# 网络安全设备维保
# 服务合同

项目编号：LBZC2026-J3-990012-GXHY

项目名称：网络安全设备维保

采购人（甲方）：来宾市人民医院

供应商（乙方）：广西勇武科技有限公司

签订地点：广西来宾市

签订日期：2026年4月16日

# 网络安全设备维保

采购人（甲方）__来宾市人民医院__
供应商（乙方）__广西勇武科技有限公司__

根据《中华人民共和国政府采购法》《中华人民共和国民法典》等法律、法规规定，按照采购文件规定条款和成交供应商承诺，甲乙双方签订本合同。

**第一条　合同标的**

1.供货一览表

| 序号 | 服务名称 | 数　量 | 单位 | 单　价（元） | 金　额(元) |
|---|---|---|---|---|---|
| 1 | 网络安全设备维保 | 3 | 年 | ¥316666.66 | ¥950000.00 |
| 人民币合计金额（大写）　玖拾伍万元整 | | | | （小写）¥950000.00 元 | |

备注：供货一览表明细见附件。

2.合同合计金额包括但不限于满足本次竞标全部采购需求所应提供的服务，以及伴随的货物和工程(如有)的价格；包含竞标服务、货物、工程的成本、运输(含 保险)、安装(如有)、调试、检验、技术服务、培训、税费等所有费用。如采购文件对其另有规定的，从其规定。

3.服务范围

（1）硬件维保：故障检测、维修、更换（核心部件板、电源等关键部件,原则上48小时内应到位）；

（2）软件及规则库升级：漏洞库、病毒库、威胁情报库等至少每日自动更新，紧急高危漏洞24小时内完成升级；

（3）安全服务：每季度至少1次现场巡检（含设备运行状态检测、安全策略审计、日志分析），每季度1次网络安全风险评估；

（4）应急响应：7×24小时热线支持，重大安全事件（如黑客攻击、数据泄露风险）2小时内到达现场处置。

**第二条　质量要求**

乙方所提供的服务及服务内容必须与响应文件承诺相一致，有国家强制性标准的，还必须符合国家强制性标准的规定，没有国家强制性标准但有其他强制性标准的，必须符合其他强制性标准的规定。

**第三条　权利和义务**

1. 乙方应保证所提供服务在使用时不会侵犯任何第三方的专利权、商标权、工业设计权等知识产权及其他合法权利，且所有权、处分权等没有受到任何限制。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或者任何合同条文、规格、计划、图纸、样品或者资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方的保密义务持续有效，不因为本合同履行终止、解除或者无效而解除。

3. 乙方在服务过程中不得采集、存储、传输甲方医疗数据，仅可在甲方授权范围内访问设备日志（日志访问需留存操作记录）；乙方及其工作人员需签署《数据保密承诺书》，对接触的甲方商业秘密、医疗数据承担终身保密义务；若因乙方原因导致数据泄露或滥用，乙方需承担由此造成的全部损失（包括但不限于行政处罚、民事赔偿等），甲方有权解除合同并要求支付合同总金额20%的违约金。

**第四条　交付和交付签收**

1. 服务期：自 2026 年 04 月 01 日至 2029 年 03 月 31 日；交付地点：来宾市人民医院。

2. 乙方应按响应文件的承诺向甲方提供相应的服务，并提供所服务内容的相关技术资料。

3. 乙方提供不符合响应文件和本合同规定的服务成果，甲方有权拒绝接受。

4. 乙方完成本合同约定的阶段性服务（如设备安装调试、年度维保服务）后，应在3个工作日内书面通知甲方进行验收，甲方应

在收到通知后七个工作日内组织验收。验收标准如下：①硬件验收：设备运行无故障，核心功能（如防火墙防护、WAF 拦截、日志审计等）符合附件《供货一览表明细》约定的技术参数要求；②软件验收：规则库（漏洞库、病毒库、威胁情报库等）升级功能正常，漏洞库版本为验收当日最新稳定版，可有效检测并拦截常见网络攻击；③服务验收：应急响应时间达标（热线响应≤30 分钟，重大安全事件现场处置≤2 小时），巡检报告、运维记录等资料内容完整（含问题清单、整改措施及优化建议）；④系统稳定性：验收期间连续 72 小时无宕机，运行故障率≤0.1%（非甲方原因导致的故障除外）。甲方逾期未组织验收的，视为验收合格；验收合格后，甲乙双方应签署《验收合格单》并加盖双方单位公章（或授权代表签字），双方各执一份作为付款依据。

5.甲乙双方应按照相关验收规定、双方合同、响应文件验收。

6.甲方在初步验收或者最终验收过程中如发现乙方提供的服务成果不满足响应文件及本合同规定的，可暂缓向乙方付款，直到乙方及时完善并提交相应的服务成果且经甲方验收合格后，方可办理付款。

7.甲方验收时以书面形式提出异议的，乙方应自收到甲方书面异议后五个工作日内及时予以解决，否则甲方有权不出具服务验收合格单。

**第五条　售后服务及培训**

1.乙方应按照国家有关法律法规和本合同所附的《售后服务承诺》要求为甲方提供相应的售后服务。

2.甲方应提供必要测试条件(如场地、电源、水源等)。

3.乙方负责甲方有关人员的培训，培训次数：至少 2 次。培训时间、地点：来宾市人民医院 。

**第六条　付款方式**

本项目费用分三期支付。自合同签订之日起，甲方收到乙方开具等额、真实、合法、有效发票后的 20 个工作日内，向乙方支付第一期费用¥ 316666.00（大写：人民币叁拾壹万陆仟陆佰陆拾陆元

整），若甲方发现发票不合规，有权要求乙方在5个工作日内更换，更换期间付款期限顺延；每年度维护期满后，乙方须在10个工作日内提交系统运维报告。第二年，甲方收到上一年度运维报告及当年维保费等额、合法、真实、有效发票后20个工作日内，支付第二期费用¥ 316666.00（大写：人民币叁拾壹万陆仟陆佰陆拾陆元整）；第三年，乙方须在10个工作日内提交系统运维报告及全部运维资料，经甲方整体验收合格后，甲方收到等额、合法、真实、有效发票后20个工作日内支付第三期费用¥ 316668.00（大写：人民币叁拾壹万陆仟陆佰陆拾捌元整）。

**第七条　履约保证金**

本项目不需要缴纳履约保证金。

**第八条　税费**

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

**第九条　违约责任**

1.除不可抗力原因外，乙方没有按照合同规定履约服务的，退还甲方所支付款项。延期履约的，甲方可要求乙方支付违约金，每推迟一天按合同金额的3‰支付违约金，该违约金累计不超过合同金额的10%。

2.乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷或者诉讼，均由乙方负责交涉并承担全部责任。

3.除不可抗力原因外，甲方延期付款的，每天向乙方偿付延期款额3‰滞纳金，但滞纳金累计不得超过延期款额5%。

**第十条　不可抗力事件处理**

1.在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

**第十一条 合同争议解决**

1. 因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2. 因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权的人民法院提起诉讼。

3. 诉讼期间，本合同继续履行。

**第十二条 合同生效及其它**

1. 合同经甲乙双方法定代表人或者授权代表签字并加盖单位公章或合同章后生效。

2. 本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

**第十三条 合同的变更、终止与转让**

1. 除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或者终止。

2. 乙方不得擅自转让其应履行的合同义务。

**第十四条 签订本合同依据**

1. 成交通知书；

2. 采购文件报价表；

3. 商务条款偏离表和服务需求偏离表；

4. 技术文件；

5. 报价文件中的其他相关文件。

6. 上述合同文件互相补充和解释。如果合同文件之间存在矛盾或者不一致之处，以上述文件的排列顺序在先者为准。

**第十五条 其他**

本合同一式肆份，具有同等法律效力，甲方执叁份，乙方执壹份，本合同甲乙双方签字盖章后生效。

（本页以下为本合同的签署页，无正文）

| | |
|---|---|
| **甲方（章）来宾市人民医院** | **乙方（章）**广西勇武科技有限公司 |
| 单位地址：<br>广西来宾市盘古大道东159号 | 单位地址：<br>广西南宁市青秀区长园路1号昊壮南湖西岸2209号 |
| 法定代表人<br>（法人代表）： | 法定代表人<br>（法人代表）： |
| 经办人： | 经办人： |
| 签订日期：2026.4.16 | 签订日期：2026.4.16 |
| 单位名称：来宾市人民医院 | 单位名称：广西勇武科技有限公司 |
| 开户行：中国农业银行股份有限公司来宾市兴宾支行 | 开户行：中国建设银行南宁长湖路支行 |
| 银行账号：21084150009100181758 | 银行账号：45050160477300000567 |
| 纳税人识别号：1245130049906845XR | 纳税人识别号：91450103MA5N5X4Q2C |
| 电话/邮箱：0772-4225788、<br>Lbsrmyy_xxglk@163.com | 电话/邮箱：15676719158<br>YW91450567@126.com |

附件：

# 供货一览表明细

| 项号 | 货物名称 | 数量 | 型号 | 技术参数及性能、配置 | 单价（元） | 合价（元） | 备注 |
|---|---|---|---|---|---|---|---|
| 1 | 网神SecGate 3600防火墙系统V3.6.6.0 | 1套 | NSG5000-TG20 | 为现网在用的出口防火墙设备提供3年硬件维修及3年全功能模块升级服务，含威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。升级完成后，设备具备以下能力：<br>1.支持静态路由、动态路由、策略路由，动态路由包括RIP v1/v2/ng、OSPF、BGP等；<br>2.支持防御IP地址欺骗，可将IP与安全域关联，即指定IP或网段从特定安全域流量流入，否则视为IP地址欺骗；<br>3.支持在IPv6环境下配置安全策略、SSL解密策略等规则，实现漏洞防护、间谍软件防护、URL过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理；<br>4.产品支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢 | 35000 | 35000 | 软件 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 弃）、增强防护（TC反弹技术）等多种防护措施；<br>5.支持上传、下载、双向的文件内容过滤；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等多种常见文件类型；<br>6.支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；<br>7.支持全面的NAT转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；<br>8.★持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计（提供功能界面截图）；<br>9.持与云端联动，实现病毒云查杀、URL云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；<br>10.产品能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀，支持对最多6级的压缩文件进行解压查杀； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 11.★洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供功能界面截图）；<br>12. 支持自定义漏洞签名；可标识自定义漏洞的CVE编号或CNNVD编号；支持自定义基于TCP、UDP、HTTP协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值；支持自定义漏洞的源端口范围及目的端口范围；<br>13. ★产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供功能界面截图）。 | | | |
| 2 | 网神SecGate 3600防火墙系统V3.6.6.0 | 1套 | NSG5000-TG35 | 为现网在用的出口防火墙设备提供3年硬件维修及3年全功能模块升级服务，含威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。升级完成后，设备具备以下能力：<br>1.支持静态路由、动态路由、策略路由，动态路由包括RIP v1/v2/ng、OSPF、BGP等； | 35000 | 35000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 2.支持防御IP地址欺骗，可将IP与安全域关联，即指定IP或网段从特定安全域流量流入，否则视为IP地址欺骗；<br>3.支持在IPv6环境下配置安全策略、SSL解密策略等规则，实现漏洞防护、间谍软件防护、URL过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理；<br>4.产品支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）等多种防护措施；<br>5.支持上传、下载、双向的文件内容过滤；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等多种常见文件类型；<br>6.支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；<br>7.支持全面的NAT转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；<br>8.★持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计（提供功能界面截图）；<br>9.持与云端联动，实现病毒云查杀、URL云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；<br>10.产品能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀，支持对最多6级的压缩文件进行解压查杀；<br>11.★洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供功能界面截图）；<br>12. 支持自定义漏洞签名；可标识自定义漏洞的CVE编号或CNNVD编号；支持自定义基于TCP、UDP、HTTP协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值；支持自定义漏洞的源端口范围及目的端口范围；<br>13. ★产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 控功能，同时支持阻断或告警动作（提供功能界面截图）。 | | | |
| 3 | 奇安信网神上网行为管理与审计系统 | 1套 | NBM5310 | 为现网在用上网行为管理设备提供3年硬件维修及3年软件和规则库升级服务，升级完成后，设备具备以下能力：<br>1.可识别用户上网设备类型并作为策略条件，可将IP、IP段、VLAN作为策略条件；<br>2.★支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略（提供功能界面截图）；<br>3.可以基于IP、MAC、终端类型等多因素进行用户认证、识别；<br>4.可以为用户添加多属性，并根据用户的属性（如职位、部门、电话、邮件等）自动进行用户分类，根据分类的结果做审计、控制策略；<br>5.支持对QQ账号制定策略，对聊天、登录及文件传输的行为进行记录与控制；<br>6.提供对微信PC版进行行为和内容审计、记录发送/接受信息的微信账号；<br>7.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；不同网页被阻塞后会跳转不同的阻塞页面，支持用户完全自定义； | 34000 | 34000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 8.支持与终端杀毒软件联动，为终端杀毒软件配置推送部署策略，并能够通过终端杀毒软件获取到PC系统信息、漏洞情况，并支持对这些信息进行准入策略设置；<br>9.Webmail基于发件人、收件人、主题、内容、附件名、附件大小维度进行记录、告警；支持根据邮件主题、正文关键字进行阻塞并进行告警；<br>10.★可审计Oracle，MySql，SqlServer，PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询（提供功能界面截图）；<br>11.支持利用微信公众号进行网络接入的身份准入认证；<br>12. 支持key免审计、key免管控、key免认证三者的灵活组合；<br>13. 可识别私接主机个数，并可制定策略以私接主机个数为阀值进行封堵；同时可建立白名单，可生成日志；<br>14. 可识别用户上网设备类型，“工具”对象，并可作为策略条件；可将IP段作为“地点”对象，并可作为策略条件；<br>15. 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志；<br>16. ★支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 本地计算资源的消耗（提供功能界面截图）；<br>17. 设备具备三权分立功能，减少超管权限，帮助超管免责：超管无论如何配置都无权看审计日志；审计员必须经过超管授权，审核员确认才能看日志；审核员仅能审核审计员权限是否合法，不能看日志；<br>18. ★支持管理员账号初始密码检测，如果发现管理员未更改初始密码，能够进行提醒（提供功能界面截图）。 | | | |
| 4 | 奇安信网神上网行为管理与审计系统 | 1套 | NBM5310 | 为现网在用上网行为管理设备提供3年硬件维修及3年软件和规则库升级服务，升级完成后，设备具备以下能力：<br>1.可识别用户上网设备类型并作为策略条件，可将IP、IP段、VLAN作为策略条件；<br>2.★支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略（提供功能界面截图）；<br>3.可以基于IP、MAC、终端类型等多因素进行用户认证、识别；<br>4.可以为用户添加多属性，并根据用户的属性（如职位、部门、电话、邮件等）自动进行用户分类，根据分类的结果做审计、控制策略；<br>5.支持对QQ账号制定策略，对聊天、登录及文件传输的行为进行记录与控制； | 34000 | 34000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 6.提供对微信PC版进行行为和内容审计、记录发送/接受信息的微信账号；<br>7.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；不同网页被阻塞后会跳转不同的阻塞页面，支持用户完全自定义；<br>8.支持与终端杀毒软件联动，为终端杀毒软件配置推送部署策略，并能够通过终端杀毒软件获取到PC系统信息、漏洞情况，并支持对这些信息进行准入策略设置；<br>9.Webmail基于发件人、收件人、主题、内容、附件名、附件大小维度进行记录、告警；支持根据邮件主题、正文关键字进行阻塞并进行告警；<br>10.★可审计Oracle，MySql，SqlServer，PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询（提供功能界面截图）；<br>11.支持利用微信公众号进行网络接入的身份准入认证；<br>12. 支持key免审计、key免管控、key免认证三者的灵活组合；<br>13. 可识别私接主机个数，并可制定策略以私接主机个数为阀值进行封堵；同时可建立白名单，可生成日志； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 14. 可识别用户上网设备类型，“工具”对象，并可作为策略条件；可将IP段作为“地点”对象，并可作为策略条件；<br>15. 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志；<br>16. ★支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗（提供功能界面截图）；<br>17. 设备具备三权分立功能，减少超管权限，帮助超管免责：超管无论如何配置都无权看审计日志；审计员必须经过超管授权，审核员确认才能看日志；审核员仅能审核审计员权限是否合法，不能看日志；<br>18. ★支持管理员账号初始密码检测，如果发现管理员未更改初始密码，能够进行提醒（提供功能界面截图）。 | | | |
| 5 | 网神SecWAF 3600 Web应用防火墙系统 | 1套 | W5000-U015P | 为现网在用Web应用防火墙提供3年软件特征库升级服务和3年硬件维保服务，升级完成后，设备具备以下能力：<br>1.★支持镜像分析数据并实现旁路阻断功能，具备专门的阻断接口设置（提供功能界面截图）；<br>2.支持智能封禁功能，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间； | 45000 | 45000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 3.支持非法URL外联检测功能，针对特定外联URL进行监控或阻断，并且支持自定义URL地址；<br>4.支持代理服务器模式，支持HTTP、HTTPS代理模式，提供针对后端服务器的代理模式；<br>5.内置有标准特征库，并且可以自定义特征，定义检查方向、严重级别、Web攻击特征等信息；<br>6.支持SQL注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少7种知识库展示说明；<br>7.支持独立的防盗链规则，支持Referer、Cookie检测方式；具备防跨站请求伪造功能，应支持Get、Post请求方式；<br>8.支持敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护；<br>9.支持防暴力破解功能，可支持攻击阈值或动态令牌的方式实现暴力破解防护；<br>10.★支持与威胁情报中心联动功能，具备FTP、API联动方式（提供功能界面截图）；<br>11.★支持对威胁情报中心提供的相关数据运用到产品防护策略中，并提供僵尸网 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 络、扫描器、钓鱼代理、网络攻击、Windows 漏洞利用等分类（提供功能界面截图）；<br>12. 支持黑/白名单机制，包含对 URL 地址、IP 地址等作为条件设置。 | | | |
| 6 | 奇安信天擎终端安全管理系统 v10 | 1500 套 | 天擎 PC 端增强包 | 全院 V6 天擎杀毒升级为 V10 版本：含防病毒、补丁管理、主机防火墙、终端管控功能。<br>防病毒：支持多引擎协同，可对病毒、木马、恶意软件等进行查杀，提供主动防御功能。<br>补丁管理：支持终端系统漏洞发现、补丁智能修复等功能<br>主机防火墙：基于网络五元组信息对主机网络的出入站流量进行控制<br>终端管控：支持外设管理、进程管理、违规外联、能耗管理、网络管控等<br>支持主流 Windows PC 客户端操作系统，提供一年升级服务。 | 150 | 225000 | |
| 7 | 奇安信天擎终端安全管理系统 V10.0（服务器端） | 30 套 | 奇安信天擎终端安全管理系统 V10.0（服务器端） | 为现网在用 windows 服务器防病毒软件提供 3 年软件规则库升级服务，升级完成后，具备以下能力：<br>1. 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描；<br>2. ★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险 | 1500 | 45000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 中完成终端能力更新（提供功能界面截图）；<br>3.支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复；<br>4.支持对终端当扫描到感染型病毒、顽固木马时，扫描时不允许终端用户暂停或停止扫描任务；<br>5.病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件；<br>6.★支持灰度发布的漏洞修复策略，将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复（提供功能界面截图）；<br>7.支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8 | 奇安信网神统一服务器安全管理系统V8.0 | 32套 | 奇安信网神统一服务器安全管理系统V8.0 | 为现网在用虚拟化安全系统提供3年软件及规则库升级服务，升级完成后，具备以下能力：<br>1.★支持VMware vShpere、Ctrix Xen、Microsoft Hyper-V、Huawei Fusioncompute、H3C CAS、浪潮云等国内外主流虚拟化厂商平台，能够采用一个管理控制中心进行统一管理（提供功能界面截图）；<br>2.支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新、客户端程序更新等功能；<br>3.支持资产信息清点功能，包括服务器基础信息、进程、账户、web站点、web服务、端口、软件应用、数据库、启动服务、系统安装包、Jar包、计划任务、环境变量、内核模块详细资产信息；<br>4.支持主动自动化病毒查杀，可支持Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式；支持病毒查杀的结果生成报告；<br>5.支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀； | 1500 | 48000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 6.★支持自定义病毒黑名单、白名单功能，包含指定文件名、文件路径、文件指纹等多种方式（提供功能界面截图）；<br>7.支持 webshell 扫描功能，支持 PHP、JSP、ASP、ASPX 等文件的恶意 webshell 检测；支持对 webshell 文件设定白名单，对文件进行加白处理，避免对网站核心系统文件造成影响；<br>8.支持 SSH、RDP、telnet 等服务的暴力破解检测，可对来自网络的暴力破解行为进行拦截，支持配置时间、破解次数、拦截时长；<br>9.支持主机防火墙功能，支持虚拟机/终端系统的双向控制，可提供对威胁情报实时分析网络流量功能，同时支持对 DDoS 等异常流量进行拦截和清洗能力；<br>10.★支持对主机进行失陷检测，并能够对失陷主机进行监控或隔离，阻止与恶意域名的连接功能(提供功能界面截图)。 | | | |
| 9 | 网神 SecGate 3600 防火墙系统 | 1 套 | NSG7000-TX45 | 为现网在用的服务器防火墙设备提供 3 年硬件维修及 3 年全功能模块升级服务，含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务。升级完成后，设备具备以下能力： | 35000 | 35000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 1.支持静态路由、动态路由、策略路由，动态路由包括RIP v1/v2/ng、OSPF、BGP等；<br>2.支持防御IP地址欺骗，可将IP与安全域关联，即指定IP或网段从特定安全域流量流入，否则视为IP地址欺骗；<br>3.支持在IPv6环境下配置安全策略、SSL解密策略等规则，实现漏洞防护、间谍软件防护、URL过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理；<br>4.产品支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）等多种防护措施；<br>5.支持上传、下载、双向的文件内容过滤；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等多种常见文件类型；<br>6.支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；<br>7.支持全面的NAT转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 8.★持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计（提供功能界面截图）；<br>9.持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；<br>10.产品能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，支持对最多 6 级的压缩文件进行解压查杀；<br>11.★洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供功能界面截图）；<br>12. 支持自定义漏洞签名；可标识自定义漏洞的 CVE 编号或 CNNVD 编号；支持自定义基于 TCP、UDP、HTTP 协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值；支持自定义漏洞的源端口范围及目的端口范围； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 13. ★产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供功能界面截图）。 | | | |
| 10 | 网神 SecGate 3600 防火墙系统 | 1 套 | NSG7000-TX45 | 为现网在用的服务器防火墙设备提供 3 年硬件维修及 3 年全功能模块升级服务，含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务。升级完成后，设备具备以下能力：<br>1. 支持静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、OSPF、BGP 等；<br>2. 支持防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗；<br>3. 支持在 IPv6 环境下配置安全策略、SSL 解密策略等规则，实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理；<br>4. 产品支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并支持警告、丢弃、普通防护（首包丢 | 35000 | 35000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 弃）、增强防护（TC反弹技术）等多种防护措施；<br>5.支持上传、下载、双向的文件内容过滤；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等多种常见文件类型；<br>6.支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；<br>7.支持全面的NAT转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；<br>8.★持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计（提供功能界面截图）；<br>9.持与云端联动，实现病毒云查杀、URL云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；<br>10.产品能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀，支持对最多6级的压缩文件进行解压查杀； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 11.★洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供功能界面截图）；<br>12. 支持自定义漏洞签名；可标识自定义漏洞的CVE编号或CNNVD编号；支持自定义基于TCP、UDP、HTTP协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值；支持自定义漏洞的源端口范围及目的端口范围；<br>13. ★产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供功能界面截图）。 | | | |
| 11 | 奇安信网神威胁监测与分析系统传感器 | 1套 | TSS10000-GM-WS-QD | 为现网在用的态势感知流量探针设备提供3年硬件维修及3年规则库升级服务。升级完成后，设备具备以下能力：<br>1.具备网页漏洞利用检测、webshell上传检测、网络攻击检测、威胁情报 检测功能；<br>2.支持对常见可执行文件的还原：EXE、DLL、OCX、SYS、COM、apk等； | 70000 | 70000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 3. 能够支持对常见扫描以及远控木马的检测；<br>4. 能够通过双向流量检测的方式发现可被利用的SQL注入、跨站、命令执行等web漏洞，并记录已经发生过的攻击事件和相关报文；<br>5. 支持通过沙箱技术精确检测多种针对PHP语言环境的WEBSHELL攻击；<br>6. ★支持对web漏洞利用检测规则、入侵检测规则等多种规则的配置，选择，可以有针对性的选择部分规则开启（提供功能界面截图）；<br>7. ★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（提供功能界面截图）；<br>8. 支持对流量中出现文件传输行为进行发现和还原，将文件MD5发送至分析平台；<br>9. 支持对HTTP、SMTP、POP3、IMAP、FTP、MSSQL、MYSQL、ORACLE、POSTGRESQL、LDAP、DNS、SSL、TDS、TFTP等协议的分析和还原；<br>10. ★支持对文件传输协议进行还原和分析，可分析的协议至少包含如下：邮件 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | （SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB（提供功能界面截图）。 | | | |
| 12 | 奇安信网神威胁监测与分析系统平台 | 1套 | TSS10000-GM-WS-QD | 为现网在用的态势感知设备提供3年威胁情报更新授权与规则升级。升级完成后，设备具备以下能力：<br>1.包括威胁情报升级、告警分析、爆破行为分析、web攻击行为分析、数据库攻击行为分析、恶意邮件行为分析；<br>2. 能够接收云端提供的威胁情报，对网络中的威胁事件进行发现和告警；威胁情报可支持在线和离线升级两种方式；<br>3. 支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、其他恶意软件，并可自定义威胁情报；<br>4. ★支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（提供功能界面截图）；<br>5. 威胁支持按照威胁事件视图、受害主机视图、受害服务器视图、受害用户视图、威胁视图进行分类展示； | 100000 | 100000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 6. 威胁告警类别需要包括 webshell 上传、网页漏洞利用、网络攻击、APT 事件、远控木马、窃密木马、僵尸网络、勒索软件、黑市工具、网络蠕虫、恶意样本执行、恶意样本投递；<br>7. 提供一键查询威胁事件详情，威胁事件详情需要包括告警来源、威胁类型、威胁名称、威胁情报 IOC、已经相关的会话记录；<br>8. ★支持与用户现网在用的防火墙设备进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断，将策略下发给防火墙，由防火墙执行阻断（提供功能界面截图）；<br>9. ★支持与用户现网在用的杀毒软件进行联动，实现恶意文件的查杀、被感染主机的网络隔离（提供功能界面截图） | | | |
| 13 | 网神 SecFox 日志收集与分析系统 | 1 套 | R2000-T1624M | 为现网在用日志审计设备提供 3 年软硬件升级服务。升级完成具备以下功能：<br>1. ★支持通过 Syslog、SNMP Trap、Netflow V5、JDBC、WMI、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能（提供功能界面截图）；<br>2. 支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警； | 22000 | 22000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 3.★支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示（提供功能界面截图）；<br>4.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；<br>5.支持日志范化策略，针对匹配的多条范化策略，系统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；<br>6.★支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息（提供功能界面截图）；<br>7. 具备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，可将原始信息进行自动索引，快速搜索分析各类安全事件；<br>8. 支持对事件依据其源目的IP和端口等各类字段信息进行深入的事件追踪调查，支持无限次数的追踪调查；<br>9. 支持以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图，且属性可增加或减少； | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 10. 具备完善的基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力；<br>11. 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；<br>12. 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等。 | | | |
| 14 | 网神SecVSS 3600 漏洞扫描系统 | 1 套 | S1500-W010P | 为现网在用漏洞扫描设备提供3年漏洞特征库升级及3年硬件维保服务。升级完成具备以下功能：<br>1. 产品至少包含系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描五大功能模块；<br>2. 采用B/S设计架构，SSL加密方式通信，无须安装客户端，用户可通过浏览器远程管理系统；<br>3. ★支持快速配置向导，简化配置过程，以满足快捷部署上线需求（提供功能界面截图）；<br>4. 支持自定义用户口令策略，包括密码更换周期、密码长度要求、密码复杂度要求；<br>5. ★支持同时下发系统扫描、Web扫描、弱口令扫描任务，无需单独下发扫描任 | 35000 | 35000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 务，扫描目标可以是IP、域名、URL的任一格式（提供功能界面截图）；<br>6.支持自定义扫描策略模板，支持按照漏洞类别、漏洞风险等级、CVE编号查看漏洞插件；<br>7.支持显示扫描剩余时间，随时查看扫描进度；支持实时显示扫描结果，在扫描过程中随时查看资产风险状况；<br>8.★支持自适应网络扫描，根据网络状况自动控制发包速率，避免影响用户网络（提供功能界面截图）；<br>9.支持自定义立即执行、定时扫描、周期性扫描等多种扫描任务执行方式，可针对指定时间、执行对象自动执行扫描任务，并自动生成报告；<br>10.支持扫描通用操作系统、路由交换设备、安全设备、物联网设备、工控专用设备等；<br>11.支持中间件漏洞扫描，涵盖Apache、Resin、Nginx、Tomcat、TongWeb、BIND、DOMINO、WebSphere、IIS、Jboss、InforSuite等；<br>12.支持主流数据库漏洞的检测，应包括但不限于：Oralce、Sybase、SQLServer、 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 15 | 奇安信网神数据库审计与防护系统 | 1套 | DAS3000-TF20 | 为现网在用数据库审计设备提供3年软硬件升级服务。升级完成后具备功能如下：<br>1. ★可通过旁路镜像或Agent插件方式部署，支持通过Agent审计回环地址的流量（提供功能界面截图）；<br>2. 支持主流数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用、神舟通用等；<br>3. 支持针对IPv6协议的审计，支持通过IPv6的地址检索事件；<br>4. 支持旁路阻断功能（非串联方式），可以对单一会话危险操作阻断，或对源IP操作的所有请求直接阻断；<br>5. ★支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息（提供功能界面截图）；<br>6. 支持B/S架构Http应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取XML返回结果；<br>7. 支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人；<br>8. 支持自动发现网络中存在的数据库，并自动添加成保护对象进行审计，简化操 | 22000 | 22000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 作，避免用户因模糊记忆引起的配置故障；<br>9. 支持对指定时间段风险数据按不同维度进行统计排行，支持对统计数据进行下钻，获取更详细的风险数据；<br>10. 支持审计规则针对访问工具、客户端IP、客户端MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL语句执行回应等条件设置等于或不等于等条件；<br>11. ★内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改等500种以上风险审计规则库，无需单独配置，直接调用（提供功能界面截图）。 | | | |
| 16 | 奇安信网神运维安全管理系统 | 1套 | C6100-H-TF20 | 为现网在用堡垒机设备提供3年硬件维保服务。升级完成具备以下功能：<br>1.支持用户多次登录失败将自动锁定账户或IP，可配置解锁时长、到期自动解锁，也可以手动解锁；<br>2.支持资源申请，运维场景中，对特定的资源发出工单请求，管理员审批后，可以在指定时间段内运维操作该资源；<br>3.★支持用户水印功能，避免数据泄露无法追责（提供功能界面截图）；<br>4.支持的运维协议包含SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin； | 22000 | 22000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 5.支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云和Ucloud云平台的资源；<br>6.支持通过Web页面访问目标支持，包括SSH、RDP、TELNET、VNC和应用发布资源；<br>7.支持SSH客户端、FTP客户端、SFTP客户端访问目标资源；支持直接在FTP、SFTP客户端进行编码切换，支持big5、GB18030和utf8编码切换；<br>8.支持将运维资源列表导出成xshell和SecureCRT格式的配置，通过客户端快速访问资源；<br>9.★运维过程中支持会话协同，可邀请其他用户参与、协助操作（提供功能界面截图）；<br>10.支持不同的用户设置不同多因子方式认证，包括手机短信和手机令牌；<br>11.支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同的部门（子部门）；<br>12.★支持工单权限申请，支持文件上传、文件下载、文件管理、剪切板权限的申请（提供功能界面截图）。 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 17 | 网神 SecSIS3600 安全隔离与信息交换 系统 V2.0 | 1 套 | G9500-TH20 | 为现网在用网闸设备提供 3 年软硬件升级服务。升级完成具备以下功能：<br>1. 系统内部采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；标配文件交换模块、数据库访问模块、FTP 访问模块、邮件访问模块、安全浏览模块、TCP/UDP 定制模块、工控模块、视频模块、SSL 通道模块；<br>2. 支持双系统冗余架构，可通过 WEB 页面进行主备系统切换，当主系统发生故障或需要升级时可切换至备系统进行工作；<br>3. 系统管理员具备多种认证方式：支持用户名/口令、Radius、LDAP、浏览器证书、U-KEY 等多种认证管理方式；<br>4. ★支持带内管理，可通过业务口进行网闸管理工作，用户可自行选择是否启用带内管理功能（提供功能界面截图）；<br>5. 支持多种同步模式：完全一致、完全复制、首次复制+新增、源端移动、源端删除等多种模式；<br>6. 配置 SSL 通道模块：可支持 SSL 隧道访问模式，针对 FTP 访问、邮件访问、数据库访问等模块，通过网闸实现访问客户端认证、授权及访问链路加密，保证客户端访问合法性及访问链路的安全性；<br>7. 支持 MySQL、ORACLE、ORACLE_RAC、SQLServer、DB2、SYBASE、POSTGRESQL | 30000 | 30000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 等常见数据库，支持神通、达梦、人大金仓、南大通用等国产数据库同步；<br>8.★数据库同步支持无客户端方式同步，同步由网闸主动发起并完成，不需要第三方软件支持（提供功能界面截图）；<br>9.支持SMTP、POP3、IMAP通用协议，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；<br>10.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；<br>11.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；<br>12.★支持双引擎病毒查杀模块，可根据用户需求选择需要的病毒引擎（提供功能界面截图）。 | | | |
| 18 | 奇安信网神统一服务器安全管理系统V8.0 | 32套 | 奇安信网神统一服务器安全管理系统V8.0 | 为现网在用虚拟化安全系统扩容增补提供3年软件及规则库升级服务，升级完成后，具备以下能力：<br>1.★支持VMware vShpere、Ctrix Xen、Microsoft Hyper-V、Huawei Fusioncompute、H3C CAS、浪潮云等国内外主流虚拟化厂商平台，能够采用一个管理控制中心进行统一管理（提供功能界面截图）； | 2000 | 64000 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 2.支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新、客户端程序更新等功能；<br>3.支持资产信息清点功能，包括服务器基础信息、进程、账户、web站点、web服务、端口、软件应用、数据库、启动服务、系统安装包、Jar包、计划任务、环境变量、内核模块详细资产信息；<br>4.支持主动自动化病毒查杀，可支持Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式；支持病毒查杀的结果生成报告；<br>5.支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀；<br>6.★支持自定义病毒黑名单、白名单功能，包含指定文件名、文件路径、文件指纹等多种方式（提供功能界面截图）；<br>7.支持webshell扫描功能，支持PHP、JSP、ASP、ASPX等文件的恶意webshell检测；支持对webshell文件设定白名单，对文件进行加白处理，避免对网站核心系统文件造成影响；<br>8.支持 SSH、RDP、telnet等服务的暴力破解检测，可对来自网络的暴力破解行为 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 进行拦截，支持配置时间、破解次数、拦截时长；<br>9. 支持主机防火墙功能，支持虚拟机/终端系统的双向控制，可提供对威胁情报实时分析网络流量功能，同时支持对 DDoS 等异常流量进行拦截和清洗能力；<br>10. ★支持对主机进行失陷检测，并能够对失陷主机进行监控或隔离，阻止与恶意域名的连接功能(提供功能界面截图)。 | | | |
| 19 | 技术服务 | 1 项 | 定制 | 基于项目涉及到的网络安全设备，提供针对性的网络交换数据支撑、现场技术支撑、故障现场排查等服务，以保证设备及网络正常运行。 | 14000 | 14000 | |
| 合同总价合计（大写）：人民币玖拾伍万元整 （¥ 950000.00 元） | | | | | | | |
| **交货期及服务衔接：**签订合同之日起 15 个工作日内完成剩余未安装设备的供货、安装及调试（若签订合同前，甲乙双方已通过书面形式协商一致提前完成部分/全部设备安装的，按双方确认的安装完成时间为准）。鉴于本项目原维保服务已于 2025 年 12 月前届满，乙方同意自 2025 年原维保到期之日起至本合同服务期起始日（2026 年 04 月 01 日）止，为甲方提供免费补保服务，补保范围包括设备故障应急处置、漏洞库紧急升级、安全事件技术支持（与本合同维保服务标准一致）；本合同约定的 3 年维保服务期仍自 2026 年 04 月 01 日起算至 2029 年 03 月 31 日止。 | | | | | | | |

# 售后服务承诺书

| | |
|---|---|
| 质量保证承诺 | 1、软件质保服务<br>1.1 质保期限<br>甲方新购乙方奇安信网神产品（以下简称“产品”或“设备”），乙方奇安信网神提供 3 年软件质保服务(以购买的软件质保合同为准)。<br>1.2 保换期服务<br>甲方购买奇安信网神软件产品后90天内如发生非人为产品故障，经过乙方奇安信网神技术支持人员定位为软件故障，则乙方奇安信网神提供免费更换新软件产品，新软件到达甲方后，重新提供90天的软件故障免费更换期。随设备附带的网线，电源线等附件均不在保修范围内。因甲方人为因素造成的产品损坏不在免费更换范围之内。 |
| 售后服 | 1.3 保修期服务<br>1.3.1设备返修服务<br>甲方购买乙方奇安信网神设备后发生软件故障或新机购买后超过90 天后发生软件故障的情况下，乙方奇安信网神提供返厂维修服务，最长维修周期不超过10个工作日（若有特殊情况不能保证时间，将提前向甲方说明）。<br>1.3.2维修备机服务<br>甲方购买奇安信网神产品后发生软件故障需要返厂维修，若收到货后10个工作日未能维修完毕，乙方奇安信网神可以根据甲方的需求，向甲方免费提供同型号或高型号备机，等到故障机维修完毕后收回备机。<br>1.3.3注意事项<br>✧ 如未经乙方奇安信网神95015客服中心报修和乙方奇安信网神技术人员确认而直接寄来的维修产品，不能提供相应软件维修服务，乙方奇安信网神不对未经报修确认的设备的丢失、损坏承担任何责任。<br>✧ 对于产品软件质保期内的设备维修，乙方奇安信网神将修复甲方设备至故障前的完好的状态。<br>✧ 特别提醒：在设备维修前，乙方提醒甲方自行做好数据的备份工作，因设备的严重故障而导致乙方的配置数据和历史日志无法保留的， |

| | |
|---|---|
| 务承诺 | 乙方奇安信网神不承诺恢复数据配置和历史日志到故障前的状态，并不承担任何因数据丢失而导致的赔偿责任。<br>✧ 若经维修后的软件产品的剩余软件质保期不足三个月的，则本次维修的部件从维修结束之日起享受三个月免费保修服务。<br>✧ 超出保修期的设备如需维修，甲方需承担设备维修检测费，乙方奇安信网神在收到具体维修配件的费用后方可进行维修。<br>✧ 在保修期内，如发生部件更换，乙方奇安信网神拥有更换后故障部件的所有权。<br>✧ 若产品发生更换，更换后的保修期按照原有设备剩余的保修期继续计算。<br>1.3.4免除免费保修义务<br>属于下列情况的产品（包括部件）出现的故障或损坏，不在免费保修之列：<br>✧ 产品或配件超出质保服务期限的，乙方奇安信网神不再提供超期产品或配件的免费服务。<br>✧ 甲方或第三方人员未按照说明书要求，错误安装、保管、使用而造成的产品或配件故障、损坏的；私自对产品进行拆解而造成的产品或配件故障、损坏的，不在乙方奇安信网神免费服务范围内。<br>✧ 因意外因素或人为原因（包括但不限于操作失误、划伤、搬运、磕碰、输入不合适的电压、篡改等）导致的乙方奇安信网神产品或配件故障、损坏的，不在乙方奇安信网神免费服务范围内。<br>✧ 因自然灾害等不可抗力或不可预见的情形（如：雷击、地震、火灾、水灾、战争、黑客攻击、计算机病毒侵入或发作、电脑病毒、通信线路故障等非可归责于乙方奇安信网神的原因等）造成的产品或配件故障、损坏的，以及其他需要技术支持的，不在乙方奇安信网神免费服务范围内。<br>2、培训<br>系统上线后乙方会派工程师为甲方信息科技术人员提供免费培训服务。 |

# 数据保密承诺书

**承诺方（乙方）**：广西勇武科技有限公司

地址：广西南宁市青秀区长园路1号昊壮南湖西岸2209号

法定代表人(法人代表)：林坚斌

联系电话：15676719158

承诺方工作人员（以下简称 “承诺人”）

承诺人：陆新宁

承诺人身份证号：452226199609155717

职务/岗位：销售经理

联系电话：18648804559

**披露方（甲方）**：来宾市人民医院（以下简称 “医院”）

地址：广西来宾市盘古大道东159号

法定代表人（法人代表）：李成荣

经办人：

联系电话：19078240003

## 一、承诺背景与依据

为保障甲方（来宾市人民医院，以下简称 “医院”）网络系统安全运行及医疗数据资产安全，明确乙方及其工作人员在网络安全维保服务过程中的数据保密责任，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国基本医疗卫生与健康促进法》《关于进一步加强医疗机构电子病历信息使用管理的通知》等相关法律法规及甲乙双方签订的《网络安全设备维保》（项目编号：LBZC2026-J3-990012-GXHY）约定，甲乙双方及承诺人自愿签署本承诺书，严格遵守以下保密义务。

乙方确认已充分知晓医院数据的敏感性及医疗行业保密要求，承诺以“数据不动程序动、数据可用不可见” 的隐私保护原则为核心，履行保密责任。

**二、保密范围**

承诺方及承诺人承诺对在网络安全维保服务过程中接触、获取、处理的甲方所有数据及相关信息承担保密责任，包括但不限于：

1. 甲方网络设备日志、系统运行日志、操作记录日志、电子病历访问日志等各类日志数据，以及日志访问过程中产生的操作记录信息；

2. 电子病历（含门急诊病历、住院病历）、患者个人信息（姓名、身份证号、联系方式、病史、检查报告等）、医务人员信息、医疗收费数据、药品耗材数据等核心医疗数据；

3. 甲方医院网络架构、安全防护方案、系统配置信息、密钥证书、医疗信息系统技术文档等未公开的技术秘密和商业秘密；

4. 其他经甲方明确标注为保密或依据医疗行业惯例应当保密的信息（含《关于进一步加强医疗机构电子病历信息使用管理的通知》明确的保密范围）。

**三、保密义务与要求**

1. 严格遵循 “最小可用” 原则，仅在完成网络安全维保服务所必需的范围内接触、使用甲方保密数据，不得超出授权范围私自访问、复制、下载、传播、泄露任何保密信息，尤其不得触碰电子病历等核心医疗数据的非授权访问权限；

2. 访问甲方设备日志时，必须严格遵守甲方日志访问管理制度及医疗行业数据安全规范，全程留存操作记录（包括但不限于操作人、操作时间、操作内容、访问终端、授权依据等信息），操作记录需至少留存 3 年，供甲方及卫生健康行政部门查验；同时配合甲方通过数字水印等技术实现操作留痕追溯；

3. 乙方应基于内生安全理念，建立健全内部医疗数据保密管理制

度，对工作人员开展医疗行业专项保密培训（含电子病历保护、患者隐私保障等内容），明确岗位保密责任，定期开展保密检查，确保符合《关于进一步加强医疗机构电子病历信息使用管理的通知》要求；

4. 承诺人在工作中应妥善保管甲方保密信息，不得私自记录、存储、携带保密信息离开工作场所，不得向任何第三方（包括乙方内部无关人员）泄露保密信息；所有接触医疗数据的操作需在甲方指定的安全环境内进行，严禁通过非授权终端传输数据；

5. 维保服务结束后（含故障修复、巡检完成等场景），承诺方及承诺人应立即停止使用甲方保密信息，及时归还或销毁所有包含保密信息的载体（包括但不限于纸质文件、电子文档、移动存储设备等），并提供书面销毁 / 归还证明，确保无残留数据风险；

6. 发现保密信息可能或已经泄露时，承诺方及承诺人应立即启动应急处置流程，采取技术阻断、数据封存等补救措施，并在 24 小时内书面通知甲方，全力配合甲方及相关部门调查处理，不得隐瞒、拖延；

7. 乙方派驻的驻场工程师（若有）需严格遵守甲方内部管理规定，其数据访问权限与服务期限严格匹配，服务结束后立即交还所有授权凭证，乙方需及时注销其相关访问权限。

**四、保密期限**

本承诺书的保密期限自承诺方及承诺人接触甲方保密信息之日起至该保密信息成为公开信息之日止，即使《网络安全设备维保合同》终止或解除，保密义务仍然有效；其中患者个人信息、电子病历等医疗数据的保密义务不受服务期限限制，终身承担保密责任。

**五、违约责任**

1. 若承诺方及承诺人违反本承诺书约定，发生保密信息泄露、违规访问日志、非授权接触电子病历等行为，应承担违约责任，违约金按实际损失给甲方支付（违约金包括但不限于直接经济损失、患者隐私侵权赔偿、行政罚款、声誉损失等），承诺方及承诺人还应赔偿甲

方的全部实际损失；

2. 若因乙方违约行为导致甲方被卫生健康行政部门处罚或影响医院评审、智慧医院建设评估等，乙方需承担全部责任，并赔偿甲方因此产生的间接损失；

3. 若违反相关法律法规，构成违法犯罪的，甲方有权向卫生健康行政部门、公安机关报案，追究承诺方及承诺人的行政责任、刑事责任。

**六、其他约定**

1. 本承诺书是《网络安全设备维保》合同的补充协议，与主合同具有同等法律效力，冲突部分以本承诺书为准；

2. 本承诺书未尽事宜，可由双方另行协商补充，补充协议需符合医疗行业数据安全相关规定，与本承诺书具有同等法律效力；

3. 因履行本承诺书发生的争议，双方应协商解决；协商不成的，任何一方均有权向甲方所在地人民法院提起诉讼；

4. 本承诺书一式肆份，甲方执叁份，乙方执一份，自双方签字盖章之日起生效。

承诺方（乙方）（盖章）：广西勇武科技有限公司

法定代表人（法人代表）（签字）：林建武

签署日期：2026 年 4 月 16 日

承诺人（工作人员签字）：陆新宁

签署日期：2026 年 4 月 16 日

披露方（甲方）：来宾市人民医院

经办人（签字）：

签署日期：2026 年 4 月 16 日