上访问不同的客户端及配置管理界面； |
| 为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时CPU占用比例，分高、中、低三个级别。低占比下不得超过CPU使用率的20%； |
| 安全防护 | ▲对于文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类 |
| ▲扫描策略必须包含清除、隔离、删除处理措施，同时还应具备对病毒/恶意软件的不予处理（锁定）、监控、更名等措施，以保证对于文件多种处理的可选择性； |
| 支持云安全扫描和传统病毒码扫描两种运行方式； |
| 支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施； |
| 产品需要支持主机入侵检测系统； |
| ▲支持针对终端根据基于源IP（支持IPv6）、目的IP（支持IPv6）、源端口、目的端口、应用程序及注册表项，出站、入站等进行安全配置； |
| 移动设备防护 | ▲对非存储设备，如bluetooth、IEEE 1394接口、红外设备、调制解调器、PCMCIA卡等进行分项权限设置； |
| 可对插入移动存储引导区或者移动设备的所有文件进行扫描设置； |
| web防护 | 具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新 |
| 客户端 | 客户端应该具备组件更新功能，同时可以查看所有引擎、病毒码版本以及更新时间等信息； |
| ▲客户端提供本地语言自适应功能，可以根据客户端系统语言变更操作语言，至少支持中文、英文、日语、韩语等四种语言； |
| ▲提供首选IP功能，针对复杂网络环境，可以选择优先使用的注册到服务器的协议； |
| 爆发阻止 | 具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击； |
| 漏洞弱点扫描 | ▲支持CVE漏洞弱点扫描功能，及时防护经由网页/电子邮件下载的文档漏洞利用(CVE) |
| 勒索软件防护 | ▲必须具备防勒索软件防护功能，管理界面提供配置项； |
| 机器学习 | ▲必须具备防勒索软件防护功能，管理界面提供配置项； |
| 升级功能 | ▲客户端更新实现并发更新数量的控制，同时可以按不同时间段进行更新并发限制； |
| 可以设置边缘中继服务器，可利用中继服务器实现样本提交、日志提交、客户端状态更新等功能； |
| 支持组件更新还原功能，支持扫描引擎和病毒码回滚机制； |
| 可疑文件提交 | 具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，并可接收； |
| 补丁防护接口 | 产品需具备补丁防护接口，必要时可外接补丁防护产品，提供漏洞防护能力。同时补丁防护及补丁更新功能不能和杀毒软件一体化，避免和第三方桌面管理软件冲突。 |
| ▲厂商资质 | ▲厂商通过CMMI5认证 |
| ▲厂商通过ISO27001信息安全管理体系认证 |

1. 亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0技术参数与要求（标有“▲”的为必须满足项）：

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0技术参数及要求** |
| **1** | ▲基本要求 | 服务器安全防护，提供服务器、虚拟机、私有云、公有云的统一安全防护，实现集中的管理、监控、更新和部署等能力，集中管理客户端防病毒、入侵检测、虚拟补丁、防火墙、Web信誉等功能；客户端授权数≥10。 |
| 2 | 控制台要求 | 1.提供一个管理控制台与虚拟化平台无缝对接以及管理虚拟化防护产品2. 控制台支持部署在Windows或Linux服务器上，支持集群化部署，满足高可用3. 产品有代理模式下支持主流的虚拟化平台，支持Windows、RHEL、Centos、Oracle Linux、SUSE、Ubuntu、Debian等多种操作系统▲4. 产品无代理防病毒，DPI（HIPS）功能支持如下虚拟化平台：- VMware NSX-V/NSX-T- 华为FusionSphere-华三CAS （3.0, 5.0）- 产品支持以上虚拟化平台的统一平台管理**▲**5.无代理部署同时支持宿主机及虚拟机的防护 |
| 3 | 多种方式添加被保护的计算机 | 1. 添加本地网络计算机2. 从Microsoft Active Directory添加计算机组，可以从任何基于LDAP的目录服务导入计算机组3. 添加Virtual Center4. 添加在VMware vCloud上托管的虚拟机5. 添加AWS云账户6. 添加Microsoft Azure云账户7. 将客户端程序安装到Amazon Machine Image（AMI）基于的实例上8. 使用部署脚本来保护大量的计算机，进行自动安装和激活客户端。 |
| 4 | 基本防护功能 | 1. AV，防恶意程序。 |
| 2. Web信誉，可以阻止用户访问恶意Web站点。 |
| 3. 完整性监控，实时检测并报告对文件和系统注册表的恶意及意外更改。 |
| 4. 防火墙，减少物理和虚拟服务器的攻击面。 |
| 5. 入侵防御（DPI），在已知漏洞修复之前，屏蔽漏洞以免遭受无限制的入侵。 |
| 6.日志审查，捕获和分析系统日志，为组织提供审计证据，可以将日志审计配置为将可疑事件转发到SIEM系统。 |
| 5 | 防恶意软件功能 | 扫描模式 | 支持本地扫描和云安全扫描，具备本地病毒码和云端病毒码，支持实时扫描，预设扫描和、手动扫描和快速扫描 |
| 预测性机器学习 | 产品支持通过预测性机器学习为未知威胁和零日攻击提供增强的恶意软件防护，预测性机器学习使用先进的机器学习技术关联威胁信息并执行深入的文件分析，以通过数字DNA指纹识别，API映射和其他文件功能检测新出现的安全风险。 |
| 智能保护功能  | 产品需支持防病毒IntelliTrap功能 ，防止病毒制造者经常试图通过实时压缩算法来避开病毒过滤，最大压缩级别:1-6，要提取的文件的最大数量:10，支持可配置 |
| 扫描嵌入式Microsoft Office对象 | 产品需支持扫描嵌入式Microsoft Office对象，防止某些Microsoft Office版本使用对象链接和嵌入（OLE）将文件和其他对象插入到Office文件中。 |
| 扫描网络目录及网盘 | 扫描驻留在网络文件系统（NFS），服务器消息块（SMB）或通用 Internet文件系统（CIFS）中的网络共享和映射网络驱动器中的文件和文件夹（仅限实时扫描）支持提供相关扫描接口与用户私有文件网盘进行集成并进行病毒扫描 |
| 恶意软件类型 | 1、病毒（COM 和 EXE、宏病毒、引导扇区病毒）2、木马（特洛伊木马、后门程序、蠕虫病毒、网络病毒、Rootkit）3、Packer（压缩和加密的可执行程序）4、间谍软件/灰色软件（间谍软件、拨号程序、黑客工具、广告程序、Cookie、按键记录软件）5、Cookie（SQL 注入和 XSS 漏洞）6、其他威胁（未在任何恶意软件类型下归类的恶意软件，例如笑话程序）7、可能的恶意软件（看似可疑的文件，但不能被归类为特定的恶意软件变体） |
| 恶意行为监控功能 | 支持恶意行为监控功能，支持检测可疑活动和未经授权的更改 |
| 勒索行为监控功能 | ▲可以防止文档遭受未授权的加密或修改。 |
| 病毒处理措施 | 对病毒的处理措施支持：清除、删除、拒绝访问、隔离、不予处理，系统针对不同的病毒类型提供默认配置，同时支持用户自定义。 |
| 扫描配置 | 病毒扫描启动后，支持在不关闭安全虚拟机或影响整体病毒防护功能的情况下，进行暂停或终止扫描的操作 |
| 扫描资源优化 | 1.手动扫描支持CPU资源使用率调整，当CPU超过阈值时暂停或者减少CPU使用率。可以设置CPU占用不高于50%或者20%。2.防病毒扫描支持VM扫描缓存3.防病毒扫描支持多线程处理 |
| 新型病毒查杀 | ▲支持和外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁，并处理。 |
| 6 | 入侵防御及虚拟补丁 | SSL支持 | 入侵防御需支持SSL配置，对于入侵防御功能能够识别https流量，从而对计算机进行防护；支持包括SSL3.0、TLS1.0、TLS1.1、TLS1.2。支持15种及以上的密码套件，凭证可用PKCS#12或PEM格式导入，Windows计算机可直接使用CryptoAPI |
| 智能推荐扫描 | 产品支持推荐扫描，根据不同计算机的扫描结果自动下发对应的入侵防御规则 |
| 扫描引擎 | HIPS采用独立的引擎来处理所有规则 |
| 定制规则 | ▲支持快速定制入侵防御规则。 |
| 无代理支持 | 无代理运行,必须可以同时保护操作系统和应用服务（数据库，Web，DHCP等），在服务器尚无安装补丁前，提供针对此补丁攻击的防护能力。 |
| 检测模式 | 提供桥接模式和分接两种模式两种检测模式。 |
| 详细日志信息 | 提供包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息，并在事件发生时，立即自动通知管理员。 |
| 7 | 防火墙 | 防火墙 | 可集中控管防火墙策略，策略定制可以针对IP,Mac地址或通讯端口，可保护所有基于IP通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等） |
| 无代理支持 | ▲该功能模块支持无代理部署，支持与NSX集成下发防火墙策略 |
| NSX支持 | ▲支持NSX安全标签，一旦检测到恶意威胁，可将NSX安全标记应用于受保护的VM，NSX安全标记可与NSX Service Composer一起使用，以自动执行某些任务，例如隔离受感染的VM。 |
| 8 | 应用程序控制 | 产品具有应用程序控制功能，应用程序控制模块监控变化，一旦启用应用程序控制，将会记录所有软件更改，并创建事件。 |
| 9 | 扩展模块 | 完整性监控 | 产品应支持功能模块扩展，必要时可提供完整性监控模块 |
| 支持完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改. |
| 日志审计 | 产品应支持功能模块扩展，必要时可提供日志审计模块 |
| 支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件  |
| 协助遵循规范(PCI DSS 10.6) 优化识别隐藏在多个日志项下的重要安全事件 |
| 将事件转至SIEM系统或中央日志服务器，做关联性分析、报告和归档； |
| 侦测可疑行为、收集数据中心的安全事件和管理操作，并使用OSSEC 语法来建立高级规则。 |
| 10 |  数据库支持 | 产品自身使用的数据库必须采用以下外挂企业级数据库 |
| - SQL Server |
| - Oracle |
| - Postgresql |
| 11 | 病毒库更新方法 | 1. 产品需要支持更新的多级部署，分流冗余节省带宽，更新速度快 |
| 2. 产品安全升级需要支持Pattern回退 |
| 3. 产品需要支持设置定时任务检查软件升级和安全升级 |
| 4. 产品需要支持自定义升级某一个或者某一些客户端的病毒码，而不是只能一次升级所有客户端的病毒码。 |
| 12 | 多租户支持 | 1. 管理中心支持多租户，可按需开启 |
| 2. 支持不同租户widget、事件、安全策略、管理、日志文件相互隔离 |
| 3. 支持不同租户计算机、终端、安全配置相互隔离 |
| 13 | 运维管理 | 产品需要支持不少于100种异常监控和告警规则，保障提供给管理员详细的日志告警。 |
| 支持虚拟化环境的WMotion，Storage VMotion以及HA集成，能够自动感知和保护虚拟环境的变更和迁移。 |
| 当产品出现问题时，管理员可以通过控制台快速诊断界面获取相关组件的debug日志，进行问题定位和分析；能够针对疑似问题虚拟机行故障排查，将系统信息，运行状态，驱动日志等状态信息导出 |
| 14 | 系统事件 | 1. 产品应支持多种系统事件记录，记录包括管理员、审计员、系统等所有审计日志。 |
| 2. 系统事件支持标记功能，根据条件自动标记事件，并可以根据标记展示和过滤时间，标记条件包括事件、事件ID和级别、目标、操作者、管理中心和事件起源. |
| 3. 产品应提供至少19个报表模板，覆盖所有功能，包括数量排名、图形展示。 |
| 4.可指定任意虚拟机/终端、计算机组、策略、时间段和标记进行报表生成，支持定义报表保密级别，支持生成报表加密. |
| 15 | ▲产品及厂商资质 | ▲产品必须和VMware Operation Manager集成 |
| ▲产品获得公安部计算机信息系统安全产品销售许可证 |
| ▲产品接口需与VMware 产品接口兼容 |
| ▲厂商通过CMMI5认证 |
| ▲厂商具备信息技术服务运行维护标准三级资质（ITSS） |