生态环境信息化系统信息安全等级保护整改设备及软件采购项目采购合同

合同编号：

甲方：赤峰市生态环境监控中心（采购人单位名称）

地址：赤峰市新城区临潢大街23号（填写详细地址）

乙方：内蒙古泰航信息技术有限公司（成交供应商单位名称）

地址：内蒙古自治区赤峰市红山区西城街道万达广场A块地1B号楼01238、01239、012310室（填写详细地址）

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关法律法规、规范性文件以及生态环境信息化系统信息安全等级保护整改设备及软件采购项目、NMGZX-2026-014HW、1包（填写项目名称、项目编号、包号）的成交结果、谈判文件、响应文件等文件的相关内容，甲乙双方经平等协商，就如下合同条款达成一致意见。

一、甲方向乙方采购的货物基本情况

（一）根据谈判文件及成交结果公告，甲方所采购的货物基本情况如下：详见附件。

（二）货物名称、数量、规格型号、生产厂家、品牌、单价、与货物相关的服务等详细内容，见合同附件-货物清单。

二、乙方交付货物的时间及地点

（一）交付时间：合同签订生效后30天内完成全部货物供货、安装、调试、验收并交付使用。

（二）交付地点：赤峰市新城区临潢大街23号赤峰市生态环境监控中心2楼机房。

（三）交付货物的名称及数量：生态环境信息化系统信息安全等级保护整改设备及软件采购项目/1项。

（四）乙方交付货物代表及联系电话：王松涛/15047610791。

（五）甲方接收货物代表及联系电话：刘佳鑫/15547617118。

三、乙方交付货物的质量

（一）乙方交付的货物应同时满足：

1.符合国家法律法规和规范性文件对货物的质量要求；

2.符合甲方谈判文件对货物的质量要求；

3.符合乙方在响应文件中或谈判、谈判过程中对货物质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方货物质量的验收依据。

（二）乙方应根据国家法律法规和规范性文件的规定、谈判文件的相关要求、响应文件及乙方承诺、声明或保证，向甲方提供相应的货物质量证明文件。

四、乙方交付货物的包装及标识

（一）乙方交付货物的包装和标识应同时满足：

1.符合国家法律法规和规范性文件对产品包装及标识的要求；

2.符合甲方谈判文件对货物包装及标识的要求；

3.符合乙方在响应文件中对货物包装及标识作出的承诺、声明或保证；

4.符合绿色环保、运输及安全性等要求。

（二）货物的包装费用由乙方承担。

五、货物的运输要求

（一）运输方式及运输线路：送货上门。

（二）运输、保险及其他相关费用由乙方承担。

六、甲方对货物的验收

（一）货物到货后7个工作日内完成外观、数量初步验收；系统联调完成后20个工作日内完成整体功能及等保相关符合性验收；区分外观瑕疵与隐蔽功能性瑕疵的异议期限，同时明确质量异议必须以书面形式送达。

（二）在甲方收到货物7日内，如发现质量问题，甲方应在3日内向乙方提出书面异议，甲方逾期提出的，视为乙方所交付的货物质量符合合同的约定。乙方在收到甲方关于质量问题的书面异议后，应当在7日内负责解决处理。

（三）乙方提交的货物数量、规格型号及质量不符合本合同要求的，甲方应在验收记录中作出明确记载，保留相关的证据，并有权拒绝接受货物，解除合同且不承担任何法律责任。

（四）在合同正文中明确：货物出厂直至现场验收合格之前，运输、装卸、

损毁、保险全部风险由乙方承担。

（五）以《内蒙古自治区政府采购项目履约验收管理办法》作为项目验收法定依据。

（六）乙方交付货物时，同步交付产品合格证、出厂检测报告、使用说明书、保修凭证、等保整改配套全套资料。

七、合同金额

在乙方提供完全符合合同要求的货物的前提下，本合同总金额为509,300.00元（小写）伍拾万零玖仟叁佰元整（大写）。

八、付款时间、金额及条件

（一）付款方式：全部货物供货、安装、调试、验收并交付使用，经甲方组织验收合格并出具验收单后，凭相应金额的发票支付全部货款。采用公对公银行转账方式支付，乙方须提供合法、有效、合规的普通发票，否则甲方有权顺延付款，不承担违约责任。

（二）乙方账户信息

乙方名称：内蒙古泰航信息技术有限公司

开户银行：中国农业银行股份有限公司赤峰松山支行

银行账号：05241101040002094

（三）本项目全部货物供货、安装、调试完毕，整体项目验收合格并出具正式验收书，乙方提供合法有效的普通发票后，甲方通过公对公转账一次性支付全部合同价款。本合同不设置谈判文件未载明的其他付款前置条件。

九、货物质量保证及售后服务

谈判文件对货物质量保证期及售后服务作出明确要求的，适用谈判文件对保证期和售后服务的规定，如乙方在响应文件及谈判、谈判过程中对货物质量保证期和售后服务作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

十、知识产权

乙方保证其提供的货物的全部及部分，均不存在任何侵犯第三方知识产权的情形。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

十一、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额的 1‰ 承担违约责任。延期达到 30 日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期交付货物的，每延期一日，乙方应按照合同总金额的 1‰ 承担违约责任。延期达到 30 日，甲方有权解除合同，拒付延期部分货物的相应货款，并要求乙方赔偿甲方的经济损失。

（四）乙方交付的货物不符合质量约定或乙方未履行相应的质量保证责任及售后服务义务、或存在侵权行为的，甲方有权退货，并要求乙方支付合同总金额10%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额 10%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（七）一方严重违约，应当先行书面催告，给予合理整改期限，期限届满仍未改正，守约方方可解除合同。

（八）本合同后续签订的补充协议，不得变更本项目采购标的、合同总价等实质性内容，追加采购金额不得超过原合同金额的 10%。

十二、不可抗力

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在 15 天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

遭受不可抗力一方应在不可抗力发生后 7 日内书面通知对方，并于 15 日内提交有效证明材料。

十三、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式解决：

（一）提交甲方住所地有管辖权的仲裁委员会仲裁。

（二）向甲方住所地有管辖权的人民法院起诉。

十四、合同保存

合同文本一式 肆 份，甲乙双方各执 贰 份。合同文本保存期限为从采购结束之日起至少保存十五年。

十五、合同附件

全部附件均属于本合同不可分割部分，全部附件应当加盖甲乙双方公章，整套合同文件加盖骑缝章，其内容与本合同具有同等的法律效力：

1、货物清单（应盖章确认）

2、乙方出具的报价单（函）

3、成交结果公告及成交通知书

4、甲方谈判文件

5、乙方响应文件

6、甲乙双方商定的其他文件

十六、双方约定的其他条款

应当按照政府采购法规规定完成本合同备案、公告工作，乙方予以配合。

十七、本合同未尽事宜，由双方另行签订补充协议，补充协议是本合同的组成部分。

十八、本合同由甲乙双方盖章生效。

甲方名称（盖章）：赤峰市生态环境监控中心

甲方法定代表人或授权代表人（签字）：

签订日期：2016年 9月 14日

乙方名称（盖章）：内蒙古泰航信息技术有限公司

乙方法定代表人或授权代表人（签字）：

签订日期：2016年 9月 14日

合同附件-货物清单

序号	货物名称	规格型号	品牌	技术要求	数量	单价（元）	总价（元）
1	防火墙授权	H3C	LIS-F1000-AV-1Y(V7)	适配原有防火墙，原有型号为H3C SecPath F1000系列,AV 防病毒安全License,1年	2套	1500	3000
2	防火墙授权	H3C	LIS-F1000-IPS1-1Y	适配原有防火墙，原有型号为H3C SecPath F1000系列,IPS 特征库升级服务,1年	2套	2300	4600
3	上网行为管理授权	H3C	LIS-ACG1000-T	适配原有上网行为管理设备，原有型号为H3C SecPath ACG1000-T,应用识别&URL特征库升级服务1年	1套	2700	2700
4	防火墙	启明星辰	USG-FW-4000-T-NF3100	1、标准1U设备，双路供电电源；16个10/100/1000M自适应千兆电接口，2个千兆SFP接口，4个SPF+万兆接口；标配64G SSD硬盘；质保期三年；最大吞吐10G，最大并发1000万，每秒新建连接100万； 2、必须支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 3、必须支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。 4、必须支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 5、支持ISP路由，支持联通、电信、教育网、移动等ISP服务商地址列表，列表可导出及导入，可通过Web界面选择不同的ISP服务商实现快速切换。 6、支持将任意接口数据完全镜像到设备自身的其他接口，用于抓包分析。 7、支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计	4台	48900	195600

				等功能,简化用户管理。 8、支持同一个地址对象中可以包含 IP、IP 段、IP range、排除地址等多种类型。 9、支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。 10、支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。 11、支持策略命中数显示，并支持通过安全策略命中数范围查询。 12、服务器负载均衡支持 10 种算法。 13、支持 DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现 spoke to spoke 互通，不必建立额外隧道。 14、SSL VPN 默认支持 200 个并发用户授权。 15、支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。 16、内置 IPS 特征库，特征规则数量不少于 3,600 条，特征库可按分组进行管理，连续 10 条以上特征库数量。支持扩展特征库，提高 IPS 的检测能力，IPS 特征规则数量合计不少于 8000 条。 17、支持细粒度的自定义 IPS 特征功能，要求支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等 17 大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。 18、支持 HTTP 类攻击重定向功能，能够把 HTTP 协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析。 19、支持基于策略的病毒扫描与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的病毒防护策略。 20、支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测			

				多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境。 21、支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。 22、支持依据协议、源目的端口、二进制特征码等条件自定义应用。 23、支持 URL 分类智能学习，可通过对已分类网站自动学习分类关键字，实现对未知网页的识别。 24、支持外发信息的控制，可实现对 BBS 发帖的限制和关键字过滤；可实现发送微博信息的限制和关键字过滤;可实现对 WEB 邮件的收发限制和关键字过滤，支持 5 种以上的 web 邮件系统。 25、支持对主流数据库基于用户的细粒度权限控制，实现对数据库服务器的保护。 26、支持针对 URL 类型进行流量管理，可以针对不同类型的 URL 配置不同的流量管理规则,包括最大带宽、保证带宽、协议流量优先级等。 27、支持 DSCP 流量分级设置。 28、支持用户的 AD 域、POP3、BJCA 单点登录，支持自定义单点登录监听端口。 29、支持至少 3 个 Syslog 服务器，发送流量、系统或默认 3 类型日志到不同服务器。 30、支持界面选择系统语言（中文、英文）。			
5	防火墙	启明星辰	USG-FW-12600-T-BM	1、标准 2U 设备，双电源；10 个 10/100M/1000M 自适应千兆电接口、8 个千兆 SFP 接口，8 个万兆 SFP+接口，3 个接口扩展槽。64G SSD 硬盘；质保期三年；整机网络层吞吐量：30Gbps，整机 TCP 并发：1200 万； 2、必须支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 3、必须支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流	1 台	68500	68500

				量智能分配到不同的链路。 4、必须支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 5、支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换。 6、支持将任意接口数据完全镜像到设备自身的其他接口，用于抓包分析。 7、支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 8、支持同一个地址对象中可以包含 IP、IP 段、IP range、排除地址等多种类型。 9、支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。 10、支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。 11、支持策略命中数显示，并支持通过安全策略命中数范围查询。 12、服务器负载均衡支持 10 种算法。 13、支持 DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现 spoke to spoke 互通，不必建立额外隧道。 14、SSL VPN 默认支持 200 个并发用户授权。 15、支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。 16、内置 IPS 特征库，特征规则数量不少于 3,600 条，特征库可按分组进行管理，连续 10 条以上特征库数量。支持扩展特征库，提高 IPS 的检测能力，IPS 特征规则数量合计不少于 8000 条。			

				17、支持细粒度的自定义IPS特征功能，支持DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等17大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。 18、支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析。 19、支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略。 20、支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境。 21、支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。 22、支持依据协议、源目的端口、二进制特征码等条件自定义应用。 23、支持URL分类智能学习，可通过对已分类网站自动学习分类关键字，实现对未知网页的识别。 24、支持外发信息的控制，可实现对BBS发帖的限制和关键字过滤；可实现发送微博信息的限制和关键字过滤;可实现对WEB邮件的收发限制和关键字过滤，支持5种以上的web邮件系统。 25、支持对主流数据库基于用户的细粒度权限控制，实现对数据库服务器的保护 26、支持针对URL类型进行流量管理，可以针对不同类型的URL配置不同的流量管理规则,包括最大带宽、保证带宽、协议流量优先级等。 27、支持DSCP流量分级设置。 28、支持用户的AD域、POP3、BJCA单点登录，支持自定义单点登录监听端口。			

				29、支持至少 3 个 Syslog 服务器，发送流量、系统或默认 3 类型日志到不同服务器。 30、支持界面选择系统语言（中文、英文）。			
6	万兆交换机	H3C	S6520-24S-SI	包括 2.56Tbps/23.04Tbps 背板带宽和 360Mpps 包转发率，支持 10M/100M/1000Mbps 及 10Gbps 多速率传输，提供 24 个 1/10G SFP Plus 端口	1 台	4000	4000
7	光模块	H3C	SFP-XG-SX-MM850-D	万兆光模块多模双纤 10G SFP+光纤模块 LC 接口 传输 300m 米	2 块	170	340
8	杀毒系统	管理中心		C/S 架构，软件包含控制中心和客户端，实现对客户端防病毒的集中管理、策略配置、智能更新、定时查杀、报表查看等功能，3 年病毒特征库升级授权，	1 套	1500	1500
		Windows 授权		三年授权	5 点	130	650
		Linux 授权		三年授权	8 点	300	2400
9	SSL 证书	天威诚信	OV	1、可以绑定域名和公网 IP 2、主流浏览器兼容性 3、中文证书字段支持 4、加密位数最高支持 256 位	4 套	2700	10800
10	VPN	启明星辰	SAG-6000-V1300	1、标准 1U 机架式设备，1 个 RJ-45Console 口，6 个 10/100/1000M 自适应电口，1 个网络接口扩展槽位，专用接口板卡，2 个 USB 口，交流单电源；SSL 加解密吞吐 300Mbps，整机吞吐 2.5Gbps；三年硬件保修和基础型技术支持服务。 2.专业 IPSec VPN 和 SSL VPN 二合一设备，采用符合国际标准 SSL、TLS 协议，同时支持 IPSec VPN 和 SSL VPN 功能，为非插卡或防火墙带 VPN 模块设备。 3.支持 IPSec、SSL、PPTP、L2TP VPN 的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部 VPN 类型接入，无需分别购买不同	1 台	35210	35210

				类型 VPN 接入授权 4.产品支持多系统引导，即系统 A、系统 B 和备份系统，可在管理员界面直接配置启动顺序，支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且配置文件分别支持加密导入导出。备份系统用于应急恢复。 5.SSL VPN 客户端同时支持国际算法和国密算法，可由用户自定义选择。 6.支持密码自助找回功能，当用户的密码忘记时，可自行通过短信验证码方式找回密码，减轻管理员维护压力。 7.客户端支持龙芯、兆芯、飞腾、鲲鹏等国产化 CPU 平台，支持中标麒麟，银河麒麟、普华、深度 OS、优麒麟、UOS 统信、中科方德等国产化操作系统客户端。 8.产品必须支持全局配置安全检测，针对检测结果支持一键优化或者一键锁定风险配置项。 9.虚拟门户支持选择多种登录方式，包含口令认证、证书认证、匿名登录、企业微信登录、钉钉扫码登录等。 10.支持 App 应用的远程安全访问加固，可以与钉钉、企业微信等移动业务应用的入口对接，实现用户在互联网访问内置 H5 应用的安全接入。支持自动拉起 VPN，实现其内置应用的安全接入。 11.支持对长时间未登录账号进行锁定功能。 12.支持单点登录功能（SSO），支持移动用户登录 VPN 后再登录内部 B/S、C/S 应用系统时不需要二次重复认证。支持针对不同的访问资源设定不同的 SSO 用户名和密码，支持用户自行修改 SSO 账号。支持 CS 单点登录工具助手，支持自动识别登录窗口自动形成配置文件 13.采用加密方式建立隧道连接，支持自主隧道配置技术。 14.采用自主研发的解析方法技术，实现对网络安全设备操作的命令行进行深度解析，同时产生解析记录。			

				15.产品必须在 Windows、统信 UOS、银河麒麟等操作系统上支持远程应用发布 B/S 和 C/S 应用功能，发布 CS 应用客户端界面而非整个桌面进行发布，只传输鼠标、键盘操作和显示数据，无需安装 CS 客户端即可支持 CS 模式软件系统的远程应用。 16.远程应用数据传输过程中使用 SSLVPN 协议加密，使用一个客户端保证远程应用数据传输的合法性和安全性。 17.产品支持自适应用户使用习惯，比如：支持本地输入法、支持文件导入导出、支持虚拟打印、本地磁盘资源映射、本地打印机、本地串行口、本地智能卡，本地输入法；支持剪切板，并能够实现剪贴板数据流控制。 18.产品必须支持集群负载均衡策略，即当存在多台终端发布服务器时，可以根据预先配置策略（轮询、会话数、CPU 占用率、内存占用、用户绑定）将用户分配到不同的终端服务器。 19.产品必须支持多数据库，根据用户规模的大小，可以灵活切换 SQLite 和 Mysql 数据库，支持数据库备份和还原操作。 20.产品支持对在线用户的实时监测，包括 VPN 用户信息、程序名称、会话 ID、客户端名称和用户类型。 21.产品支持用户访问策略，支持访问痕迹的留存、支持对访问用户的详细信息查询（客户端名称、客户端特征码、客户机 MAC、登录时间、登录用户名等）、支持账号和客户端 MAC 的关联绑定，仅允许绑定的 MAC 地址客户机访问。 22.支持用户 IE 配置一键复制，提高部署效率，可以复制各种 IE 插件设置、cookie 设置、权限设置等。 23.支持用户将文件存储在服务器端私人文件夹当中，具有用户私人属性，仅允许用户访问到自己私人文件夹的方法。 24.通过磁盘映射方式，进行客户端本地磁盘的物理映射，满足从应用导出数据到本地磁盘或者从本地磁盘选择文件导入到应用上的需求。通过私			

				有“云盘”方式进行进行文件的上传和下载控制，且实现单向控制，即只允许下载不能上传或者只能上传不能下载。			
11	入侵检测系统	启明星辰	NT3000-CS-M-PLUS	1、1U 上架设备（1 个 RJ-个 Console 口，6 个 10/100/1000 Base-T 接口，2 个 USB 口，2 个千兆光接口插槽（不包含光模块），2 个万兆光口插槽（不包含光模块），支持 2 个扩展插槽，冗电，包含 2T 硬盘，含 CS-PLUS 软件）一台， 2、支持常见 HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、Dcerpc、DNS、IKEV2、NFS、Krb5、DHCP、SNMP、SIP、RFB、RDP 等应用层协议； 3、支持物联网 Mqtt 协议； 4、支持常见工控协议 Modubus、Enip 等协议； 5、支持导入 HTTPS 证书，对加密流量进行解密及还原：支持 SSL3.0，TLS1.0/1.1/1.2； 6、支持基于不完整会话流的单包攻击检测能力； 7、支持对检测的告警事件结合双向检测机制、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果，至少包含的结果类型为：攻击尝试、攻击成功、正在利用； 8、支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，完美兼容业界主流 snort 规则； 9、系统具备攻击链分析模型，通过被攻击者视角展示主机遭受攻击状态迁移图和攻击阶段统计，分析内部资产被外部地址攻击详情，多维度分析攻击异常开始时间，使用手段； 10、系统具备专有的挖矿分析场景:基于特征库和威胁情报检测挖矿主机，对挖矿主机进行不同阶段的展示，至少包括连接矿池阶段、获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络	2 台	59000	118000

				中的挖矿主机活跃程度，挖矿币种有直观的图形化展示； 11、支持通过扫描方式发现资产的类型，包括终端、视频设备、办公设备、网络设备、服务器、安全设备、工控设备等； 12、支持通过扫描实现对资产精准识别，粒度包含设备类型，操作系统类型（如 Windows，linux 等），MAC 地址，IP 地址，端口服务等资产信息； 13、具备通过 web 页面导入 pcap 包离线回放检测能力，单个导入回放的数据包最大支持 1G，支持批量导入或选择文件夹导入，最多支持导入 100 个数据包，支持选择回放流量业务口； 14、支持通过页面，对告警前后存储报文数量进行配置，最多支持存储和下载告警前 50 个和后 50 个数据包； 15、kafka 外发方式支持开启/关闭安全认证，支持的加密套件包括 PLAIN、SHA-256、SHA512 方式； 16、支持设备系统管理，可通过页面下发诊断对设备关键进程进行监测，同时可一键恢复关键进程，增强设备易用性与运维便捷度。 17、包含三年的特征库升级，并提供三年原厂质保。			
12	数据库审计	启明星辰	DA-FT-1200U	审计一体机，1U 上架专用设备，6 个电口（含 1 个管理口，1 个 HA 口），4 个千兆 SFP 接口插槽，3 个接口扩展槽，可扩展天玥 DA-FT 系列接口板卡，1 个 RJ45 串口，硬盘 4T。含嵌入式审计软件一套，支持主流数据库如 Oracle、SQL-Server、MySQL、达梦、人大金仓等数据库的审计，同时具备基础网络协议如 HTTP、Telnet 等协议的审计功能。 2、支持 Oracle、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、Teradata、CACHE、Clickhouse、marialDB、TiDB、Greenplum 等主流数据库的审计。 3、支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息。 4、支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨	1 台	62000	62000

				杉、OceanBase、AnalyticDB MySql 、AnalyticDB MySql、AnalyticDB PostgreSQL、RDS MySql、RDS PostgreSQL 等数据库的审计。 5、支持 MongoDB、redis 数据库的审计。支持 Hbase、hive、ES 的审计。。 6、支持对针对数据库的 SQL 注入、CVE 高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 7、支持审计访问数据库的时间，源/目的 IP，源/目的端口，源/目的 mac，资源账号，数据库名，规则名称，表名，命令，SQL 语句、级别，响应时间、错误码，影响行数，连接方式，客户端程序名，模式名，客户端用户，SQL 执行结果。 8、支持审计 HTTP 和 HTTPS 协议的 URL、访问模式、cookie、页面内容、Post 内容。。 9、支持对邮件协议的审计，包括 smtp、pop3、imap 协议，能够审计发件人、收件人、时间、返回码等。 10、支持基于网络流量的资产发现功能，能够发现数据库表和资源账号，其中数据库表的自动发现支持表名、数据库名、发现次数和发现日期，资源账号自动发现支持在线天数、首次发现日期、末次发现日期。 11、数据库审计策略支持频次统计，某一操作在周期时间内达到设定的次数阀值后可以进行单独记录和展示，周期事件和次数可按需配置。 12、支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源 ip、客户端程序名、命令、表名、错误码等按需定义，可根据昨天、最近七天、最近 30 天以及自定义时间进行轨迹显示，可显示下一节点数量，可在某一维度中进行筛选，支持钻取功能。 13、支持基于数据库访问时间、源/目的 IP、数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、SQL 语句关键字、SQL 响应时间、数据库返回行数、客户端程序、客户端用户、级别、数据库返回码等不低于 36 种查询条件，其中支持数据库返回码实时说明，帮助管理员快			

				速对返回码进行识别。 14、支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多 IP 登录、上下班操作量对比异常、操作响应时间分析、用户变更、弱口令检测。 15、支持疑似暴力破解、疑似撞库攻击、场景的操作异常分析；行为周期与阀值可按需定义。 16、查询需返回全部符合查询条件的事件，不可限制最大返回数量，防止因返回结果不全导致异常信息遗漏。 17、可支持根据 sql 语句关键字进行查询，查询事件为 sql 语句中包含该关键字的所有符合条件的操作记录。 18、含 3 个被审计数据库服务数，并提供三年原厂质保。			

甲方名称（盖章）：赤峰市生态环境监控中心　　乙方名称（盖章）：内蒙古泰航信息技术有限公司