河南机电职业学院2024年课程建设、信息化建设项目

（包1）合同

甲方（全称）： 河南机电职业学院

乙方（全称）： 河南众信汇赢信息科技有限公司

根据《中华人民共和国民法典》《中华人民共和国政府采购法》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，双方同意按照下述条款订立本合同，共同信守。

一、供货范围及分项价格表

序号	标的物名称	品牌	规格型号	技术参数（完整的技术参数信息）	计量单位	数量	单价（元）	总价（元）
1	综合日志审计平台	安恒信息	DAS-LOG 3900	满足招标参数，详见附件1	套	1	145925	145925
2	大数据态势感知平台	安恒信息	DAS-ABL-AXDR2000	满足招标参数，详见附件1	套	1	249736	249736
3	校园网威胁溯源分析平台	安恒信息	DAS-APT SP5390	满足招标参数，详见附件1	套	1	134172	134172
4	漏洞扫描系统	深信服	YJ-1000-B1075	满足招标参数，详见附件1	套	1	102833	102833
5	信息化考核平台	安恒信息	DAS-ABL V2.0	满足招标参数，详见附件1	套	1	138090	138090
6	终端安全及防病毒系统	深信服	深信服统一端点安全管理系统V6.0（aES）	满足招标参数，详见附件1	套	1	61699	61699
7	服务器区防火墙	山石网科	SG-6000-A3700-AD	满足招标参数，详见附件1	台	1	116545	116545
合计金额（含13%增值税）				**人民币大写：玖拾肆万玖仟元整（￥949000.00）**				

本合同总价包括但不限于货物价款、包装、运输、装卸、保险费、安装及相关材料费、调试费、软件费、检验费、培训费等各种伴随服务的费用以及税金等。

合同总价之外，甲方不再另行支付任何费用。

二、质量及技术规格要求

乙方须按合同要求提供全新货物（包括零部件、附件、备品备件等）货物的质量标准、规格型号、具体配置、数量等应符合招标文件要求，其产品为原厂生产，且应达到乙方投标文件及澄清文件中承诺的技术标准。

乙方应在本合同生效后 7 个工作日内向甲方提供安装计划及质量控制规范；并于合同生效 15 日内进驻安装现场；所有货物运送到甲方指定地点后，双方共同验收并签署验收意见。如甲方无正当理由，不得拒绝接收；在安装调试过程中，甲方有权采取适当的方式对乙方货物质量标准、规格型号、具体配置、数量以及安装质量和进度等进行检查。甲方如果发现乙方所供货物不符合合同约定，甲方有权单方解除合同，由此产生的一切费用由乙方承担。

三、包装与运输

货物交付使用前发生的所有与货物相关的运输、安装及安全保障事项等均由乙方负责；货物包装应符合抗震、防潮、防冻、防锈以及长途运输等要求，对由于包装不当或防护措施不力而导致的货物损坏、损失、腐蚀等损失均由乙方承担；在货物备交付使用前所发生的所有与货物相关的经济纠纷及法律责任均与甲方无关。

四、质保期与售后服务

1. 所有设备免费质保期为 叁 年（自验收合格并交付给甲方之日起计算），终身维护、维修。

2. 在质保期内，因产品质量造成的问题，乙方免费提供配件并现场维修，且所提供的任何零配件必须是其原设备厂家生产的或经其认可的。产品存在质量问题，甲方有权要求乙方换货。

3. 乙方须提供一年全免费（配件+人力）对产品设备的维护保养。

4. 乙方承诺凡设备出现故障，自接到甲方报修电话 1 小时内响应，3 小时内到达现场，24 小时内解决故障问题。保修期外只收取甲方零配件成本费，其他免费。

5. 乙方未在规定时间内提供原配件或认可的替代配件，甲方有权自行购买，费用由乙方承担。

6. 其它：无

五、技术服务

1. 乙方向甲方免费提供标准安装调试及国内操作培训。

2. 乙方向甲方提供设备详细技术、维修及使用资料。

3. 软件免费升级和使用。

4. 乙方有责任对甲方相关人员实施免费的现场培训或集中培训措施，保证甲方相关人员能够独立操作、熟练使用、维护和管理有关设备。

六、知识产权

乙方应保证甲方在使用该货物或货物的任何一部分时免受第三方提出的侵犯其知识产权、商业秘密权或其他任何权利的起诉。如因此给甲方造成损失，已方承诺赔付甲方遭受的一切损失。

七、免税

1. 属于进口产品，用于教学和科研目的的，中标价为免税价格。

2. 免税产品应由甲乙双方依据海关的要求签订委托进口代理协议，确认甲乙双方的责任与义务。委托进口代理协议作为本合同的不可分割部分。

3. 免税产品通关时乙方必须进行商检，未商检的，造成的损失由乙方承担。

八、交货时间、地点与方式

1. 乙方于合同生效后 15 日内将货物按甲方要求在甲方指定地点交货、安装、调试完毕，并具备使用条件，未经甲方允许每推迟一天，按合同总额的千分之五支付违约金。

2. 乙方负责所供货物包装、运输、安装和调试，并承担所发生的费用；甲方为乙方现场安装提供水、电等便利条件。

3. 安装过程中若发生安全事故由乙方承担。

4. 乙方安装人员应服从甲方的管理，遵守国家法律法规和学校相关制度，否则一切后果均由乙方承担。

5. 货物交付使用前，乙方负责对提供货物进行看管，并承担货物的丢失、损毁等风险。

九、验收方式

1. 初步验收。甲方按合同所列质量标准、规格型号、技术参数以及数量等在现场验收，并填写初步验收单。验收时，甲方有权提出采用技术和破坏相结合的方法。

乙方应向甲方移交所供设备完整的使用说明书、合格证及相关资料。乙方在所有设备（工程）安装调试、软件安装完毕后，开展现场培训，使用户能够独立熟练操作使用仪器或设备，尔后由供需双方共同初步验收；甲乙双方如产生异议，由第三方重新进行验收。如果乙方提供的货物与合同不符，甲方有权拒绝验收，由此所产生的一切费用由乙方承担。

2. 正式验收：依据河南省财政厅“《关于加强政府采购合同监督管理工作的通知》【豫财购（2010）24号】”文件要求，政府采购合同金额50万元以上的货物采购项目，由使用单位初验合格后，向国有资产管理处提出验收申请，由采购单位领导牵头，会同财务、审计、资产管理及专家成立验收专家组进行正式验收。学校验收通过后，才能支付合同款项。

十、付款方式及条件

1. 本合同总价款（大写）为：**玖拾肆万玖仟元整（小写：¥949000元）**。

2. 付款方式：合同内产品经甲方验收合格，能够正常投入使用；乙方提供付款所需的相关手续及开具正规发票，甲方在收到相关手续及发票，经核对无误后支付合同总额的100%。

十一、履约担保

合同签订生效前，乙方向甲方提供合同总额10%的银行履约保函或履约保证金，货物（设备）经甲方验收合格并正常运行一年后，合同内产品无质量问题，双方无任何纠纷，经使用部门签字确认后，甲方一次性无息退还履约保证金。

十二、违约责任

乙方所交的货物产地、品牌、型号、规格、质量以及技术标准、数量等不符合合同要求，甲方有权拒收，由此产生的一切费用由乙方负责；因货物更换而造成逾期交货，则按逾期交货处理，乙方应向甲方每天支付合同标总额日千分之五的违约金。

甲方无正当理由拒收设备，应向乙方偿付拒收设备款额百分之五的违约金。甲方逾期付款，应向乙方支付本合同标的总额的日万分之四的违约金。

十三、其它

1. 组成本合同的文件及解释顺序为：本合同及其附件、双方签字并盖章的补充协议和文件；投标书及其附件；招标文件及补充通知；中标通知书；国家、行业或企业（以最高的为准）标准、规范及有关技术文件；投标书及其附件。

2. 双方在执行合同时产生纠纷，协商解决；协商不成，向甲方所在地人民法院提起诉讼。

3. 本合同共 13 页，一式 陆份，甲方执肆份（用于合同备案、进口产品免税、验收、报账等事项），乙方执壹份，招标公司执壹份。

4. 本合同未尽事宜，甲方双方可签订补充协议，与本合同具有同等法律效力。

5. 本合同经双方法定代表人或其授权代理人签字并加盖单位公章或合同章后生效。

甲方：河南机电职业学院

地址：河南省郑州市新郑市龙湖镇泰山路 1 号

签字代表（或委托代理人）：

电话：0371-55383029

开户银行：中国银行新郑市支行

账号：248124853251

乙方：河南众信汇赢信息科技有限公司

地址：河南省郑州市管城回族区紫荆山路 60 号 16 层 1617 号

签字代表：朱俊瑞

电话：13673377233

开户银行：中国光大银行股份有限公司郑州紫荆山路支行

账号：77320188000088433

统一社会信用代码：91410104MA464FE60X

企业规模（大/中/小/微）：小型企业

合同签署日期：2024 年 11 月 19 日

附件 1

序号	产品名称	投标产品技术参数
1	综合日志审计平台	1、硬件及性能：支持 500 个日志源，性能 15000eps。2U 机架式，冗余电源，内存 64G ，硬盘 48T，网络接口（千兆电口 6 个，万兆光口 2 个）； 2、平台系统支持单节点部署、分布式多节点部署和分级部署模式。采用 B/S 架构操作方式。支持 IPv4、IPv6 校园网环境部署； 3、支持实时不间断地采集校园网数据中心现有的各种系统设备、网络设备、主机、操作系统、应用系统、虚拟化平台日志以及自定义等产生的所有日志信息，实现全网日志的统一收集和集中存储；满足留存相关的网络日志不少于六个月； 4、支持对全网日志进行标准化或范式化处理，可对日志进行分类；支持原始日志、范式化日志转发，可以进行自定义配置过滤掉不关心的日志。 5、对于无法直接采集日志的系统提供 Agent 方式抓取日志，Agent 支持统一管控，支持 Agent 客户端软件的统一批量下发启停、安装、卸载、升级等。Agent 支持压缩加密转发，数据传输安全。支持国产操作系统日志外发。 6、平台需支持对接校园网任何大数据日志收集或分析类平台，实现解析字段兼容，解析规则可以根据学校要求随时定制扩展，满足个性化分析和数据共享需求。 7、支持安全事件的关联分析，通过预设规则来判断不同系统和字段之间或与非的关系进行告警分析；日志审计平台支持与学校堡垒机进行数据实时同步关联分析，对绕过堡垒机而登录任何数据中心主机的行为，日志审计平台可进行实时告警，实现安全关联性分析； 8、具备报表管理功能，内置多样化的报表模板，包括等级保护合规报表、综合自动化审计报表、趋势报表和支持用户自定义报表；外部攻击日志数据可实时同步给主管或监管单位，以便于学校进行安全威胁告警数据统一梳理和挖掘分析； 9、支持对产品升级、规则升级，支持手动或定期按预设周期自动备份系统配置；提供 API 接口信息； 10、提供可视化视图，内置全球地图、中国地图、资产拓扑图等多种数据展示模式； 11、支持脆弱性管理，支持可开放漏洞扫描类平台导入弱点漏洞信息。内置 CVE

		漏洞数据知识库和 Web 漏洞数据知识库； 12、提供 24 小时支持热线。本地应急响应时间≤2 小时。提供安装调试后 5 天在线操作培训和日志数据兼容解析培训。提供三年免费软硬件质保升级服务。
2	大数据态势感知平台	1、为灵活适应现场环境，满足软硬一体化形态和纯软件形态部署模式，硬件配置：2U，CPU 24 核，内存 256GB，硬盘 64T，网络接口（千兆电口 4 个，2 万兆光口）； 2、支持采集不同来源的数据，至少包括网络流量数据、主机数据、Web 应用数据、威胁日志、脆弱性数据、安全事件数据、威胁情报数据等，可实现校园网安全数据融合并与现有的认证系统规则同步实现告警上网账号的自动关停、复通、标记等；支持与现有的智慧校园平台组织机构、人员信息、消息服务自动同步。 3、具备智能化威胁检测引擎、多维度攻击溯源引擎、场景化威胁感知引擎、集成化联动响应引擎、启发式威胁狩猎引擎、安全运营工作台模块、可视化模型编排引擎、重大活动保障模块； 4、内置多种安全分析场景模型，包括机器学习、AI 算法、智能统计等；支持智能检索语句分析，检索语句可直接一键生成检测模型，对实时数据进行分析与告警； 5、为便于统一管理和提高告警处置效率，平台功能支持与学校教育行业信息技术类网络安全监测保障系统告警数据融合实现安全事件的实时共享与处置同步； 6、平台支持提供对外 Open API，告警的结果可通过 API/kafka 形式提供给第三方安全威胁平台； 7、支持建立安全态势预警模型，对全网的安全态势、潜在的安全风险进行趋势分析和预警，并建立对未知安全威胁的发现能力； 8、支持安全态势的可视化呈现，以大屏的方式从攻击事件、追踪溯源、运行监测等多个维度进行可视化展示； 9、支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办事项、最新通报预警状态；支持将预警信息直接转为内部通报，支持将外部通报内容自动生成工单定向指派； 10、支持 kafka、短信、邮件、syslog、ftp、钉钉等告警方式；可实现与现有的校园网数据分析系统数据共享实现数据格式统一，可支持与任何可开放的域名系统联动实现编排处置响应；

		11、支持为学校现场提供隐蔽性的安全威胁分析、安全事件追溯、安全场景优化、安全告警确认等，并输出现场分析报告，分析报告包括但不限于：基于供隐蔽性的安全威胁分析、告警追踪溯源分析、安全攻击检测与确认等； 12、为保障安全运维服务的安全性与保密性提供学校堡垒机、上网行为管理系统三年免费升级服务，包含系统软件质保升级、规则库升级。 13、售后服务要求：服务期内根据学校校园网安全运行中具体业务需求，随时对平台策略动态更新；提供培训服务保证使用单位能熟练操作和进行常规维护；提供 7*24 小时支持热线；本地应急响应时间≤2 小时。
3	校园网威胁溯源分析平台	1、硬件：吞吐 10Gbps，2U 标准机架式，CPU 10 核 20 线程*2，内存 128GB，1+1 冗余电源，网络接口（管理口 2 千兆电，业务口 4 千兆电+4 千兆光、2 万兆光）。 2、支持旁路部署网络环境中；支持 Agent 代理部署，解决云环境、虚拟化环境、终端横向等环境下的数据采集；支持对 Agent 端的管理功能，通过列表方式查看终端任务状态，内置 Agent 安装升级包。 3、支持将分析到的恶意文件攻击行为同步到可开放的主机安全管理，实现检测分析与联动查杀；支持自定义联动的等待时长，支持深度溯源检测，进行二次分析，提高攻击检测的准确性； 4、支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell 等恶意程序检测规则；支持将分析到的 WEBSHELL 攻击、木马回连和攻击行为同步到本项目大数据态势感知平台实现深度威胁分析，具备告警数据同步能力； 5、支持对网络中的 IP 地址、端口等进行统计，快速识别未登记资产。可基于特定应用或服务对内部资产进行梳理（系统类型、IP、域名、端口等），查看资产端口暴露情况，特别是以非标端口提供的服务情况； 6、事件分级：应能够设置事件分级策略以区分事件的安全级别，审计记录应包含事件分级信息； 7、主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用； 8、告警归并：支持展示高度聚合告警列表，对告警进行自动归并；支持多维度告警查询，支持威胁告警快速过滤，包括筛选、排除操作；

		9、支持跨三层 MAC 地址获取，用户可新增指定 SNMP 服务器，配置包括服务器 IP、ARP OID、获取时间间隔、每次获取最大个数、SNMP 版本（V1、V2C、V3）；支持自动识别或手动添加交换机的 MAC 地址并进行识别排除，可自定义配置自动识别的个数阈值； 10、自动关联行为分析的详细展现，包含 SQL 注入取数据、表单破解、XSS 测试、目录穿越读取文件、多人访问 Webshell、APT 攻击等，支持实现基于恶意数据库操作语句的关联告警，提供功能呈现证明文件或承诺函； 11、为促进服务的高质量，提供平台检测现场分析服务；提供 24 小时支持热线；本地应急响应时间≤2 小时；提供针对此项目的三年免费售后服务承诺函。
4	漏洞扫描系统	1、软硬件性能指标：授权许可 512 个无限制 IP；网络接口：千兆电口 6 个;并发主机数 80;并发任务数 10；具备主机、系统、弱口令扫描；web 应用扫描模块、网站事件及内容检测模块，支持对网页暗链、坏链、挂马、挖矿脚本、黑页、不良信息等内容的检测分析； 2、总体要求：系统为 B/S 架构，并采用 SSL 加密通信方式，用户可以通过浏览器远程访问设备，方便用户操作，支持多用户同时登录操作。首页直观展示资产及资产弱点统计信息，包括资产总量分布、弱点总量分布、资产风险分布、风险主机 TOP5、风险网站 TOP5、主机资产风险/服务分布、弱点发现趋势等模块。 3、漏洞知识库：支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。 4、VPN 代理扫描：支持 VPN 代理扫描，可在产品界面添加代理网络配置，实现公有云、隔离网等特殊网络环境下的漏洞扫描。 5、系统漏扫功能要求：支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。支持扫描云平台的漏洞，覆盖 OpenStack、KVM、VMware、Xen 等主流的云计算平台。支持扫描物联网设备的漏洞。 5、弱口令扫描：具备弱口令扫描功能，支持弱口令扫描协议数量≥22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。

		6、Web 应用漏洞扫描：支持常见 Web 漏洞类型的扫描，包括 SQL 注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL 跳转、文件包含、反序列化漏洞、文件上传、CSRF 跨站请求伪造、信息泄露等。支持 OWASP TOP10 等主流安全漏洞。 7、数据库扫描功能：支持 Oracle、MySQL、SQLServer、DB2、Informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。数据库扫描支持的检测类型至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL SQL 注入、危险程序、安全信息查看等。 8、支持资产授权管理，对已知用户名和密码的资产可预先进行配置存放至授权管理模块，下发扫描任务时能对该部分资产的授权信息进行同步。 9、日志管理：提供审计功能，能够对登录日志、操作日常进行记录和查询，并可以将日志导入导出操作。 10、对外接口：具备对外接口，支持任务下发接口，扫描结果上报接口，任务进度接口，任务查询接口。支持与任何可开放态势预警类系统对接实现告警同步和处置同步； 11、用户管理：提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用。 12、安全事件共享：为便于统一管理和提高告警处置效率，支持与学校任何第三方网络安全监测保障类系统告警数据融合实现安全事件的实时共享与处置同步； 13、升级维护：产品支持在线升级和离线升级，至少每周进行一次漏洞特征库定期升级。提供 24 小时支持热线。本地应急响应时间≤2 小时。提供免费三年软硬件质保升级。
5	信息化考核平台	1、平台支持考核指标库根据每年以及季度主管、监管单位指标考核体系要求动态维护，能灵活生成考核模板，被考核二级单位根据指标项的考核形式和考核要求进行考核填报，系统支持对考核结果的统计和考核单位间以及多次考核的横向和纵向对比分析功能； 2、系统将采用“框架+组件”的体系架构，确保系统具有良好的可扩充性。平台的兼容性、扩展性、灵活性好，平台应该提供标准的数据传输加密接口和应用软

		件接口，以便于该系统能和单位任何第三方管理系统进行有效的集成； 3、为了保证系统的兼容性和数据的延续性，我司能够确保所投考核系统与用户任何第三方资产数据平台相关认证数据兼容与对接，提供兼容与对接的有效技术证明与实施方案； 4、平台具备年度安全考核指标库管理、考核模板管理、周期性任务与临时性任务管理、统计管理、异议任务管理、电子签章管理等功能；考核数据内部可分权限查看，外部可实现与主管或监管部门考核时数据共享对接。 5、考核指标库由具体考核指标项组成，支持添加、删除、修改考核指标项，每个指标项的考核内容可自定义设计。可以弹窗形式显示具体考核指标详细内容、评分规则等信息，管理员和用户可进行查看； 6、考核管理会针对所有提交考核指标项设置人工审核，针对用户提交的考核数据，依据评分标准进行评分。考核指标的分值变化有两种，一种是根据完成值进行加分，一种是根据完成值进行减分；评分完成，用户通过系统能查看到本单位各指标项的得分。 7、对接微信公众平台实现系统类通知消息自动通过微信下发到用户单户负责人，消息类型包括系统通知、考核任务通知、评分通知及考核过程其他通知。消息通知下发后系统自动记录用户是否查看。 8、提供根据学校具体需求的动态更新与调整的承诺证明文件； 9、提供三年免费升级服务。
6	终端安全及防病毒系统	1、提供软硬一体设备，硬件要求 CPU 核数 16 核、内存 32GB；软件不低于 200 点服务器授权； 2、支持病毒查杀、网马查杀、漏洞管理、微隔离、主动防御等功能；支持已知和未知类型勒索病毒检测查杀，挖矿防御查杀；支持高级威胁防御、渗透攻击防护；支持系统防御，包括系统登录防护、防暴力破解、进程防御、文件访问监控等功能；支持 web 应用防护。 3、提供三年免费升级服务。
7	服务器区防火墙	1、功能具备防火墙、应用识别、链路负载均衡、IPV6、VPN、IPS、AV、僵尸网络防护等功能的硬件下一代防火墙产品，支持扩展 URL 过滤、垃圾邮件过滤、云沙

		箱等功能。 2、硬件参数：至少配备独立的 1 个 CON 口，2 个 USB3.0 口， 1 个千兆 MGT 口；配备万兆 SFP+光口 6 个，千兆 SFP 光口 8 个，千兆电口 16 个；双冗余电源。 3、性能参数：吞吐量 25Gbps，最大并发连接数 600 万，新建会话 14 万；IPS 吞吐量 8.6Gbps，AV 吞吐量 5.2Gbps ；最大 IPsec VPN 隧道数 16000；配备 SSL VPN 并发用户数 8 个，支持扩展 8000 个； 4、提供三年免费硬件保修和软件升级维护服务以及三年 IPS、AV 和 Ti(威胁情报安全服务特征库升级和维护服务)。 5、支持透明网桥旁挂部署模式下的基于 vlan 标签改写替换功能； 6、支持通过 ping、tcp、dns 等方式进行 NAT 探测，支持基于指定源 IP 进行探测，支持对 NAT 转换后的地址是否有效进行探测； 7、支持虚拟路由器功能，可以划分出多个虚拟路由器，每个虚拟路由中拥有独立的路由表，实现不同区域的路由隔离；支持自定义虚拟系统的资源，包括会话数、策略数、NAT 规则数的最大限额设定。 8、支持系统的日志功能记录并输出安全网关的各种日志信息，包括事件日志、配置日志、操作日志、网络日志、威胁日志、文件过滤日志、内容过滤日志、上网行为审计日志、流量日志、云沙箱日志和调试信息日志； 9、SSLVPN 支持安卓、IOS、MAC OS、windows、linux 等平台的客户端。 10、支持丢网页关键字、WEB 外发信息控制、邮件过滤、应用行为控制等内容过滤功能，支持基于文件名称、文件大小、文件类型、协议、动作等参数配置文件过滤策略。 11、提供 SaaS 模式的安全运维 APP：通过手机可以第一时间获知设备的实时 CPU、内存、流量趋势，以及应用、用户排名、威胁信息等安全状态、 帮助快速定位问题、安全可视化实时呈现。提供 App 下载 URL。该 APP 不能是 VPN 客户端软件。该 APP 不限制使用用户数； 2、12、支持数据包路径检测，可以自定义新建检测对象，检测对象可基于接口、源地址、源用户、源端口、目的地址、目的 URL、目的端口、协议、应用等参数配置； 13、支持监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步

		破坏。支持 C&C IP 和域名两种方式检测以及支持 TCP 和 HTTP、DNS 协议检测。 14、支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等； 15、为保证产品系统稳定性，产品支持软件并存，在 web 界面就能直接操作系统版本的快速回滚，设备支持历史配置文件，以便遇到故障后快速进行配置的回滚； 16、支持基于国家地理位置、URL 等元素建立安全策略；支持策略助手支持生成基于服务的安全策略，SNAT/DNAT 支持策略命中数分析，显示策略创建时间、命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对策略进行删除或禁用。 17、为了实现威胁深度分析，所投设备支持针对本设备检测到的威胁行为，可跳转至威胁情报平台查询与溯源，云端提供对 IoC 威胁类型、多源情报等多维度的溯源分析； 18、为满足后续软件扩展能力，所有产品提供容器化服务，支持第三方容器镜像的加载；； 19、支持基于标准 SYSLOG 以及二进制的日志两种格式；二进制日志支持分布式存储到多台日志服务器，分布的算法至少支持轮询、源 IP HASH 方式。