合同编号：JSZKS2500199CGN00

2025年度江苏省农业农村厅网络与数据安全运维保障合同

委托方（甲方）：江苏省农业信息中心

地址：南京市龙江小区月光广场8号

法定代表人/负责人：王平涛

项目联系人：冯祥

联系电话：025-86263608

受托方（乙方）：中国电信股份有限公司江苏分公司

地址：南京市中央路260号

法定代表人/负责人：彭鹏

项目联系人：魏家植

联系电话：15301582498

甲、乙双方根据政府采购编号JSZC-320000-ZCZB-C2025-0003 2025年度江苏省农业农村厅网络与数据安全运维保障项目竞争性磋商采购的结果，经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下合同，并由双方共同恪守。

第一条 甲方委托乙方进行服务的内容如下：

1.1服务的目标：2025年度江苏省农业农村厅网络与数据安全运维保障。

1.2服务的内容：见附件1。

1.3 服务的方式：对厅机关及直属单位所有在建在用政务信息系统及资产（包括但不限于省农业农村大数据云平台、厅行政权力智慧办公系统、厅门户网站、省农村产权交易信息服务平台、农技耘等）开展风险评估、渗透测试、漏洞扫描、攻防演练、应急演练、安全运维支撑、协助厘清网络安全工作任务、数据安全检查，增强全员网络与数据安全意识，提升网络与数据安全事件应急处置能力，夯实安全保障基础。

第二条 项目周期和服务地点：

2.1 服务地点：省农业农村厅。

2.2 服务周期：自合同签订之日起 1 年。

第三条 为保证乙方有效进行服务工作，甲方应当向乙方提供必要的资料及工作条件。

第四条 甲方向乙方支付服务报酬及支付方式为：

4.1 本合同费用总额（含税价）：人民币大写壹佰柒拾柒万元，小写 1770000.00 元。

本合同费用总额已包括甲方就乙方履行本合同所应支付的全部报酬、所需的全部费用及税费（包括但不限于营业税、增值税等）。

除另有约定外，甲方无需就本合同项下委托事项向乙方支付上述费用之外的任何其他费用及税费（包括但不限于营业税、增值税等）。

4.2 甲方凭乙方开具的相应金额的、符合国家规定的[增值税专用/增值税普通/营业税/其他]发票支付本合同费用总额，并按以下第 2 种方式向乙方付款：

（1）一次性支付：[/]。

（2）分期支付

第一期付款：签订合同后，乙方先向甲方开具符合国家规定的发票，后由甲方支付乙方合同总价的 50%预付款。第二期付款：项目验收合格后，乙方先向甲方开具符合国家规定的发票，后由甲方支付乙方合同总价的 50%。

4.3 因乙方未按甲方要求出具相应票据导致的延迟付款，甲方不承担违约责任。若乙方提供发票顺延/遇法定节假日的，则甲方的付款时间相应顺延。

4.4 本项目的付款时间为甲方向政府采购支付部门提出支付申请的时间，不含支付部门审查的时间，乙方应充分理解年初财政预算下达和支付审核所需时间，不因此延迟交付成果和向甲方索赔任何额外费用及追究甲方责任。

4.5 本合同费用总额的所有支付由甲方以银行转账方式（银行转账方式）付至乙方指定的收款银行账户。乙方指定的收款银行账户信息如下：

开户行：工商银行城北支行

户名：中国电信股份有限公司南京分公司

账号：4301010919001154390

4.6 若根据本合同约定乙方应当支付违约金和/或承担赔偿责任，则甲方有权从上述任何一笔付款中直接扣除相应金额。上述款项不足以支付违约金或赔偿金的，甲方可向乙方另行主张，该违约金或赔偿金包括甲方因乙方的违约行为所支出的律师费、诉讼费、鉴定费、交通费、和解金额或生效法律文书中规定的赔偿金额等合理支出。

第五条 保密

5.1 乙方对甲方所提供的所有资料以及在本合同签订、履行过程中所接触到的甲方及其关联单位的商业秘密、技术资料、客户信息等资料和信息（统称“保密资料”）负有保密义务。未经甲方书面许可，乙方不得向任何第三方披露，不得将保密资料的部分或全部用于本合同约定事项以外的其他用途。乙方有义务对保密资料采取不低于对其本身商业秘密所采取的保护手段予以保护。乙方可仅为本合同目的向其内部有知悉保密资料必要的雇员披露保密资料，但同时须指示其雇员遵守本条规定的保密及不披露义务。

5.2 乙方仅有权为履行本合同之目的对保密资料进行复制。乙方不得以任何方式（如软硬盘、图纸、采样、照片、菲林、光盘等）留存保密资料。乙方应当在完成委托事项或本合同终止或解除时将保密资料原件全部返还甲方，并销毁所有复制件。乙方应当妥善保管保密资料，并对保密资料在乙方期间发生的被

盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成甲方损失的，乙方应负责赔偿。

5.3 当出现下述情况时，本条对保密资料的限制不适用。当保密资料：

（1）并非乙方的过错而已经进入公有领域的。

（2）已通过该方的有关记录证明是由乙方独立开发的。

（3）由乙方从没有违反对甲方的保密义务的人合法取得的。或

（4）法律要求乙方披露的，但乙方应在合理的时间提前通知甲方，使其得以采取其认为必要的保护措施。

5.4 如乙方违反本合同关于保密的约定，乙方应赔偿因此而给甲方造成的一切损失。

5.5 本保密条款自保密资料提供或披露之日起至本合同终止或解除后 3 年内持续有效。

第六条 未经甲方事先书面同意，乙方不得将本合同项目部分或全部服务工作转由第三人承担。

第七条 违约责任

7.1 双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

7.2 乙方未能按本合同约定按期提供服务的，每逾期 1 日，乙方应当按照本合同费用总额的 1‰向甲方支付违约金。逾期超过 30 日的，甲方有权终止本合同，乙方仍应支付上述违约金、退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息。7.3 乙方提供服务不符合本合同要求的，乙方应当按照甲方要求更正和修改，并承担由此产生的全部费用。同时，甲方有权终止本合同，乙方应当退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息，并赔偿甲方的相应损失。

第八条 双方确定，在本合同有效期内，甲方指定冯祥为甲方项目联系人，乙方指定魏家植为乙方项目联系人。一方变更项目联系人的，应当及时以书面形式

通知另一方。未及时通知并影响本合同履行或，若造成损失的，应承担相应的责任。

第九条 双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能的，可以解除本合同：

9.1 发生不可抗力。

9.2[政策变化原因]。

第十条 法律适用和争议解决

10.1 本合同适用中华人民共和国法律。

10.2 所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可向甲方所在地有管辖权的人民法院起诉。诉讼进行过程中，双方将继续履行本合同未涉诉讼的其它部分。

第十一条 双方确定，本合同及相关附件中所涉及的有关名词和技术术语，其定义和解释如下：

11.1“不可抗力”：地震、台风、水灾、火灾、战争以及其它本合同各方不能预见，并且对其发生和后果不能防止或不能避免且不可克服的客观情况。

11.2[/]。

第十二条 双方约定本合同其他相关事项为：

12.1 任何一方未经另一方同意，不得向任何第三方透露本合同的签订及其内容。甲方向其关联单位透露的，不在此限。

12.2 任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同作出的任何修改和补充应为书面形式，由双方签字并加盖单位公章或合同专用章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时，以补充合同或补充协议为准。

12.3 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、

合同和协议。

12.4 甲乙双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面信函形式或双方确认的传真或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。任何一方变更送达地址的，应当立即通知另一方，否则，按照本合同地址送达的视为已送达。

第十三条 本合同自双方法定代表人或授权代表签字并加盖单位公章或合同专用章之日起生效。本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

第十四条 附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

补充附页

经友好协商，对本合同条款补充、修改如下，本补充附页为合同正文的一部分，与合同正文冲突时，以本补充附页为准：/。

甲方：江苏省农业信息中心

法定代表人/负责人

或授权代表：（签字）王泽涛

[2025]年[6]月[3]日

乙方：[中国电信股份有限公司江苏分公司]

法定代表人/负责人

或授权代表：（签字）沈振勇

[2025]年[6]月[3]日

附件 1：

服务内容

一、项目概况

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》等法律法规的要求，通过本项目的实施，全面落实 2025 年度厅党组网络安全工作责任制要求，进一步加强全厅信息系统网络与数据安全运行维护能力建设。项目计划对厅机关及直属单位所有在建在用政务信息系统及资产（包括但不限于省农业农村大数据云平台、厅行政权力智慧办公系统、厅门户网站、省农村产权交易信息服务平台、农技耘等）开展风险评估、渗透测试、漏洞扫描、攻防演练、应急演练、安全运维支撑、协助厘清网络安全工作任务、数据安全检查，增强全员网络与数据安全意识，提升网络与数据安全事件应急处置能力，夯实安全保障基础。

二、项目内容

1、服务要求

（1）资产管理：开展信息化资产核查，采用内部自查与上门清查相结合、人工统计与技术探测相结合的方式，对全厅所有联网信息化资产进行核查。核查范围包括厅机关及所有直属单位，包含但不限于所有基于互联网、政务外网、政务云、阿里云等非涉密网络环境部署的资产，及时完成省委网信办有关资产普查、动态更新上报工作。

开展互联网暴露面探测，发现违规暴露在互联网中的资产及存在的风险并进行处置，降低暴露面资产的风险。主要工作内容包括：

1） 互联网暴露面清查。对全厅所有信息化资产每月开展一次互联网暴露面探测，及时发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控。

2） 敏感信息发现。及时发现我厅有可能泄露的敏感信息、敏感数据，包括跨境泄露的敏感信息或数据。通过百度网盘及文库监控（百度、豆

丁、360 文库、道客巴巴、e 文库、在线文库、新浪共享文库等），发现厅机关及直属单位泄露的敏感文档，并提供处置建议。

（2）漏洞扫描：每月开展一次漏洞扫描，每次漏洞扫描包括初测、指导漏洞整改以及复测。依靠带有安全漏洞知识库的网络安全扫描工具对我厅的管理终端、服务器、网络设备、网站、业务系统等资产进行漏洞扫描，出具漏洞扫描报告。对自主发现的漏洞进行登记，推送到相关处室（单位）进行整改；对各级主管部门、安全部门、公共平台通报的漏洞进行登记、验证、转发，并及时将处置情况向通报单位回复。对已经证实的漏洞进行分析，防范同一漏洞在类似环境同样存在；对整改的结果进行验证，保证漏洞得到有效控制。

（3）应急演练：制定应急演练方案，选择 1-2 个重要信息系统开展一次应急演练，锻炼应急保障队伍，总结应急演练效果，按照网络安全责任制落实要求提供应急演练总结报告。对大规模病毒暴发、网络入侵事件、拒绝攻击、主机或网络异常事件等进行应急响应，规范化检测、抑制、恢复等应急流程。

（4）安全加固和策略分析：制定安全加固实施方案，加固完成后，跟踪各系统处理加固进展。测试加固后的完整性、可用性等，保证加固工作对信息系统的安全稳定运行无负面影响。为每一个加固对象编制加固报告，方便管理员更快的适应加固后的设备操作。

摸清我厅安全设备访问控制情况，制定相应设备访问控制表，并协调态势感知平台和防火墙、入侵防御等设备的数据交换。日常对访问控制措施进行检查，制定检查记录报告。同时，对管理员操作的合法性进行审计。

（5）重要时期安全值守：在国家护网行动、重要安全保障及国际规定的法定节假日、重大会议、政治活动等重大活动期间，聘请专业安全服务工程师驻守现场，做好安全加固及防护，实时监测网络安全状况，及时响应突发安全事件，做好重保期间重要信息系统的网络安全监测防护、值班值守、事件处置等，确保重保期间网络安全。

（6）供应链安全性检测：通过平台化工具和人工服务，在应用系统正式上

线运行之前，增加有关系统安全检测步骤，发现应用开发过程中的安全问题，并归纳梳理，给出修复建议和措施，从源头解决问题。保障应用系统最终交付的安全性。不定期对所有外包服务公司开展安全检查工作。

（7）攻防演练：开展一次攻防演练，提高全厅网络安全防护和应急响应能力。演练由经验丰富的红队专家组成攻击队，采用不限攻击路径和手段的实战方式，对参演单位的目标系统进行有组织的网络攻击。通过实战的方式帮助发现并识别潜在的安全漏洞，包括系统漏洞、应用漏洞以及网络设备漏洞等。通过攻防演练，可以深入了解网络攻击方式和相应的网络安全漏洞，进而针对性地进行安全整改，提升自身的安全防御能力，促进处室（单位）之间的协作。

（8）入侵痕迹检查：每季度开展一次入侵痕迹检查，对我厅机房和相关政务云所有在用的服务器（含虚拟机）中可能存在的木马、后门等恶意程序进行检测，出具检测报告，并在系统运维单位及软件开发商确认的基础上进行清理。

（9）日常监测预警：根据全厅网络情况，立体化组建威胁感知，响应，处置的纵深防御系统，从而具备精准化威胁检测，全方位感知和体系化联动的能力。对重要系统加强安全检查力度，形成每月汇总报告。对全厅互联网、政务外网、政务云业务进行统一监测，统一预警，一旦发现篡改、漏洞等常规安全事件，实时进行处置，对突发的网络入侵、网络攻击、大规模的病毒爆发、主机或网站异常事件等紧急安全问题提供全天候的技术支持，控制事态的发展，提取攻击证据，跟踪追查攻击源，保障系统的安全稳定运行。

对相关网络安全主管部门和技术平台发现及通报的各层面的系统漏洞、国内外最新网络安全漏洞进行跟踪，持续开展重要漏洞披露平台的跟踪与分析，在发现高危风险后实时向系统责任处室（单位）发送安全预警通告，并由其运维团队通过每月或实时通过书面报告的形式将监测与处理结果进行报告。

监测预警及响应标准：

(一)整体监测要求：对我厅的互联网业务及政务外网业务，提供 7*24 小时不间断监测服务；

(二)针对服务范围内资产扫描到的高危可利用漏洞，提供漏洞修复方案和安全设备防护策略。

(三)对我厅所有互联网资产开展 24 小时的日常监测服务，跟踪和匹配主流漏洞平台发布的漏洞信息，及时进行预警通报。并对突发的安全事件进行响应，开展定位、分析、协调、处理，提交事件调查和处理报告。

(四)对政务云上系统

1)通过采集安全设备和监测工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，提供 7*24 小时持续不间断的安全威胁分析鉴定。

2)及时发现重大安全漏洞，制定解决方案，通过应急检测服务迅速、精准的梳理出受影响的资产与设备，从而快速进行漏洞修复，缩短漏洞的影响范围。

3)针对我厅突发安全事件，按事件级别及事件影响范围，在规定时间内对突发的重要安全事件进行响应，立即开展定位、分析、协调、处理，提交事件调查和处理报告。

4)可视化展示服务成果，能通过可视化的数据，清晰的了解系统安全状况。

（10）渗透测试：通过扫描已经发现的安全漏洞，模拟入侵者的攻击方法对互联网系统进行非破坏性质攻击性测试，保证整个渗透测试过程都在可以控制和调整的范围之内。每月开展一次渗透测试，通过渗透测试发现系统是否存在被恶意攻击者真实利用的安全漏洞情况、防护情况和数据安全情况，以及可能发生的安全风险事件，并且检测已有安全产品及安全策略是否能够实时防御

安全攻击。评估目标系统当前的风险等级和安全防护能力的高低，针对发现的安全风险，提出安全解决方案，完善现有防御体系，优化安全策略。

对渗透测试范围中发现的信息系统资产漏洞、木马、后门等恶意程序，出具渗透测试报告。有新设备或新业务上线时，对业务及设备进行安全扫描检查，并提供结果报告。对于报告中发现的风险，提供切实可行的解决方案。

（11）网络安全运维支撑：针对信息系统在等级保护测评及密码测评过程中发现的不足（中高危漏洞）提供整改咨询与指导，提出整改优化建议，并对整改后的问题进行复测与确认，增强信息系统运维支撑人员的网络安全技能。

（12）数据安全：加强对数据流转全链条安全管理，包括对数据生成、流转、归档、共享等环节制定数据安全管理制度，开展数据安全技术措施、管理制度检查，形成检查报告。针对指定的系统开展数据分类分级，并开展数据安全风险评估。

2、工具要求

提供以下安全技术工具，满足日常政务云上安全检测防护服务需求。

- 政务云流量传感器

指标项		指标要求
流量采集	网络协议	支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs 等。
	文件协议	支持对流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk 等）、压缩格式文件（RAR、ZIP、GZ、7Z 等）、文档类型文件（word、excel、pdf、rtf、ppt 等）。
	数据库协议	支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL 等协议。
	会话流量	支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述。
	自定义协议	支持自定义协议和端口，满足特殊场景下的流量抓取。
威胁检测	威胁情报	支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 100+万条。
	混淆攻击检测	▲支持对使用 base64、unicode、url 编码等混淆手段攻击检测。（提供产品界面截图，并加盖厂家公章）

	Web 攻击检测	支持检测针对 WEB 应用的攻击，如 SQL 注入、XSS、系统配置等注入型攻击。
		支持基于 webshell 函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace 代码执行等。
		支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等。
	弱口令检测能力	▲支持基于自定义正则表达式以及自定义弱口令字典的弱口令登录行为检测， 同时要支持不同协议弱口令分析。自定义弱口令正则表达式方式支持自定义弱口令强度、复杂度规则。支持配置多条弱口令检测的正则表达式。（提供产品界面截图，并加盖厂家公章）

- 政务云安全分析平台

指标项		指标要求
威胁情报告警检测	威胁情报检测	支持基于流量日志进行实时和历史回溯的威胁情报匹配，并自动标记告警标签，包括：情报回溯、自定义情报、内生情报等；IOC 类型包括 IP，域名等类型；检测类型包含 APT 事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒、其他恶意软件。
	威胁情报分析	▲支持在告警列表中，针对疑似恶意攻击 IP/IOC 发起情报查询，点击跳转到云端威胁情报平台，可查看此疑似恶意 IOC 的详细威胁信息，包括 IOCtag 信息、情报研判结果网络场景、IP 用途、用户类型、归属组织、地理信息，相关安全报告、相关样本、相关 URL、相关漏洞信息、开源情报信息、情报社区等。（提供产品界面截图，并加盖厂家公章）
告警分析	告警加白	支持基于自定义白名单的告警过滤，白名单设置条件涵盖告警类型、威胁名称、威胁情报 IOC/规则 ID、URI、XFF 代理、Payload、域名、referer、目的端口、协议、受害资产组、攻击资产组、受害 IP、攻击 IP、源 IP、目的 IP 等。
	告警专项分析	支持在告警日志中展示出 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为和传输文件行为的活动趋势；支持以可视化拓扑结构形式展示告警所命中的 ATT&CK 攻击技术及其与组织的关联关系；支持兼容 wireshark 过滤语法关联展示本地 PCAP 会话数据，用于告警分析，可以查看会话数量，会话时间、源/目的 IP、协议、会话信息等。
	勒索专项分析	支持对勒索告警进行专项分析，可识别勒索家族包括：Cerber、Tescrypt、Strictor、WannaCry 等。
		威胁统计包括：活跃勒索家族（受害资产数）分布统计、勒索受害资产 Top10、勒索告警趋势图。
	安全专项分析	支持以单独威胁情报、应用安全、系统安全和设备安全专项分析页面。其中应用安全具备 web 安全、数据库安全、中间件安全和邮件安全分析纬度；系统安全具备暴力破解、弱口令等。
威胁溯源	行为分析	▲支持基于网络日志进行专项行为分析，包括：DNS 行为，非常规访问，邮件行为，登录行为，WEB 行为，数据库行为，访问行为，旁路阻断行为等。（提供产品界面截图，并加盖厂家公章）
	日志检索	支持基于资产组，时间、IP、端口、协议、上下行负载等多重字段组合对网络流量日志进行检索，日志类型包括：TCP，UDP，web 访问，文件传输，域名解析，SSL 加密协商，数据库操作，FTP 控制通道，邮件行为，登录动作，mq 流量，telnet 行为，radius 行为，kerberos 认证。

- 政务云服务器防护

指标项		指标要求
风险发现	风险总览	支持统计总风险及各类风险数量，展示影响服务器信息。通过各类图表展示安全评分趋势、风险项趋势、账户风险类型分布、口令风险应用排行 Top5/Top10、漏洞风险项数量 Top5/Top10、配置风险排行 Top5/Top10 等相关统计信息。
	账户风险	支持对 Windows 和 Linux 服务器中的风险账户进行检测，发现可能存在的风险账号，包括：高权限账户、过期账户、默认账户被启用、可远程账户、克隆账户、隐藏账号等，并可对风险账号进行标记修复、加白等操作。
	软件漏洞检测	支持从服务器视角和风险视角切换查看服务器上的漏洞情况。
	基线检查	内置等保二级、三级、CIS、系统服务核查、账户安全核查、系统配置安全检查、应用配置安全检项等基线检查模板，方便快速进行基线检查。
系统防护	防恶意下载	支持监控和阻止包括 bitsadmin、mshta、msiexec、rundll32、js/vbs 脚本解释器、powershell、certutil、regsvr32、base64、Web 服务、各类对外服务进程、下载工具等进行的可执行文件下载行为。
	系统加固	支持监控和阻止对外提供服务的高风险进程相关行为，包括更改配置文件、添加定时任务、修改账户信息、修改系统日志、执行危险命令、编译文件、修改 SSH 认证文件、下载可执行文件、创建危险扩展名文件、执行威胁扩展名文件等行为。
应用防护	全链路漏洞监控防护	▲支持对主机业务系统中未知 WebShell、未知 SQL 注入漏洞、未知上传漏洞、Struts 2 漏洞、反序列化漏洞、任意文件读取漏洞、命令执行漏洞、T3 协议漏洞、IIOP 协议漏洞的监控及防护；对于 T3 协议漏洞和 IIOP 协议漏洞可以添加例外 IP，添加为例外的 IP 可以正常访问。（提供产品界面截图，并加盖厂家公章）
	自定义防护	▲支持对主机的 SQL 注入、XSS 攻击、应用漏洞利用的防护，可以选择针对利用特定 SQL 注入、XSS 攻击、应用漏洞的规则进行防护、监控和关闭的设置；对于 SQL 注入、XSS 攻击，用户可自定义设置检测访问流量的 URL、Cookie、POST 和 UA；支持白名单设置，将 URL 加入白名单后则访问时不再进行规则匹配；支持自定义拦截页状态码。（提供产品界面截图，并加盖厂家公章）
	URL 控制	支持对 URL 的控制。用户可以自定义设置特定 URL 的允许访问 IP，非设置的 IP 禁止访问。

3、人员要求

提供项目经理 1 名，总体负责本次安全运维项目，要求项目经理具有本科及以上学历，五年以上工作经验，并承担过同类型安全运维项目管理，熟悉国家网络安全等级保护、商用密码应用安全性评估、数据安全管理等技术要求，具备一定的网络安全技术，需要具备项目经理具备高级工程师（通信工程或电子信息专业）职称认证证书。

提供安全运维工程师 2 名，要求具有两年及以上工作经验，并具备同类型项目运维经验。

项目组成员不得少于 3 名，应掌握全面的网络安全技术能力，包括数据安全、网络安全等级保护、商用密码应用安全性评估、网络安全应用检测及防御、渗透测试等方面的技术能力。同时每名成员需至少具备 1 种不同类别的证书，证书类别包含注册信息安全工程师证书 CISP、信息安全保障人员认证证书 CISAW（安全运维或应急服务）、网络安全能力认证证书 CCSC。

4、运维计划要求

本次安全运维项目服务期为 1 年，本次项目开展分为四个阶段，分别为项目准备阶段、实施方案阶段、现场实施阶段，总结验收阶段。需提供项目实施方案，明确各阶段工作内容与交付。

5、项目保密要求

必须严格规范项目组成员的行为，执行各项保密制度，合同签订完成后签订保密协议，对在项目实施过程中接触的各类信息进行保密管理，杜绝敏感信息泄露事件的发生。

6、项目验收要求

必须严格规范项目组成员的行为，执行各项保密制度，合同签订完成后签订保密协议，对在项目实施过程中接触的各类信息进行保密管理，杜绝敏感信息泄露事件的发生。

7、资质要求

至少具备 1 种资质证书，证书类别包含 ISO27001《信息安全管理体系认证证书》、国家信息安全测评信息安全服务资质证书（安全运营类一级及以上）、国家信息安全测评信息安全服务资质证书（风险评估或安全运维一级及以上）、中国网络安全审查技术与认证中心信息安全服务资质证书（信息系统网络安全审计）、中国国家信息安全漏洞库（CNNVD）技术支撑单位、检验检测机构资质认定证书（CMA）。