合同登记编号：BJIPO2024-130511-309

政务云安全运维扩展服务采购项目合同

项目名称：政务云租用及网络安全运维项目安全运维服务采购项目

项目委托方（甲方）：中关村知识产权促进中心

项目承担方（乙方）：太极计算机股份有限公司

委托时间：2024 年 6 月 1 日至 2025 年 5 月 31 日

项目名称		政务云租用及网络安全运维项目安全运维服务采购项目		
合同名称		政务云安全运维扩展服务采购项目合同		
合同金额		￥1611690.00 元 （大写：壹佰陆拾壹万壹仟陆佰玖拾元整）		
甲方	单位名称	中关村知识产权促进中心		（单位盖章） 2024年5月27日
	负责人（签章）	石英	职务	主任
	项目联系人	梁正央	手机	18811033015
	地址及邮编	北京市西城区东联大厦 2 层 207		
	电话	010-82354948		
乙方	单位名称	太极计算机股份有限公司		（单位盖章） 2024年5月27日
	负责人（手签）	牛占华	职务	总裁
	项目联系人	牛占华	电话	18600546111
	地址及邮编	北京市朝阳区容达路 7 号		
	电话及传真	010-57702888		
	电子邮箱	niuzh@mail.taiji.com.cn		
	开户名	太极计算机股份有限公司		
	开户银行	工商银行北太平庄支行		
	帐号	0200010009200088408		

甲、乙双方根据《中华人民共和国政府采购法》及相关的政府采购规定，经过友好协商，就乙方为甲方提供政务云租用及网络安全运维项目安全服务采购项目包2政务云安全运维扩展服务(下称“服务”)事宜达成本合同，以兹共同遵守。

一、 项目期限

乙方为甲方提供政务云安全运维扩展服务的期限为2024年6月1日至2025年5月31日止。鉴于该项目为财政预算资金，需执行政府采购流程。为保障甲方信息运行工作的持续正常运行。如委托期满，在后续项目承担单位未确定之前，由乙方继续提供本合同约定的运维服务，确保工作不间断，连续性。

二、项目主要服务内容、成果和合作模式

（一）项目委托工作内容

1.根据北京市经济和信息化局印发的《北京市市级政务云管理办法》通知，该项目持续租赁北京市级政务云服务，为北京市知识产权资助链系统、保护中心信息平台系统、北京市海外知识产权公共服务信息库、北京市知识产权公共信息服务平台租用北京市级政务云提供的安全服务，保障以上4套业务系统安全稳定运行。

序号	应用系统名称	备注
1	北京市知识产权资助链系统	无
2	保护中心信息平台系统	无
3	北京市海外知识产权公共服务信息库	无
4	北京市知识产权公共信息服务平台	无

2.乙方提供市级政务云服务安全运维扩展项目如下

服务子类	计价单位	报价单位	数量	期限
主机杀毒服务	台	元/月	68	12
主机安全加固	台	元/次	136	——

主机漏洞扫描	台	元/次	136	——
主机日志分析	台	元/次	136	——
数据库审计服务	套	元/月	4	12
安全态势感知服务	系统	元/月	4	12
等保测评	系统二级等保测评	元/个	2	——

（二）合作模式

1.热线支持服务

乙方应提供7×24小时电话、邮件等方式解答、响应甲方的服务请求和故障申报。（电话：江河 15600595199；邮箱：zhengwuyun@mail.taiji.com.cn）

2.现场支持服务

对甲方的服务请求，若乙方无法通过电话或邮件方式解决的，应在接到甲方通知1小时内，提供及时的现场支持服务;乙方应对政务云机房提供7*24小时全天候运维值守服务。

（三）项目工作成果及质量要求

1.质量要求

（1）乙方需为甲方提供应用系统的部署上线及运维服务。

（2）乙方所提供的整体运维服务应遵循客观、科学、公平、公正原则，符合国家和相关部门、评估专家对该类项目内容和深度规定的要求及甲方的技术、质量要求。

（3）乙方提供的云平台平均可用性应达到99.99%；提供普通和高性能存储服务，要求稳定可靠，结合其他技术，确保数据可靠性99.9999%。

（4）乙方根据政务云的整体技术架构与标准,在其范围内为甲方提供基础设施资源动态调整,乙方为甲方的业务系统所提供的政务云

基础资源服务（计算、存储、网络带宽）应随业务系统的实际需求做动态调整，如遇业务系统高峰期应按照实际业务需要增加政务云资源，费用以北京市级政务云基础服务目录价格为准，并经甲乙双方共同协商确认。

2. 成果要求

项目书面成果包括：

（1）《政务云安全运维扩展服务月报》

（2）《政务云安全运维扩展服务总结报告》

三、项目进度安排及要求

（一）进度安排

1. 乙方应于签订合同时向甲方报送项目方案，甲方可就乙方提供的项目方案提出修改意见。乙方应按照甲方要求及时调整和修改。经甲方审定后，乙方在甲方的指导下开展后续工作。

2. 乙方应在合同生效期间负责北京市知识产权局政务云上系统的安全运维服务工作。

3. 2025 年 5 月 31 日前完成项目工作，并形成完整的项目总结报告；服务期至项目成果验收合格止。

（二）具体要求

（1）保密要求

乙方须严格遵守甲方的相关信息安全规定，不得利用系统维护服务时的便利对甲方数据及其他信息擅自修改或透漏给第三方。

（2）响应的及时性

乙方应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人 7*24 小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在 1 小时内到达运维现场提供服务。系统发生宕机问题时，乙方应在 30 分钟内响应，在 4 个小时之内使系统

恢复正常，故障处理完毕后提供相关系统宕机报告。

（3）重点保障要求

为保障五一、十一、春节、两会等重要时期以及业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求乙方根据业务周期性特点，加大运维保障力度，保证在重要时期以及业务高峰期内系统平稳运行。

（4）安全及扩展服务

1）安全要求

乙方应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全三级等保要求，并积极配合甲方根据业务系统具体等保需求，开展相应等保评估、检查、整改等工作。乙方管辖范围内的硬件、软件及支撑环境资源，至少达到业务系统的最高安全等级要求。

2）扩展要求

乙方应按照各系统的特点灵活调整计算、存储等各类资源供给，并能够根据业务数据的变化及时扩容或缩减存储空间，确保系统高峰时段或特殊时期的访问需求。

四、合同履行地点

本合同项下的北京市政务云服务履行地点为：北京市丰台区西三环南路1号北京市政务服务中心北京市政务云机房。

五、服务费用及支付方式

本合同服务费用共计人民币小写：￥1611690.00元（大写：壹佰陆拾壹万壹仟陆佰玖拾元整）。上述金额为含税价格。

除本合同约定的项目经费，甲方无义务向乙方支付其他任何费用。乙方因组织实施本项目而支出的一切费用，包括但不限于劳务费、专家费、食宿费、交通费、税费等，均应由乙方自行承担。

本合同项下项目经费共分【3】次支付：

1.甲方于本合同生效之日起【10】个工作日内向乙方支付项目经费预算金额的【30】%，即人民币（大写）肆拾捌万叁仟伍佰零柒元整（人民币小写：¥ 483507.00 元整）。

2.甲方于项目中期成果通过评估后【10】个工作日内向乙方支付项目中期款，以本年度项目财政资金执行金额为准，人民币大写伍拾万陆仟肆佰玖拾叁元整（人民币小写：¥ 506493.00 元整）。项目中期工作成果未通过甲方评估的，甲方有权延迟支付项目中期款，直至乙方按照甲方提出的具体意见完成项目调整或修改。甲方对此不承担违约责任。（如有中期付款）

3.项目委托工作全部完成后，乙方将项目经费决算报告以书面形式提供给甲方，甲方进行项目验收和决算评审，项目费用最终结算金额以决算评审结果为准。项目通过验收并决算评审结束后【10】个工作日内，甲方向乙方支付剩余全部费用。

4.双方一致同意本项目最终结算金额以甲方决算评审结果为准，最高不超过本项目预算金额。如决算评审结果低于甲方已经向乙方支付的经费数额，乙方应在评审结束后【10】个工作日内向甲方退还多支付的经费。

项目经费列表：

1.技术服务费：¥1611690.00 元

合计：人民币 ¥1611690.00 元。

六、双方权利和义务

双方均应共同遵守《中华人民共和国民法典》等法律法规和相关政策规定，严格遵守并认真履行本合同各项条款。

（一）甲方的权利义务

1. 甲方有权督促项目的实施进度及质量，并对乙方的服务进行监督、提出建议及满意度评价，将结果反馈给乙方；

2. 甲方有权要求乙方现场技术指导、处理故障及其他服务。

3. 甲方有权要求乙方对获取的甲方所有信息、数据及资源保密，严禁外泄、另行使用。

4. 甲方应参照有关规定进行北京市政务云服务的申请、变更、续用和撤销；

5. 甲方应在应用系统部署上线过程中支持和配合乙方的工作；

6. 甲方的应用系统在正式上线前应由乙方进行安全扫描，若有安全隐患，需按照乙方出具的安全扫描结果报告对应用系统进行安全加固；

7. 甲乙双方协商，定期对应用系统进行安全扫描，并针对扫描结果双方共同配合完成安全加固；

8. 甲方如须对已上线应用系统进行应用维护升级，须向乙方提交有关申请工单并在得到乙方确认后到乙方指定地点进行升级维护；

9. 甲方不得私自改动设备的配置和安装、使用非法软件；

10. 甲方其他的权利义务：__无__。

（二）乙方的权利义务

1. 乙方需根据合同要求，在甲方的管理和监督下，开展具体运维服务工作。

2. 甲方提出的服务申请经乙方审核通过后，乙方有责任提供技术咨询并配合甲方执行相关工作；

3. 乙方负责北京市政务云基础环境的运维和安全，包括物理安全、网络安全、主机安全、数据安全、应用安全、虚拟化安全等，并在此基础上提供主机防护、网页防篡改和主机杀毒等服务。

4. 乙方负责提供资源调度管理和维护，提供北京市政务云主机状

态监控，对甲方所申请使用的资源提供运维服务，未经甲方书面授权不得访问甲方的应用系统和数据库，不得擅自修改应用系统数据或发布信息等；

5. 应用系统正式上线后，乙方需定期向甲方提供上月系统运行监控与维护报告，以便甲方及时获取应用系统详细运行情况；

6. 乙方须按照合同约定的标准服务内容向甲方提供相关资源，做到资源专用，不得私自另行使用。

7. 乙方应采取相应的技术措施，确保无法从指定的运维操作地点以外的场所对应用系统进行任何操作；

8. 乙方需按照有关规定进行操作，确保应用系统不被人为地损坏；

9. 乙方在发现应用系统故障后，须通过电话和邮件等有效方式及时联系甲方对应负责人员，进行故障上报和处理；

10. 乙方现场值守人员应遵守甲方的相关规定，在接到甲方故障报告后，应及时做好相关信息的登记工作，并进行故障排查。故障未排除前现场值守人员应定时向甲方反馈检查进度及结果，故障排除后，现场值守人员应将结果及时反馈甲方并做好故障记录工作；故障排除后乙方需向甲方提交故障报告，经乙方确认后向甲方提交故障处理报告；

11. 甲方如需乙方提供重启服务器操作时，乙方有权要求甲方提供书面申请。除本款约定外，乙方原则上不接受甲方提出的其他可能对甲方服务器造成损坏的任何操作要求；

12. 乙方应提供技术支持服务，以维护甲方应用系统的正常运行。由于甲方指定的其他技术服务提供商提供的软件或产品的缺陷，造成的应用系统运行故障、安全漏洞、信息泄露等事故，乙方不承担相应责任，但需要配合甲方进行整改。

13. 乙方提供云主机备份服务，备份策略是每天增量，每周全

备。

14. 乙方其他的权利义务：__无__ 。

七、知识产权归属

1.在本合同签订前已经存在的或履行过程中产生的其他与本合同应用系统无关的成果，包括但不限于设计方案、各种说明书、测试数据资料、计算机软件以及其他技术文档，知识产权归属原权利人所有；

2.本合同履行过程中产生的相关运维报告的知识产权归甲方所有。

3.乙方保证所提交的项目成果没有侵害任何第三方的知识产权等相关权利。如发生侵犯第三方知识产权等相关权利的相关情形，乙方承担因侵犯第三方知识产权等权利而产生的法律责任。

八、违约责任

1. 甲乙双方均应全面履行本合同，任何一方不履行或不按约定履行均构成违约，违约方应赔偿因此给其他方造成的损失。

2. 甲方迟延支付服务费的，每延期一日，应向乙方支付延迟应付服务费__0.01__%的违约金。但如因财政国库支付受限等非主观故意原因，致使甲方不能及时支付乙方服务费用时，甲方可以延迟相应服务费用的支付并及时通知乙方，该延期支付不视为甲方违约，并不减轻乙方对本合同服务项目的责任。

3. 乙方应在本合同期限内按照本合同约定向甲方提供运维服务。如因乙方原因造成服务延迟，甲方有权要求乙方采取有效补救措施，继续履行本合同约定的义务，并承担由此给甲方造成的所有损失（包括但不限于实际损失、可得利益损失及甲方因此向第三方支付的律师费、诉讼费、仲裁费、鉴定费、保险费等，本合同项下的损失均为此

义）。

4. 乙方未尽日常维护义务或维护不当造成应用系统运行障碍的，由乙方负责排除，并承担由此给甲方造成的所有损失。因乙方的服务缺陷造成甲方服务器与 Internet 长时间中断的，乙方按照合同约定服务费折算出的日服务费用，每中断一日向甲方支付对应合同额 0.01 %的违约金。

5. 乙方工作人员未经甲方书面授权，擅自篡改甲方业务数据，或利用甲方现有业务应用系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三方损失的，由乙方承担法律责任并负责赔偿相应损失。

6. 如委托期满，在后续项目承担单位未确定之前，乙方应继续提供本合同约定的数据和服务，确保工作不间断，连续性。否则，视为乙方违约，乙方应当向甲方支付相当于本合同约定项目预算经费金额【10】%的违约金，并赔偿由此给甲方造成的全部损失。

九、 免责条款

1. 由于网络运营商的核心设备故障造成的网络中断、阻塞，从而影响到系统的正常访问或响应速率降低，属于不可控事件，甲方应对此表示认同。

2. 本合同中不可抗力指地震、台风、洪水、战争、罢工以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

3. 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并在不可抗力发生之日起 15 天内提供有关相关政府部门或公证机关出具的证明文件。

4. 由于不可抗力致使合同无法履行的，本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无须承担违约责任。不可抗力事件消除后，双方应就合

同的履行及后续问题进行协商，按照该事件对合同履行的影响程度，决定继续履行合同或终止合同。

十、 保密条款

1. 信息传递

在本合同的履行期内，任何一方可以获得与本项目相关的对方的保密信息，对此双方皆应谨慎接受并不得向任何第三方披露。

2. 信息披露

获取对方保密信息的一方仅可将该信息用于履行其在本合同项下的义务，且只能由相关的工程技术人员使用。获取对方保密信息的一方应当采取适当有效的方式保护所获取的信息，未经对方书面同意或授权不得使用、传播或者公开。

3. 保密措施

甲乙双方必须采取相应的安全措施，遵守和履行上述保密约定。经双方协商，一方可以检查其他方所采取的安全措施是否符合上述约定。

4. 违法保密义务的责任

甲乙双方任何一方违法本条款约定的保密义务，给其他方造成损失的，应承担全部赔偿责任。

本保密期限为长期，直至保密信息经正当程序而成为公开信息为止；本保密条款为独立条款，不因本合同的变更、解除、终止而失效。

十一、争议的解决

1. 本合同按中华人民共和国相关法律、法规进行解释。

2. 甲、乙双方在合同履行过程中发生的一切争议，均应通过友好协商解决；协商不成的，任何一方均可向甲方住所地人民法院提起诉讼。

3. 在本合同履行过程中，甲方申请服务需求变更需严格按照《北京

市市级政务云管理办法》通知规定的流程进行。

4.合同内容的任何变更均须经甲、乙双方同意，并签署书面的补充协议；在变更达成一致前，双方应继续履行其原约定义务。

十二、其他

1. 本合同自双方法定代表人或其委托代理人签名并加盖本单位合同专用章或单位公章后生效，至双方履行完毕本合同规定的全部义务时终止。

2. 未尽事宜，经双方协商一致，签订书面补充协议，补充协议与本合同不一致的，以补充协议为准。

3. 本合同一式 柒 份，甲方执 伍 份，乙方执 贰 份，具有同等法律效力。

4. 本合同包括以下文件作为附件，包括不限于：项目工作初步组织实施方案。附件与本合同具有相同法律效力。

5. 以下无正文

附件 1 实施组织方案

一、项目概述

1.1 项目简介

根据北京市经济和信息化局印发的《北京市市级政务云管理办法》通知，将北京市知识产权资助链系统、保护中心信息平台系统、北京市海外知识产权公共服务信息库、北京市知识产权公共信息服务平台（以下简称“应用系统”）部署到北京市政务云上，并保证其服务符合管理办法。

1.2 项目必要性

2015 年 10 月，北京市经济和信息化委员会已通过公开招标方式确定市级政务云服务商，按照相关文件要求，以“上云为常态、不上云为例外”原则，各部门现有信息系统应逐步迁移上云，停止服务器、存储等相关软硬件采购。

1.3 项目目标

1.3.1 总体目标

本项目的总体目标是对北京市知识产权局各业务系统的运行环境进行持续优化与改造，提供政务云扩展服务，充分保障系统整体安全性，提高系统可靠性。

1.3.2 技术目标

租用政务云服务商提供的主机杀毒服务、主机安全加固、主机漏洞扫描、主机日志分析、数据库审计、安全态势感知等各类服务，完成业务系统的安全运维服务工作，确保入云系统安全、稳定的运行。

二、项目服务内容及要求

2.1 总体服务要求

按照甲方的有关规定及要求，提供租赁服务。

服务清单如下：

服务子类	计价单位	报价单位	数量	期限
主机杀毒服务	台	元/月	68	12
主机安全加固	台	元/次	136	——
主机漏洞扫描	台	元/次	136	——
主机日志分析	台	元/次	136	——
数据库审计服务	套	元/月	4	12
安全态势感知服务	系统	元/月	4	12
等保测评	系统二级等保测评	元/个	2	——

2.2 云平台运维服务

乙方按照甲方的相关规定及要求，实现对应用系统云主机的运维服务等工作。

1）硬件系统的监控及维护

按照甲方的有关管理规定及应用系统的需求，乙方需提供对基于云计算架构的硬件基础资源的监控及维护，并对监控与维护情况及时与甲方和对应系统的应用开发厂商做好协调沟通工作。

2）云平台监控及维护

按照甲方的有关管理规定及应用系统的需求，乙方需提供对基于云计算架构的云平台的监控及维护，并对监控与维护情况及时与甲方和对应系统的应用开发厂商做好协调沟通工作。

2.3 安全保障服务

按照甲方的有关管理规定及各个应用系统的需求，乙方需提供对各应用系统安全保障服务，承诺云平台底层物理环境满足等级保护三级要求，并在此基础上提供其它安全保障服务，以全方位满足入云系统的安全需求。

2.4 安全要求

乙方应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，能满足安全三级等保要求，并积极配合甲方根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。乙方管辖范围内的硬件、软件及支撑环境资源，至少达到业务系统的最高安全等级要求。

2.5 服务要求

1）服务规范

乙方须严格按照甲方制定的管理办法、流程及其他汇报制度、应急制度、文档管理、资产管理、基线管理、人员管理、培训与考试、知识库管理、安全管理等相关制度，开展标准化运维工作。

2）服务方式

乙方需利用监控系统或人工对机房环境、硬件设备及应用系统的运行情况进行每周7*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

乙方负责设立技术支持热线，并安排专人值守，为运维工作提供每周7*24小时热线支持服务。乙方针对甲方要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据甲方要求配合开展相关维护服务。

3）安全及保密要求

乙方须严格遵守甲方的相关信息安全规定，不得利用系统维护服务时的便利对甲方数据及其他信息擅自修改或透漏给第三方。

4）响应的及时性

乙方应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人每周7*24小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在1小时内到达运维现场提供服务。

系统发生宕机问题时，乙方应在30分钟内响应，在4个小时之内使系统恢复正常，故障处理完毕后提供相关系统宕机报告。

5）重点保障要求

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求乙方根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。

三、服务方案

为确保入云系统安全稳定地运行，租用政务云服务商提供的主机杀毒服务、主机安全加固、主机漏洞扫描、主机日志分析、数据库审计、安全态势感知等各类服务内容。

3.1 政务云扩展服务方案

主机杀毒与主机防护服务

对68台虚拟机安装防病毒软件与主机防护软件。

序号	项目子类	项目描述	数量	租用期限（月）
1	主机杀毒服务	1台	68	12

选用性能良好的防病毒软件和云平台系统软件结合，通过接口实现针对虚拟系统和虚拟主机之间的全面防护，无需在每个虚拟主机的操作系统中安装Agent程序，即可实现实时的针对所有虚拟主机的病毒防护。

防病毒服务是在不消耗虚拟机资源的情况下，对虚拟化环境进行有效的病毒防护和查杀。

通过无代理的网络版防病毒软件实现虚拟机环境下的病毒查杀，并对查杀结果和病毒防护状态进行监控。

虚拟化系统安全软件采用分布式的体系结构，整个防病毒体系是由五个相互关联的子系统组成：管理中心、安全虚拟设备、日志中心、

升级中心、查杀协作。各个子系统协同工作，共同完成对整个虚拟化平台的病毒防护工作，为企业级用户的虚拟化系统提供全方位防病毒解决方案。

并提供符合等保三级要求的主机权限管理及安全防护软件。

主机漏洞扫描与安全加固

提供136台次的主机安全加固与主机漏洞扫描服务。

序号	项目子类	项目描述	数量	租用期限（月）
1	主机安全加固	元/次	136	12
2	主机漏洞扫描	元/次	136	12

太极政务云提供的绿盟远程安全评估系统（NSFOCUS Remote Security Assessment System 简称：NSFOCUS RSAS）是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。

通过漏扫发现的漏洞，开展操作系统层漏洞安全加固工作。

日志分析

提供136次主机日志分析服务。

序号	项目子类	项目描述	数量	租用期限（月）
1	主机日志分析	1次	136	12

针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况。

系统采集的数据来源于主机、服务器、虚拟机的操作系统。通过

使用NT Eventlog（即在Windows计算机上安装通用代理，在通用代理上指定接受Windows日志的Syslog服务代理的IP地址）或采用WMI（直接在Windows计算机指定接受Windows日志的Syslog服务代理的IP地址，而不必安装通用代理）来采集Windows系列操作系统的日志信息，通过使用Syslog协议采集SUN Solaris、IBM AIX、Linux等操作系统的日志信息，能够全面记录系统特权命令的使用，包括：

Windows操作系统：

账户登录日志

账户管理日志

目录服务访问日志

审核登录日志

对象访问日志

审核策略更改日志

特权使用日志

详细跟踪日志

审核系统日志

文件操作日志：指定目录下的文件/子目录修改、删除日志

操作系统性能日志

Linux、Solaris、AIX操作系统：

账户登录注销日志

服务启停日志

账户管理日志

su日志

MODEM活动日志

FTP会话

Web访问日志

通过事件监控模块监控网络各个主机系统的日志信息，及时挖掘系统隐患、故障预警、异常操作、业务关联信息，通过响可视化分析和针对模板、趋势、峰值的关联，提供针对异常的检测应管理模块采取措施，保证系统的安全、可靠运行，实时将其结果输入综合分析决策支持与预警平台。

通过定期调度被保存的检测模板实现异常主动检测及告警事件生成。能够主动分析海量日志中的异常信息，向事件处理平台传递告警信息。

系统将收集来的数据统一存储和归档，选用企业级数据库Oracle、sqlserver作为支撑，支持海量数据存储，同时也支持磁盘柜、分布式文件、NAS和SAN等多种存储方式，便于扩充和统一查询检索。可以按照日志数据的不同类型和重要程度去设置不同数据的备份保存天数，从而满足不同级别的监管需求。

基于日志的审计主要体现在：

1）日志的综合查询搜索

用户随时按需定位和关联事件；

提供直观搜索和分析查询语言，实现在不具备了解数据必备知识的条件下获取有价值信息的功能；

可以交叉查询，支持复杂的查询语句，最后通过直观的方式表现出来；

支持关键字、基于时间、类型、协议、等级等多个条件的组合查询，便于快速产生所需的结果；

可以通过标签为数据进行附加注释，从而提升搜索和分析的有效性；

支持基于检索到的内容进行日志上下文关联查看及在线导出；

2）灵活多样的日志报表。

包括实时的在线报表和非实时的离线报表；

可以按照操作人员的角色分别生成报表；

可以按照所管理的设备生成报表；

可以生成有关审计事件严重程度等相关的 TOP10 报表；

报表输出格式可以转换为 PDF、pdf、html 等多种常用的标准格式；

支持报表内容的客户化定制，使用户可以通过管理界面对报告内容或格式进行定制，上述报表均可以以图形化方式输出显示或者打印。

数据库审计服务

提供 4 套数据库审计服务，通过 DAS 数据库审计软件来实现。

序号	项目子类	项目描述	数量	租用期限（月）
1	数据库审计服务	1 套	4	12

DAS 为了区分多个数据资产、业务应用系统，因此配置完部署模式后，需要配置业务系统，用于标识各个不同的数据资产。支持主流的数据库业务系统审计，包含 Oracle、SQL server、Mysql、DB2、WEB 系统。

DAS 是一款专业、实时进行数据库访问监视与审计的安全设备，为事后追查提供可靠的依据和来源。支持数据库操作行为审计记录，具体如下：

（1）支持多种数据库协议： Oracle、SQL server、Mysql、DB2。

（2） 审计内容包含：发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间等。

DAS 支持 web 审计的主要目的是为了支持三层关联功能。因为 DB 审计日志，所有的源 IP 都是来自 web 系统的，源 IP 只有一个，通常不方便做问题追溯。通过三层关联，可以还原 SQL 操作真实的访问者。web 审计需要镜像 web 端数据，同时策略开始 web 审计功能。通过审计 Web 日志，为三层关联分析提供数据来源。

安全态势感知服务

提供 4 套系统的安全态势感知服务。

序号	项目子类	项目描述	数量	租用期限（月）
1	安全态势感知服务	1 套	4	12

安全态势感知服务（TDP）能够对系统整体安全态势进行评估，帮助决策者快速感知系统的安全情况等级，提供清晰明了的安全态势大屏，帮助重大安全决策以及日常安全运营；由于大部分被外部攻击者控制的主机，都需要跟黑客控制端进行网络通讯，由于微步在线拥有业界领先的威胁情报，所以可以支持 TDP 精准发现连接黑客端的主机，从而精准定位失陷主机；与此同时，微步在线采用旁路双向流量检测的模式，能够精确识别是否攻击成功，安全运营人员只需要聚焦成功攻击，从而节约安全管理人员宝贵时间，提供安全运营效率；TDP 还能够为用户提供资产梳理功能，以及风险排查功能，帮助用户建立全局视角，明确自身弱点。最后，TDP 提供了科学的安全报告，报告类型丰富，满足多种场景，同时能够提供安全事件处置流程，帮助用户完成安全事件处置闭环。