证券代码：300297　　证券简称：蓝盾股份　　上市地：深圳证券交易所

蓝盾信息安全技术股份有限公司

Bluedon Information Security Technologies Co.,Ltd

（广东省广州市天河区天慧路 16 号）

2020 年创业板非公开发行 A 股股票预案

二〇二〇年二月

公司声明

1、本公司及董事会全体成员保证本预案内容真实、准确、完整，并确认不存在虚假记载、误导性陈述或重大遗漏。

本预案按照《创业板上市公司证券发行管理暂行办法》、《公开发行证券的公司信息披露内容与格式准则第 36 号—创业板上市公司非公开发行股票预案和发行情况报告书》等要求编制。

2、本次非公开发行 A 股股票完成后，公司经营与收益的变化，由公司自行负责；因本次非公开发行 A 股股票引致的投资风险，由投资者自行负责。

3、本预案是公司董事会对本次非公开发行 A 股股票的说明，任何与之相反的声明均属不实陈述。

4、投资者如有任何疑问，应咨询自己的股票经纪人、律师、专业会计师或者其他专业顾问。

5、本预案所述事项并不代表审批机关对于本次非公开发行 A 股股票相关事项的实质性判断、确认、批准或核准，本预案所述本次非公开发行 A 股股票相关事项的生效和完成尚待取得有关审批机关的批准或核准。

特别提示

1、本次非公开发行股票相关事项已经公司第四届董事会第十九次（临时）会议审议通过，尚需经公司股东大会审议通过并经中国证监会核准后方可实施。

2、本次非公开发行股票数量不超过本次发行前上市公司总股本的 30%，以截至 2020 年 2 月 26 日，公司总股本 1,249,799,145 股计算，即不超过 374,939,743 股（含本数）。在董事会对本次非公开发行股票作出决议之日至发行日期间，上市公司若发生派息、送红股、资本公积金转增股本等除权、除息事项及股权激励等引起公司股份变动的，则本次发行的股份数量将作相应调整。最终发行数量由公司董事会根据股东大会授权及发行时的实际情况与保荐机构（主承销商）协商确定。

3、本次非公开发行股票的定价基准日为发行期首日。本次非公开发行股票的价格不低于定价基准日前二十个交易日公司股票交易均价（定价基准日前 20 个交易日股票交易均价=定价基准日前 20 个交易日股票交易总额/定价基准日前 20 个交易日股票交易总量）的 80%。具体发行价格由股东大会授权董事会在取得中国证监会关于本次非公开发行核准批文后，由董事会和保荐机构（主承销商）按照相关法律法规的规定和监管部门的要求，根据竞价结果与保荐机构（主承销商）协商确定。

4、本次非公开发行的发行对象为不超过 35 名特定投资者，包括符合中国证监会规定的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者、其他境内法人投资者和自然人。证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托投资公司作为发行对象，只能以自有资金认购。最终发行对象由股东大会授权董事会在获得中国证监会发行核准文件后，按照中国证监会相关规定，根据竞价结果与保荐机构（主承销商）协商确定。所有发行对象均以现金方式认购本次发行的股票。

5、本次非公开发行股票完成后，发行对象所认购的股票自本次非公开发行股票上市之日起 6 个月内不得转让。限售期结束后按中国证监会及深圳证券交易所的有关规定执行。

6、本次非公开发行募集资金总额不超过 200,000 万元（含 200,000 万元），扣除发行费用后的募集资金净额将全部用于如下项目：

单位：万元

序号	分类	项目名称	项目总投资	拟投入募集资金
1	基础网络安全产业化	全线网络安全产品国产化及可信研发	73,333.50	35,700.00
2		新一代 APT 威胁检测与防御系统	18,843.00	9,550.00
3		工业网络统一威胁管控平台	23,560.00	11,150.00
4		自主可控终端检测与高级防御系统	24,365.00	12,000.00
5	安全应用产业化	大数据安全监控与交换平台	24,854.00	12,300.00
6		安全云虚拟终端系统	17,308.00	7,900.00
7		视频安全接入与威胁管控平台	22,175.50	10,100.00
8		网络空间仿真靶场实训竞技平台	22,742.00	11,300.00
9		新一代智慧城市安全运营平台	56,318.00	30,000.00
项目合计			283,499.00	140,000.00
补充流动资金			60,000.00	60,000.00
合计			**343,499.00**	**200,000.00**

注：合计数据尾数因四舍五入原因，与相关单项数据计算得出的结果略有不同。

本次实际募集资金净额相对于上述项目所需资金存在不足的部分本公司将通过自筹资金解决。在不改变本次募投项目的前提下，公司董事会可根据项目的实际需求，对上述项目的募集资金投入顺序和金额进行适当调整。在本次非公开发行募集资金到位之前，若公司用自有资金投资于上述项目，则募集资金到位后将按照相关法规规定的程序予以置换。

7、本次非公开发行后，公司控股股东、实际控制人不会发生变化。本次非公开发行股票不会导致公司股权分布不具备上市条件。

8、本次发行前公司滚存的未分配利润由本次发行完成后的新老股东共享。

9、公司实施连续、稳定的利润分配政策，重视对投资者的合理回报。根据《关于进一步落实上市公司现金分红有关事项的通知》、《上市公司监管指引第 3 号——上市公司现金分红》等相关法律、法规、规范性文件及《公司章程》等相关制度的规定，结合公司的实际情况，公司董事会对股东回报规划进行了补充修改，特制定了公司《未来三年（2020-2022 年）股东分红回报规划》。

关于公司利润分配政策、现金分红政策的制定及执行情况、最近三年现金分红金额及比例、股东回报规划，未分配利润使用安排等情况，详见本预案“第五节 发行人利润分配情况”。

10、根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）、和《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证券监督管理委员会公告[2015]31 号）要求，公司就本次非公开发行股票事宜对即期回报摊薄的影响进行了分析并提出了具体的填补回报措施，相关主体对公司填补回报措施能够得到切实履行作出了承诺。相关情况详见本预案 “第六节 与本次发行相关的董事会声明及承诺事项”相关说明。

公司所制定的填补回报措施不等于对公司未来利润做出保证。投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。提请广大投资者注意。

目 录

释 义

除特别说明，在本预案中，下列词语具有如下意义：

简称	指	含义
本公司、公司、发行人、蓝盾股份	指	蓝盾信息安全技术股份有限公司
中经汇通	指	中经汇通有限责任公司
本次发行 本次非公开发行	指	蓝盾信息安全技术股份有限公司2020年创业板非公开发行A股股票
本预案	指	蓝盾信息安全技术股份有限公司2020年创业板非公开发行A股股票预案
定价基准日	指	本次非公开发行的发行期首日
国务院	指	中华人民共和国国务院
国家发改委	指	中华人民共和国国家发展和改革委员会
工信部	指	中华人民共和国工业和信息化部
《公司法》	指	《中华人民共和国公司法》
《证券法》	指	《中华人民共和国证券法》
《公司章程》	指	《蓝盾信息安全技术股份有限公司章程》
中国证监会	指	中国证券监督管理委员会
股东大会	指	蓝盾信息安全技术股份有限公司股东大会
董事会	指	蓝盾信息安全技术股份有限公司董事会
A股	指	人民币普通股
元、万元	指	人民币元、人民币万元
CNVD	指	国家信息安全漏洞共享平台（ChinaNationalVulnerabilityDatabase）
CMMI5	指	软件能力成熟度模型集成，是由美国国防部与卡内基-梅隆大学和美国国防工业协会共同开发和制定的一套评估认证体系，CMMI模型分为5级，其中CMMI5级为最高级，标志着企业在标准化、规范化、成熟度等方面表现优秀
安全产品	指	用于保证信息安全的各种软件产品和相关的软硬一体化产品
安全服务	指	根据客户需求提供与信息安全相关的安全测评、技术支持、安全管理咨询、系统维护、运营管理、安全培训、安全托管等内容
安全运营	指	利用先进的云计算技术，搭建云安全综合运营平台，为客户提供诸如网站安全防护等一系列服务，让客户得到"零部署"、"零维护"等一站式的智能安全防护体验
等级保护	指	信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护的一种工作，包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段，要求不同安全等级的信

		息系统应具有不同的安全保护能力
数据库审计	指	能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断
云安全	指	一是云计算安全，是指云计算自身的安全保护；二是安全云服务，是指传统安全产品的云化
虚拟化技术	指	一种资源管理技术，是将计算机的各种实体资源，如服务器、网络、内存及存储等，予以抽象、转换后呈现出来，打破实体结构间的不可切割的障碍，使用户可以比原本的组态更好的方式来应用这些资源

注：本预案中若出现总计数与所列数值总和不符，均为四舍五入所致

第一节 本次非公开发行股票方案概要

一、公司基本情况

中文名称：	蓝盾信息安全技术股份有限公司
英文名称：	Bluedon Information Security Technologies Co.,Ltd.
注册地址：	广东省广州市天河区天慧路16号
办公地址：	广东省广州市天河区天慧路16号-蓝盾信息安全产业基地
成立时间：	1999年10月29日
股份公司设立日期：	2009年8月11日
上市时间：	2012年3月15日
注册资本：	1,249,716,932元
经营范围：	计算机软、硬件开发；计算机信息系统集成、布线，承接网络工程建设项目，信息技术、数码技术开发、服务，计算机网络技术服务，网络安全信息咨询；计算机信息安全设备制造；监控系统工程安装服务；保安监控及防盗报警系统工程服务；计算机网络系统工程服务；安全技术防范系统设计、施工、维修；安全系统监控服务；科技信息咨询服务；网络技术的研究、开发；计算机整机制造；计算机零部件制造；计算机电源制造；计算机外围设备制造；计算机应用电子设备制造；计算机房维护服务；计算机及通讯设备租赁；计算机技术开发、技术服务；计算机房设计服务；计算机信息安全产品设计；计算机和辅助设备修理；电子产品设计服务；安全技术防范产品制造。（具体经营范围以章程内实际记载为准）。
法定代表人：	柯宗贵
统一社会信用代码：	91440000707689817C
股票上市地：	深圳证券交易所
股票简称：	蓝盾股份
股票代码：	300297
联系电话：	020-85639340
传真电话：	020-85639340
邮政编码：	510665
公司网址：	www.bluedon.com
电子信箱：	stock@chinabluedon.cn

二、本次非公开发行股票的背景和目的

（一）本次非公开发行股票的背景

1、信息安全上升至国家战略，行业迎来巨大发展契机

随着我国综合国力的增强，国家发展迎来巨大机遇的同时，国家安全也面临着多方面的挑战。特别是现在我国正处于发展转型期，情况复杂、矛盾多发，安全形势呈现多样化、复杂化、动态化的特点。在此背景下，国家对安全特别是信息安全的重视与日俱增：2013 年 11 月，国家安全委员会正式成立；2014 年 2 月，中央网络安全与信息化领导小组正式成立；2015 年 7 月，《中华人民共和国国家安全法》正式施行；2017 年 6 月，《中华人民共和国网络安全法》（简称“《网络安全法》”）正式施行，从立法的角度彰显了信息安全的战略高度；2019 年 12 月，《网络安全等级保护基本要求》（GB/T22239-2019）正式执行，网络等级保护进入 2.0 时代（简称“等保 2.0”），等保 2.0 时代将监管范围从政府事业单位扩大到所有网络运营主体，评级对象的范围扩大到云计算平台、工控、物联网、移动设备等新一代 IT 基础设施，还增加了评级的工作内容，极大扩展了网络安全保护的广度和深度。

从政策趋势来看，未来政府对信息安全建设的支持力度仍将持续提升。随着国家信息安全战略规划以及相关政策的稳步推进落实，信息安全市场正面临爆发式增长需求，信息安全行业将迎来巨大政策性红利和前所未有的发展契机。

2、国产化基础软硬件与可信计算的结合已成为今后我国网络安全保护的基石

随着美国持续加大对中国的技术封锁，核心技术和关键产品自主可控的重要性凸显。近年来，国家高度重视自主可控信息产业的发展，明确了计算机信息系统的自主、可控、安全需求，大力推进党、政、军及关系国家安全的关键行业的网络安全建设和自主可控信息系统建设，并相应的出台了一系列的政策和要求，牵引自主可控信息产业的发展。早在 2014 年科技部、工信部等部门就发布了《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》，提出至 2019 年各银行业金融机构对安全可控信息技术的应用达到不低于 75%的总体

占比目标。2016 年，中共中央办公厅、国务院办公厅印发了《国家信息化发展战略纲要》指出，到 2025 年根本改变核心关键技术受制于人的局面，形成安全可控的信息技术产业体系。实现技术先进、产业发达、应用领先、网络安全坚不可摧的战略目标。

随着我国国产化基础软硬件的逐步成熟，以龙芯、飞腾、兆芯、申威为代表的国产 CPU，以及以中标麒麟、银河麒麟为代表的国产操作系统，已经由基本可用实现了初步具备替代能力的跨越。2018 年央采目录选入了国产 CPU 设备更是为国产化的发展注入了强大的助推力。同时，可信计算也迈入了主动免疫的可信计算 3.0 时代，在最新推出的等保 2.0 中，“可信”已成为了网络安全保护不可或缺的一部分。国产化基础软硬件与可信计算的结合已成为今后我国网络安全保护的基石。自主可控要求带来的信息系统软硬件国产替代，也将给信息安全行业带来巨大的市场增量。

3、安全威胁驱动行业快速增长

随着信息技术的快速发展和广泛应用，各类网络安全威胁呈现迅速提升的趋势，黑客攻击专业化、网络攻击目的商业化、传统防御体系失效，使得网络安全威胁日益复杂化。安全威胁是安全支出的主要驱动因素，是信息安全行业的典型特点，即“问题就是机会”。因此，建立可靠的信息安全环境、提升信息安全的保障水平，成为我国政府高度关注的重大课题之一，将直接带动各类信息安全产品和服务等市场需求的增长。尤其“棱镜门”事件将政府和公众对网络信息安全的关注程度推向了高潮，并为国内信息安全行业创造了良好的发展契机。同时，云计算、移动互联网、物联网、大数据、智慧城市等新技术、新应用和新模式的出现，对信息安全提出了新的要求，拓展了信息安全产业的发展空间和应用场景，并触发了网络安全新热点，将进一步带动各类用户的信息安全投入，促进信息安全整体市场需求的增长。

4、全局化、智能化成为网络安全行业的发展趋势，将带动用户信息安全支出的全面提升

安全形势的复杂化，驱动安全防护理念全面升级。全局化、智能化成为网络安全行业的两大趋势，相较于单点防御，对于整体解决方案的需求正在提升；相

较于边界防护，对于基于数据驱动的智能化新产品和新技术的需求正在提升；而相较于产品采购，对于外部专业安全服务的需求也在持续提升。全局化趋势一方面体现在为提高防护能力，将网络安全纳入组织信息化顶层设计方案，将安全关口前置，而非传统安全机制下对于信息化的补充；另一方面则体现在基于整体来考虑和设计安全防护方案，体系化部署双重身份验证、入侵检测或防护系统（IPS）、网站漏洞恶意软件防护及全网 Web 安全网关在内的全面安全防护系统而非单点防御。网络安全智能化趋势则体现在安全思维从传统的“应急响应”转变为“持续响应”，在阻止之外加大对于检测、响应、预测方面的安全投入，加大对于应用安全风险管理(ASRM)、安全信息与事件管理(SIEM)、网络态势感知(CSA)、安全运营中心(SOC)、态势感知与安全运营平台(NGSOC)、用户行为分析(UEBA)、威胁情报(TI)等数据驱动类应用的投入。网络安全行业的变化趋势将带动用户信息安全支出的全面提升。

5、持续强大的技术研发能力成为行业竞争着眼点

信息安全行业是技术密集型行业，持续且强大的核心技术研发能力是信息安全企业保持市场竞争力与行业地位的关键。随着云计算、大数据、移动互联网、物联网等新技术的快速发展，信息安全行业也不断发生变革。新的威胁和攻击方法从被发现、曝光到大范围的传播和爆发，留给安全防护团队的时间窗口只有数小时甚至更短。这需要传统的安全防护体系做出变革，搭建更加敏捷和开放的防护架构、实现更加广泛的防护体系协同，并支持对威胁情报的共享机制。安全防护体系的变革进一步要求信息安全产品和服务进行变革，在安全决策智能性、协同性和运营效率方面实现显著提升。《“十三五”国家信息化规划》提出建设全天候全方位感知网络安全态势，对我国信息安全企业的技术实力提出了新的要求。在这种背景下，持续提升自身技术研发能力成为信息安全企业竞争的关键点。

6、云计算从技术导入到迅速普及，有望引爆安全产业需求

当前云计算已经从技术导入阶段进入到了应用迅速普及阶段，各行业迫切需要通过构建云计算系统，满足转型及效率、成本需求。企业持续将 IT 基础设施云化并将业务向云迁移这一趋势将加快，企业的网络边界也随之扩展到云端，加上云的开放、复杂、分散的特点，安全的防护难度及需求将急剧上升。根据调查

机构 Gartner 调研预测，全球云安全市场规模已达 36 亿美元，未来几年增速有望达到 23%，预计到 2022 年，市场规模将达到 120 亿美元左右，这将为与云计算相关的信息安全产品带来巨大的市场增长空间。

2017 年 4 月，工信部发布《云计算发展三年行动计划（2017-2019 年）》，提出到 2019 年，我国云计算产业规模达到 4,300 亿元，加强云计算网络安全防护管理，落实公有云服务安全防护和信息安全管理系统建设要求，完善云计算服务网络安全防护标准。2018 年，工信部印发了《推动企业上云实施指南（2018-2020）》，提出了企业上云的工作目标，到 2020 年，云计算在企业生产、经营、管理中的应用广泛普及，全国新增上云企业 100 万家。国内云安全市场有望伴随云产业的爆发而迅猛增长，成为未来几年信息安全行业增长的主要驱动因素之一。

7、智慧城市建设高速发展，亟待信息安全保障能力同步发展

2014 年 8 月，发改委等八部委印发《关于促进智慧城市健康发展的指导意见》，要求到 2020 年建成一批特色鲜明的智慧城市，并要求实现网络安全长效化。我国智慧城市建设迎来高速发展，成为政府提升治理能力、改善城市运行管理、培育壮大数字经济、重构公共服务体系的新动力、新途径。随着智慧城市建设进程的推进，我国智慧城市 IT 投资规模持续扩大。根据智研咨询数据，我国智慧城市 IT 投资规模 2021 年将达到 12,341 亿元，2017-2021 年复合增长率达到 34.7%。智慧城市高度集成了物联网、云计算、大数据等新一代信息通信技术，而其中广泛使用的摄像头等绝大部分物联网设备在安全性上十分脆弱，各种物联网设备产生的视频、图像及其他海量城市数据信息，涉及各行各业多元数据及政府、各行业敏感信息，个人隐私信息。如何保护智慧城市设备和大数据安全，成为智慧城市建设过程中亟待解决的重大任务。

8、网络安全行业发展亟需解决人员匮乏及信息安全教育问题

根据智联招聘发布的《2019 网络安全人才市场状况研究报告》，网络安全人才市场的需求在三年的时间内，扩大到了 2016 年初的 10 倍以上。在 2019 年国家网络安全宣传周上，与会专家和业内人士表示，当前网络空间安全人才数量缺口高达 70 万，预计到 2020 年将超过 140 万。目前我国每年网络安全学历人才培

养数量不足 1.5 万，网络空间安全人才培养的数量远远满足不了社会需求。2018 年 10 月，公安部发布《公安机关互联网安全监督检查规定》，该行政文件从 11 月 1 日开始正式实施，规定客观上要求被检查单位必须建立常态化的安全队伍。2019 年，“等保 2.0”的发布及正式执行，对互联网企业、安全厂商、各大政企单位提出更高的安全合规要求。这些制度的落实推动了网络安全人才的需求增长，网络安全人员的需求缺口进一步扩大。

人才是网络安全建设的核心资源，人才的数量、质量、结构和作用的发挥，直接关系到网络安全建设水平的高低和保障能力的强弱。2017 年 6 月，《网络安全法》的正式实施，进一步界定关键信息基础设施范围，对重点行业的信息安全问题将提升至国家安全层面，重点行业亟需解决内部员工的信息安全素质及教育问题。《网络安全法》明确支持企业、学校开展网络安全相关教育与培训，采取多种方式培养网络安全人才。高校是我国培养网络空间安全人才的主阵地，擅长理论教学，缺乏参与产业实践的机会和动力，知识更新成难题。其中问题之一缺乏良好的攻防演练平台，验证性实验多，而综合性、自主防御性试验难以构建，许多院校的学生缺少接触实际网络安全问题。大型企业往往通过定期举办信息安全或技能评比类的内部竞赛促进员工安全技能的提高，不成体系，而中小机构则可能因为专业能力和条件忽视安全培训。因此，体系性的、持续性的、具有考核评价的安全培训体系成为了企业安全教育的关键，可为企业人员提升安全技能提供有力的帮助。

（二）本次非公开发行股票的目的

公司本次非公开发行股票的目的是：聚焦网络信息安全主业及“智慧安全”发展理念，进行业务拓展及产业扩张。顺应等保 2.0 对安全广度和深度的拓展要求，抓住自主可控行业机遇，拥抱信息安全产品全局化智能化趋势，在新一代 IT 基础设施的大数据、云计算、物联网、人工智能等安全领域深入布局，为智慧城市发展提供安全保障，为网络安全行业发展培养具有实战经验的安全人才。

1、顺应我国国产化替代以及基于可信计算的安全防护的必然趋势，抓住国产安全产品和服务市场带来的发展机遇

随着美国加大对中国的技术封锁，核心技术和关键产品自主可控的重要性突显，自主可控已经上升到国家战略高度，也成为我国信息化建设的关键，对实现安全保护目标具有重大意义。依靠自主研发设计和核心技术，要实现从硬件到软件的自主研发、生产、升级、维护的全过程可靠，就要求在网络安全上具有足够的防护能力，因此网络安全产品和服务国产化需求强劲。

目前，自主可控的推进路径和节奏较为明确，首先应用于党政军等安全可控要求较高的领域，在生态体系成熟后再向其他行业领域渗透。包括金融、石油、电力、电信、交通、航空航天、医院、教育为代表的八大重要行业将率先启动国产化替代项目并稳步推进，根据估算党政和重要行业未来 2~3 年终端替换规模达到 500 万台，对应国产系统建设总经费超 1,000 亿元。若未来国产化替代向重点行业全面拓展，根据公开数据，目前全国党政机关公务员超过 700 余万人，事业单位编制人员 3,100 余万人、中央企业员工 1,200 余万人，总数合计约 5,000 万人，简单测算 5,000 万台终端计算机及系统替换，对应的基础软硬件、应用和安全市场总规模超过 1 万亿元。

在 2019 年 12 月执行的“等保 2.0”中，对可信计算已提出了明确要求，“可信”要求已全面覆盖等保第一级至第四级各级安全保护要求，并融入了安全保护的方方面面。只有引入可信，才能满足用户符合“等保 2.0”、遵从《网络安全法》的需要。

因此，基于国产化基础软硬件以及可信计算，对公司的全线产品进行适配、改造，以研制出运行于国产化基础软硬件及可信计算之上的安全产品；以及针对重点行业更换的新的国产化自主可控终端主机，利用安全防护和行为审计技术、采用大数据、AI 智能分析，研发终端检测与安全防护系统。顺应了我国自主可控国产化替代以及基于可信计算的安全防护的必然趋势，有助于公司抓住重点行业安全产品和服务国产化市场带来的发展机遇。

2、使用大数据分析、AI、体系架构再造等技术对传统产品进行改造，提高产品全局化、一体化、智能化水平

为了不断应对新的安全挑战，企业和组织部署防火墙、UTM、入侵检测和防护系统、漏洞扫描系统、防病毒系统、终端管理系统等多道安全防线应对来自各方面的安全威胁，随着物联网等技术的发展，工业设备面临来自互联网的威胁，工业安全设备使用防火墙、入侵防护、内容审计等多种产品来对外部威胁进行防御。

纵观近年来的网络攻击手段，APT 攻击已经成为最具威胁的攻击方法之一。机构先后部署防火墙、UTM、入侵检测和防护系统、漏洞扫描系统、防病毒系统、终端管理系统等多道安全防线，解决来自各个方面的安全威胁。但在 APT 攻击中，由于攻击的多样性和融合性，所以无法使用一种方法有效检测出 APT 攻击。彼此孤立的多道安全防线在 APT 攻击面前显得无能为力。因此，面对新型 APT 攻击，通过全面采集网络中包括原始网络数据包、业务和安全日志等各种数据形成大数据库，再通过大数据分析技术和智能分析算法来检测 APT 攻击是最可靠的办法。随着信息时代的快速发展，IT 运维已经成为 IT 服务内涵中重要的组成部分，面对越来越多复杂的业务、多样化的用户需求，不断扩展的 IT 应用需要越来越合理的模式来保障 IT 服务能灵活便捷、安全稳定地持续保障。从初期的数台服务器发展到庞大的数据中心，单靠人工已无法满足在技术、业务、管理等方面的需求。标准化、自动化、架构优化、过程优化等降低 IT 服务成本的因素越来越受广大行业客户重视。使用大数据分析与 AI 等技术对传统产品进行全局化智能化改造，将成为信息安全行业的重要发展方向。

从工业互联网安全保障现实情况来看，随着信息安全威胁的多样性和隐蔽性不断增强，首先，原有的以防火墙、入侵防护、内容审计等单功能产品各自为战的安全解决方案，很难应对攻击多样化和融合性，这些产品产生大量不同形式的安全信息，使得整个系统的相互协作和统一管理成为安全管理的难点，已经很难满足用户对高效信息安全维护的需求。其次，传统工业安全设备对外部威胁进行防御，但却无法处理工业内主机发生的威胁，也无法做到内外网安全策略的统一管理，从而也给目前的工业控制网络埋下了众多安全隐患；再次，单功能产品系

统配置、规则设置、反应处理、设备管理、运行管理的复杂性所带来的管理成本和管理难度都直接制约了安全防御体系的有效性，从而也给网络的安全性带来重大隐患。

公司基于工业网络统一威胁管控平台产品将创新性的改变原有工业安全设备的体系架构，将 UPM（统一策略管理）、UEM（统一终端管理）、UCM（自适应通道管理）整合成全新的体系架构，并通过运用自主开发的 SM-XML 安全联动管理协议、关联事件报警机制、Object Policy 通用策略对象化管理、自动化管理流程等新功能，将原来分散的防御技术整合成为立体的安全管理平台。通过体系架构的再造，革新性地解决网络“点”（即主机）、“线”（即工业）、“面”（即安全策略关联管理）的难题，并通过加密隧道的联动机制，形成一个联动的覆盖整体网络及设备的立体安全防御体系，形成“一点报警，全网联防”的点、线、面立体防护安全产品，其整体防护能力和效率均较传统工业安全设备产品大幅提升，能更好解决用户的综合安全防护需求。

3、为政企大数据开放共享提供安全保障，完善数据安全领域布局

在社会经济高度发展的今天，信息数据对于个人、企业乃至整个国家的政治安全、经济安全和国防安全都起着越来越重要的作用，因而信息数据安全在整个信息产业布局乃至国家战略格局中也有着举足轻重的地位和作用。为充分发挥大数据价值，需要盘活数据资产，开发共享数据。电信运营商和互联网公司等拥有海量大数据，他们积极探索并投身建设大数据开放平台，一方面，封装自有的数据资源以及数据存储、数据加工、数据挖掘分析能力，以数据服务的方式开放给第三方（尤其是中小企业以及应用开发者），开发各种大数据创新服务；另一方面，与政府、公共服务部门以及跨领域行业开展合作，融合加工多源异构数据，融合开放跨行业数据，带动产业发展新型业务形态。

政府互联网+政务战略下，政务大数据在安全与开放方面难以平衡。跨域数据交换认证机制不完善，非法对象可能与内部系统进行数据交换导致数据泄露；端到端数据机密性和完整性缺乏防护措施，传输过程存在非法截获及监听的威胁；数据交换记录缺乏审计，可能导致双方数据不一致时无法追溯，责任无法明

确；数据交换缺乏权限控制及有效的病毒检测措施，数据结构和内容有暴露风险，传输数据或文件可能含有恶意代码。

在大数据开放、运营或者变现过程中，如何保证开放数据的合规性、避免敏感信息的泄漏、对交易数据进行计量或者计费以及对数据进行审计等成为当前亟需解决的问题。

公司大数据安全监控与交换平台将实现数据归集、共享安全策略，提供独立于应用系统的信息共享安全控制手段，全方位满足跨域数据交换以及等保 2.0 有关数据访问细腻度的要求。聚焦网络信息安全主业，为政企大数据开发和共享提供安全保障，完善公司信息安全产业在数据安全细分领域的布局。

4、持续加码云安全，保护政企敏感信息

近年来，云计算技术获得了快速发展，各行业机构纷纷转向云架构，提升信息系统的安全性和管理效率。云计算环境下，由于虚拟化技术使得传统安全边界消失，用户的动态变化及移动性强，数据安全保护要求更高，合规检查更难等，对于信息安全产品提出了更高的要求。传统安全产品不能满足云时代的安全需求，因此全新的云安全产品的需求得到激发，市场规模保持快速增长。

公司紧紧抓住云时代的安全发展趋势，通过本次募投项目进一步加码云安全领域。一方面，将云安全进一步应用于云办公和云安全教育领域；公司在云安全技术基础上开发的全国产化云桌面产品、云安全教育产品，满足了云时代远程办公和云计算安全培训需求，协助政企提高员工网络安全素质，规范员工行为，保障政企敏感数据安全。另一方面，公司视频安全接入与威胁管控平台，通过技术手段将公共安全区域视频摄像机进行可控管理，防止伪造终端接入、木马注入、病毒注入、DDOS 攻击等风险，满足公共安全视频云建设前端接入安全防护要求。

5、进一步提高公司在智慧城市、平安中国建设中的安全保障能力

随着智慧城市及物联网蓬勃发展，越来越多设备通过网络互连，IDC 预测，到 2025 年，全球物联网设备数将达到 416 亿台。这些前端设备大多处在无人值守的环境中，且大多数设备存在弱口令，远程端口开放等安全隐患。如何保证前端设备安全，防止不法分子利用入侵、控制前端设备，防止不法分子通过前端设

备入侵核心业务网络是智慧城市及物联网发展环境下亟待解决的问题。安全准入控制系统将在网络安全防御体系中扮演越来越重要的角色。

此外，基于智慧城市复杂、开放、互联的特点，以及区别于传统信息系统的服务方式、网络架构、数据资源等技术因素，加之受制于智慧城市主体建设的连带效应，导致了智慧城市在信息安全上面临种种困难和挑战。

视频监控是智慧城市管理体系的关键组成环节。近年来，视频监控被广泛应用于平安城市、天网工程、雪亮工程、社会治安、交通出行、环境保护、城市管理等多个领域。据统计，截至 2017 年 9 月全国安装的公共安全视频监控摄像机数量已达到 3,000 万台，初步覆盖了公共区域、重点单位和要害部位，视频监控已成为提升平安中国建设能力和水平的基础性工程。

新一代智慧城市安全运营平台满足用户对信息安全产品全局化智能化的防护需求，以“人、技术、制度流程”为核心，构建市、区两级互联互通、信息共享的标准规范、技术接口及建设指南，构筑智慧城市信息安全保障体系，实现对智慧城市关键基础设施全面的安全监测、预警、分析及快速处理。

公司视频网络接入安全管理平台为国家推动智慧城市、平安城市、雪亮工程、天网工程保驾护航，为社会治安、交通出行、疫病防控、环境保护、城市管理等多个领域提供安全保障。一方面，视频网络接入安全管理平台保证视频设备安全，防止不法分子利用入侵、控制前端设备，通过前端设备入侵核心业务网络；另一方面，系统集成的红外热成像人体测温解决方案，部署于人流密集的公共场所，如机场、火车站、汽车站、轮渡、医院、学校、企业、门店等，实现无接触感应、智能化测温、高温实施预警，解决传统测温需要人员近距离接触的问题，实现快速精准筛查和告警，避免交叉感染，高效率通行，成为防控疫情、保障安全返程和复工的“智能哨兵”。

6、满足新形势下信息安全教育人员培养的需求，为公司未来在云安全教育领域取得优势地位提供保障

随着信息安全行业的发展，企业对安全人才具备的技术和管理能力提出了更高要求，从信息安全人才的需求及培养角度可以看出，如何快速、高效地培养具

备丰富实操经验和技能的实用型人才，是安全教育与实战方案的重要目标。对于行业从业人员，也存在信息安全继续教育的需求，并以内部培训绩效评估作为激励考核。行业从业人员对安全教育有其特殊性需求，例如信息安全意识培训将适用于企业的大多数人员，并应当作为教育的重点。对技术类人员，应当在常规安全技术教育的基础上，增加漏洞原理以及贴近行业生产环境的信息安全教育内容，以提升安全技能应用的针对性以及专业性。我国信息安全高等教育课程改革也为从事教育行业的企业带来了新的机遇和挑战。对于培养实用型技能人才而言，需要在国内信息安全企业建设信息安全实训基地，开展网络空间安全实战技能培养和实习实训，由企业与高校共同制定学生实习实训方案，主动接收学生开展实习实训，以培养实战技能。

网络空间仿真靶场实训竞技平台基于公司的云管理平台，发力云安全教育，顺应国家推行网络安全法及对网络安全教育人才培养计划之趋势，培养安全人才，缓解行业人员匮乏的局面、解决高等学校重理论轻实战的弊端、能为客户提供体系性的、持续性的、具有考核评价的安全培训体系，为公司未来在云安全教育领域取得优势竞争地位提供有力保障，提高公司在信息安全产品、解决方案、服务及运营等方面的实施能力，提升公司的业务竞争力，从而进一步提升公司的竞争优势。

7、满足中长期发展战略需要，提高公司竞争力

近年来，云计算技术获得了快速发展，各行业机构纷纷转向云架构，提升信息系统的安全性和管理效率。在此背景下，云桌面产品的市场需求得到激发，产品需求量大大提升，市场规模保持快速增长。而在国家自主可控、安全教育等相关政策的支持下，国产厂商在国内信息安全软硬件、安全教育、安全服务等市场将会占据越来越重要的地位。募投项目的实施，是公司顺应自主可控和等保 2.0 趋势，在原有技术基础上，创新性地应用软件基因分析、恶意代码及恶意流量映射为图片基因图谱分析、深度学习等前沿尖端 AI 智能学习技术，对现有安全产品进行国产化适配、全局化智能化改造，提高公司技术和研发实力，深化公司在云计算、移动安全、数据安全、工业互联网、智慧城市等领域布局，满足公司中长期战略发展的需要。为公司未来在下一代关键基础设施、客户重点行业、安全

教育等领域取得优势竞争地位提供有力保障，保障公司未来业务的持续快速发展。

8、有效丰富公司产品系列，提升业务竞争力

经过多年的发展，公司已开发出了边界安全、安全管理、应用安全、审计安全、保密安全、工控安全、云安全等多个类型的安全产品，同时也承担了公安部及保密局的多种专项产品开发任务，开发出了多款部级、省级专用安全产品，积累了丰富的产品开发经验。为进一步提高公司的市场竞争力，公司仍在不断进行技术创新和产品类别扩展，以扩大公司的业务范围，促进公司持续快速发展。

通过募投项目的建设实施，一方面可以对公司现有产品形成良好的补充，进一步丰富公司的产品系列，另一方面也可以提高公司在信息安全产品、解决方案、服务及运营等方面的实施能力，提升公司的业务竞争力，从而进一步确立公司的竞争优势。

三、发行对象及其与公司的关系

本次非公开发行股票的发行对象不超过 35 名，为符合规定条件的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者、其他合格的境内法人投资者和自然人。其中，证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托投资公司作为发行对象的，只能以自有资金认购。

最终发行对象由股东大会授权董事会在获得中国证监会发行核准文件后，按照中国证监会相关规定及本预案所规定的条件，根据竞价结果与保荐机构（主承销商）协商确定。

公司本次非公开发行股票尚无确定的发行对象，因而无法确定发行对象与公司的关系。公司将在发行结束后公告的发行情况报告书中披露发行对象与公司的关系。

四、本次非公开发行方案概要

若国家法律、法规、规章、规范性文件及证券监管机构对非公开发行股票有最新规定、监管意见或审核要求的，公司将根据最新规定、监管意见或审核要求进行相应的调整。

（一）发行股票的种类和面值

本次非公开发行的股票种类为境内上市人民币普通股（A 股），每股面值为人民币 1.00 元。

（二）发行方式

本次发行采取非公开发行的方式，公司将在中国证监会核准之日起的十二个月内择机发行。

（三）发行对象及认购方式

本次非公开发行股票的对象为符合规定条件的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者、其他合格的境内法人投资者和自然人，发行对象不超过 35 名。证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托投资公司作为发行对象的，只能以自有资金认购。

若国家法律、法规、规章、规范性文件及证券监管机构对非公开发行股票的发行对象及认购方式有最新规定、监管意见或审核要求的，公司将根据最新规定、监管意见或审核要求等对发行对象及认购方式进行相应的调整。

最终发行对象由股东大会授权董事会在获得中国证监会发行核准文件后，按照中国证监会相关规定，根据竞价结果与保荐机构（主承销商）协商确定。所有发行对象均以现金方式认购本次发行的股票。

（四）定价基准日、发行价格与定价原则

本次发行的定价基准日为发行期首日，定价原则是：发行价格不低于定价基准日前 20 个交易日股票交易均价（定价基准日前 20 个交易日股票交易均价=定价基准日前 20 个交易日股票交易总额/定价基准日前 20 个交易日股票交易总量）的 80%。

在定价基准日至发行日期间，上市公司若发生派息、送红股、资本公积金转增股本等除权、除息事项，本次发行底价将作相应调整。

若国家法律、法规、规章、规范性文件及证券监管机构对非公开发行股票的定价基准日、发行价格及定价原则有最新规定、监管意见或审核要求的，公司将根据最新规定、监管意见或审核要求等对定价基准日、发行价格及定价原则进行相应的调整。

本次非公开发行股票的最终发行价格将由股东大会授权董事会在取得中国证监会发行核准文件后，按照中国证监会相关规定，根据竞价结果与保荐机构（主承销商）协商确定。

（五）发行数量

本次非公开发行股票的发行数量=募集资金总额/发行价格，同时本次非公开发行股票数量不超过本次发行前上市公司总股本的 30%，截至 2020 年 2 月 26 日，上市公司总股本为 1,249,799,145 股，按此计算，本次非公开发行股票数量不超过 374,939,743 股（含本数）。

在董事会对本次非公开发行股票作出决议之日至发行日期间，上市公司若发生派息、送红股、资本公积金转增股本等除权、除息事项及股权激励等引起公司股份变动的，则本次发行的股份数量将作相应调整。

若国家法律、法规、规章、规范性文件及证券监管机构对非公开发行股票的数量有最新规定、监管意见或审核要求的，公司将根据最新规定、监管意见或审核要求等对发行数量进行相应的调整。

最终发行股份数量由公司董事会根据股东大会的授权于发行时根据市场化询价的情况与保荐机构（主承销商）协商确定最终发行数量。

（六）锁定期安排

本次非公开发行股票完成后，发行对象所认购的股票自本次非公开发行股票上市之日起 6 个月内不得转让。限售期结束后按中国证监会及深圳证券交易所的有关规定执行。

若国家法律、法规、规章、规范性文件及证券监管机构对非公开发行股票的限售期有最新规定、监管意见或审核要求的，公司将根据最新规定、监管意见或审核要求等对限售期进行相应的调整。

（七）本次发行前滚存利润的安排

本次非公开发行完成后，公司发行前滚存的未分配利润由公司新老股东按照发行后的股份比例共享。

（八）上市地点

本次非公开发行的股票将申请在深圳证券交易所上市交易。

（九）本次发行股票决议的有效期

本次非公开发行决议在本议案经股东大会审议通过之日起 12 个月内有效。

（十）募集资金用途

本次发行的募集资金总额不超过 200,000 万元（含 200,000 万元），计划投资于以下项目：

单位：万元

序号	分类	项目名称	项目总投资	拟投入募集资金
1	基础网络安全产业化	全线网络安全产品国产化及可信研发	73,333.50	35,700.00
2		新一代 APT 威胁检测与防御系统	18,843.00	9,550.00
3		工业网络统一威胁管控平台	23,560.00	11,150.00

序号	分类	项目名称	项目总投资	拟投入募集资金
4		自主可控终端检测与高级防御系统	24,365.00	12,000.00
5	安全应用产业化	大数据安全监控与交换平台	24,854.00	12,300.00
6		安全云虚拟终端系统	17,308.00	7,900.00
7		视频安全接入与威胁管控平台	22,175.50	10,100.00
8		网络空间仿真靶场实训竞技平台	22,742.00	11,300.00
9		新一代智慧城市安全运营平台	56,318.00	30,000.00
项目合计			283,499.00	140,000.00
补充流动资金			60,000.00	60,000.00
合计			**343,499.00**	**200,000.00**

注：合计数据尾数因四舍五入原因，与相关单项数据计算得出的结果略有不同。

本次实际募集资金净额相对于上述项目所需资金存在不足的部分本公司将通过自筹资金解决。在不改变本次募投项目的前提下，公司董事会可根据项目的实际需求，对上述项目的募集资金投入顺序和金额进行适当调整。在本次非公开发行募集资金到位之前，若公司用自有资金投资于上述项目，则募集资金到位后将按照相关法规规定的程序予以置换。

五、本次非公开发行是否构成关联交易

截至目前，本次发行尚未确定发行对象，最终是否存在因关联方认购公司本次非公开发行股票构成关联交易的情形，将在发行结束后公告的《发行情况报告书》中披露。

六、本次非公开发行是否导致公司控制权发生变化

截至 2020 年 2 月 26 日，公司实际控制人柯宗贵、柯宗庆合计持有公司 313,903,797 股股份（其中柯宗贵直接持有 156,473,504 股，柯宗庆直接持有 157,430,293 股），占公司股份总数的 25.12%。中经汇通持有公司 89,935,042 股，占公司股份总数的 7.20%，系公司控股股东、实际控制人的一致行动人。公司的实际控制人及其一致行动人合计持有公司 403,838,839 股，占公司股份总数的 32.31%。

若按照本次非公开发行的股票数量上限 374,939,743 股测算，本次发行完成后，本公司总股本将增加到 1,624,738,888 股。假设柯宗贵、柯宗庆及中经汇通不参与本次发行认购，设柯宗贵、柯宗庆及其一致行动人控制的股份比例将变为 24.86%，仍处于控股地位，仍为公司实际控制人。

因此，本次发行不会导致公司控制权发生变化。

七、本次发行方案尚需呈报批准的程序

本次非公开发行股票相关事项已经公司第四届董事会第十九次（临时）会议审议通过，尚需经过公司股东大会审议。

根据《公司法》、《证券法》、《创业板上市公司证券发行管理暂行办法》等相关法律、法规和规范性文件的规定，本次非公开发行还需获得中国证监会的核准。在获得中国证监会核准后，公司将向深圳证券交易所和中国证券登记结算有限责任公司深圳分公司申请办理股票登记、发行和上市事宜，完成本次非公开发行全部申报和批准程序。

第二节 董事会关于本次募集资金使用的可行性分析

一、本次募集资金的使用计划

本次发行的募集资金总额不超过人民币 200,000 万元（含 200,000 万元），将投资于以下项目：

单位：万元

序号	分类	项目名称	项目总投资	拟投入募集资金
1	基础网络安全产业化	全线网络安全产品国产化及可信研发	73,333.50	35,700.00
2		新一代 APT 威胁检测与防御系统	18,843.00	9,550.00
3		工业网络统一威胁管控平台	23,560.00	11,150.00
4		自主可控终端检测与高级防御系统	24,365.00	12,000.00
5	安全应用产业化	大数据安全监控与交换平台	24,854.00	12,300.00
6		安全云虚拟终端系统	17,308.00	7,900.00
7		视频安全接入与威胁管控平台	22,175.50	10,100.00
8		网络空间仿真靶场实训竞技平台	22,742.00	11,300.00
9		新一代智慧城市安全运营平台	56,318.00	30,000.00
项目合计			283,499.00	140,000.00
补充流动资金			60,000.00	60,000.00
合计			**343,499.00**	**200,000.00**

注：合计数据尾数因四舍五入原因，与相关单项数据计算得出的结果略有不同。

本次实际募集资金净额相对于上述项目所需资金存在不足的部分本公司将通过自筹资金解决。在不改变本次募投项目的前提下，公司董事会可根据项目的实际需求，对上述项目的募集资金投入顺序和金额进行适当调整。在本次非公开发行募集资金到位之前，若公司用自有资金投资于上述项目，则募集资金到位后将按照相关法规规定的程序予以置换。

二、本次募集资金投资项目的可行性分析

（一）国家政策支持，行业发展快速

党和国家对信息安全保护及产业发展高度重视。在目前国内信息化建设快速普及过程中，为保障国民经济的健康发展，党和国家高度关注和重视信息安全保护和信息安全产业的发展，《国家信息化领导小组关于加强信息安全保障工作的意见》、《国家中长期科学和技术发展规划纲要（2006-2020 年）》以及《“十三五”国家信息化规划》等都对发展信息安全产业提出了明确的要求。《国家信息化领导小组关于加强信息安全保障工作的意见》明确提出要实行信息安全等级保护，加强以密码技术为基础的信息保护和网络信任体系建设，建设和完善信息安全监控体系，重视信息安全应急处理工作，加强信息安全技术研究开发，推进信息安全产业发展。在《“十三五”国家信息化规划》中，政府提出要从多个维度强化国家网络安全科技创新能力。

不同于其他行业自由竞争和开放发展模式，信息安全在整个信息产业布局乃至国家战略格局中都具有举足轻重的地位和作用，因为其关系到国家政治安全、经济安全和国防安全。这就意味着中国信息安全行业的发展不能依赖国外，必须走自主可控的道路，因此政府对信息安全行业发展引导力度很大，采取了采购与专项双推动的发展模式。信息安全专项基金逐年增加，为我国信息安全行业的持续发展提供了坚实的市场需求保障。

（二）技术推动和政策驱动下的信息安全行业市场空间广阔

云计算、移动互联网、物联网、大数据和智慧城市等新技术和新应用模式的出现与发展，对信息安全提出了新需求和新挑战。随着数据信息进一步集中，数据量不断增大，现有的信息安全手段已经难以满足这些新技术和新应用模式的新要求，对海量数据进行安全防护变得更加困难，数据的分布式处理也加大了数据泄露的风险。因此，保护数据安全已经成为云计算、移动互联网、物联网、大数据和智慧城市等新技术和新应用模式的焦点。新技术、新应用和新模式的出现，对信息安全提出了新的要求的同时，也为信息安全产品和服务创造广阔的市场空间，进一步带动各类用户的信息安全投入，促进信息安全整体市场需求的增长。

（三）公司丰富的人才资源储备为项目实施提供智力支持

公司拥有大量优秀的信息安全技术人才，组成了一支基础扎实、技术水平高、开发能力强、实践经验丰富、专业与年龄结构合理的人才队伍，是公司在竞争中立于不败之地的重要保证。

为增强公司科技人才持续竞争能力，公司与广州天河软件园管理委员会、华南理工大学博士后管理办公室签订协议，联合培养企业博士后研究人员。同时，公司也参与建立了网络与信息安全产学研创新联盟，在广东省科技厅省部产学研办公室指导下，与信息安全领域国内高等院校、科研单位和企业联合开展网络与信息安全的技术研发与产业化工作。

此外，公司还聚集了一大批包括归国学者、国内著名专家、专业人才以及国内软件业和网络界的优秀人才。大量的人才储备为本次募集资金投资项目的实施提供了智力支持。

（四）公司丰富技术经验为项目实施提供技术支撑

经过十余年的发展，公司共开发出了边界安全、安全管理、应用安全、审计安全、保密安全、工控安全、云安全等多个类型的安全产品，同时也承担了公安部及保密局的多种专项产品开发任务，开发出了多款部级、省级专用安全产品，积累了丰富的产品开发经验。以丰富的研发经验为基础，公司在信息安全产品的研发设计、产品检测等主要技术领域均已达到国内领先水平，部分技术已接近国际先进水平。

除了先进性外，公司的技术实力也体现在全面性上。公司全面应用了人工智能、软件基因、大数据分析、虚拟化等前沿核心技术，并推出了虚拟化（云）安全产品、容器云平台、云等保高密度安全虚机等一系列具有核心竞争力前沿领域产品。同时，公司在传统防火墙、IDS/IPS、漏洞扫描等每个单项产品上，也都有着深厚的技术积累，从而使得公司基本不存在技术短板，在产品整合方面具有较好的技术支撑。

（五）公司完善的经营管理体系助力项目建设实施

作为技术密集型的企业，公司采取了研发与销售为前端和后端、生产为中端的两头大中间小的“哑铃”经营模式。即公司专注于核心软件产品与系统的设计开发，而将大部分通用化、标准化的硬件采购与生产环节外包给专业硬件厂商，并依托营销网络，向客户提供信息安全产品和服务。这种“哑铃形”的模式能有效防范经营风险并支撑公司快速发展，快速实现产品的市场推广，确立公司在信息安全领域的领先地位。

公司自成立以来，一向重视产品和服务的质量管理，恪守“专业铸就安全”的质量方针，以高水平、高质量和专业的产品和服务满足各类客户的需求。公司制订质量管理标准的依据主要来自于信息安全行业的国际标准（技术规范）、国家标准和行业标准等。公司通过多年积累的经验，不断优化公司质量管理的部门职责和流程，在产品及业务的市场需求定位、设计开发、生产检验和安装服务等过程中，逐步建立并完善了一整套产品及业务的质量控制管理体系，全方位覆盖公司的业务流程。公司完善的经营管理体系将助力本次募集资金投资项目的建设实施。

三、本次募集资金投资项目的具体情况

（一）全线网络安全产品国产化及可信研发项目

1、项目概况

本项目是基于国产化基础软硬件以及可信计算，对蓝盾股份的全线产品进行适配、改造，以研制出运行于国产化基础软硬件及可信计算之上的安全产品。适配的国产化基础软硬件将涵盖龙芯、飞腾、兆芯、申威、海光、华为海思等主流国产 CPU 以及中标麒麟、银河麒麟、中科方德、神威睿思、深度、普华等主流国产操作系统，以满足不同用户的选型需要。可信计算将采用最新的可信计算 3.0 架构，其是以国产密码算法为基础、控制芯片为支柱、双融主板为平台、可信软件为核心的全新的可信计算体系结构框架，可形成完整的主动免疫综合防护系统。

项目的建设目标是基于国产化基础软硬件及可信计算在已有产品的基础上进行技术升级，结合蓝盾股份在通信网络安全产品、区域边界安全产品、计算环境安全产品、安全管理支持产品和云计算产品、工控安全产品、物联网安全产品积累的丰富研制经验，完成全线产品的国产化及可信的功能适配和性能调优。

2、项目投资计划

本项目估算新增总投资 73,333.50 万元，其中新增设备购置费 21,734.00 万元、新增软件购置费 3,266.00 万元、开发技术人员人工费 20,823.00 万元，铺底流动资金 14,530.00 万元，分别占总体新增投资额的 29.64%、4.45%、28.39%和 19.81%。本项目拟使用募集资金 35,700.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	比例	拟以募集资金投资金额
一	设备购置费	21,734.00	29.64%	21,734.00
二	软件购置费	3,266.00	4.45%	3,266.00
三	开发人员人工费	20,823.00	28.39%	7,200.00
四	运营技术服务团队	2,972.00	4.05%	209.50
五	市场开拓费	6,718.00	9.16%	-
六	试验检验费	3,290.50	4.49%	3,290.50
七	铺底流动资金	14,530.00	19.81%	-
合计		**73,333.50**	**100.00%**	**35,700.00**

3、项目实施的背景

随着我国国产化基础软硬件的逐步成熟，以龙芯、飞腾、兆芯、申威为代表的国产 CPU，以及以中标麒麟、银河麒麟为代表的国产操作系统，已经由基本可用实现了初步具备替代能力的跨越。2018 年央采目录选入了国产 CPU 设备更是为国产化的发展注入了强大的助推力。同时，可信计算也迈入了主动免疫的可信计算 3.0 时代，在最新推出的等保 2.0 中，“可信”已成为了网络安全保护不可或缺的一部分。国产化基础软硬件与可信计算的结合已成为今后我国网络安全保护的基石。

4、项目的必要性

（1）基于国产化平台，响应国家的国产化替代号召

2006 年，国务院颁布了《国家中长期科学和技术发展规划纲要（2006 年-2020 年）》，将核心电子器件、高端通用芯片及基础软件产品列为 16 个科技重大专项之首。自此，我国国产化基础软硬件的自主研制起步。2013 年，斯诺登事件后，国家明显加大了网络与信息安全的重视程度，先后成立中央国家安全委员会和中央网络安全与信息化领导小组，这两个机构都由习总书记担任主任和组长，站在国家安全角度持续推动自主可控工作。

2014 年，银监会、发改委、科技部和工信部联合发布《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》，并制定目标至 2019 年各银行业金融机构对安全可控信息技术的应用达到不低于 75%的总体占比。2015 年，国家开展了党政机关电子公文系统安全可靠应用第一批试点。2016 年，中共中央办公厅、国务院办公厅印发了《国家信息化发展战略纲要》，根据新形势对《2006-2020 年国家信息化发展战略》进行了调整和发展。指出，到 2025 年根本改变核心关键技术受制于人的局面，形成安全可控的信息技术产业体系。实现技术先进、产业发达、应用领先、网络安全坚不可摧的战略目标。

网络安全保护是信息系统不可或缺的一个部分，基于国产化平台的自主可控网络安全产品更是今后网络安全保护的标配。公司基于国产化平台对全线产品进行适配，响应国家的国产化替代号召。

（2）引入可信，满足用户符合等保 2.0 的需求

我国《网络安全法》第二十一条指出“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。在新发布的网络安全等级保护制度 2.0 之 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》中，对可信计算提出了明确要求，“可信”要求已全面覆盖等保第一级至第四级各级安全保护要求，并融入了安全保护的方方面面。只有引入可信，才能满足用户符合等保 2.0、遵从《网络安全法》的需要。

（3）适配全部主流国产化平台，满足不同行业的要求

由于不同行业针对国产化平台有各自的一些特定的要求，比如可供选择的主流国产化平台包括飞腾、龙芯、兆芯、申威、海光等等。因此，为了满足不同行业的要求，项目将适配全部主流国产化平台，以覆盖高端领域行业的需求。

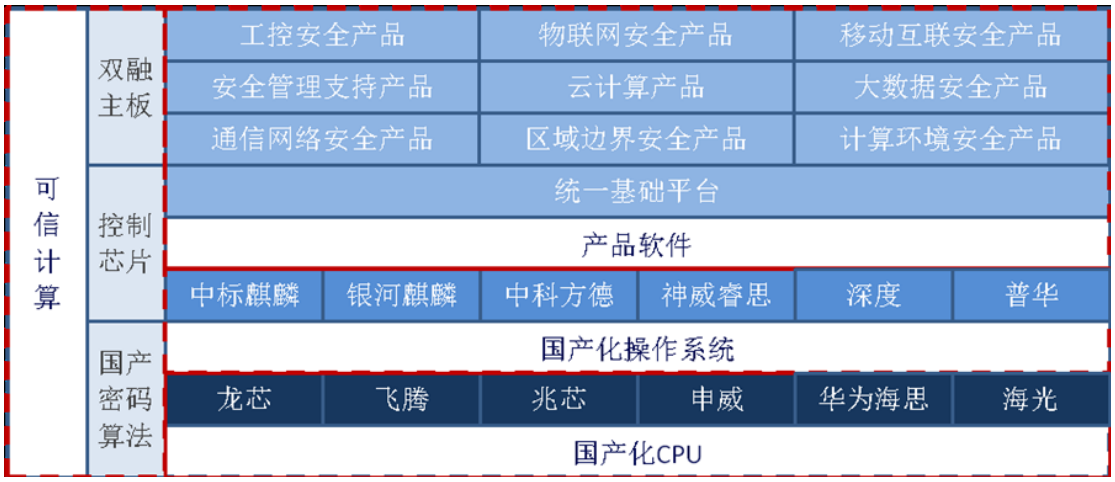
（4）全线产品适配，提供完整的网络安全保护解决方案

项目通过适配公司全线产品，从而可以基于现有产品实现对等保中安全通信网络、安全区域边界、安全计算环境、安全管理中心等各要求部分的全覆盖，继续为用户提供完整的网络安全保护解决方案。

5、项目建设方案

（1）总体设计

全线网络安全产品国产化及可信化研发项目是基于国产化平台及可信计算的产品，以向市场提供符合国产化替代需求以及等保 2.0 要求的全系列产品，从而为用户提供完整的国产化替代及等级保护解决方案。



蓝盾股份基于国产化平台及可信计算的产品，以国产化 CPU 和国产化操作系统为基础、以可信计算为支撑，至下而上实现整体的国产化及可信计算支持。

对于国产化平台的支持，不是仅仅适配单一的某个国产化 CPU 和某款国产化操作系统，而是全面适配所有主流的国产化 CPU 和国产化操作系统组合，包括但不限于：

国产化 CPU	国产化操作系统			
龙芯	中标麒麟	深度	普华	
飞腾	中标麒麟	深度	银河麒麟	
兆芯	中标麒麟	深度	中科方德	普华
申威	中标麒麟	深度	神威睿思	
海光	中标麒麟	深度	中科方德	普华
海思	中标麒麟	深度	银河麒麟	

同时，基于国产 CPU 不同的型号（如龙芯 3A3000、3B3000，飞腾 FT-1500A/4、FT-1500A/16、FT-2000+/64，兆芯 ZX-C、ZX-D、ZX-E，申威 221、421、1621，海光 3100、5100、7100，海思 650、710、980 等）研制百兆、千兆、万兆等系列产品。

对于可信计算的采用，不仅仅局限于系统的某一局部，而是完整地从控制芯片、主板、BIOS、CPU、操作系统到产品软件全栈基于国产密码算法构建可信计算体系，实现可信计算 3.0 对系统的整体免疫。

（2）项目建设内容

1）通信网络安全产品。包括但不限于 VPN、入侵检测、上网行为管理、数据库审计；

2）区域边界安全产品。包括但不限于 UTM、防火墙、防毒墙、入侵防御、网闸、单导；

3）计算环境安全产品。包括但不限于主机监控与审计、Web 应用防火墙、网页防篡改、数据防泄漏、数据库脱敏；

4）安全管理支持产品。包括但不限于堡垒机、漏洞扫描、高级持续威胁检测、安全综合运维管理平台、态势感知；

5）云计算产品。包括但不限于瘦终端、胖终端、云平台、云漏扫、云防护；

6）工控安全产品。包括但不限于工控防火墙、工控防毒墙、工控入侵检测；

7）物联网安全产品。包括但不限于视频设备准入；

8）移动互联安全产品。包括但不限于移动安全卫士、EMM；大数据安全产品。包括但不限于大数据漏扫。

蓝盾股份基于国产化平台及可信计算的产品与现有产品的区别和联系如下：

项目	现有产品	项目产品	区别联系
技术	基于 Intel/ 高通 CPU 及 Ubuntu/CentOS/Windows/Android 操作系统，不支持可信计算	基于龙芯、飞腾、兆芯、申威、海光、海思等国产 CPU 及中标麒麟、银河麒麟、中科方德、神威睿思、深度、普华等国产操作系统，支持可信计算	在已有产品的基础上进行技术改造，融入可信计算并适配国产化软硬件环境
性能	因 CPU 性能较高而产品性能较强	因 CPU 性能较低而产品性能较弱	单台设备性能有所下降，但通过叠加、融合等技术可满足用户对性能的需求
用途	大中型网络	大中型网络	安全性更强，符合等保 2.0
客户	需满足等保 1.0 的企事业通用市场	需满足等保 2.0 的企事业通用市场，以及政府、公检法、银行、轨交、电力、军工等需国产化替代的领域	新产品可继承和发展高端客户群体

竞争优势	符合等保 1.0，全面支持各种复杂网络环境的安全保护	符合等保 2.0，全面支持更严格的安全保护要求，并可满足各领域国产化替代的需求	紧跟政策步伐，与时俱进
服务	一些特定行业的定制开发需求实现周期长	可快速满足特定行业的定制开发需求	对特定领域的需求响应更快捷

6、项目的实施主体

本项目由蓝盾股份全资子公司蓝盾信息安全技术有限公司（简称“蓝盾技术”）自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年销售收入	万元	27,027.78
2	年均净利润	万元	6,728.26
3	财务内部收益率	%	28.75
4	财务净现值（ic=10%）	万元	24,210.56
5	投资回收期	年	2.87

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007203。

（二）新一代 APT 威胁检测与防御系统

1、项目概况

公司新一代 APT 威胁检测与防御系统将在已有产品蓝盾 APT 系统的基础上进行技术升级，对蓝盾 NxSOC 安全运维管理系统、ITIL 工单流程处置系统、态势感知以及应急服务队伍的丰富经验进行功能整合与扩展，建设一套以攻防自动化安全防御为核心的新一代 APT 威胁检测与防御系统平台。将数据、操作、技术、流程、规范、自动化作为关键因素，采用流量还原、AI 人工智能、动态沙箱、情报关联等重点技术，实现安全、风险、数据、工单、处置与环境协同的信

息安全解决方案。最终目标是建立 AI 技术和大数据安全情报体系关联，针对 APT 攻防自动化安全防御。

新一代 APT 威胁检测与防御系统，基于大数据 AI 智能：恶意代码及恶意流量映射为图片基因图谱分析，文件基因分析等；同时也结合静态特征匹配、威胁情报关联及动态行为检测，能很好地弥补传统被动的防御体系检测缺陷，能更精确、更迅速地检测 APT 攻击。

2、项目投资计划

本项目估算新增总投资 18,843.00 万元，其中新增设备购置费 4,227.39 万元、新增软件购置费 2,572.61 万元、开发技术人员人工费 5,386.00 万元，铺底流动资金 3,830.00 万元，分别占总体新增投资额的 22.43%、13.65%、28.58%和 20.33%。本项目拟使用募集资金 9,550.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	4,227.39	22.43%	4,227.39
二	软件购置费	2,572.61	13.65%	2,572.61
三	开发人员人工费	5,386.00	28.58%	2,300.00
四	运营技术服务团队	744.00	3.95%	51.00
五	市场开拓费	1,684.00	8.94%	-
六	试验检验费	399.00	2.12%	399.00
七	铺底流动资金	3,830.00	20.33%	-
合计		**18,843.00**	**100.00%**	**9,550.00**

3、项目实施的背景

随着 IT 技术的迅速发展和信息化建设的不断深入，各企事业单位的 IT 环境变得日趋复杂，各种 IT 基础设施的数量和类型在不断增多，各企业单位常用的业务系统由于作业需要也在不断扩充，同时更多的安全风险也进一步显露出来，安全威胁发生了很大变化，尤其是高级持续性威胁（APT）有愈演愈烈之势。

为了不断应对新的安全挑战，企业和组织先后部署了防火墙、UTM、入侵检测和防护系统、漏洞扫描系统、防病毒系统、终端管理系统等等，构建了多道

安全防线，解决来自某个方面的安全威胁，然而纵观近年来的网络攻击手段，APT 攻击已经成为最具威胁的攻击方法之一。

在 APT 攻击中，由于黑客可能尝试多种方式进行攻击，所以无法使用一种方法就能有效的检测出 APT 攻击。因此彼此孤立的多道安全防线在 APT 攻击面前显得无能为力，需要利用多种检测手段，对监测到的海量日志数据进行综合关联挖掘分析，才能更有效的发现 APT 攻击行为。

面对新型 APT 攻击，通过全面采集网络中包括原始网络数据包、业务和安全日志等各种数据形成大数据库，再通过大数据分析技术和智能分析算法来检测 APT 攻击是最可靠的办法，所以，通过大数据分析、AI 等技术对安全产品进行全局化智能化升级成为信息安全行业的重要发展方向。

4、项目实施的必要性

（1）弥补传统 APT 设备检测能力问题

传统的恶意代码检测识别技术主要包括两类：一类是以恶意代码二进制特征作为判识依据的静态技术，这类技术只能识别特征库中已有特征的恶意代码，随着恶意代码的种类激增，特征库将越发巨大，查杀效能也会急剧下降，即以体征为视角无法得知恶意代码的行为，识别范围受到认知的体征种类限制；另一类是以恶意代码行为特征作为判识依据的动态技术，这类技术能够识别具有已知恶意行为的代码，但由于需要虚拟环境执行恶意代码，因此只能运行在用户终端，难以在高速链路的防护中使用，即以行为为视角无法与恶意代码的体征关联，难以以较高的速度来识别恶意代码。

因此，无论采用“动”还是“静”的恶意代码识别技术，都需要对恶意代码进行分析，然后将其二进制特征或行为特征，采用“亡羊补牢”的方式添加到查杀或防御工具之中。目前，受限于传统代码分析技术，多数安全界人士还是采用半人工半自动的动态调试技术进行恶意代码分析，难以实现恶意代码“行为”和“体征”的关联。这种“亡羊补牢”式的防御，割裂式地对待恶意代码的“行为”和“体征”，造成了传统恶意代码识别技术逐步陷入困境。

当前，我们需要符合现代信息安全要求技术能力的 APT 检测设备。

（2）补齐传统安全设备检测短板问题

当今社会已经进入到“无时不在线，无处不互联”的信息化网络时代，人们的生产、生活，社会的政治、经济，国家的稳定、安全，离开网络空间安全都无从谈起。恶意代码作为网络空间安全威胁的重要源头，日趋“泛化”、“多源化”，其威胁目标从主机、服务器，拓展到移动终端、工业控制系统，甚至是可穿戴设备，呈现出快速增长、种类日益繁杂、威胁愈发严重的态势。因此，对恶意代码的检测、识别和分析一直是网络空间安全领域的重要研究课题之一。

而现有网络安全设备普遍不具备对 APT 类型的攻击的检测能力。

（3）针对性的攻击越发频繁影响巨大

近年来，各类媒体披露的未知攻击不胜枚举。一些专业级黑客组织在不断对我国的各级政府部门、行业组织和企业单位发起攻势。这些攻击针对性极强，一旦成功不只对企事业单位、政府机关、科研机构造成不可弥补的损失，还会造成重大的社会影响。此类攻击往往借助漏洞并且使用社会工程学，有组织有纪律，传统防御手段对此深感无力。APT 攻击难以被发现，不仅窃取网络内部的敏感信息，甚至控制或破坏整个网络。因此，市场迫切需要一款能快速，精确检测 APT 攻击的设备。

（4）实现威胁发现及自动化处理流程

随着信息时代的快速发展，IT 运维已经成为 IT 服务内涵中重要的组成部分。面对越来越多复杂的业务、多样化的用户需求，不断扩展的 IT 应用需要越来越合理的模式来保障 IT 服务能灵活便捷、安全稳定地持续保障。从初期的数台服务器发展到庞大的数据中心，单靠人工已无法满足在技术、业务、管理等方面的需求。标准化、自动化、架构优化、过程优化等降低 IT 服务成本的因素越来越受广大行业客户重视。

基于大数据 AI 智能分析、威胁情报关联的新一代防御系统，能很好地弥补传统的基于特征库的被动防御体系的检测缺陷，并且根据事件的重要性、严重性和威胁可能性，实时自动计算风险，帮助企业实现安全风险分析与运维管理，自动完成事件的采集、分析、评估、响应等全过程。能自动识别 APT 攻击，并可

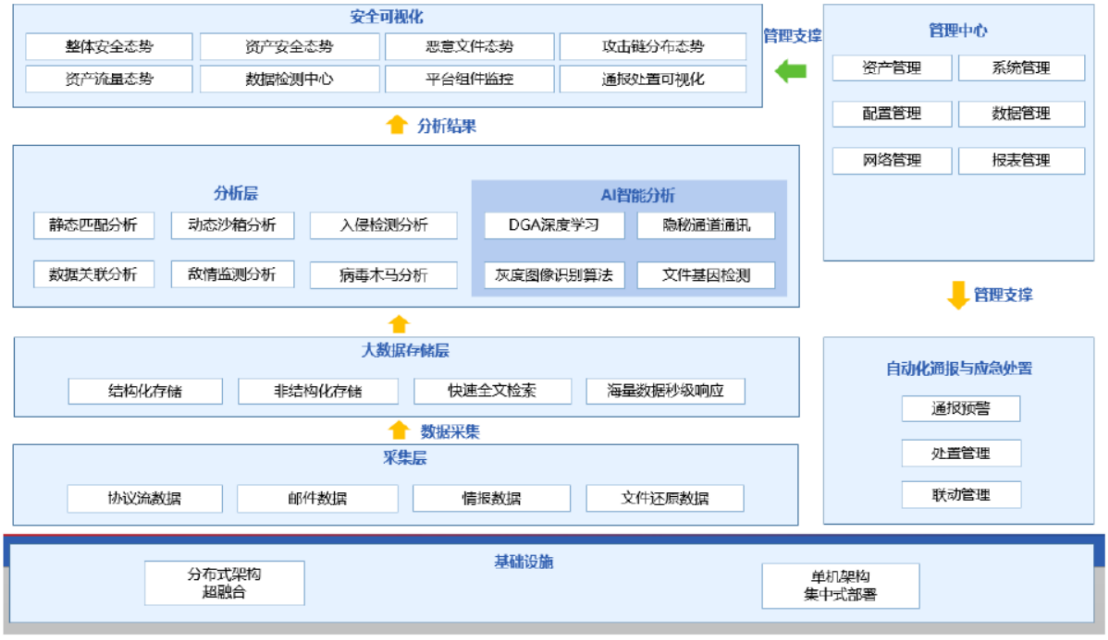
与防火墙等串行网络安全设备联动，提升防护 APT 攻击的能力。实现针对 APT 攻击的自动化安全防御。

5、项目建设方案

（1）总体设计

蓝盾新一代 APT 威胁检测与防御系统将人工智能、大数据技术与安全技术相结合，实时分析网络流量，监控可疑威胁行为。不仅可以通过多病毒检测引擎有效识别出病毒、木马等已知威胁；通过基因图谱检测技术检测恶意代码变种；还可以通过沙箱（Sandbox）行为检测技术发现未知威胁，对检测及防御 APT 攻击起到关键作用。

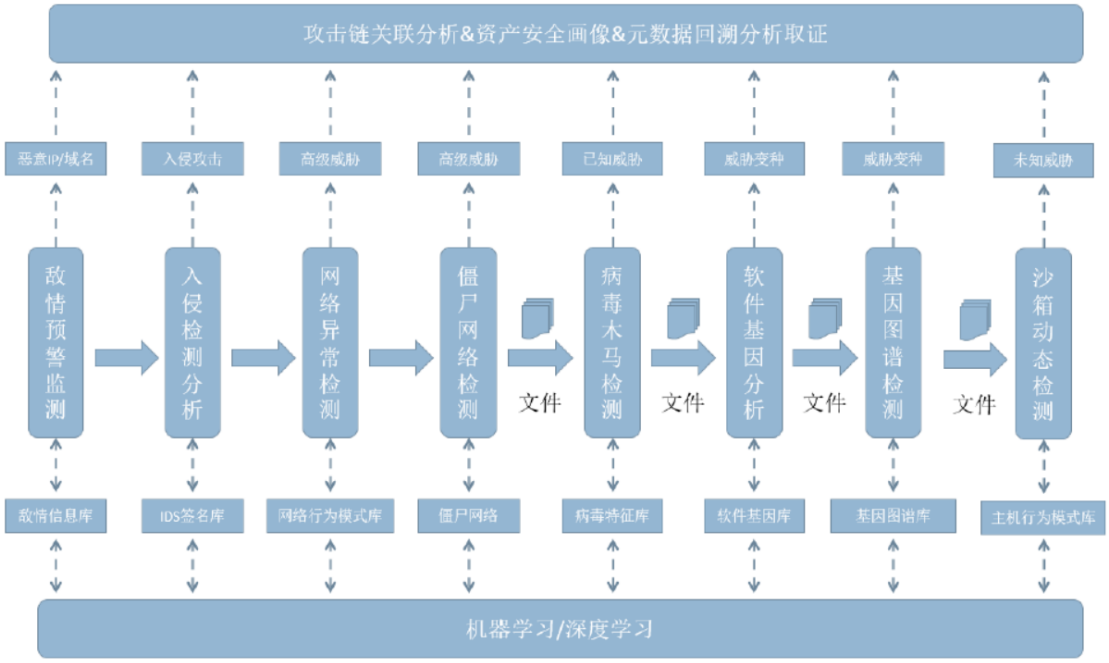
整体架构图如下：



项目采用大数据分布式架构体系，使用接口通信，降低模块之间的耦合度，可以灵活的进行分布式部署。同时，对于小型场景提供单节点部署模式，有效降低小企业落地成本。通过异构计算模型，将各类计算设备通过高速网络连接而成并行计算环境。充分利用各个设备性能优势，完成应用任务。

（2）具体建设内容

新一代高级持续性威胁（APT）检测系统按模块功能组件划分包含：灵活部署架构，异构计算，敌情预警监测，下一代入侵检测，网络异常检测，僵尸网络检测，病毒/木马检测，软件基因分析，基因图谱检测，沙箱动态行为检测，元数据追溯取证，攻击链分析等。



各个子系统的技术要求如下：

1）敌情预警监测

支持敌对安全信息数据在线收集，包括内部发现的敌对威胁信息与外部敌情信息。通过实时下发敌情数据与大数据引擎紧密结合，提升全面检测能力。通过联动提交 IP、域名、URL、文件或文件的 HASH 值、漏洞等到云端敌情分析系统进行追溯取证及可视化关联分析。

2）网络异常检测

异常检测子系统支持 DoS&DDoS 攻击检测、会话连接行为异常检测、中间人劫持攻击检测、非标准协议检测、SMTP 行为异常检测、可疑 SMTP 源 IP 检测、垃圾邮件检测、钓鱼邮件检测、扫描行为检测、密码猜测行为检测、密码暴力破解行为检测等。

3）僵尸网络检测

通过检测网络流量中的 DGA 域名，可以有效定位网络内部已经被僵尸/木马控制的主机（失陷主机）。DGA（DomainGenerateAlgorithm，域名生成算法）域名常用于僵尸/木马的 C&C（Command&Control，命令与控制）通讯，一般是用一个私有的随机字符串生成算法，按照日期或者其他随机种子，每天生成一些随机字符串然后用其中的一些当作 C&C 域名。在僵尸/木马程序里面也按照同样的算法尝试生成这些随机域名然后碰撞得到当天可用的 C&C 域名。

4）入侵检测

对网络内部的扫描探测、入侵攻击、横向渗透等行为进行检测。支持 SQL 注入攻击检测、Bash 漏洞攻击检测、心脏出血漏洞攻击检测、协议动态识别、、网络应用攻击检测、C&C 通讯检测、网络木马检测等。支持协议分析及文件还原，包括 PE 格式文件还原、TXT 格式文件还原、OFFICE 格式文件还原、FLASH 格式文件还原、PDF 格式文件还原、JAVA 格式文件还原、WEB 格式文件还原、PYTHON 格式文件还原、RAR 格式文件还原、ZIP 格式文件还原、VBS 格式文件还原等。

5）病毒木马检测

采用多个反病毒引擎对流量中的文件进行交叉检测和交叉验证，从而发现其中的已知威胁。

6）基因图谱检测

通过采用基因图谱模糊比对技术对流量中的文件进行静态检测，通过结合图像文理分析技术与恶意代码变种检测技术，将可疑文件的二进制代码映射为无法压缩的灰阶图片，与已有的恶意代码基因库图片进行相似度匹配，根据相似度判断是否为威胁变种。支持 Windows、Linux 和 Android 所有的文件格式；支持基因树快速查找比对技术。

7）沙箱行为检测

采用沙箱行为模式匹配技术对流量中的文件进行动态检测，根据恶意行为判断是否为威胁变种。支持沙箱环境定制；支持各种 Windows 文件、PE 文件、Office 文件、PDF 文件、HTML 文件等；支持反沙箱行为检测；支持恶意代码的行为相似性聚类。通过聚类分析和文件追溯判断该文件是否为恶意文件。若该文件具有多个恶意行为且成功逃过多个反病毒引擎的检测及基因图谱检测，则该文件极有可能为新型的恶意代码，即未知威胁。

8）软件基因检测

使用静态反编译技术对文件进行逆向和碎片化切割，根据软件的功能语义提取基因片段，并结合大数据分析方法，对未知软件进行恶意性判定、同源性分析、漏洞基因检测等。

9）元数据追溯取证

元数据追溯取证：内置网络流量元数据审计取证引擎，对网络流量中的应用层元数据进行提取及事后追溯取证；

协议解析：对网络流量进行协议解析；

应用识别：对网络流量进行应用识别；

会话分析：对网络流量进行会话分析；

10）攻击链分析

高级持续性威胁（APT）检测系统能够对 APT 攻击链的各个阶段进行全面的安全检测，包括 1、扫描探测 2、工具投送 3、漏洞利用 4、木马下载 5、远程控制 6、横向渗透 7、行动收割。

11）溯源取证

支持解析并存储 http、dns、ftp、smtp 等几十种协议的元数据，具有完整的追溯取证能力。通过可视化操作，可快速定位攻击者，并定位出攻击者的 IP，MAC，攻击方式，攻击协议，以及攻击目标等详细信息。

12）资产监测分析

系统支持通过关联分析结果、规则特征配结果、算法模型分析结果、动态行为分析结果与敌情情报关联，确定网络内部已经出现问题的资产。

13）安全联动

能自动识别 APT 攻击，并可与防火墙、入侵防御、网闸等串行网络安全设备联动，提升防护 APT 攻击的能力。

6、项目的实施主体

本项目由蓝盾股份的子公司蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年均销售收入	万元	6,951.11
2	年均净利润	万元	1,798.96
3	财务内部收益率	%	28.76
4	财务净现值（ic=10%）	万元	6,372.49
5	投资回收期	年	2.93

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007217。

（三）工业网络统一威胁管控平台项目

1、项目概况

本项目是以公司现有的工业安全产品（工控防火墙、工业入侵检测、漏洞扫描、内容审计等安全类产品）为基础，整合公司优势的其他安全产品作为工业网络统一威胁管控平台，并形成各系列工业安全设备产品，为政府、企业提供高性

能、多功能、体系灵活、部署方便的高端工业安全设备产品，增强公司在工业互联网安全市场的竞争力，减少新产品的开发时间与成本。各系列工业安全设备产品将逐步取代目前公司在售的工控防火墙、工业入侵检测、工业审计、工控主机安全设备等传统工业安全产品。

2、项目投资计划

本项目估算新增总投资 23,560.00 万元，其中新增设备购置费 5,860.65 万元、新增软件购置费 2,139.35 万元、开发技术人员人工费 5,911.00 万元，铺底流动资金 5,780.00 万元，分别占总体新增投资额的 24.88%、9.08%、25.09%和 24.53%。本项目拟使用募集资金 11,150.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	5,860.65	24.88%	5,860.65
二	软件购置费	2,139.35	9.08%	2,139.35
三	开发人员人工费	5,911.00	25.09%	2,687.50
四	运营技术服务团队	1,063.00	4.51%	71.50
五	市场开拓费	2,415.00	10.25%	-
六	试验检验费	391.00	1.66%	391.00
七	铺底流动资金	5,780.00	24.53%	-
合计		**23,560.00**	**100.00%**	**11,150.00**

3、项目的实施背景

工业信息安全产业肩负着为我国工业自动化、信息化基础设施和信息系统的安全保障提供安全产品和服务的重要任务，是我国建设制造强国和网络强国的重要支撑，是保障国家网络安全的重要基础。当前日益复杂严峻工业信息安全形势引发全球关注，世界各国政府与产业高度重视工信息安不断加大势引发全球关注，世界各国政府与产业界高度重视工业信息安全，不断加大安全投入，工业信息安全产业迎来发展机遇。

“十三五”以来，党中央、国务院科学构建工业信息安全战略布局，以《网络安全法》为基础，出台了一系列法规政策、战略规划和指导意见，强化企业的安全主体责任，明确工业信息安全工作的方向和目标，工业信息安全产业发展环

境不断优化。在工业互联网、工业云、工业大数据等产业发展需求的带动下，工业信息安全领域的技术和产品创新升级，威胁情报、态势感知、安全可视化、虚拟化等新技术不断涌现，以工业安全、监测审计为代表的工业信息安全产品市场增长迅猛，工业信息安全市场逐步扩大。

4、项目实施的必要性

（1）提高国内工业安全产业的创新力，增强核心竞争优势

伴随着信息安全行业的快速发展，国内信息安全企业的技术创新能力和市场拓展能力也得到了大幅提升。但与 Fortinet、Cisco、WatchGuard 等国际企业相比，国内企业在整体技术创新能力方面还存在较大差距，而这也是一直以来困扰国内企业持续发展的重要制约因素。公司工业安全设备通过技术架构的革新，实现了工业安全设备产品的立体防护，对于提升国内信息安全产业的创新能力，增强国内信息安全产业核心竞争力具有推动作用。

（2）提高信息安全防护能力，保障企业信息的安全

在社会经济高度发展的今天，信息对于个人、企业乃至国家的政治安全、经济安全和国防安全都起着越来越重要的作用，因而信息安全在整个信息产业布局乃至国家战略格局中都有着举足轻重的地位和作用。但从信息安全保障现实情况来看，随着威胁攻击的越来越复杂，无论是防火墙、入侵防护、内容审计等单功能产品，还是传统的工业安全设备产品都很难实现真正有效的安全防护。比如工业安全设备虽然能对外部威胁进行防御，但却无法处理工业内主机发生的威胁，也无法做到内外网安全策略的统一管理，从而也给目前的工业控制网络埋下了众多安全隐患。

公司工业安全设备通过体系架构的再造，革新性地解决网络“点”（即主机）、“线”（即工业）、“面”（即安全策略关联管理）的难题，并通过加密隧道的联动机制，形成一个联动的覆盖整体网络及设备的立体安全防御体系，使得安全防御效率得到大幅提高，能更加有效保障用户的信息安全。因此，通过此项目的实施，将有效提高企业的信息安全，保障社会经济生产的正常运行。

（3）满足用户信息安全一体化的无缝整合需求

随着信息安全威胁的多样性和隐蔽性不断增强，原有的以防火墙、入侵防护、内容审计等单功能产品各自为战的安全解决方案已经很难满足用户对高效信息安全维护的需求。因为基于攻击多样化和融合的特点，原来各自为战的安全产品总是处于疲于应付的状态，无法很好的实现对生产网络安全的保护，生产环境中可能部署的防火墙、入侵防护、内容审计等一系列安全产品，产生大量不同形式的安全信息，使得整个系统的相互协作和统一管理成为安全管理的难点。由此带来安全管理任务的大幅增加，企业的安全管理体制也变得非常复杂，其系统配置、规则设置、反应处理、设备管理、运行管理的复杂性所带来的管理成本和管理难度都直接制约了安全防御体系的有效性，从而也给网络的安全性带来重大隐患，使得用户的需求在不断向多功能一体化的方向发展。

公司工业安全设备能够实现对信息安全防护和管理的一体化，简化安全解决方案、规避设备兼容性问题，实现各种安全功能的无缝连接，使原本复杂的安全防护和管理问题简单化，顺应市场发展趋势，满足用户信息安全一体化的无缝整合需求。

（4）引领工业安全产品的技术革新，大幅提高产品性能

工业安全设备作为近年来快速兴起的信息安全产品，凭借突出的性价比、人性化的管理优势赢得了众多用户的青睐。

与目前市场上大多数工业安全设备产品相比，公司基于工业网络统一威胁管控平台产品将创新性的改变原有工业安全设备的体系架构，将 UPM（统一策略管理）、UEM（统一终端管理）、UCM（自适应通道管理）整合成全新的体系架构，并通过运用自主开发的 SM-XML 安全联动管理协议、关联事件报警机制、ObjectPolicy 通用策略对象化管理、自动化管理流程等新功能，将原来分散的防御技术整合成为立体的安全管理平台。

通过项目实施，公司工业安全设备将引领网关类产品的技术革新趋势，通过联动协议和算法优化使全网的安全防御效率大幅提高，而通过架构优化和通用策略对象化则使公司工业安全设备具有更好高能、达到更高的联动性能水平。

（5）顺应行业发展趋势，促进公司持续发展

项目的实施是顺应行业发展趋势的需要。工业安全设备作为信息安全产品领域功能、技术的集大成者，满足用户一体化防护的需要，深受用户青睐，特别是在新型中小生产企业市场，已成为未来信息安全行业发展的趋势之一。

公司工业网络统一威胁管控平台设备是在原有工业安全设备产品及技术的基础之上，通过产品体系架构的革新性改造，形成“一点报警，全网联防”的点、线、面立体防护安全产品，其整体防护能力和效率均较传统工业安全设备产品大幅提升，能更好解决用户的综合安全防护需求，因此将更加受到用户青睐，产品在未来市场上也将具有更强的竞争力。

通过项目的实施，顺应信息安全行业发展趋势，提升公司的市场竞争力，为公司未来的发展打下坚实基础。

（6）有效整合公司资源，提高公司业务运营效率

公司工业网络统一威胁管控平台设备是在现有工业安全设备的基础上，通过体系架构再造形成信息安全综合管理平台，该平台下的产品将取代目前公司在售的防火墙、入侵防护、内容审计等单功能工业安全产品。因此，通过项目的实施，形成解决信息安全管理的多功能综合管理平台，将有效整合公司的人力、财力及物力资源，集中资源进行工业安全设备的技术研发和市场推广，减少因开发、推广各种单功能产品，资源分散而造成的不利影响，提高公司业务运营的效率和资源利用的效率，有利于公司未来发展。

（7）易于产品开发，快速响应客户需求

不同于一般产品的新品开发模式，公司工业网络统一威胁管控平台设备在通过对现有工业安全产品进行革新性的产品架构体系再造基础上实现。以平台架构形式存在，易于产品开发，且能根据客户需求快速组合成特定形态的产品，实现对客户需求的快速响应，从而有利于提升公司的客户服务能力，促进公司业务的发展。

5、项目建设方案

项目以工业安全产品（工业安全设备、防火墙、IDS 入侵检测、漏洞扫描等工业安全类产品）为基础，创新性的提出以工业安全设备公用终端管理、公用策略管理、公用信令管理、自适应通道管理的体系架构，形成以公用终端管理为网络点防御、以工业安全设备公用信令管理为网络线防御、以公用策略管理为覆盖全网的安全策略监控管理中心，并以自适应通道管理适应异构网络、复合网络的全面安全联动体系。实现“一点报警，全网联防”的点、线、面立体防御工程。

项目主要由工业协议识别模块、工业审计模块、工业安全防护模块、工业网络异常监控模块、工业设备基线学习模块、工业设备准入系统、工业设备安全运维模块、统一管理系统等八个子系统组成。

将原有基于规则匹配的产品改造为全线的人工智能化（即“AI-enabled”）产品，从而打造更加智慧的工业大安全战略生态。实现工业安全全覆盖，减少用户工业组态成本。

项目主要建设内容如下：

建设内容	内容描述
高可靠硬件及软件的研发工作	该研发工作包括基于宽工作环境的硬件研究、核心系统程序改造、性能提升算法改造三项内容。
工业协议、工业安全控制及 AI 深度学习的研发	该研发工作包括工业协议识别（通用工业协议：modbus 通讯协议、DNP3 协议、OPC 协议、IEC104、IEC101、Pofinet、S7、Ethercat 以及我国提出的标准 EPA 等）、工业安全控制、网络异常监控模块、工业设备基线学习、设备资产自动发现模块五个主要新模块研发，以及原有旧模块（防火墙模块、网络层流量模块、入侵检测系统模块、身份认证模块、内容审计模块）等模块的升级改造。
基于工控公用管理平台体系架构研发及升级	该研发工作包括公用终端管理系统、公用信令管理系统、公用策略管理系统共三个子系统的研发。
全栈系列产品部署灵活性研发及升级	该研发工作包括部署模式配置向导模块、在线帮助模块、报表预警模块、功能实时更新模块共四个模块研发。

（1）高可靠硬件及软件的研发工作

公司计划将原有的全线网关产品改造为多核架构，实现性能的整体提高和降低能耗，节约成本。包括三项内容：1）基于多核架构的硬件研究、2）核心系统程序改造、3）性能提升算法改造。具体如下：

序号	研发内容	说明
1	基于多核架构的硬件研究	对原有硬件平台改造，实现更高性能/更低能耗及更低硬件成本。采用低功耗、多核硬件平台，研究的硬件主要基于 ARM、MIPS 处理器的网络平台硬件，通过硬件研究及测试、开发包研究及测试、demo 版制作，各类网络环境测试得出最佳硬件组合，作为工业安全设备的硬件平台。
2	核心系统程序改造	这是对原有工业安全产品的操作系统进行改造，以适应多核架构硬件。根据选择的多核平台及配套 SDK 开发包，进行核心程序（蓝盾安全操作系统及内核各个基础模块）的改造升级。
3	性能提升算法改造	这是需要新开发的内容，针对多核架构硬件，采取网口驱动改造，包分类算法改造，模块调度算法改造等研发，在软件层面提高性能，最大限度发挥多核架构的优势，提升性能指标和整体功能稳定性。

（2）工业协议、工业安全控制及 AI 深度学习的研发

新研发功能模块包括：1）工业协议识别、2）工业安全控制、3）网络异常监控模块、4）工业设备基线学习、5）设备资产自动发现模块

升级的现有模块包括：1）防火墙模块、2）内容审计模块、3）入侵检测系统模块、4）网络层流量模块、5）身份认证模块

（3）基于工控公用管理平台体系架构研发及升级

新研发三个子系统：1）公用终端管理系统、2）公用信令管理系统、3）公用策略管理系统。

序号	研发内容	说明
1	公用终端管理系统	通过与主机插件进行联动，能够统计终端系统补丁、强制 IP-MAC 绑定、启动主机端 ARP 防火墙、发现木马、对敏感文件信息进行保护、对违规的主机强制断网等操作。该模块研发成功后可作为工业安全设备产品的一个增值子系统，或者通过更细化的功能合成一个终端管理产品进行销售。

2	公用信令管理系统	能够对 IPv4/IPv6 协议进行自适应通道管理，适合异构网络、复合网络全面聚合安防。该模块研发成功后可作为工业安全设备产品的一个增值子系统进行销售。
3	公用策略管理系统	能够通过统一策略中心制定安全策略规范，进行安全关联协防，联动多台工业及内网安全设备，组成整体化网络安全体系。该模块研发成功后可作为工业安全设备产品的一个增值子系统进行销售。

（4）全栈系列产品部署灵活性研发及升级

主要为四个模块研发：1）配置向导模块、2）在线帮助模块、3）报表预警模块、4）功能实时更新模块。

序号	研发内容	说明
1	配置向导模块	支持 NAT/路由/透明/混合等多种部署模式，通过人性化的配置向导帮助用户一步一步配置工业安全设备的各项功能，减少配置错误的几率，提高配置简易程度，进而提高用户满意度。可作为工业安全设备产品的一个标准功能进行销售。
2	在线帮助模块	通过提供在线帮助文档、动画演示、远程配置协助工具的方式为用户提供帮助。可作为工业安全设备产品的一个增值模块进行销售。
3	报表预警模块	支持多种告警方式（实时告警、屏幕报警、邮件报警、SNMP 报警、短信报警、自定义程序报警等）以及多种动态报表，综合分析及展现。可作为工业安全设备产品的一个标准模块进行销售。
4	功能实时更新模块	通过建立一个产品升级中心服务器的方式为工业安全设备产品提供远程实时功能升级/下载式离线功能升级等功能。可作为工业安全设备产品的一个标准模块进行销售。

6、项目实施主体

本项目由蓝盾股份的子公司蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年销售收入	万元	9,700.00
2	年均净利润	万元	2,356.95

3	财务内部收益率	%	29.72
4	财务净现值（ic=10%）	万元	8,455.53
5	投资回收期	年	2.94

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007234。

（四）自主可控终端检测与高级防御系统

1、项目概况

项目将在已有产品蓝盾内网安全管理及审计系统的基础上进行技术升级，对终端主机安全防护、安全审计、安全运维等进行功能整合与扩展。在平台兼容性方面，增加对国产化自主可控操作系统和国产化自主可控 CPU 等硬件平台的支持；在终端防护方面，增加对未知威胁的自动防护；在安全管控方面，增加 WINDOWS 和国产化自主可控等不同终端主机的统一管控和统一威胁分析与处理；在安全联动方面，将内网中不同类型的终端主机接入控制与防火墙等边界安全防护系统进行联动，实现核心业务系统的准入控制和终端行为审计，与 APT 统一威胁分析系统进行联动，实现对终端主机在 WINDOWS 平台和国产化自主可控平台下可执行、电子文档等类型文件的未知威胁分析。

项目建设一套以自动化安全防御为主和自动化安全审计及安全运维为辅的自主可控终端检测与高级防御系统，将采用操作系统内核层钩子及应用层钩子技术、机器学习技术、大数据分析技术、安全联动技术，统一安全策略技术实现细粒度的自主可控终端安全防护、安全审计和安全运维，实现不同类型终端主机的统一安全管理、安全审计和安全运维。

2、项目投资计划

本项目估算新增总投资 24,365.00 万元，其中新增设备购置费 7,000.00 万元、新增软件购置费 2,000.00 万元、开发技术人员人工费 5,960.00 万元，铺底流动资金 5,650.00 万元，分别占总体新增投资额的 28.73%、8.21%、24.46%和 23.19%。本项目拟使用募集资金 12,000.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	7,000.00	28.73%	7,000.00
二	软件购置费	2,000.00	8.21%	2,000.00
三	开发人员人工费	5,960.00	24.46%	2,600.00
四	运营技术服务团队	1,071.00	4.40%	120.00
五	市场开拓费	2,404.00	9.87%	-
六	试验检验费	280.00	1.15%	280.00
七	铺底流动资金	5,650.00	23.19%	-
合计		**24,365.00**	**100.00%**	**12,000.00**

3、项目的实施背景

随着 IT 技术的迅速发展和信息化建设的不断深入，各企事业单位的 IT 环境变得日趋复杂，各种 IT 基础设施的数量和类型在不断增多，各企业单位常用的业务系统由于作业需要也在不断扩充，同时更多的安全风险也进一步显露出来，安全威胁发生了很大变化，随着互联网的发展，网络安全和信息安全越来越多受到政府单位、企业的重视，为防止重要的信息被黑客通过互联网进行窃取而泄密，许多政府单位和企业通常通过在网络边界部署防火墙和入侵检测等边界安全防护系统进行网络边界防护。但是，这些主要针对外网的安全防护在面对内网安全威胁时，往往形同虚设，因为“内忧”胜于“外患”，政符及企事业单位不仅需要坚固的边界安全，更需要稳定的内网安全。

据美国联邦调查局（FBI）和计算机安全协会（CSI）对 484 家公司进行的网络安全专项调查显示：超过 85%的安全威胁来自于内部，有 16%来自于内部未授权的存取。内网泄密导致的损失，是黑客造成损失的 16 倍，是病毒造成损失的 12 倍。充分说明了内部人员泄密的严重危害，同时也提醒政府单位和企业单位进行网络外部安全建设的同时应尽快加强网络内部安全的建设，特别是终端安全建设。

随着自主可控国家战略的实施，自主可控办公设备的更换已上升到国家战略。随着国家对军工、政符和企业事业单位安全的重视，越来越多的传统终端将更换成自主可控终端，预计近几年，国产操作系统将从国家战略核心部门进一步

扩大到 8+2 行业。目前包括金融、石油、电力、电信、交通、航空航天、医院、教育为代表的八大重要行业将启动国产化替代项目并稳步推进，而根据估算党政和重要行业未来 2~3 年终端替换规模达到 500 万台，对应国产系统建设总经费超 1,000 亿元。若未来国产化替代向重点行业全面拓展，根据公开数据，目前全国党政机关公务员超过 700 余万人，事业单位编制人员 3,100 余万人、中央企业员工 1,200 余万人，总数合计约 5,000 万人，简单测算 5,000 万台终端计算机及系统替换，对应的基础软硬件、应用和安全市场总规模超过 1 万亿元。

在国产化计算机的安全软件方面，须从接入控制、主机安全、数据安全、通信安全和病毒木马查杀等方面，通过网络接入控制、主机安全监控审计、安全补丁、终端身份鉴别、应用安全管理、数据安全管理、安全即时通信和网络防病毒等技术手段，来确保国产化计算机的安全、可控、可运维。这为国产化计算机安全软件的设计与开发指明了方向，提供了具体的技术要求依据，也为终端主机安全市场带来了新的业务增长点。

4、项目实施的必要性

（1）兼容新的国产化自主可控终端主机

近年来，军工、政符及关系到国计民生的重要部门将逐渐把传统终端主机更换成国产化自主可控主机，会催生新的主机安全防护与审计需求，需要一套部署在国产化自主可控终端主机上的主机型安全防护与审计系统，对国产化自主可控终端主机进行安全防护、安全审计及安全运维。

当前，军工、政府和关系到国计民生的企事业单位急需支持自主可控终端主机安全产品。

（2）补齐传统主机安全检测与安全防护的短板问题

伴随着虚拟货币的炒作，勒索病毒和挖矿木马渐渐成为了近几年终端安全的热点话题，各种新的未知病毒的木马应运而生，各种新的攻击方法层出不穷。面对未知的终端安全威胁，基于传统的固定式的安全策略防护已经无能为力，必须采用全新基于机器学习和关联分析的 AI 分析和防护技术才能有效对未知的威胁进行检测与防护。

当前基于传统的固定式安全策略防护主机安全产品已经无法适应新的主机安全形势，基于 AI 技术的自动化检测和防护是未来发展方向，也是客户所迫切需求的安全产品。

（3）支持跨平台的统一安全管理及大数据日志分析需求

政府及企事业单位对自主可控的需求不只针对办公设备，对安全产品本身也要求软硬件基础平台采用自主可控服务器主机，所以系统管控中心也要全面适配自主可控操作系统和国产 CPU 等硬件平台，需要采用能适应自主可控软硬件基础和平台的 WEB 前端管理系统、大数据后台分析和调度系统。同时自主可控部署有个过渡期，系统安全管控中心必须能同时兼容传统 WINDOWS 终端主机和新的自主可控终端主机两种机型的客户端管理，必须满足两种不同类型主机的安全策略管理和主机分类管理。

（4）需要与其它安全防护系统进行安全联动

终端安全管理系统实现对终端主机安全防护和审计，对于未知病毒木马的检测和防护需要通过联动技术借助新一代 APT 安全检测产品的平台可执行文件安全仿真功能进行检测。

终端安全管理系统需要与边界防火墙一起通过联动技术实现终端主机的准入控制，只有终端安全防护产品才能实现精准识别终端主机的真正身份和实现细粒度的行为审计，真正实现内网安全准入控制。

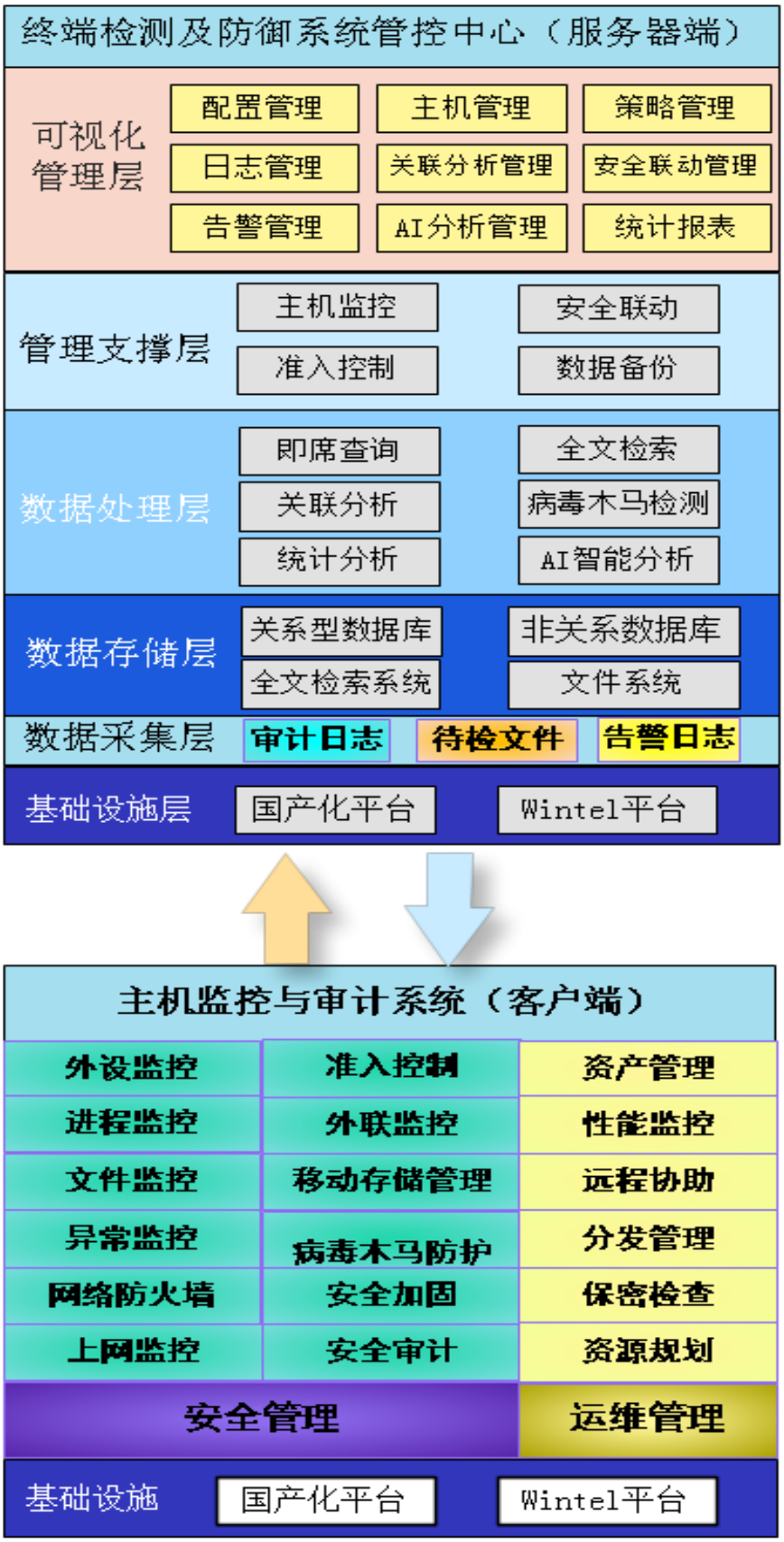
安全产品的“单兵作战”方式已经无法适应新的安全形势，需要不同类型的安全产品进行“联合协同作战”方能适应新的安全威胁。

因此市场迫切需要一款能兼容国产化的支持大数据分析的统一终端安全管理平台。

5、项目建设方案

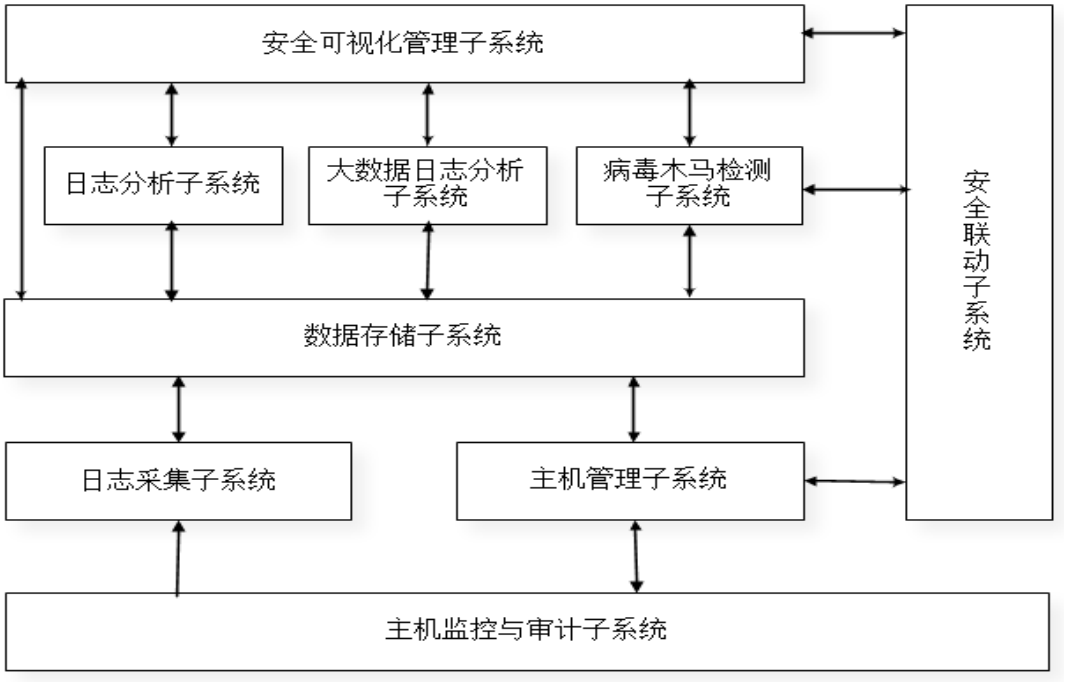
（1）总体设计

蓝盾自主可控终端检测与高级防御系统由管控中心（服务器端）、主机监控与审计系统（客户端）两部分组成，其整体架构图如下：



（2）具体建设内容

自主可控终端检测与高级防御系统包含九个子系统，分别是主机监控与审计子系统、日志采集子系统、主机管理子系统、安全可视化管理子系统、数据存储子系统、日志分析子系统、大数据日志分析子系统、病毒木马检测子系统、安全联动子系统，九个子系统关系如下：



1）主机监控与审计子系统

主机监控与审计子系统以代理软件形式部署在国产化终端主机上，采用国产化操作系统内核层钩子技术和应用层钩子技术双层钩子技术，实现主机进程、文件、网络、外设等多个层面的实时安全监控和主动防御，实现对受控主机的安全防护、安全审计、安全运维等监控功能。该子系统接收管控端的安全策略，把监控和审计结果上报给管控端。

2）日志采集子系统

以 TCP Socket 的通信方式接收来自主机监控与审计子系统上报主机审计日志和主机告警日志，把日志数据进行规范处理后存储到数据存储子系统。

3）主机管理子系统

主机管理子系统以 TCP Socket 的通信方式与主机监控与审计子系统进行数据交互，下发管控端配置的安全策略，同时支持受控主机进行远程控制，包括关机、重启、远程桌面管理、卸载监控软件等操作，主机管理子系统把主机端通信状态数据和资产配置数据存储到数据存储子系统。

4）数据存储子系统

数据存储子系统存储来自主机上报的日志和文件数据，同时存储管控端分析结果数据和配置管理策略，由国产化关系型数据库、非关系数据库、文件系统、全文检索系统组成。其中关系型数据库用于存储少量结构化数据，包括配置信息、主机资产信息、统计结果信息、分析结果等信息和规模较小的审计和告警日志数据；非关系数据库用于存储规模较大的结构化数据和半结构化数据，包括主机审计日志、主机告警日志等；文件系统用于存储待检测文件；全文检索系统用于存储审计日志和告警日志元数据、文件索引数据等。

5）日志分析子系统

日志分析子系统负责数据规模较少的审计日志和告警日志的关联分析、统计分析和 AI 智能分析，该子系统从数据存储子系统中读取日志数据，把统计和分析结果存储到存储子系统中供安全可视化系统调用查询和展示。

6）大数据日志分析子系统

大数据日志分析子系统负责数据规模较大的审计日志和告警日志的关联分析、统计分析和 AI 智能分析，该子系统从存储子系统中的大数据平台中读取日志数据，把统计和分析结果存储到存储子系统中供安全可视化系统调用查询和展示。当本系统部署到客户市级、省级、或集团总部级别作为总控中心时，日志规模将会很大，传统单机日志分析系统无法支撑海量数据分析处理，将采用分布式服务器集群进行大数据分析处理。

7）病毒木马检查子系统

通过采用多个病毒木马检检测引擎（可扩展）对主机上传的待检文件进行病毒木马检测，如果检测结果发现中标，则把检测结果下发给受控主机；如果不中标则把文件通过安全联动子系统把文件转发给沙箱行为检测系统行恶意行为检测，当沙箱行为检测系统发给结果时，把结果反馈给受控主机。

8）安全联动子系统

安全联动子系统负责与其它安全实产品进行安全联动处理，与其它安全产品一起“联合协同作战”，完成单个安全产品较难或无法完成的安全检测和安全防护，提升整体防护能力。安全联动把受控主机的在管控中心本地无法检测的文件转发给沙箱恶意行为检测系统，把检测结果发送给相应受控主机；通过与边界防火墙系统进行安全联动可实现主机安全业务准入、主机精确身份识别和精化的行为审计。

9）安全可视化管理子系统

安全可视化管理子系统依托国产化中间件，实现 WEB 管理界面与用户交互，包括主机管理、日志管理、策略管理、告警管理、关联分析管理、安全联动管理、统计报表等可视化管理功能。

6、项目的实施主体

本项目由蓝盾股份的子公司蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年销售收入	万元	9,884.44
2	年均净利润	万元	2,198.46
3	财务内部收益率	%	27.56%
4	财务净现值（ic=10%）	万元	7,917.43

5	投资回收期	年	3.00

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007240。

（五）大数据安全监控与交换平台

1、项目概况

项目为各级政府部门建设一个集信息共享、安全防护和安全管理为一体的对外数据交换与信息共享安全平台，从而规范跨域数据交换和信息共享方式，保障跨域数据交换和信息共享安全可控，着力响应国家推动信息共享和整合要求。

2、项目投资计划

本项目估算新增总投资 24,854.00 万元，其中新增设备购置费 6,450.28 万元、新增软件购置费 2,149.72 万元、开发技术人员人工费 6,868.00 万元，铺底流动资金 5,480.00 万元，分别占总体新增投资额的 25.95%、8.65%、27.63%和 22.05%。本项目拟使用募集资金 12,300.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	6,450.28	25.95%	6,450.28
二	软件购置费	2,149.72	8.65%	2,149.72
三	开发人员人工费	6,868.00	27.63%	3,187.50
四	运营技术服务团队	1,061.00	4.27%	71.50
五	市场开拓费	2,404.00	9.67%	-
六	试验检验费	441.00	1.77%	441.00
七	铺底流动资金	5,480.00	22.05%	-
合计		**24,854.00**	**100.00%**	**12,300.00**

3、项目的实施背景

政务大数据趋势明显，政府机关、大型企业等单位因业务需要和外部单位（不同安全域）进行数据交换，各类公众信息服务需要将数据与服务对外开放，政务大数据在安全与开放方面难以平衡。

（1）跨域数据交换认证机制不完善，非法对象可能与内部系统进行数据交换导致数据泄露；

（2）端到端数据机密性和完整性缺防护措施，传输过程存在非法截获及监听的威胁；

（3）数据交换记录缺乏审计，可能导致双方数据不一致时无法追溯，责任无法明确；

（4）数据交换缺乏权限控制及有效的病毒检测措施，数据结构和内容有暴露风险，传输数据或文件可能含有恶意代码。

根据安全防护需求不能将内部网络与外部网络直接互通，相关行业法规要求大数据平台进行物理隔离、数据校验、恶意内容防护等安全措施，通过跨安全域数据交换系统+安全隔离网闸实现数据的安全隔离、数据适配、安全处理和传输。

大数据安全监控与交换平台是配合响应政府工作，提供跨局域网的安全数据交换平台，平台集成前后置机、单导或者网闸、集控审计三大部分，整合了多样化的数据采集、数据清洗、数据交换、数据推送等功能，提供多样化、安全、高效、稳定的数据交换服务。

公司大数据安全监控与交换平台主要用于解决部门之间数据共享问题、业务互访问题以及部门之间的边界安全问题。

（1）数据交换问题：解决跨部门的信息共享、互联互通等问题，消除信息孤岛，为政府部门之间的业务协同、数据共享提供基础支撑。

（2）服务共享问题：解决跨部门之间的服务调用，数据服务发布问题，并提供安全认证、服务监控等功能。

（3）边界安全问题：从应用层进一步加强边界的安全，主要包括数据传输过程加解密、文件安全检查控制、服务访问安全控制、数据访问精细化控制等。

4、项目实施的必要性

（1）提高国内信息安全产业的创新力，增强核心竞争优势

为各级政府部门建设一个集信息共享、安全防护和安全管理为一体的对外数据交换与信息共享安全平台，从而规范跨域数据交换和信息共享方式，保障跨域数据交换和信息共享安全可控，着力响应国家推动信息共享和整合要求。迈出了国内信息安全企业技术创新的重要一步，对于提升国内信息安全产业的创新能力，增强国内信息安全产业核心竞争力具有重要的推动作用。

（2）提高数据共享及安全能力，推动信息化建设步伐

在社会经济高度发展的今天，信息数据对于个人、企业乃至整个国家的政治安全、经济安全和国防安全都起着越来越重要的作用，因而信息数据安全在整个信息产业布局乃至国家战略格局中也有着举足轻重的地位和作用。为充分发挥大数据价值，需要盘活数据资产，开发共享数据。电信运营商和互联网公司等拥有海量大数据，他们积极探索并投身建设大数据开放平台，一方面，封装自有的数据资源以及数据存储、数据加工、数据挖掘分析能力，以数据服务的方式开放给第三方（尤其是中小企业以及应用开发者），开发各种大数据创新服务；另一方面，与政府、公共服务部门以及跨领域行业开展合作，融合加工多源异构数据，融合开放跨行业数据，带动产业发展新型业务形态。

在大数据开放、运营或者变现过程中，如何保证开放数据的合规性、避免敏感信息的泄漏、对交易数据进行计量或者计费以及对数据进行审计等成为当前亟需解决的问题。

（3）满足等保有关数据访问细腻度的要求

从 2007 年~2017 年，中国的网络安全等级保护技术主要应用 1.0 版本。最新发布的 2.0 版本针对新技术提出扩展性要求，在聚焦于等级保护的基本要求时，更多用技术思维解读标准。

中国的网络安全等级保护技术 1.0 版本主要强调物理主机、应用、数据、传输，2.0 版本在云计算、大数据、物联网、工业控制系统等新技术新应用方面有涉及。等保 2.0 要求对数据库访问能够精确到库、表、字段一级的访问，并且对不同用户设置不同访问权限。

大数据安全监控与交换平台能够实现数据归集、共享安全策略，提供独立于应用系统的信息共享安全控制手段，病毒查杀校验防止病毒及恶意代码流入内部，数据脱敏有效防止关键数据泄露，灵活多样的信息共享方式，双向交互，全方位满足跨域数据交换需求，数据交换防抵赖可审计，能及时有效地确认问题与明确责任，满足等保有关数据访问细腻度的要求。

（4）引领跨域数据交换类产品的技术革新

系统六大组件形成一个有机组合的平台，解决跨部门之间的数据共享、服务访问以及安全问题。

（5）顺应行业发展趋势，促进公司持续发展

政府互联网+政务战略下，政务大数据在安全与开放方面难以平衡。跨域数据交换认证机制不完善，非法对象可能与内部系统进行数据交换导致数据泄露；端到端数据机密性和完整性缺乏防护措施，传输过程存在非法截获及监听的威胁；数据交换记录缺乏审计，可能导致双方数据不一致时无法追溯，责任无法明确；数据交换缺乏权限控制及有效的病毒检测措施，数据结构和内容有暴露风险，传输数据或文件可能含有恶意代码。

大数据安全监控与交换平台将为各级政府部门建设一个集信息共享、安全防护和安全管理为一体的对外数据交换与信息共享安全平台，从而规范跨域数据交换和信息共享方式，保障跨域数据交换和信息共享安全可控，着力响应国家推动信息共享和整合要求。因此，通过项目的实施，顺应信息安全行业发展的趋势，将提升公司未来在市场上的竞争力，为公司未来发展打下坚实基础。

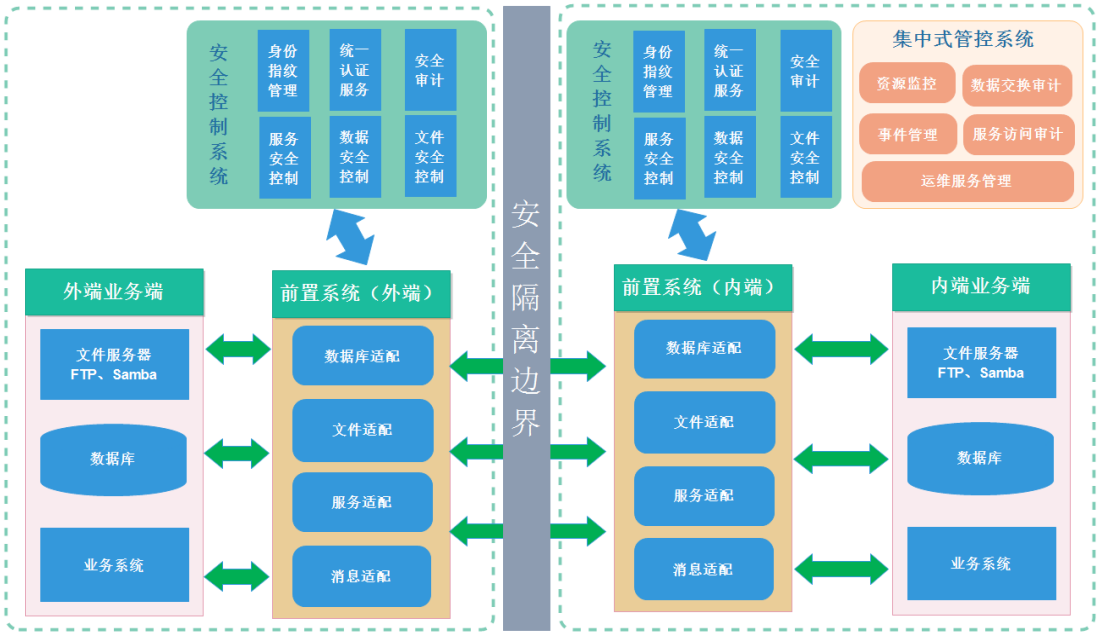
（6）有效整合公司资源，提高公司业务运营效率

大数据安全监控与交换平台是在蓝盾原有网闸、防火墙、入侵检测、防毒墙等边界安全类产品基础上，通过扩展前置系统，打造服务总线、数据总线，形成

整体跨域数据安全交换平台及边界安全防护整体解决方案。因此，通过此项目的实施，形成跨安全域数据安全共享平台及整体区域边界安全防护解决方案，将能有效整合公司的人力、财力及物力资源，集中资源进行技术研发和市场推广，减少因开发、推广各种单功能产品而形成资源分散所造成的不利影响，提高公司业务运营的效率和资源利用的效率，有利于公司未来发展。

5、项目建设方案

本项目由前置模块（外端）、前置模块（内端）、安全控制模块、集中式管控模块组成，总体逻辑框架如下图：



系统六大组件形成一个有机组合的平台，解决跨部门之间的数据共享、服务访问以及安全问题。

（1）前置模块（外端）：主要实现外端数据数据采集、文件采集、服务请求接收、消息接收等处理，并与安全控制模块结合，审计数据和服务情况。

（2）前置模块（内端）：主要实现内端数据数据采集、文件采集、服务请求接收、消息接收等处理，并与安全控制模块结合，审计数据和服务情况。

（3）安全交换模块（外端）：实现外端身份、认证的统一管理，并对数据交换、服务访问、文件交换过程进行安全审计。

（4）安全交换模块（内端）：实现内端身份、认证的统一管理，并对数据交换、服务访问、文件交换过程进行安全审计。

（5）集中式管控系统：对平台各个组件进行运维、监控、设计、管理等。

（6）安全隔离边界：实现部门之间的边界安全隔离，可以通过网闸、光闸、防火墙等机制实现。

6、项目实施主体

本项目由蓝盾股份的子公司蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年销售收入	万元	9,517.51
2	年均净利润	万元	2,258.83
3	财务内部收益率	%	27.94
4	财务净现值（ic=10%）	万元	8,075.89
5	投资回收期	年	2.95

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007245。

（六）安全云虚拟终端系统

1、项目概况

云桌面是云计算下的一种新型应用，可以替代传统的 PC 办公，进入云办公模式。云安全和移动安全涉及两大安全领域，因复杂性和技术深度，目前市面上绝大多数云桌面产品都无法满足等保 2.0 的相关要求。为顺应国家推行《网络安全法》和等保进入 2.0 时代的趋势，公司结合多年积累的网络安全经验，致力于

开发安全云虚拟终端系统产品。公司安全云虚拟终端系统的研发对推动国内安全管理和云办公桌面具有重要的作用。

项目建设目标是简化企业 IT 维护，提高运维效率，并根据信息化安全保密需求，对企业业务和数据安全加固，加强数据非法外泄行为管控，为企业建设业务安全性、办公高效性的办公环境，降低企业 TCO 成本。公司安全云虚拟终端系统为企业带来的价值体现在：

（1）规范员工行为，防止数据泄露，所有数据都在云平台，员工本地没有任何数据，设置后，无法拷贝、刻盘等；

（2）绿色办公，节能环保，普通电脑一般都在 200 瓦左右，而云终端功耗在 10 瓦，可以大幅节能，节省电费；

（3）便捷办公，只要能上网，就可以通过云终端、PC、智能手机、PAD 等连接到云桌面上进行办公，尤其适合出差工作者；

（4）统一管理和监控：应用程序和数据等的升级、变更、维护工作交由后台统一管理和运行，不需终端用户处理，大大减少终端的运维力度；

（5）用户分权分域集中管控：提供一体化的安全准入控制，依据相应的权限策略实现对不同安全域、不同类型用户集中管控；

（6）统一快速部署和维护：终端配置一致性，而且免安装各种环境和程序，一领即用；设备硬件结构简单要求不高，使用寿命长，易维护。

2、项目投资计划

本项目估算新增总投资 17,308.00 万元，其中新增设备购置费 3,335.26 万元、新增软件购置费 2,164.74 万元、开发技术人员人工费 5,256.00 万元，铺底流动资金 3,860.00 万元，分别占总体新增投资额的 19.27%、12.51%、30.37%和 22.30%。本项目拟使用募集资金 7,900.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	3,335.26	19.27%	3,335.26

二	软件购置费	2,164.74	12.51%	2,164.74
三	开发人员人工费	5,256.00	30.37%	2,050.00
四	运营技术服务团队	733.00	4.24%	51.00
五	市场开拓费	1,660.00	9.59%	-
六	试验检验费	299.00	1.73%	299.00
七	铺底流动资金	3,860.00	22.30%	-
合计		**17,308.00**	**100.00%**	**7,900.00**

3、项目的实施背景

云桌面是云计算的一种服务模式，是将底层物理设备与上层操作系统、软件分离的一种去耦合技术，它通过虚拟监控器（Hypervisor）构建虚拟层并对其进行管理，把物理资源映射成逻辑的虚拟资源，对逻辑资源的使用与物理资源的使用几乎没有区别。

安全云虚拟终端系统则从云桌面架构和各个组件入手部署安全机制、实施访问控制，为云桌面环境提供全面安全防护。

本项目产品是结合安全操作系统、安全加固 Hypervisior、高可用集群、密码技术和身份认证的全国产化云桌面产品，是云计算时代国家战略发展布局基础软件的重要产品。

随着 2017 年 6 月 1 日《网络安全法》正式实施，网络安全等级保护也进入 2.0 时代。等保 2.0 将目前整个信息领域的五大区域：云计算、物联网、移动互联网、大数据、工业控制系统的相关安全全部纳入等保制度，在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理等八类技术和管理方面上提出了详细的要求。需要特别指出的是，《网络安全法》中指出网络运营者不履行相关网络安全保管业务的，会根据后果的严重情况，处以不同的罚款。

4、项目实施的必要性

（1）满足企业规范员工行为和信息安全管理的需求

近年来，为了提高工作效率，降低娱乐、炒股等软件频繁使用挤占正常工作时间，降低工作效率的不利影响，企业通过安装网络监测软件，禁止网络端口等手段，来规范员工工作时间在工作电脑上的不规范行为。而工作电脑使用过程中的软件突然崩溃，可能导致数据损坏丢失；员工离职拷走属于公司的成果资料后删掉源文件等都会对公司造成数据丢失的威胁。因此，公司如何规范员工行为、保证公司资料信息安全成为日益现实的问题。

安全云虚拟终端系统通过部署安全云虚拟终端系统，每个员工办公桌面的软件都由管理员安装在服务器里每个虚机里，员工没有权限再安装其他软件，可以有效规范员工行为，提升工作效果。即便用户在桌面系统中保存了数据，该数据也仍然是在企业数据中心，而没有在用户的终端设备上保存任何副本。通过数据隔离措施，企业能够有效的保证数据不被违规带出企业，保障了数据安全。

（2）加快云桌面发展，满足用户随时随地便捷办公需求

在外出未携带公司办公电脑而又紧急事项需要处理时，因各种原因不便出门等原因需要远程办公时，用户可以通过云桌面满足云办公需求。安全云虚拟终端系统支持胖瘦终端、windows 客户端、web、ios、android、一体机等等，只要手机安装了安全云虚拟终端系统，就可通过 app，处理简单的文档工作，如果需要处理媒体文件如画图，处理音视频等，也可以通过浏览器直接登录个人云桌面，使用自己的工具、素材、各种资料，在熟悉的工作环境下，处理工作，满足用户随时随地便捷办公需求。

（3）加快推进云桌面应用，满足不同类别用户需求

由于价格较高，目前云桌面在中国市场的应用水平还比较低，且应用主要集中于政府、教育、国企、医疗、制造等行业大中型客户中，而在中小型网络组织中的应用水平基本处于空白，产品价格和功能扩展能力的限制也在一定程度上阻碍云桌面产品在市场上的应用和发展。

安全云虚拟终端系统将从产品设计和价格上打破这一应用“壁垒”。云桌面的底层架构云管理平台是公司自主研发的，通过云管理平台基础，公司实施该项目更能控制成本，实现底层技术和上层功能的完美结合，保证产品提供稳定的基础框架和基本功能模块，并能方便快捷实现定制扩展开发，实现功能与客户实际需求情况的最大程度的贴合。此外，通过合理的定价机制，安全云虚拟终端系统的性价比也将得到进一步提高，使产品在满足上述既有高端客户需求的基础上，也能以优异的性价比和随需应变的可扩展性满足众多中小型网络组织用户的需求，从而将有利于加快云桌面的推广和发展。

（4）实现大企业终端硬件采购与运维的简易管理

对于一般的文档处理，网页浏览等需求使用瘦终端即可应付，对于图形图片编辑处理，音视频编辑，程序开发等，可以使用胖终端，仅两种配置，有助于企业运维团队轻松完成硬件采购。

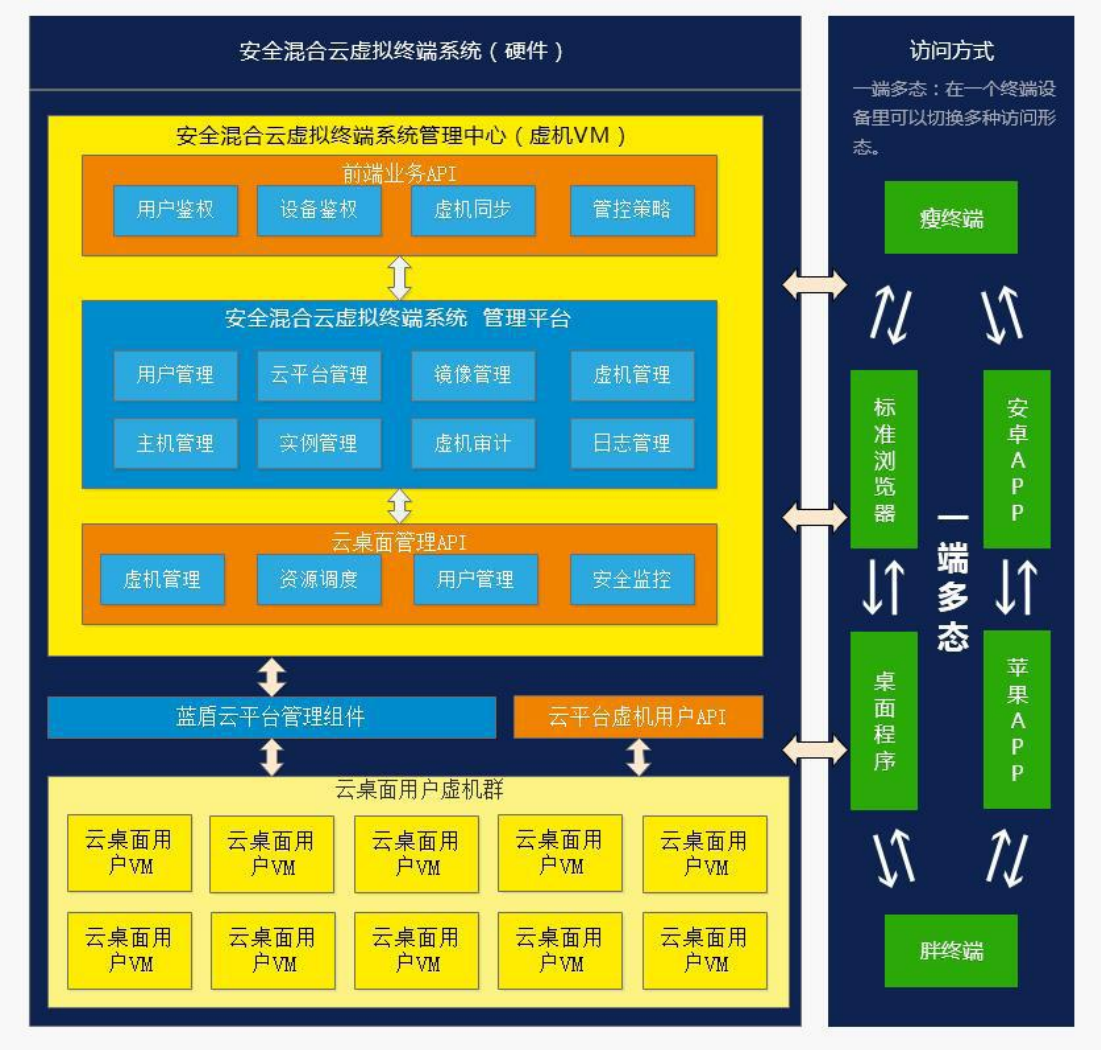
而在运维方面也实现了简易管理：第一、维护方便，所有程序和数据都在云平台，可以统一进行安装、杀毒、升级和备份数据；第二、快速部署，新员工报道，领取云终端，配上显示器、键盘、鼠标，插上网线就能办公，不用安装系统、安装程序、拷贝工作所需数据；第三、设备更换频率低，普通电脑淘汰更新快，而云终端因为结构简单，对 CPU、内存等又没有性能上的要求，使用寿命可达 8~10 年，运维工作大大减少。

5、项目建设方案

安全云虚拟终端系统使用蓝盾自主研发的蓝盾云平台产品作为底层技术支撑，产品形态为蓝盾硬件产品，包括服务器产品与胖瘦终端产品构成，胖瘦终端产品为可选部件。

安全云虚拟终端系统从现有《十三五国家信息化规划》和《促进大数据发展行动纲要》入手，结合等级保护 2.0 标准，融合云计算、大数据、流量采集、SIEM、机器学习算法、网站监测、数据泄露监测、数据安全管理、用户与实体行为分析、大数据可视化、ITIL 运维等技术，创新地提出安全云端系统体系架构。

系统架构如下：



蓝盾安全云虚拟终端系统建设内容如下：

序号	建设内容	内容描述
1	授权管理	提供云桌面的授权管理功能
2	用户管理	实现云桌面管理系统与云桌面终端的账号管理功能，支持三权分立
3	分组管理	实现云桌面用户与虚机配置的关联管理和配置功能
4	云桌面管理	实现云桌面的相关管理功能，包括桌面管理、镜像配置管理、主机配置、USB 管控、网络配置等模块
5	云平台配置	实现云桌面对接的云平台的相关参数配置功能
6	日志管理	实现对操作日志、登录日志的相关查阅功能
7	系统管理	提供对云桌面管理系统的相关功能配置，包括云桌面自身的网络配置、第三方登录（如 LDAP）验证配置等功能
8	资源监控	实现对云桌面系统的资源与配置监控功能，通过仪表板的方式提供直观的性能指标图
9	虚机安全防护	提供对云桌面虚机的相关安全防护功能

10	镜像支持 HTTP 和 P2P 双引擎下载	防止服务器带宽瓶颈，提高带宽利用率，加快部署速度
11	快照功能、快照同步备份功能	快速回滚，防止用户数据丢失，跨终端使用
12	软件黑白名单管控	对可执行文件进行黑白名单访问控制，避免病毒程序及违规程序的执行
13	USB 管控	对 USB 外设进行管控，可对 USB 设备实时监控，防止泄密与病毒入侵
14	终端网络安全准入控制机制	防止服务器和企业网络因存在不合规性终端而中病毒被攻击。主要功能：用户身份认证、终端完整性检查、终端安全隔离与修补、非法终端网络阻断、接入强制技术
15	一端多态访问	在一个终端设备里实现多种访问形态间的自由切换。减轻服务器访问负载，节省系统资源和提升整个系统的可伸缩性
16	可靠全面的网络安全组件	保障云环境下的多种安全需求。安全组件库包括：虚拟防火墙、虚拟 Web 应用防护、虚拟网页防篡改保护、虚拟数据库及业务应用安全监控审计、虚拟信息安全管理审计、虚拟安全扫描、虚拟安全综合运维管理、VPN 和虚拟内网保密

6、项目实施主体

本项目由蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年均销售收入	万元	6,713.06
2	年均净利润	万元	1,602.39
3	财务内部收益率	%	29.45
4	财务净现值（ic=10%）	万元	5,830.13
5	投资回收期	年	2.91

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007252。

（七）视频安全接入与威胁管控平台

1、项目概况

项目用于满足公共安全视频传输专网前端接入安全管控需求及疫情防控智能测温需求，在公司原有防火墙、入侵检测、防毒墙、VAC 等边界安全类产品基础上，结合公司热成像人体测温解决方案等技术，形成视频接入安全防护整体解决方案。

一方面建立视频前端安全防护机制，实现对前端接入资源的有效识别、攻击防御、病毒过滤、弱口令检测预警和一体化安全管理平台；另一方面，系统集成的热成像人体测温解决方案，通过部署于人流密集的公共场所，如机场、火车站、汽车站、轮渡、医院、学校、企业、门店等的测温红外摄像机等设备，实现无接触感应、智能化测温、高温预警，可以突发疫情的应急响应需求，解决传统测温需要人员近距离接触的问题，实现快速精准筛查和告警，避免交叉感染，高效率通行，成为防控疫情的“智能哨兵”。

公司热成像人体测温解决方案，使用测温设备、双目红外摄像头为基础结合后端管理平台为核心，以红外热图及高清图像处理、精确测温等核心技术，实现指定区域人员识别、精测及基于人体发热病理的筛查、报警，对应的技术已经应用到蓝盾疫情应急响应系统，可以助力人流密集各场景的疫情监控及响应机制的可靠执行。

2、项目投资计划

本项目估算新增总投资 22,175.50 万元，其中新增设备购置费 5,475.28 万元、新增软件购置费 1,824.72 万元、开发技术人员人工费 5,843.00 万元，铺底流动资金 5,300.00 万元，分别占总体新增投资额的 24.69%、8.23%、26.35%和 23.90%。本项目拟使用募集资金 10,100.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	5,475.28	24.69%	5,475.28
二	软件购置费	1,824.72	8.23%	1,824.72

三	开发人员人工费	5,843.00	26.35%	2,300.00
四	运营技术服务团队	1,033.00	4.66%	91.50
五	市场开拓费	2,291.00	10.33%	
六	试验检验费	408.50	1.84%	408.50
七	铺底流动资金	5,300.00	23.90%	
合计		**22,175.50**	**100.00%**	**10,100.00**

3、项目的实施背景

近年来，视频监控被广泛应用于平安城市、天网工程、雪亮工程、社会治安、交通出行、环境保护、城市管理等多个领域。据统计，截至 2017 年 9 月全国安装的公共安全视频监控摄像机数量已达到 3,000 万台，初步覆盖了公共区域、重点单位和要害部位，视频监控已成为提升平安中国建设能力和水平的基础性工程。

由于视频监控业务的广泛应用，联网规模的不断扩大，智能应用的不断拓展，视频监控图像信息资源已成为国家重要的基础信息资源。视频监控已成为安全管控的重要窗口和手段，特别是疫情期间，通过视频监控协助体温筛检排查成为公共区域疫情监测的主要防控手段之一。

随着国内外网络安全形式的变化，视频专网面临各种安全威胁，视频专网上存有大量敏感信息，这些敏感信息泄漏、或视频监控失效等可能对社会治安、经济发展甚至国家安全产生严重危害。而利用视频管控协助智能筛查疑似病患，特别是在大规模返程高峰及复工来临，人流巨大、人员密集区域，筛查效率的提高则直接关系到疫病的控制和公众的安全。

目前视频专网在建设中缺乏整体信息安全体系规划，存在前端设备非法接入、非法访问、病毒传播、安全管理缺失等问题。给视频监控传输网络带来很大的安全风险。公共安全视频专网建设规模大、周期长，涉及的施工和维护人员众多，而且缺乏有效的技术手段规范 IPC 摄像头和计算机接入视频网的流程，所以很难避免非授权的 IPC 摄像头和计算机被接入视频网。一旦非授权 IPC 被当作正常的摄像头被接入视频网，很可能会隐藏后门、病毒等潜在危险，一旦发作后果不堪设想。摄像机前端设备部署分布极为广泛，大多处于道路、街区等极易被

恶意侵入的公共场所等无人看守区，安全隐患较大。在公共安全视频专网网络边界，视频专网与其他专网、视频专网与互联网网络边界，缺乏安全技术规范指导和防护措施。

因此，一方面，如何保证前端设备安全，防止不法分子利用入侵、控制前端设备，防止不法分子通过前端设备入侵核心业务网络是视频专网发展环境下亟待解决的问题。另一方面，如何使得视频监控更好用于保障公共安全，通过嵌入智能测温等利于疫病防控的智能解决方案，也成为视频监控保障公众安全的重要尝试。

在视频网逐步发展的趋势下，安全准入控制系统及视频监控安全解决方案的应用将在网络安全防御体系中扮演越来越重要的角色。

4、项目实施的必要性

（1）提高信息安全产业创新力，增强核心竞争优势

随着物联网蓬勃发展，越来越多设备通过网络互连，IDC 预测，到 2025 年，全球物联网设备数将达到 416 亿台。这些前端设备大多处在无人值守的环境中，且大多数设备存在弱口令，远程端口开放等安全隐患。

如何保证前端设备安全，防止不法分子利用入侵、控制前端设备，防止不法分子通过前端设备入侵核心业务网络是物联网发展环境下亟待解决的问题。在物联网逐步发展的趋势下，安全准入控制系统将在网络安全防御体系中扮演越来越重要的角色。

项目的实施对于提升信息安全产业的创新能力，增强产业核心竞争力都具有重要的推动作用。

（2）提高视频网络接入安全管控能力，推动信息化建设步伐

近年来，视频监控被广泛应用于平安城市、天网工程、雪亮工程、社会治安、交通出行、环境保护、城市管理等多个领域。据统计，截至 2017 年 9 月全国安装的公共安全视频监控摄像机数量已达到 3,000 万台，初步覆盖了公共区域、重

点单位和要害部位，视频监控已成为提升平安中国建设能力和水平的基础性工程。

在公共安全视频专网运行着大量的前端摄像头、其服务器与办公终端之间没有采取任何隔离和控制手段，这就使得视频专网重要服务器存在很大的病毒木马传播风险。前端网络摄像机（IPC）接入地理位置十分分散、人为监管困难等，导致现在公共安全视频专网在运行时在网络摄像机等设备的安全接入控制方面存在入侵和非法数据的访问的安全风险。

公司视频网络接入安全管理平台将用于保证前端设备安全，防止不法分子利用入侵、控制前端设备，防止不法分子通过前端设备入侵核心业务网络，为国家推动平安城市、雪亮工程、天网工程保驾护航，为社会治安、交通出行、环境保护、城市管理等多个领域提供安全保障。

（3）满足公共安全视频云建设前端接入安全防护要求

随着视频监控设备应用越来越广泛，在视频监控保障社会公共安全的同时，自身安全也越来越被重视，但频频曝出视频监控设备被攻破，监控内容被窃取，视频监控设备监控安全已成为人们关注的焦点。

项目通过技术手段将公共安全区域视频摄像机进行可控管理，只允许授信终端接入才能进入公共安全视频专网，保证网络前端边界安全可控。同时防范非法私接，做到设备可知、入网可信、边界可控。功能上进行安全加固与信息安全监管，防止伪造终端接入、木马注入、病毒注入、DDOS 攻击等风险。能够满足公共安全视频云建设前端接入安全防护要求。

（4）引领视频网络接入安全类产品的技术革新

项目满足视频传输专网前端接入安全管控需求，能够准确识别前端接入设备的 IP 地址、MAC 地址、生产厂商、操作系统等信息，对新出现的前端设备类型进行识别和管理。对于前端设备的各种变更能够及时发现，并对设备进行精准识别，对于非法接入设备能及时识别并上报告警，同时能够主动阻断非法设备的接入。项目综合使用端口识别、关联识别等技术，抽丝剥茧逐步解析流经设备的网络数据，精准识别应用，可直接阻断非视频应用的网络流量，保证专网专用。进

行数据流的检测，标记外发流量，检测同一会话的后续流量，若发现异常则可阻断异常外发流量，防止核心数据外泄。

根据重点区域和一般区域的不同安全防护需求，采用不同的安全防护方案，可以支持分布式或集中式部署策略，对于一般区域可以选择旁路方式或主路方式进行集中式部署，对于重点区域采用分布式部署，分局区县局将前端设备非法入侵、非法接入日志上传市局安全管理平台，安全管理平台实时展示网络现状与安全态势，帮助用户了解网络风险点，从管理层面进一步提升公共安全视频专网健壮性。

（5）顺应行业发展趋势，促进公司持续发展

视频监控是智慧城市管理体系的关键组成环节。视频监控被广泛应用于平安城市、天网工程、雪亮工程、社会治安、交通出行、环境保护、城市管理等多个领域。据统计，截至 2017 年 9 月全国安装的公共安全视频监控摄像机数量已达到 3,000 万台，初步覆盖了公共区域、重点单位和要害部位，视频监控已成为提升平安中国建设能力和水平的基础性工程。

保证前端设备安全，防止不法分子利用入侵、控制前端设备，防止不法分子通过前端设备入侵核心业务网络是视频网发展环境下亟待解决的问题。在视频网逐步发展的趋势下，安全准入控制系统将在网络安全防御体系中扮演越来越重要的角色。

项目的实施顺应了公共视频安全行业发展的趋势，将提升公司未来在市场上的竞争力，为公司未来发展打下坚实基础。

（6）有效整合公司资源，提高公司业务运营效率

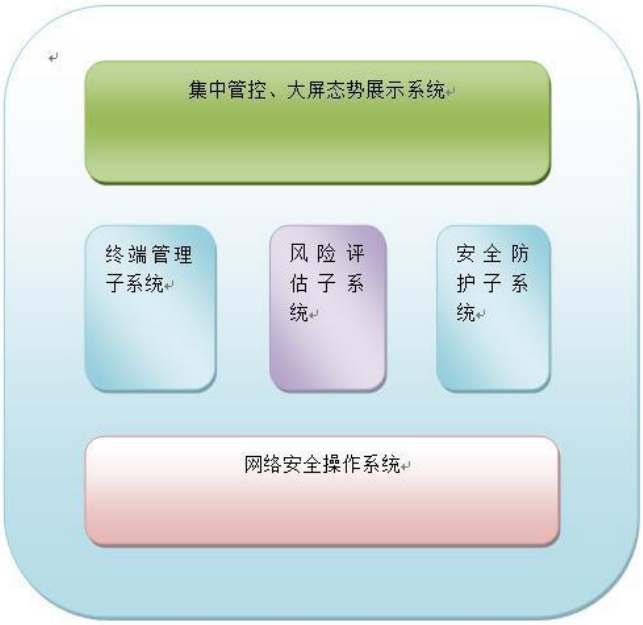
视频网络接入管理平台是在公司原有防火墙、入侵检测、防毒墙、VAC 等边界安全类产品基础上，形成整体视频接入安全防护整体解决方案。因此，通过此项目的实施，将能有效整合公司的人力、财力及物力资源，集中资源进行技术研发和市场推广，减少因开发、推广各种单功能产品而形成资源分散所造成的不利影响，提高公司业务运营的效率和资源利用的效率，有利于公司未来发展。

（7）满足人流密集公共场所的疫病防控需求

系统集成的热成像人体测温解决方案，可部署于人流密集的公共场所，如机场、火车站、汽车站、轮渡、医院、学校、企业、门店等，实现无接触感应、智能化测温、高温实施预警，解决传统测温需要人员近距离接触的问题，实现快速精准筛查和告警，避免交叉感染，高效率通行，成为防控疫情的“智能哨兵”，能够满足人流密集公共场所智能测温的疫病防控需求。

5、项目建设方案

视频安全接入与威胁管控平台由终端管理、安全风险评估、安全防护、集中式管控模块组成，总体逻辑框架如下图：



终端管理系统：主要实现终端识别、终端准入、终端私接/仿冒、终端阻断、终端在线/离线管理等功能。

风险评估系统：主要实现终端风险识别，包括漏洞及弱密码等。

安全防护系统：主要实现防止木马注入、病毒注入、DDOS 攻击、信息泄漏等风险，对从前端发起的各种攻击行为进行探测，检测到攻击后可立即阻断攻击行为并告警。

网络安全操作系统：主要提供网络安全产品的底层网络功能与操作系统功能，比如收发包、包转发、包过滤、流量控制等功能。

集中式管控系统：对平台各个组件进行运维、监控、设计、管理等，管理平台实时展示公共场所及网络现状与安全态势，帮助用户了解风险点，一方面提升视频专网安全性和健壮性，另一方面，与双目红外摄像头结合，满足疫情应急响应需求，通过安全事件大屏展示协助温度预警，提升公共场所体温筛检效率。

视频安全接入与威胁管控平台主要建设内容如下：

系统	模块	开发功能描述
网络安全操作系统	基础网络适应性	桥接、路由、NAT、虚拟线、旁路等网络部署模式 IPV6 地址/地址组配置，基于 IPV6 地址/地址组配置防火墙安全策略、设备准入策略、应用过滤策略、流量控制策略 IPV6GRE 隧道技术，IPv6over、IPv46to4、IPv6overIPv4ISATAP 技术；NAT64、DNS64 翻译技术 IPV6 包过滤、策略路由、静态路由、HTTP 应用协议、自动获取 IPV6 地址 多出口负载均衡，支持轮流、加权最少、权重轮流、最少连接等算法，支持多运营商智能选路
终端管理系统	终端准入	基于 IPV4/IPV6 地址的准入控制 基于 MAC 地址的准入控制 基于 IP-MAC 绑定的准入控制 基于终端黑/白名单的准入控制,可配置 IP/IP 段黑名单 通过设备 IP、设备厂家、设备所在区域、具体位置、接入端口、设备说明等信息管理设备
	终端监控	监控设备在线状态、地理位置、接入端口、IP/MAC 地址，支持关键字模糊查询和高级查询 监控设备上/下线动作、上/下线时间，及其他相关信息，支持关键字模糊查询和高级查询；支持设备异常离线告警
	终端设备兼容性	全面兼容海康、大华、宇视、全睿、中威等品牌的终端设备
安全防护系统	异常流量检测	对外发异常流量进行检测，支持对异常流量配置报警/阻断策略，实现核心业务系统的双向防护
	防火墙	自定义安全策略，可基于 MAC 地址、IP 地址、端口、服务、应用、时间计划定义安全策略；能识别 2000+种应用 检测 IP 地址盗用，并拦截盗用 IP 地址的主机经过设备的各种访问 基于源 IP/目的 IP 配置并发连接数上限 对 ARPFLOOD 攻击、ICMPFLOOD 攻击、UDPFLOOD 攻击、SYNFLLOD 攻击、DNSFLOOD 攻击、TearDrop 攻击、

系统	模块	开发功能描述
		Smurf 攻击、LAND 攻击、WinNuk 攻击、ICMP 大包攻击进行防护 IP-MAC 绑定，可自动扫描内网设备的 IP-MAC 地址；支持管理员手动配置；支持从外部文件导入 IP-MAC 地址列表；支持配置例外 IP 和例外端口； 检测并阻断 HTTP、FTP、SMTP、IMAP、POP3、TELNET、DNS、RPC、FINGER、MYSQL、ORACLE、NNTP、DHCP、LDAP、VOIP、NETBIOS、TFTP、TCP、UDP、ECHO、NFS、SIP、SSH 等多种网络协议和应用的攻击入侵行为
	流量控制	支持基于 IP/IP 组、应用、时间计划的带宽控制策略 配置保障通道和限制通道；限制同一设备组内单 IP 上下行带宽 可分高、中、低三级通道优先级，动态调整带宽、利用空闲带宽 基于 IP 的流量统计，实时流量趋势监控，实时掌控流量信息
	应用过滤	基于 IP/IP 组、设备名称对 SIP、FTP、HTTP、RTSP、RTCP、RTP、LRTP、DRTP 等常用控制信令及传输协议进行识别和管控
安全风险评估系统	终端扫描	主动扫描发现终端的安全漏洞，并有针对视频终端的漏洞库，能够扫描出大华，海康威视等主流品牌的安全漏洞 支持视频终端设备的弱口令扫描
集中管理系统	系统管理	管理员角色三权分立，支持管理员用户名+密码/UKEY 双因子认证；支持按模块为管理员角色配置权限，支持配置管理员密码安全策略，密码更换时间、密码最小长度等详细要求 可配置 IPV4/IPV6 可信管理主机 支持 SNMP 协议；支持 NTP 协议 支持图形化系统调试工具；内置抓包工具 支持按系统备份历史记录回滚 支持对规则库手动升级，支持配置定时升级，支持自动升级； 支持操作系统冗余，具备双系统，可在页面上配置启动顺序，可将备份系统一键恢复到任一系统 支持基于 IP/IP 组配置用户认证策略，支持策略优先级配置 支持不需要认证、外部认证、本地认证、短信认证几种认证模式，外部认证支持 Radius 和 LDAP 服务器认证 支持为不同 IP/IP 组定制用户认证页面 支持配置向导，为用户提供常用功能配置指导；支持配置检查功能
	安全事件及大屏展示	支持本地存储日志、syslog 多发日志；支持覆盖、暂停、报警三种日志满响应方式；支持配置日志入库归档周期 支持系统登录日志、恢复与备份日志、重启关机日志、管理员操作日志、资源告警日志、防火墙日志、DDOS 攻击防护

系统	模块	开发功能描述
		日志、设备认证日志、异常流量检测日志、应用管控日志 支持用户自定义日志任务，支持分模块、基于时间、响应方式、协议、源地址/目的地址等维度导出 Excel 格式日志 支持配置日志审计平台或者第三方日志服务器，提供强大的日志管理和日志审计功能（存储、审计、报表） 支持导出流量统计报表，支持基于应用、协议等维度统计流量并排行 支持应用过滤统计，支持基于协议、IP 地址、时间范围的应用告警阻断次数统计并支持图形化、图表化多方式展示 支持设备上下线情况统计，支持基于时间范围、登录状态的设备安全情况统计并支持图形图表化多方式展示 支持非法接入统计，支持基于时间范围、IP 地址的非法接入阻断告警次数统计，并支持图形化、图表化多方式展示 支持异常流量统计，支持基于协议、IP 地址、时间范围的告警与阻断流量统计，支持单 IP 基于时间范围的异常流量统计信息钻取。支持图形化、图表化多方式展示 满足疫情应急响应需求，通过可见光视频图像与红外信息采集，支持温度 K 线关联图像，可根据 K 线查证事件图像，快速定位事件发生时的温度，快速追溯或复核事件形成原因； 支持温度预警策略，实时抓拍、报警、联动上传、弹窗、显示、信息推送，实现第三方设备联动控制等
	报警	支持对入侵事件、攻击事件等进行报警，并记录报警数据 支持对系统运行状态进行报警，如 CPU、内存、带宽超过阈值 支持邮件、短信、SNMPTrap、声音报警等报警方式 疫情应急响应中，支持任意检测区域的最低温、最高温、平均温度的报警阀值可设，高/低温报警模式均独立可设
高可用性	高可用性	支持主-主模式、主-备模式的双机热备 支持硬件 bypass，支持物理设备状态监测，即主设备出现断电或其他故障时，备设备能及时发现并接管主设备的工作； 支持软件 bypass,支持设备容量监测，即网络流量负载超出设备的流量时，则停止设备的安全检测功能，新的会话请求自动直通以保证网络的可用性 支持会话状态、配置同步 支持冗余心条线机制 支持 VRRP 协议和 STP 协议 支持链路状态检测的双机热备 支持基于集群工作模式的负载均衡功能，使多台设备能够协同工作均衡网络流量 支持电源冗余电源；支持电源热插拔；支持业务接口卡热插拔

6、项目实施主体

本项目由蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年均销售收入	万元	9,266.67
2	年均净利润	万元	2,217.10
3	财务内部收益率	%	31.20
4	财务净现值（ic=10%）	万元	8,199.62
5	投资回收期	年	2.81

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007254。

（八）网络空间仿真靶场实训竞技平台

1、项目概况

项目顺应国家推行《网络安全法》及对网络安全教育人才培养计划之趋势，公司结合多年积累的网络安全经验，推出致力于安全教育的产品。对于大行业客户而言，人员本身的安全技能和意识对企业的生产、运作和管理极为关键，《网络安全法》的颁布与实施，进一步促进了企业对内部员工的安全教育和培训。

建成具有统一的身份认证、数据访问、资源管理、考试管理、培训管理、实景模拟等多种功能兼具安全培训和实战竞赛的综合性信息安全教育与实战平台，可为大行业客户提供整体性的解决方案。通过在线信息安全培训平台提供体系性的安全知识培训和实训，并且经历实战技能的检验，最后通过理论考试、数据分析、实战评估等机制，对人员形成综合性的评估，可为企业人员安全技能提供有力的帮助。

2、项目投资计划

本项目估算新增总投资 22,742.00 万元，其中新增设备购置费 5,788.35 万元、新增软件购置费 3,011.65 万元、开发技术人员人工费 4,544.00 万元，铺底流动资金 5,590.00 万元，分别占总体新增投资额的 25.45%、13.24%、19.98%和 24.58%。本项目拟使用募集资金 11,300.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	5,788.35	25.45%	5,788.35
二	软件购置费	3,011.65	13.24%	3,011.65
三	开发人员人工费	4,544.00	19.98%	1,912.50
四	运营技术服务团队	1,016.00	4.47%	76.50
五	市场开拓费	2,281.00	10.03%	-
六	试验检验费	511.00	2.25%	511.00
七	铺底流动资金	5,590.00	24.58%	-
合计		**22,742.00**	**100.00%**	**11,300.00**

3、项目的实施背景

2017 年 6 月，《网络安全法》正式实施，进一步界定关键信息基础设施范围；对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施；增加惩治网络诈骗等新型网络违法犯罪活动的规定等。这意味着，国家对重点行业的信息安全问题将提升至国家安全层面，行业也亟需解决内部员工的信息安全素质及教育问题。

对于行业从业人员，需要持之以恒地进行信息安全继续教育，并以内部培训绩效评估作为激励考核。行业从业人员对安全教育有其特殊性需求，例如信息安全意识培训将适用于企业的大多数人员，并应当作为教育的重点。对技术类人员，应当在常规安全技术教育的基础上，增加漏洞原理以及贴近行业生产环境的信息安全教育内容，以提升安全技能应用的针对性以及专业性。

网络空间仿真靶场实训竞技平台，是基于公司首创的软件定义安全实训（SDSE）全新理念设计的新一代信息安全教育实训平台，定位于实景靶场模拟

应用、信息安全教育、培训以及实训，是蓝盾信息安全教育生态圈的重要平台产品之一。

网络靶场与攻防实训作为新一代信息安全人才培养类产品，系统集“学、练、测、评”一体化设计，提供安全基础、安全实战、科研开发、创新创业、网络安全竞赛、大屏展示等各类精品课程和海量练习资源，平台基于公司特有的云管理中心，通过大数据精准分析，形成完整的人才能力评价体系，将成为信息安全行业人才培养的重要系统。

4、项目实施的必要性

（1）满足信息安全教育人员培养的需求

随着信息安全行业的发展，企业对安全人才具备的技术和管理能力提出了更高要求，从信息安全人才的需求及培养角度可以看出，如何快速、高效地培养具备丰富实操经验和技能的实用型人才，是安全教育与实战方案的重要目标。

对于行业从业人员，需要持之以恒地进行信息安全继续教育，并以内部培训绩效评估作为激励考核。行业从业人员对安全教育有其特殊性需求，例如信息安全意识培训将适用于企业的大多数人员，并应当作为教育的重点。对技术类人员，应当在常规安全技术教育的基础上，增加漏洞原理以及贴近行业生产环境的信息安全教育内容，以提升安全技能应用的针对性以及专业性。

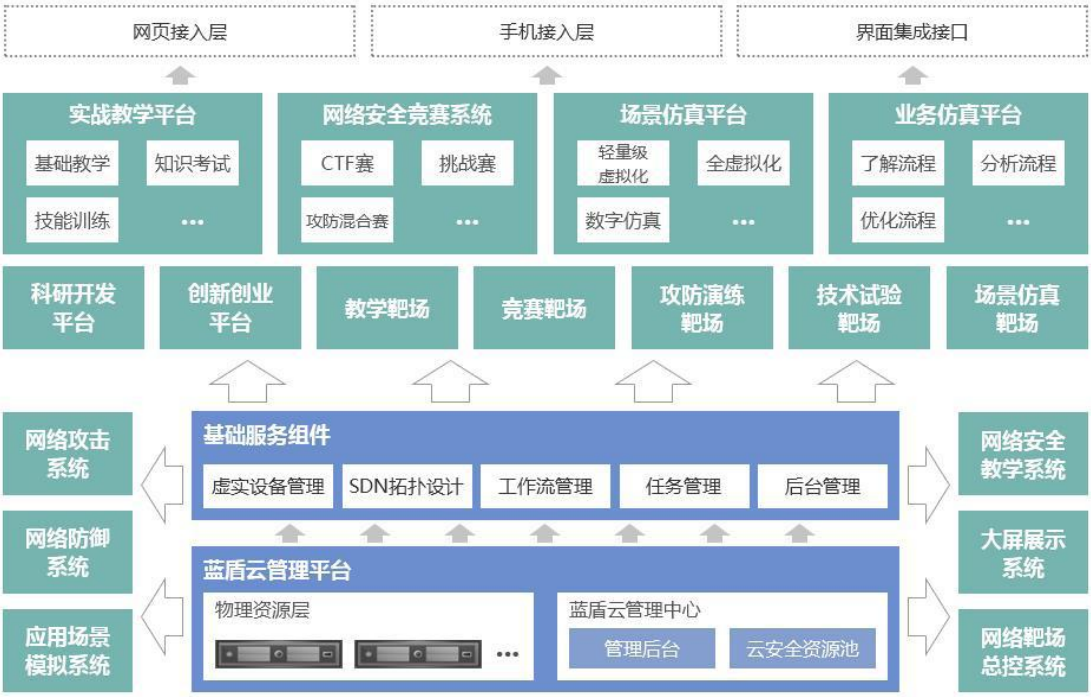
（2）满足新形势下的教育改革需求

我国信息安全高等教育课程改革也为从事教育行业的企业带来了新的机遇和挑战。面对新的学科内容和教学标准，我们需要重新审视安全教育和实战类产品及方案，以适应市场和教育的需要。对于培养实用型技能人才而言，需要在国内信息安全企业建设信息安全实训基地，开展网络空间安全实战技能培养和实习实训，由企业与高校共同制定学生实习实训方案，主动接收学生开展实习实训，以培养实战技能。

5、项目建设方案

从逻辑架构来讲，平台分为基础设施层、基础服务组件层、业务功能层以及接入层等主要逻辑设计。所有的安全课程和靶场实战资源，均通过基础服务组件中的虚拟化服务，以虚拟化的形式进行管理和操作。

网络空间仿真靶场实训竞技平台系统架构总体如下：



网络空间仿真靶场实训竞技平台主要建设内容如下：

序号	建设内容	内容描述
1	实战教学平台	提供多至 9 个技术方向 20 多个分类的课程，分初中高级难度来迎合每个基础知识不同的学员的不同要求，每个课程包括多个章节，章节分类有理论、视频和实验三类，真正的实现多角度学习，学习简单易懂，知识覆盖面广。 实战教学平台内置考试中心，考试分两种形式，一种是统一考试的形式，另一种是支持自由考试的形式。学员通过统一的界面进行作答。考试中心提供试卷管理、题目管理、成绩管理等功能，供后台人员管理使用。
2	场景仿真平台	主要使用虚拟机软件 VMware+Wireshark（网络分析工具），实现计算机网络安全的攻击和防御过程的场景仿真以及进一步的分析。将虚拟化技术和数字仿真技术结无缝融合，使用一种基于云平台的轻量级虚拟化、全虚拟化与数字仿真三种尺度融合网络复现技术，实现全虚拟化、轻量级虚拟化与数字仿真融合仿真系统

序号	建设内容	内容描述
		的交互通信，以及仿真网络的灵活接入与规模扩展。
3	业务仿真平台	借助公司云平台，业务仿真平台通过虚机架构设计模型、时间设置和参数制定，再现整个业务流程生产环境和运作条件。通过动态观察业务运行情况和综合分析模型输出参数报表，学员能够获得直观、可靠和详细的辅助信息。
4	科研开发平台	建设成为网络安全科研开发与学术交流的平台，研究方向主要有密码学研究、网络安全研究、系统安全研究、内容安全研究、信息对称研究、网络空间安全研究等。 支撑学员对源码开发和应用的实训教学，通过内置的源码开发的实际案例，同时通过虚拟化技术内置安全研发实训环境，让学员掌握理论方面开发知识后，可以根据系统内置经典案例，直接进入实操环节，通过理论和实际动手相结合的方法，快速掌握开发方面知识技能。
5	创新创业平台	搭建创新创业平台，为创业团队提供创业活动、学员互动交流、创业培训指导等服务，为创业项目提供一条龙服务。通过系统为学生提供实习推荐、就业推荐、政策宣传、校企交流、人才输送等各项服务。实现就业信息发布管理、就业培训服务管理、就业服务管理，为青年提供多方位的就业服务。
6	教学靶场	模拟真实的业务环境进行攻防实战，选手或学员在具有某些业务特征的靶场环境内，对靶场的关键设施进行攻防渗透，例如针对 Web 应用系统进行攻防，靶场环境可以包括 Web 应用系统、WAF 防御系统、路由交换设备、数据库等关键设施，需要选手在高仿真度的环境内进行安全训练。
7	竞赛靶场	提供超过 200 题 CTF 高质量题目，供学员进行练习。考察参赛人员理论知识和专项攻防技术的掌握程度，参赛人员通过解决网络安全技术挑战题目而得分，以分值和时间来排名。
8	攻防演练靶场	支持多组互相攻击，每个小组都可分配 3-5 成员，小组里分别有 2 个渗透人员，2 名防护人员，1 名指挥人员，在攻击其它小组靶场同时，也要对本组靶场进行实时防护，通过攻防演练提升技能。
9	技术试验靶场	专门针对最新的网络威胁进行特征研究，并进行相关的技术验证，从而对网络安全市场的各厂家最新产品进行综合评估。技术试验靶场提出透析式的“一个中心、两个基本点”的 APT 高级持续性威胁解决试验仿真解决情景。以“全流量解析还原”为中心，实现流量自学习分析和威胁情报共享，以“AI 防病毒引擎检测”、“动静态复合检测”两个基本点进行专业式防护，实现全文追溯，让使用者从展示层开始一步步钻取到核心取证模块，还原 APT 威胁的所有攻击场景。
10	场景仿真靶场	提供各种仿真场景的实操应用，包括内网、互联网、校园网、工控网络等，实现学以致用。场景仿真靶场的管理后台，实现对前台所有仿真任务进行管理，提供任务管理、成绩统计、实践监控三大功能模块。

序号	建设内容	内容描述
11	网络攻击系统	攻击原理是：攻坚者利用大量的数据包“淹没”目标主机，耗尽可用资源乃至系统崩溃，而无法对合法用户作出相应。
12	网络防御系统	可以对缓冲区溢出、SQL 注入、暴力猜测、DOS/DDOS 攻击、扫描探测、蠕虫病毒、木马后门、间谍软件等各类黑客攻击和恶意流量进行实时阻断及报警。通过规则关联分析发现潜在安全威胁，根据预先定义响应方式进行定制响应与定制拦截。
13	应用场景模拟系统	能够快速搭建高度模拟真实网络环境的场景，发起并且追踪和记录信息安全事件发生的完整过程，支持攻击数据的采集，攻击路径的绘制、攻击操作的回放以及整个攻击过程的全程可视化演示。
14	网络安全教学系统	是一个可交互的线上教学系统，在功能设计上充分考虑教学对象、学习环境，体现出面向工作过程、工作任务、工作岗位的教育特点。主要包括学员信息管理、课程管理、教学中心、教学管理等功能。
15	网络安全竞赛系统	提供竞赛的模拟演练功能，学员可以在平台上进行比赛练习或赛前练兵，也可以基于本平台进行比赛的强化培训。提供观战的大屏展示功能，实时显示比赛的得分、排名、时间等对抗信息，对抗演练过程了如指掌。
16	大屏展示系统	采用动态实时的网络安全分析与可视化技术，对存在的主要安全威胁和攻击事件进行检测，利用大数据分析方法对各种安全信息进行深层次关联融合，以攻防的视角，从整体安全态势、DDOS 攻击态势、僵木蠕毒攻击态势、网站安全态势、0days 漏洞态势、APT 威胁安全态势、资产安全态势、数据泄露安全态势、账号安全态势、流量态势、业务应用态势、脆弱性利用态势、内外网连接态势等维度进行立体化深入分析及可视化展示，从而实现对大型系统网络安全状况动态实时分析，也为大型信息系统安全运维管理提供整体安全视图，并对安全状况发展趋势进行预测。
17	网络靶场总控系统	对整个靶场平台进行统一管理调度，采用 B/S 架构模式，无需安装客户端，升级维护灵活方便。其一方面通过 API 接口访问 OpenStack 云计算资源，另一方面负责对靶场场景进行镜像管理和参数配置，并提供实时监控、分析统计、可视化展示、系统管理等功能。

6、项目实施主体

本项目由蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

本项目建设期为 1.5 年，本项目正式进入运营期后，经测算，预计可实现年均净利润不低于 2,227.31 万元，经济效益良好。

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年均销售收入	万元	9,376.67
2	年均净利润	万元	2,227.31
3	财务内部收益率	%	28.71
4	财务净现值（ic=10%）	万元	7,974.30
5	投资回收期	年	2.96

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007258。

（九）新一代智慧城市安全运营平台

1、项目概况

新一代智慧城市安全运营平台采用云计算、AI、5G、大数据、物联网等新兴技术，以“人、技术、制度流程”为核心，从法律、制度、标准、技术等方面构筑智慧城市信息安全保障体系。通过对智慧城市关键基础设施全面的安全监测、预警、分析及快速处理，做到安全问题可管理、可控制、可度量、可治理、可预防，真正解决智慧城市工程网络安全、系统安全、数据安全和综合安全全方位的信息安全问题。并初步构建市、区两级互联互通、信息共享的标准规范、技术接口及建设指南，为后期市级平台建设及市、区两级系统对接打下基础。平台的建设目标包含五个方面：构建信息安全组织保障体系、构建信息安全技术保障体系、构建信息安全制度保障体系、构建信息安全管理保障体系、构建信息安全灾难恢复体系、构建信息安全风险测评评估机制。

2、项目投资计划

本项目估算新增总投资 56,318.00 万元，其中新增设备购置费 16,000.00 万元、新增软件购置费 6,000.00 万元、开发技术人员人工费 13,904.00 万元，铺底流动资金 11,200.00 万元，分别占总体新增投资额的 28.41%、10.65%、24.69%和 19.89%。本项目拟使用募集资金 30,000.00 万元。新增研发投资构成如下表所示：

单位：万元

序号	工程或费用名称	投资金额	所占比例	拟以募集资金投资金额
一	设备购置费	16,000.00	28.41%	16,000.00
二	软件购置费	6,000.00	10.65%	6,000.00
三	开发人员人工费	13,904.00	24.69%	6,000.00
四	运营技术服务团队	2,243.00	3.98%	210.00
五	市场开拓费	5,181.00	9.20%	-
六	试验检验费	1,790.00	3.18%	1,790.00
七	铺底流动资金	11,200.00	19.89%	-
合计		**56,318.00**	**100.00%**	**30,000.00**

3、项目的实施背景

智慧城市已经进入了高速发展期，由于智慧城市复杂、开放、互联的特点，同时智慧城市区别与传统信息系统的服务方式、网络架构、数据资源等技术因素，加之受制于智慧城市主体建设的连带效应，导致了智慧城市在信息安全上面临种种困难和挑战。如何评价智慧城市的安全管控能力，如何识别智慧城市从顶层设计到技术实现再到最终应用中的各类风险，如何准确把握智慧城市信息安全趋势和动向成为亟待解决的问题。

4、项目实施的必要性

（1）满足智慧城市发展对全局化智能化产品的需求

随着信息安全威胁的多样性和隐蔽性不断增强，原有的以防火墙、IDS/IPS、VPN、防病毒等单功能产品各自为战的安全解决方案已经很难满足用户对高效信息安全维护的需求。因为基于攻击多样化和融合的特点，原来各自为战的安全产品总是处于疲于应付的状态，无法很好的实现对智慧城市网络安全的保护，智慧城市的运营中涉及的防病毒、防火墙、入侵检测等一系列安全产品，这些产品产生大量不同形式的安全信息，使得整个系统的相互协作和统一管理成为安全管理的难点。由此带来的是安全管理的任务大幅增加，安全管理体制也变得非常复杂，其系统配置、规则设置、反应处理、设备管理、运行管理的复杂性所带来的管理成本和管理难度都直接制约了安全防御体系的有效性，从而也会给网络的安全性带来重大隐患，也使得用户的需求在不断向全局化智能化的方向发展。

（2）适应智慧城市发展需要，符合公司战略发展需求

新一代智慧城市安全运营平台适应当前智慧城市的发展潮流，是新形势下安全防护的迫切要求。项目的建成满足公司中长期战略发展需要，为公司未来的优势竞争地位提供有力保障。项目的实施和运营是中长期利润的重要来源，符合公司长期发展的利益。

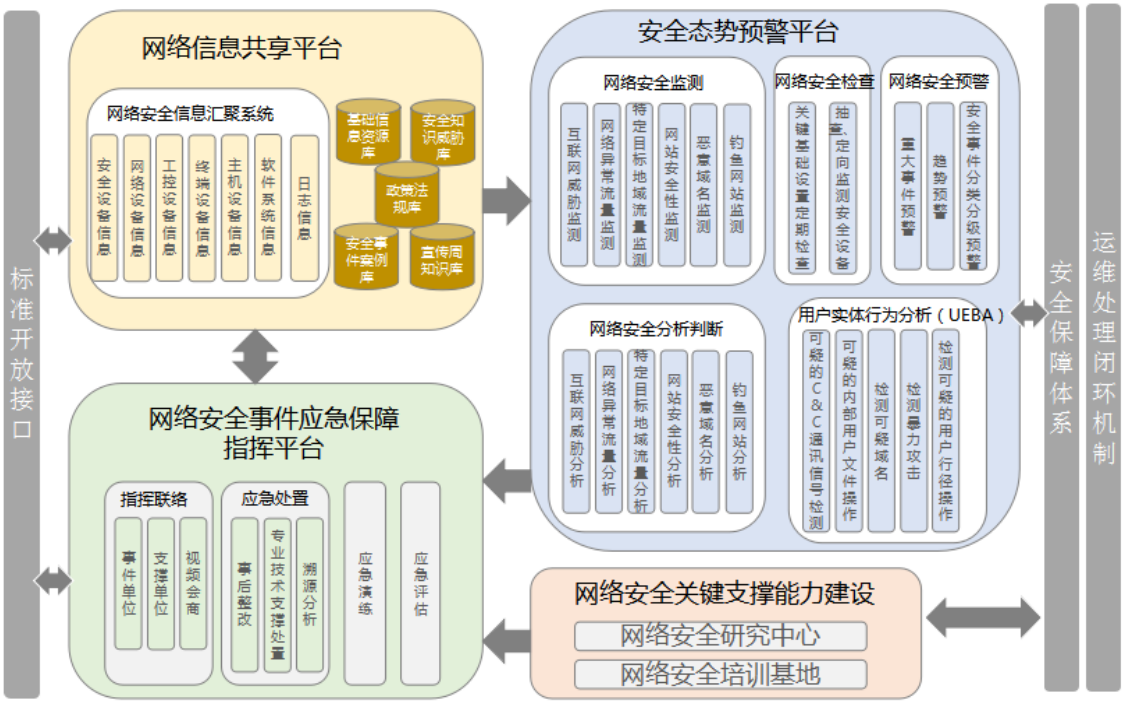
5、项目建设方案

（1）总体设计

项目积极融入 OpenStack 开源框架，添加安全管控组件；向用户提供一个整体完整的管理界面，确保对新一代智慧城市安全运营平台每个环节进行了严格的安全保护。

（2）具体建设内容

项目包括网络信息共享平台、安全态势预警平台、网络安全事件应急保障指挥平台以及网络安全关键支撑能力四个子平台的建设。通过网络信息共享平台以及安全态势预警平台实现信息安全技术保障体系的构建；通过网络安全事件应急保障指挥平台实现信息安全组织保障体系、信息安全制度保障体系以及信息安全灾难恢复体系的构建；通过网络安全关键支撑能力的建设实现信息安全风险测评评估机制的建设。具体如下：



1）网络信息共享平台

包含网络安全信息汇聚系统，汇聚安全设备、网络设备、主机设备、终端设备、软件系统的基本信息，并且采集上述设备各种日志信息；同时共享平台包含知识体系的建设，包括基础信息资源库、安全知识威胁库、政策法规库、安全事件案例库、宣传周知识库等。

2）安全态势预警平台

网络安全监测包括互联网威胁监测、网络异常流量监测、特定目标地域流量监测、网站安全性监测、恶意域名监测、钓鱼网站监测；网络安全检查包括关键基础设置定期检查、安全设备抽查、定向监测；网络安全分析判断包括互联网威胁分析、网络异常流量分析、特定目标地域流量分析、网站安全性分析、恶意域名分析、钓鱼网站分析；网络安全预警包括重大事件预警、趋势预警、安全事件分类分级预警；用户实体行为分析包含可疑的 C&C 通讯信号检、可疑的内部用户文件操作、检测可疑域名、检测暴力攻击、检测可疑的用户行径操作。

3）网络安全事件应急保障指挥平台

指挥联络包括事件单位、支撑单位的联络和视频会商；应急处置包括事后整改、专业技术支撑处置、溯源分析；另外还包括应急演练和应急评估。

4）网络安全关键支撑能力建设

包括网络安全研究中心和网络安全培训基地的建设。

6、项目实施主体

本项目由蓝盾技术自行建设，建设地点设在广州天河软件园。

7、项目效益情况

经测算，项目主要财务分析指标如下：

序号	指标	单位	金额
1	年均销售收入	万元	20,850.00
2	年均净利润	万元	5,273.27
3	财务内部收益率	%	26.89%
4	财务净现值（ic=10%）	万元	18,174.69
5	投资回收期	年	2.98

8、项目批准情况

本项目已取得广东省广州市天河区发展和改革局出具的《广东省企业投资项目备案证》，项目代码 2020-440106-65-03-007262。

（十）补充流动资金项目

1、项目概况

公司拟将本次非公开发行股票募集资金中的 60,000 万元用于补充流动资金，以满足公司业务不断发展对营运资金的需求，进而促进公司主营业务持续健康发展。

2、补充流动资金项目的必要性与可行性

（1）业务规模增长将占用更多营运资金

报告期内，公司主营业务不断发展，产业链不断延伸，新产品市场积极开拓，公司业务运营对资金需求不断增加，本项目将有效缓解公司营运资金压力，增强公司资金实力。

（2）实现公司发展战略需要资金支持

公司聚焦网络信息安全主业及“智慧安全”发展理念。公司需要持续关注信息安全技术领域的最新科研成果，通过加大高端人才培养与引进力度，拓展产学研合作范围，从而增强公司的核心竞争力，相应需要投入较大的资金。

（3）优化资本结构，提高公司短期偿债能力

通过本次非公开发行股票募集资金，公司资本结构将得到优化，有利于降低财务成本，提高短期偿债能力，降低财务风险。

综上，本次非公开发行股票补充流动资金项目具有合理性，与公司资产和经营规模相匹配。

四、本次非公开发行对公司经营管理和财务状况的影响

（一）对公司经营管理的影响

本次募集资金投资项目符合国家相关的产业政策，以及未来公司整体战略发展方向，具有良好的市场发展前景和经济效益。募集资金的运用合理、可行，符合公司及全体股东的利益。项目完成后，能够进一步提升公司的竞争能力，提高公司盈利水平，增加利润增长点。

（二）对公司财务状况的影响

本次非公开发行股票完成后，公司总资产与净资产规模将同时增加，资产负债率水平将有所下降，有利于增强公司抵御财务风险的能力，进一步优化资产结构，降低财务成本和财务风险，增强未来的持续经营能力。同时，随着本次募集

资金投资项目的逐步实施和投产，公司的收入水平将稳步增长，盈利能力进一步提升，公司的整体实力和抗风险能力将进一步加强。

五、募集资金投资项目可行性结论

综上所述，本次募集资金投资项目符合国家相关产业政策、公司所处行业发展趋势和公司未来发展规划，具有良好的市场前景和经济效益，有利于提升公司的盈利能力。本次募集资金投资项目合理、可行，符合公司及公司全体股东的利益。

第三节 董事会关于本次发行对公司影响的讨论与分析

一、本次发行后公司业务及资产、公司章程、预计股东结构、高管人员结构、业务结构的变动情况

（一）业务及资产整合、业务结构变动情况

本次非公开发行募集资金的投向围绕主营业务展开。本次募集资金投资项目实施后，公司主营业务得到进一步增强，行业竞争优势得到进一步提升，能够保证公司未来持续发展，提升公司的盈利能力。

本次发行不会对公司主营业务结构产生重大不利影响，也不涉及资产与业务的整合计划。

（二）本次发行对公司章程的修订

本次非公开发行股票完成后，公司的股本总额将增加，导致公司股本结构和注册资本发生变化。公司将按照发行的实际情况对《公司章程》中与股本相应的条款进行修改，并办理工商变更登记。除此之外，公司暂无其它因本次发行而修改或调整公司章程的计划。

（三）本次发行对股东结构的影响

截至 2020 年 2 月 26 日，实际控制人柯宗贵、柯宗庆合计持有公司 313,903,797 股股份（其中柯宗贵直接持有 156,473,504 股，柯宗庆直接持有 157,430,293 股），占公司股份总数的 25.12%。中经汇通持有公司 89,935,042 股，占公司股份总数的 7.20%，系公司控股股东、实际控制人的一致行动人。公司的实际控制人及其一致行动人合计持有公司 403,838,839 股，占公司股份总数的 32.31%。

若按照本次非公开发行的股票数量上限 374,939,743 股测算，本次发行完成后，本公司总股本将增加到 1,624,738,888 股。假设柯宗贵、柯宗庆及中经汇通不参与本次发行认购，设柯宗贵、柯宗庆及其一致行动人控制的股份比例将变为 24.86%，柯宗贵、柯宗庆仍处于控股地位，仍为公司实际控制人。

因此，本次发行不会导致公司控制权发生变化。

（四）本次发行完成后，对公司上市地位的影响

本次发行完成后，社会公众持有公司的股份占总股本的比例不低于 25%，符合《公司法》、《证券法》以及《深圳证券交易所股票上市规则》等法律法规规定的股票上市条件，不会导致股权分布不具备上市条件的情形。

（五）本次发行对高管人员结构的影响

本次发行不会对高级管理人员结构造成重大影响。截至本预案出具日，公司尚无对高级管理人员结构进行调整的计划。

二、本次发行后公司财务状况、盈利能力及现金流量的变动情况

（一）财务结构变动情况

本次非公开发行股票募集资金到位后，公司总资产与净资产规模将同时增加，资产负债率水平将有所下降，有利于增强公司抵御财务风险的能力，进一步

优化资产结构，有利于改善公司的流动性、提高公司的偿债能力，降低财务成本和财务风险，增强未来的持续经营能力。

（二）对公司盈利能力的影响

本次非公开发行股票完成后，由于募集资金使用产生效益尚需一定时间，经济效益不能立即体现，因此存在短期内公司的每股收益等财务指标出现一定摊薄的风险。但随着本次募投项目顺利实施，公司业务规模将有效扩大，有利于扩宽客户渠道及稳步提升营业收入，从而能够更好地满足快速增长的市场需求，公司整体盈利能力将得以增强。同时，公司财务结构的优化，也将对公司的持续盈利能力产生积极影响。

（三）现金流量的变化

本次非公开发行股票完成后，公司筹资活动产生的现金流入量将明显增加。这将有助于提高公司营运能力，降低经营风险，也为公司未来的战略发展提供有力的资金保障。在募投项目建设期间，公司投资活动产生的现金流出较高；随着项目建成并运营成熟后，未来经营活动现金流量净额将逐渐提升，公司现金流量状况将得到进一步优化。

三、本次发行完成后，公司与控股股东及其关联人之间的业务关系、管理关系、关联交易及同业竞争等变化情况

（一）公司与控股股东及其关联人之间的业务关系变化情况

本次发行完成后，公司与控股股东及其关联人之间的业务关系不会因本次发行而发生重大变化。

（二）公司与控股股东及其关联人之间的管理关系变化情况

本次发行完成后，公司与控股股东及其关联人之间的管理关系不会因本次发行而发生重大变化。

（三）公司与控股股东及其关联人之间的关联交易变化情况

本次发行完成后，公司与控股股东及其关联人之间的关联交易不会发生重大变化。

（四）公司与控股股东及其关联人之间的同业竞争变化情况

本次发行完成后，公司与控股股东及其关联人之间不会因本次发行而产生同业竞争。

四、本次发行完成后，公司是否存在资金、资产被控股股东及其关联人占用的情形，或公司为控股股东及其关联人提供担保的情形

截至本预案出具日，公司不存在资金、资产被控股股东及其关联人占用的情形，亦不存在公司为控股股东及其关联人违规提供担保的情形；本次非公开发行股票完成后，公司不存在资金、资产被实际控制人、控股股东及其关联人占用的情形，亦不存在公司为实际控制人、控股股东及其关联人提供担保的情形。

五、本次非公开发行对公司负债情况的影响

本次非公开发行股票完成后，公司总资产与净资产将相应增加，资本结构得以优化，不存在通过本次发行大量增加负债（包括或有负债）的情况。本次非公开发行股票募集资金到位后，公司的资产负债率有所降低，将进一步改善公司资本结构和财务状况。

第四节 本次股票发行相关的风险说明

投资者在评价公司本次非公开发行股票时，除预案提供的各项资料外，应关注下述各项风险因素：

一、市场竞争风险

信息安全行业是一个竞争较为充分的行业，随着市场环境的逐步成熟和市场规模的迅速扩大，国内越来越多企业涉足信息安全领域，特别是行业内一些规模较小、技术水平较低的中小企业的进入，对国内信息安全行业的良性竞争造成一定的负面影响。同时，随着信息安全行业部分产品和服务开放程度的扩大，越来越多的境外资本和境外企业也加入本行业的竞争，尤其是境外的优势企业凭借其在产业链中的地位和资金优势，对国内信息安全企业造成一定冲击。尽管公司在信息安全华南区域市场处于领先地位，已经成为国内信息安全领域的主要厂商之一，并且公司在技术研发、专业资质、综合服务能力、客户资源以及人才等方面优势将有助于公司巩固及提高现有市场地位，但随着国内外新竞争者的出现，市场竞争进一步加剧，公司可能面临盈利能力下滑、市场占有率无法持续提高等风险。

二、经营管理风险

项目的实施将带动公司产品品种的扩展和规模的不断扩大，但同时也对公司的经营管理提出了更高要求，公司管理层须提高经营管理能力与公司的业务发展规模相适应，另一方面，只有具备科学化的经营管理制度，才促进公司业务的持续发展。因而，随着项目实施进度的不断深入，也将一定程度上增加公司的经营管理风险。

三、技术风险

公司经十多年的研发积累，已经形成了一支高质量的研发队伍，并掌握了众多的具有自主知识产权的技术，在安全产品相关技术上基本不存在短板。针对项目开发过程中的技术难点，公司将组织专门的技术攻关队伍，对项目实施中的各种技术难关进行针对性的研究攻克，并增强产品的技术测试来攻克项目开发中的技术难点。但项目实施过程中仍可能面临网络产品及国产化软硬件的异构风险、可信计算联动风险、安全设备联动风险、威胁预警误报、重报、漏报风险等与项目开展相关的技术风险。

四、进度风险

公司将在项目研发进行中进行精确规划，使用 PERT 和 CPM 方法对项目实行定量分析规划，精确项目进度规划进度；对项目实时监控，实时检查并掌握项目进度信息，及时制定实施调整与补救措施；同时预留进度时间，充分考虑困难和可能的突发情况，预留机动时间，保障进度安排。但信息安全产品在研发过程中，仍可能因估算不精确、方法不科学及缺乏控制等多种因素产生进度风险。

五、人才风险

项目的实施无论是在人员数量和人员质量方面，都对公司提出了新的要求，而如何组建一只高素质的人才队伍，对于保障项目成功顺利实施也有着至关重要的作用，因此，项目的实施面临人才不足的风险。

六、募投项目实施风险

尽管公司对前述募集资金投资项目的可行性已进行了充分论证。但相关结论均是基于当前市场环境、产业政策和公司战略做出的，在项目实施过程中，上述因素有可能发生较大变化，从而导致本次募集资金投资项目存在实施进度或效益未达预期的风险。

同时，本次募投项目涉及的研发项目投资总额较大且主要为固定资产、无形资产投资，预计项目建成后每年将新增较大的折旧摊销费用，在一定程度上影响公司的盈利水平，如果公司无法保持盈利能力，上述新增折旧摊销费用将对公司盈利能力产生影响，从而使公司面临盈利能力下降的风险。

七、因发行新股导致原股东分红减少的风险

本次非公开发行后，公司股本及净资产规模将上升，公司滚存未分配利润由新老股东共享，将可能导致原股东分红减少。随着募投项目效益体现，公司的盈利水平将逐步提升，公司将根据公司章程中关于利润分配的相关政策，积极回报投资者。

八、表决权被摊薄的风险

本次非公开发行后，公司股本将上升，公司原股东在股东大会上所享有的表决权会相应被摊薄，从而存在表决权被摊薄的风险。

九、股东即期回报被摊薄的风险

本次发行成功且募集资金到位后，公司的总股本和净资产将有较大幅度增加，由于募集资金投资项目从建设到取得经济效益需要一定的时间，项目产生效益需要一定的时间，如果公司净利润在募投项目建设期内未能实现相应幅度的增长，则公司基本每股收益和加权平均净资产收益率等指标将出现一定幅度的下降。因此，本次募集资金到位后公司即期回报存在被摊薄的风险。

十、与本次非公开发行相关的审批风险

本次非公开发行股票需经公司股东大会审议批准，本方案存在无法获得公司股东大会表决通过的可能。此外，本次非公开发行股票尚需取得中国证监会的批准或核准，能否取得相关的批准或核准以及最终取得批准和核准的时间存在不确定性。

十一、股价波动风险

本次非公开发行将对公司的生产经营和财务状况产生一定的影响，公司基本面的变化将影响公司股票的价格；宏观经济形势变化、国家重大经济政策的调控、本公司经营状况、股票市场供求变化以及投资者心理变化等种种因素，都会对公司股票价格带来波动，给投资者带来风险。

此外，公司本次非公开发行需要一定的时间周期方能完成，在此期间公司股票的市场价格可能会出现波动，从而直接或间接地影响投资者的收益，请投资者注意相关风险。

第五节 发行人利润分配情况

一、公司现行《公司章程》对利润分配政策的相关规定

根据《公司法》和《公司章程》的规定，公司现行有关利润分配政策如下：

（一）上市公司利润分配政策

《公司章程》中对利润分配政策的相关规定如下：

1、利润分配原则

公司实行连续、稳定、积极的利润分配政策，公司的利润分配应重视对投资者的合理回报并兼顾公司的可持续发展。公司采取现金、股票以及现金与股票相结合的方式分配股利，并优先考虑现金分红，利润分配不得超过累计可分配利润的范围，不得损害公司持续经营能力。公司利润分配政策的决策和论证过程中应充分考虑和听取股东（特别是公众投资者）、独立董事和监事的意见。

除特殊情况外，公司实施现金分红时须满足下列条件：

1、公司该年度或当期实现的可分配利润（即公司弥补亏损、提取盈余公积金后所余的税后利润）为正值；

2、审计机构对公司的财务报告出具标准无保留意见的审计报告。

特殊情况指：公司有重大投资计划或重大现金支出等事项发生（募集资金项目除外），可以不进行现金分红。

重大投资计划或重大现金支出指以下情形之一：

（一）公司未来十二个月内拟对外投资、收购资产或购买设备累计支出达到或超过公司最近一期经审计净资产的 50%，且超过 5,000 万元；

（二）公司未来十二个月内拟对外投资、收购资产或购买设备累计支出达到或超过公司最近一期经审计总资产的 30%。

2、利润分配期间间隔

在符合利润分配原则、保证公司正常经营和长远发展的前提下，在满足现金分红条件时，公司原则上每年度进行一次现金分红。公司每年以现金方式分配的利润不少于当年实现的可分配利润的 10%，或连续三年以现金方式累计分配的利润不少于该三年实现的年均可分配利润的 30%。公司在实施上述现金分配股利的同时，可以派发红股。公司的公积金用于弥补公司的亏损、扩大生产经营规模或者转增公司资本，法定公积金转为资本时，所留存的该项公积金将不少于转增前公司注册资本的 25%。

3、利润分配的条件和比例

公司董事会应当综合考虑所处行业特点、发展阶段、自身经营模式、盈利水平以及是否有重大资金支出安排等因素，区分下列情形，并按照公司章程规定的程序，提出差异化的现金分红政策：

（一）公司发展阶段属成熟期且无重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 80%；

（二）公司发展阶段属成熟期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 40%；

（三）公司发展阶段属成长期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 20%；

（四）公司发展阶段不易区分但有重大资金支出安排的，可以按照前项规定处理。

公司股东大会按照既定利润分配政策对利润分配方案作出决议后，公司董事会须在股东大会召开后二个月内完成股利（或红股）的派发事项；在条件允许的情况下,公司董事会可以根据公司的盈利及资金需求状况提议公司进行中期现金分配，并提交公司股东大会批准。

4、利润分配决策程序

公司制定利润分配政策时，应当履行以下决策程序：

（一）公司进行利润分配时，应当由公司董事会先制定分配预案，再行提交公司股东大会进行审议。对于公司当年未分配利润，董事会在分配预案中应当说明使用计划安排或者原则。

（二）公司在制定现金分红具体方案时，董事会应当认真研究和论证公司现金分红的时机、条件和最低比例、调整的条件及其决策程序要求等事宜，独立董事应当发表明确意见。

股东大会对现金分红具体方案进行审议时，应当通过多种渠道主动与股东特别是中小股东进行沟通和交流，充分听取中小股东的意见和诉求，并及时答复中小股东关心的问题。

（三）公司对《公司章程》确定的现金分红政策进行调整或者变更的，应当经出席股东大会的股东所持表决权的三分之二以上通过。

（四）公司应当在定期报告中详细披露现金分红政策的制定及执行情况，说明是否符合《公司章程》的规定或者股东大会决议的要求，分红标准和比例是否明确和清晰，相关的决策程序和机制是否完备，独立董事是否尽职履责并发挥了应有的作用，中小股东是否有充分表达意见和诉求的机会，中小股东的合法权益是否得到充分维护等。对现金分红政策进行调整或变更的，还要详细说明调整或变更的条件和程序是否合规和透明等。

（五）在公布定期报告的同时，董事会提出利润分配预案并在董事会决议公告及定期报告中公布。

（六）公司股东大会按照既定利润政策对分配方案进行审议并作出决议。公司应切实保障社会公众股股东参与股东大会的权利，董事会、独立董事和符合一定条件的股东可以向公司股东征集其在股东大会上的投票权。

公司将根据自身实际情况，并结合股东（特别是公众投资者）、独立董事和监事的意见制定或调整股东回报计划。

公司利润分配政策不得随意调整而降低对股东的回报水平，因国家法律法规和证券监管部门对上市公司的利润分配政策颁布新的规定或公司外部经营环境、自身经营状况发生较大变化而需调整分红政策的，公司董事会应以股东权益保护为出发点，详细论证和说明原因，应当充分听取独立董事和中小股东的意见，并在调整议案中详细论证和说明原因。

在审议公司有关调整利润分配政策、具体规划和计划的议案或利润分配预案的董事会、监事会会议上，需分别经公司二分之一以上独立董事、二分之一以上监事的同意，方可提交公司股东大会审议。

公司独立董事可在股东大会召开前向公司社会股股东征集其在股东大会上的投票权，独立董事行使上述职权应取得全体独立董事二分之一以上同意。

对于报告期内公司实现盈利但董事会未作出现金利润分配预案的，董事会应说明原因，独立董事应当对此发表独立意见。公司在召开股东大会审议之时，除现场会议外，还应当向股东提供网络形式的投票平台。

二、最近三年公司利润分配情况

公司最近三年每年以现金方式进行利润分配的金额分别为 35,263,381.70 元、42,312,885.69 元和 39,963,284.79 元，最近三年以现金方式累计分配的利润占该三年实现的年均可分配利润的比例为 31.08%，最近三年现金分红情况符合上市公司《公司章程》等相关规定。公司最近三年具体现金分红实施情况如下：

单位：元

项目	2018年度	2017年度	2016年度
合并报表中归属于上市公司股东的净利润	397,943,111.27	413,809,537.85	322,894,873.34
现金分红（含税）	39,963,284.79	42,312,885.69	35,263,381.70
当年现金分红占归属于上市公司股东的净利润的比例	10.04%	10.23%	10.92%
最近三年累计现金分配合计			117,539,552.18
最近三年年均可分配利润			378,215,840.82
最近三年累计现金分配利润占年均可分配利润的比例			31.08%

为保持公司的可持续发展，公司历年滚存的未分配利润作为公司业务发展资金的一部分，继续投入公司生产经营。

三、公司未来三年的股东回报规划

为进一步建立和完善科学、持续、稳定、透明的分红决策和监督机制，积极回报投资者，引导投资者树立长期投资和理性投资理念，根据中国证券监督管理委员会《关于进一步落实上市公司现金分红有关事项的通知》（证监发[2012]37号）、《上市公司监管指引第 3 号——上市公司现金分红》（证监会公告[2013]43号）及《公司章程》的有关规定，公司董事会结合公司实际情况，制订了《未来三年（2020 年-2022 年）股东回报规划》（以下简称“本规划”）。具体内容如下：

“一、公司制定本规划考虑的因素

公司制定本规划着眼于公司的长远和可持续发展，并在综合分析公司的经营现状、社会资金成本、外部融资环境等因素的基础上，充分考虑公司的战略发展规划及发展所处阶段、目前及未来三年盈利能力和规模、现金流状况、项目投资资金需求和银行信贷及债权融资环境等情况，建立对投资者持续、稳定、科学的回报规划与机制，以保证利润分配政策的连续性和稳定性。

二、本规划制订的原则

在符合国家相关法律法规及《公司章程》的前提下，公司将充分重视对投资者的合理投资回报，并兼顾公司当年的实际经营情况和可持续发展，在充分考虑

股东利益的基础上处理公司短期利益及长远发展的关系，同时充分考虑、听取并采纳公司独立董事、监事和中小股东的意见、诉求。未来三年内，公司将积极采取现金分红政策，重视对股东特别是中小投资者的合理投资回报，保持利润分配政策的连续性和稳定性。

三、本规划的制定周期

公司以每三年为一个周期，根据公司经营的实际情况及股东、独立董事和监事的意见，按照《公司章程》确定的利润分配政策制定股东分红回报规划，并经董事会审议通过后提交股东大会审议通过后实施。

如在已制定的规划期间内，公司因外部经营环境、自身经营状况发生较大变化，需要调整规划的，公司董事会应结合实际情况对规划进行调整。新制定的规划须经董事会、监事会审议通过后提交股东大会并审议通过后执行。

四、公司未来三年（2020 年-2022 年）具体股东回报规划

（一）公司可以采取现金方式或现金与股票相结合等法律、法规允许的其他方式分配利润。

（二）未来三年内，在符合相关法律法规及公司章程的有关规定和条件下，公司每年以现金方式分配的利润原则上不低于当年实现的可分配利润的 10%，且连续三年以现金方式累计分配的利润不低于该三年实现的年均可分配利润的 30%。具体每个年度的分红比例由董事会根据公司年度盈利状况和未来资金使用计划提出预案。

（三）公司实施现金分红时须同时满足下列条件：

1、公司该年度或当期实现的可分配利润（即公司弥补亏损、提取盈余公积金后所余的税后利润）为正值；

2、审计机构对公司的财务报告出具标准无保留意见的审计报告。

（四）在符合分红条件的情况下，公司未来三年原则上每年进行一次现金分红。在有条件的情况下，公司董事会可以根据公司的资金状况提议公司进行中期现金分配。

（五）公司董事会应当综合考虑所处行业特点、发展阶段、自身经营模式、盈利水平以及是否有重大资金支出安排等因素，区分下列情形，并按照公司章程规定的程序，提出差异化的现金分红政策：

1、公司发展阶段属成熟期且无重大资金支出安排的，进行利润分配时，现金分红在当期利润分配中所占比例最低应达到 80%；

2、公司发展阶段属成熟期且有重大资金支出安排的，进行利润分配时，现金分红在当期利润分配中所占比例最低应达到 40%；

3、公司发展阶段属成长期且有重大资金支出安排的，进行利润分配时，现金分红在当期利润分配中所占比例最低应达到 20%；

4、公司发展阶段不易区分但有重大资金支出安排的，进行利润分配时，现金分红在当期利润分配中所占比例最低应达到 20%。

重大投资计划或重大现金支出指以下情形之一：

（1）公司未来十二个月内拟对外投资、收购资产或购买设备累计支出达到或超过公司最近一期经审计净资产的 50%，且超过 5,000 万元；

（2）公司未来十二个月内拟对外投资、收购资产或购买设备累计支出达到或超过公司最近一期经审计总资产的 30%。

（六）公司发放股票股利的具体条件：公司经营情况良好，并且董事会认为公司股票价格与公司股本规模不匹配、发放股票股利有利于公司全体股东整体利益时，可以提出股票股利分配预案，并经股东大会审议通过后实施。

（七）若年度盈利但未提出现金分红方案，公司应在年度报告中详细说明未提出现金分红的原因、未用于现金分红的资金留存公司的用途和使用计划。

五、利润分配方案的决策机制

（一）公司进行利润分配时，应当由公司董事会先制定分配预案，经公司董事会、监事会审议通过后，再行提交公司股东大会进行审议。

（二）公司在制定现金分红具体方案时，董事会应当认真研究和论证公司现金分红的时机、条件和最低比例、调整的条件及其决策程序要求等事宜，独立董事应当发表明确意见。

（三）公司股东大会应当按照既定利润政策对分配方案进行审议并作出决议。股东大会对现金分红具体方案进行审议时，应当通过多种渠道主动与股东特别是中小股东进行沟通和交流，充分听取中小股东的意见和诉求，并及时答复中小股东关心的问题。公司股东大会审议利润分配方案时，公司应当为股东提供网络投票方式。

（四）公司对《公司章程》确定的现金分红政策进行调整或者变更的，应当经出席股东大会的股东所持表决权的三分之二以上通过。

（五）公司应当在定期报告中披露利润分配方案并详细披露现金分红政策的制定及执行情况，说明是否符合《公司章程》的规定或者股东大会决议的要求，分红标准和比例是否明确和清晰，相关的决策程序和机制是否完备，独立董事是否尽职履责并发挥了应有的作用，中小股东是否有充分表达意见和诉求的机会，中小股东的合法权益是否得到充分维护等。对现金分红政策进行调整或变更的，还要详细说明调整或变更的条件和程序是否合规和透明等。”

第六节 与本次发行相关的董事会声明及承诺事项

一、关于除本次发行外未来十二个月内是否有其他股权融资计划的声明

根据公司未来发展规划、行业发展趋势，考虑公司的资本结构、融资需求以及资本市场发展情况，除本次非公开发行外，公司董事会将根据业务情况确定未来十二个月内是否安排其他股权融资计划。若未来公司根据业务发展需要及资产负债状况需要安排股权融资时，将按照相关法律法规履行相关审议程序和信息披露义务。

二、本次发行摊薄即期回报对公司主要财务指标的影响及公司董事会作出的有关承诺并兑现填补回报的具体措施

根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）和《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（证监会公告[2015]31 号）的要求，为保障中小投资者利益，公司就本次非公开发行 A 股股票对即期回报摊薄的影响进行了认真分析，并拟定了填补回报的具体措施。公司的相关主体就保证发行人填补即期回报措施切实履行作出了承诺。具体情况如下：

（一）本次非公开发行摊薄即期回报对公司主要财务指标的影响

公司本次非公开发行股票募集资金总额不超过 200,000 万元，非公开发行股票数量不超过 374,939,743 股。公司就本次非公开发行对发行当年公司主要财务指标的影响做了相关分析，具体测算过程如下：

1、主要假设

（1）假设本次非公开发行于 2020 年 6 月 30 日实施完毕，该完成时间仅为公司用于本测算的估计，最终以经中国证监会核准后实际发行完成时间为准；

（2）假设本次非公开发行股票数量为 374,939,743 股，该发行股票数量仅为公司用于本测算的估计，最终以经中国证监会核准后实际发行股票数量为准。募集资金总额为 200,000 万元，不考虑发行费用等因素的影响；

（3）假设宏观经济环境、产业政策、行业发展状况等方面没有发生重大变化；

（4）不考虑本次非公开发行募集资金运用对公司生产经营、财务状况（如营业收入、财务费用、投资收益）等的影响；

（5）在预测公司总股本时，以本次非公开发行前，截至 2020 年 2 月 26 日的总股本 1,249,799,145 股为基础，仅考虑本次非公开发行股票的影响，不考虑其他因素（如资本公积转增股本、股票股利分配）导致公司总股本发生的变化；

（6）2020 年 1 月 22 日，公司公告了《2019 年年度业绩预告》，公司预计 2019 年度归属于上市公司股东的净利润为亏损 98,500 万元至 99,000 万元，预计本期计提的商誉、应收账款、无形资产等减值准备金额为 117,000 万元，非经常性损益对净利润的影响金额预计为 700 至 900 万元。假设公司 2019 年度实现的归属于母公司所有者的净利润为-98,750 万元，本期计提的商誉、应收账款、无形资产等减值准备金额为 117,000 万元，非经常性损益金额为 800 万元，则扣除非经常性损益后归属于母公司所有者的净利润为-99,550 万元，若不考虑商誉和无形资产等减值准备对公司净利润的影响，则公司 2019 年度实现的归属于母公司所有者的净利润为 18,250 万元，扣除非经常性损益后归属于母公司所有者的净利润为 17,450 万元。

（7）假设 2020 年归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润分为以下三种情况：

①2020 年归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润与 2019 年剔除商誉和无形资产等减值准备的预测数据持平；

②2020 年公司归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润与 2018 年持平；

③2020 年公司归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润较 2018 年增长 10%。

（8）假设公司 2019 年度、2020 年度不进行利润分配，也不以资本公积转增股本；

上述假设仅为测算本次非公开发行对公司即期回报主要财务指标的摊薄影响，不代表公司对未来年度经营情况及财务状况的判断，亦不构成盈利预测。公司收益的实现取决于国家宏观经济政策、行业发展状况、市场竞争情况和公司业务发展状况等诸多因素，存在较大不确定性。投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。

（二）对发行人即期回报的摊薄影响

根据以上假设，公司测算了本次发行对投资者即期回报的影响，具体如下：

项目	2019 年度/ 2019 年 12 月 31 日	2020 年度/ 2020 年 12 月 31 日	
		本次发行前	本次发行后
总股本（万股）	124,979.62	124,979.91	162,473.89
预计非公开发行完成时间	2020 年 6 月 30 日		
假设情形 1：假设 2020 年归属于上市公司股东的净利润、归属于上市公司股东的扣除非经常性损益后的净利润与 2019 年剔除商誉和无形资产等减值准备的预测数据持平			
归属于母公司股东的净利润（万元）	-98,750.00	18,250.00	18,250.00
归属于母公司股东的扣除非经常性损益的净利润（万元）	-99,550.00	17,450.00	17,450.00
基本每股收益（元/股）	-0.814	0.146	0.127
稀释每股收益（元/股）	-0.814	0.146	0.127
扣除非经常性损益的基本每股收益（元/股）	-0.821	0.140	0.121
扣除非经常性损益的稀释每股收益（元/股）	-0.821	0.140	0.121
假设情形 2：2020 年公司归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润与 2018 年持平			
归属于母公司股东的净利润（万元）	-98,750.00	39,794.31	39,794.31
归属于母公司股东的扣除非经常性损益的净利润（万元）	-99,550.00	34,579.42	34,579.42
基本每股收益（元/股）	-0.814	0.318	0.277

项目	2019 年度/2019 年 12 月 31 日	2020 年度/2020 年 12 月 31 日	
		本次发行前	本次发行后
稀释每股收益（元/股）	-0.814	0.318	0.277
扣除非经常性损益的基本每股收益（元/股）	-0.821	0.277	0.241
扣除非经常性损益的稀释每股收益（元/股）	-0.821	0.277	0.241
假设情形 3：2020 年公司归属于母公司所有者利润及扣除非经常性损益后归属于母公司所有者净利润较 2018 年增长 10%			
归属于母公司股东的净利润（万元）	-98,750.00	43,773.74	43,773.74
归属于母公司股东的扣除非经常性损益的净利润（万元）	-99,550.00	38,037.36	38,037.36
基本每股收益（元/股）	-0.814	0.350	0.305
稀释每股收益（元/股）	-0.814	0.350	0.305
扣除非经常性损益的基本每股收益（元/股）	-0.821	0.304	0.265
扣除非经常性损益的稀释每股收益（元/股）	-0.821	0.304	0.265

注：按照《公开发行证券的公司信息披露编报规则第 9 号——净资产收益率和每股收益的计算及披露》（2010 年修订）的规定计算。

三、本次非公开发行摊薄即期回报的风险提示

本次非公开发行完成后，公司的总股本将有所增加，但由于募集资金实现回报需要一定周期，即募集资金实现的相关收入、净利润在短期内难以全部释放，公司的每股收益存在短期内下降的可能性，公司股东即期回报存在被摊薄的风险。此外，一旦前述分析的假设条件或公司经营发生重大变化，不能排除本次非公开发行导致即期回报被摊薄情况发生变化的可能性。

特此提醒投资者关注本次非公开发行可能摊薄即期回报的风险。

四、董事会选择本次融资的必要性和合理性

关于本次非公开发行募集资金投资项目的必要性和合理性分析，请见本预案“第一节 本次非公开发行股票方案概要”之“二、本次非公开发行股票的背景和目的”之“（二）本次非公开发行股票的目的”。

五、本次募集资金投资项目与公司现有业务的关系、公司从事募集资金投资项目在人员、技术、市场等方面的储备情况

（一）募集资金投资项目与公司现有业务的关系

本次非公开发行股票的募集资金拟投项目与公司当前主营业务方向一致，有利于公司抢占市场，同时巩固公司的行业地位，提高公司的盈利水平，为公司实现中长期战略发展目标奠定基础。

（二）公司从事募集资金投资项目在人员、技术、市场等方面的储备情况

1、人员储备

公司拥有大量优秀的信息安全技术人才，组成了一支基础扎实、技术水平高、开发能力强、实践经验丰富、专业与年龄结构合理的人才队伍，是公司在竞争中立于不败之地的重要保证。

为增强公司科技人才持续竞争能力，公司与广州天河软件园管理委员会、华南理工大学博士后管理办公室签订协议，联合培养企业博士后研究人员。同时，公司也参与建立了网络与信息安全产学研创新联盟，在广东省科技厅省部产学研办公室指导下，与信息安全领域国内高等院校、科研单位和企业联合开展网络与信息安全的技术研发与产业化工作。

此外，公司还聚集了一大批包括归国学者、国内著名专家、专业人才以及国内软件业和网络界的优秀人才。大量的人才储备为本次募集资金投资项目的实施提供了智力支持。

2、技术储备

经过十余年的发展，公司共开发出了边界安全、安全管理、应用安全、审计安全等多个类型的安全产品，同时也承担了公安部及保密局的多种专项产品开发任务，开发出了多款部级、省级专用安全产品，积累了丰富的产品开发经验。以

丰富的研发经验为基础，公司在信息安全产品的研发设计、产品检测等主要技术领域均已达到国内领先水平，部分技术已接近国际先进水平。

除了先进性外，公司的技术实力也体现在全面性上。在 Cloudfence 云防线、云安全管理平台、云计算安全监控与管理中心等信息安全前沿领域，目前公司均已实现了一定的研发成果，同时，公司在传统防火墙、IDS/IPS、漏洞扫描等每个单项产品上，也都有着深厚的技术积累，从而使得公司基本不存在技术短板，在产品整合方面具有较好的技术支撑。

3、市场储备

云计算、移动互联网、物联网、大数据和智慧城市等新技术和新应用模式的出现与发展，对信息安全提出了新需求和新挑战。随着数据信息进一步集中，数据量不断增大，现有的信息安全手段已经难于满足这些新技术和新应用模式的新要求，对海量数据进行安全防护变得更加困难，数据的分布式处理也加大了数据泄露的风险。因此，保护数据安全已经成为云计算、移动互联网、物联网、大数据和智慧城市等新技术和新应用模式的焦点。新技术、新应用和新模式的出现，对信息安全提出了新的要求的同时，也为信息安全产品和服务创造广阔的市场空间，进一步带动各类用户的信息安全投入，促进信息安全整体市场需求的增长。

六、公司应对本次非公开发行摊薄即期回报采取的措施

（一）增强公司整体竞争力，提高公司盈利水平

未来公司将聚焦网络信息安全主业，提升产品及服务质量，保障公司稳健经营，提升公司整体盈利水平，促进业绩持续增长。同时，公司未来将继续保持对技术和研发的投入，积极引进技术人才，不断提高公司的核心竞争能力与持续发展能力。

（二）加强募集资金管理，保证募集资金合理规范使用

为规范公司募集资金的使用与管理，确保募集资金的使用规范、高效，公司已制定了《募集资金管理制度》，对募集资金的专户存储、使用、管理与监督等

内容进行了明确的规定。本次发行募集资金将存放于董事会批准设立的专项账户管理，并就募集资金账户与保荐机构、存放募集资金的商业银行签订募集资金专户存储监管协议，由保荐机构、开户银行与公司共同对募集资金进行监管。公司将严格按照相关法规和《募集资金管理制度》的要求，管理募集资金的使用，保证募集资金按照既定用途得到充分有效利用。

（三）积极稳健推进本次募投项目建设

本次发行募集资金投资项目经过董事会的充分论证，有利于扩展公司在信息安全行业的业务品种，提升技术水平，增强公司的盈利能力，提高公司的盈利水平。公司将积极推动本次募集资金投资项目的建设，积极调配资源，提高资金使用效率，在确保质量的前提下争取项目早日实现效益，回报投资者，降低本次发行对股东即期回报摊薄的风险。

（四）加强经营管理和内部控制

公司将严格遵循《公司法》、《证券法》、《上市公司治理准则》等法律法规和规范性文件的要求，不断完善公司治理结构，确保股东能够充分行使权利，确保董事会能够按照法律法规和公司章程的规定行使职权、作出决策，确保独立董事能够认真履行职责，维护公司的整体利益和股东的合法权益，确保监事会能够独立有效地行使对董事、高级管理人员及公司财务的监督权和检查权，为公司发展提供制度保障。

（五）保持稳定的股东回报政策

为建立对投资者持续、稳定的回报规划与机制，保证利润分配政策的连续性和稳定性，公司已经按照《关于进一步落实上市公司现金分红有关事项的通知》和《上市公司监管指引第 3 号——上市公司现金分红》及其他相关法律、法规和规范性文件的要求，在《公司章程》、《现金分红管理制度》、《未来三年（2020 年-2022 年）股东回报规划》等制度文件中，明确了公司利润分配尤其是现金分红的具体条件、比例、分配形式和股票股利分配条件等，完善了公司利润的决策程序和机制以及利润分配政策的调整原则，强化了中小投资者权益保障机制。本

次发行完成后，公司将严格执行现金分红政策，在符合利润分配条件的情况下，积极落实对股东的利润分配，努力提升对股东的回报。

七、公司的董事、高级管理人员对公司本次非公开发行摊薄即期回报采取填补措施的承诺

公司全体董事、高级管理人员根据中国证监会相关规定，对公司填补回报措施能够得到切实履行作出如下承诺：

“1、本人承诺不无偿或以不公平条件向其他单位或者个人输送利益，也不采用其他方式损害公司利益。

2、本人承诺对本人的职务消费行为进行约束。

3、本人承诺不动用公司资产从事与本人履行职责无关的投资、消费活动。

4、本人承诺由董事会或薪酬委员会制定的薪酬制度与公司填补回报措施的执行情况相挂钩。

5、若公司后续推出股权激励计划，本人承诺拟公布的公司股权激励的行权条件与公司填补回报措施的执行情况相挂钩。

6、自本承诺出具日至公司本次非公开发行股票实施完毕前，若中国证监会作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足中国证监会该等规定时，本人承诺届时将按照中国证监会的最新规定出具补充承诺。

7、本人承诺切实履行本承诺，若违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任。”

八、公司的控股股东及实际控制人对公司本次非公开发行摊薄即期回报采取填补措施的承诺

公司的控股股东及实际控制人根据中国证监会相关规定，对公司填补回报措施能够得到切实履行作出如下承诺：

“1、继续保证上市公司的独立性，不越权干预上市公司的经营管理活动，不侵占上市公司的利益。

2、本人承诺切实履行公司制定的有关填补回报措施以及本人对此作出的任何有关填补回报措施的承诺，若本人违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或投资者的补偿责任。

若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和深圳证券交易所等证券监管机构按照其制定或发布的有关规定、规则，对本人作出相关处罚或采取相关管理措施。”

特此公告。

（以下无正文，为《蓝盾信息安全技术股份有限公司 2020 年创业板非公开发行 A 股股票预案》的盖章页）

蓝盾信息安全技术股份有限公司

董 事 会

2020 年 2 月 28 日