证券代码：300369　　证券简称：绿盟科技

北京神州绿盟信息安全科技股份有限公司

非公开发行股票预案

（三次修订稿）

二〇一六年八月

发行人声明

1、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，并对公告中的虚假记载、误导性陈述或重大遗漏承担个别和连带的法律责任。

2、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。

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

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

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

6、本预案所述事实并不代表审批机关对于本次非公开发行股票相关事宜的实质性判断、确认或批准，本预案所述本次非公开发行股票相关事宜的生效和完成尚待取得有关审批机关的批准或核准。

重大事项提示

1、本次非公开发行股票方案已经公司第二届董事会第二十三次会议、2016年第一次临时股东大会、第二届董事会第二十八次会议、第二届董事会第三十次会议、第二届董事会第三十四次会议审议通过。

2、本次非公开发行股票的发行对象范围为符合中国证监会规定的证券投资基金管理公司、证券公司、保险机构投资者、信托投资公司、财务公司、合格境外机构投资者，以及符合中国证监会规定的其他法人、自然人或其他合格的投资者，发行对象不超过 5 名。最终发行对象将在本次发行申请获得中国证监会的核准文件后，根据发行对象申购报价情况，由董事会与本次发行的保荐机构（主承销商）协商确定。

3、本次非公开发行股票数量不超过 2,600 万股，最终发行数量由董事会根据股东大会的授权、中国证监会相关规定及实际认购情况与保荐人（主承销商）协商确定。若公司股票在关于本次非公开发行的董事会决议公告日至发行日期间有除权、除息行为，本次非公开发行的股票数量将进行相应调整。

4、本次发行的定价基准日为发行期首日，定价原则为：发行价格不低于发行期首日前二十个交易日公司股票均价的百分之九十，或不低于发行期首日前一个交易日公司股票均价的百分之九十。最终发行价格由董事会根据股东大会授权在本次非公开发行申请获得中国证监会的核准文件后，按照中国证监会相关规则，根据竞价结果与本次发行的保荐人（主承销商）协商确定。

若发行人股票在定价基准日至发行日期间发生派息/现金分红、送红股、资本公积金转增股本等除权除息事项，本次非公开发行价格将进行相应调整。

5、公司本次发行募集资金总额不超过 80,121.58 万元，扣除发行费用后用于以下募投项目：

序号	项目名称	项目总投资额（万元）	拟投入募集资金数额（万元）
1	智慧安全防护体系建设项目	70,584.68	39,488.41
2	安全数据科学平台建设项目	30,045.42	20,633.17

3	补充流动资金	20,000.00	20,000.00
合计		**120,630.10**	**80,121.58**

若实际募集资金净额低于拟投入募集资金额,公司将根据实际募集资金净额，按照项目的轻重缓急等情况，调整并最终决定募集资金的具体投资项目、优先顺序及各项目的具体投资额,不足部分由公司以自有资金或自筹资金方式解决。在本次非公开发行募集资金到位之前，公司将根据项目进度的实际情况以自有资金或自筹资金先行投入，并在募集资金到位之后予以置换。

6、本次非公开发行股票完成后，特定投资者所认购的股份限售期需符合《创业板上市公司证券发行管理暂行办法》和中国证监会、深圳证券交易所等监管部门的相关规定：（1）发行价格不低于发行期首日前一个交易日公司股票均价的，本次发行股份自发行结束之日起可上市交易；（2）发行价格低于发行期首日前二十个交易日公司股票均价但不低于百分之九十，或者发行价格低于发行期首日前一个交易日公司股票均价但不低于百分之九十的，本次发行股份自发行结束之日起十二个月内不得上市交易。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。

7、关于公司的利润分配政策、最近三年现金分红及未分配利润使用、未来股东回报规划等情况，详见本预案“第五节 发行人的股利分配情况”。

8、本次非公开发行股票前公司的滚存未分配利润由本次发行完成后新老股东共享。

9、本次非公开发行股票完成后，公司股权分布将发生变化，但不会导致公司不具备上市条件。

10、特别提醒投资者仔细阅读本预案“第四节 本次股票发行相关的风险说明”的有关内容，注意投资风险。

目 录

释 义

在本预案中，除非另有说明，下列简称具有如下意义：

发行人、公司、本公司、绿盟科技	指	北京神州绿盟信息安全科技股份有限公司
股东大会	指	北京神州绿盟信息安全科技股份有限公司股东大会
董事会	指	北京神州绿盟信息安全科技股份有限公司董事会
监事会	指	北京神州绿盟信息安全科技股份有限公司监事会
《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》
《管理办法》	指	《创业板上市公司证券发行管理暂行办法》
本预案	指	北京神州绿盟信息安全科技股份有限公司非公开发行股票预案
本次发行/本次非公开发行	指	北京神州绿盟信息安全科技股份有限公司非公开发行股票
定价基准日	指	绿盟科技本次非公开发行股票的发行期首日
A 股	指	人民币普通股
中国证监会/证监会	指	中国证券监督管理委员会
工信部	指	中华人民共和国工业和信息化部
元、万元、亿元	指	人民币元、人民币万元、人民币亿元
云计算	指	基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源
云服务	指	基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网以按需、易扩展的方式获得所需服务；这种服务可以是 IT 和软件、互联网相关，也可以是其他服务
虚拟化	指	采用虚拟化技术将物理基础资源集中，形成一个共享虚拟资源池；通过服务器虚拟化、存储虚拟化、桌面和应用虚拟化等方式，帮助企业优化资源利用率、简化管理、建立动态 IT 基础设施环境、节约成本和降低能耗
大数据	指	一种针对数据的分析处理应用，目的是在数据量爆发性增长的背景下，能够使用一定技术手段，从庞杂数据中挖掘出有用信息，实现对海量数据的有效利用
SDN	指	“Software Defined Network”的缩写，即“软件定义网络”
平台	指	一系列通用软件组件和软件工具的集合，其中软件组件

		是根据应用系统开发所涉及的技术和业务、经过适当抽象和归纳、具有通用性的软件模块，这些软件模块构成了一个应用系统的基本骨架和结构，平台中的软件工具提供了配置和管理这些软件组件的手段；在基于平台开发具体应用系统的过程中，可根据用户的个别需求进行灵活定制和少量开发，可以大幅度缩短应用系统的开发周期
API	指	“Application Programming Interface”的缩写，即应用程序编程接口；它是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节
组件	指	软件系统中具有相对独立功能、有明确接口定义、可组装、可重复使用的软件实体模块
Openstack	指	一个开源的云计算管理平台项目，由几个主要的组件组合起来完成具体工作。Openstack 支持几乎所有类型的云环境，项目目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台。Openstack 通过各种互补的服务提供了基础设施作为服务的解决方案，每个服务提供 API 以进行集成
Nova	指	Openstack 中的一套控制器，用于为单个用户或使用群组管理虚拟机实例的整个生命周期，根据用户需求来提供虚拟服务。负责虚拟机创建、开机、关机、挂起、暂停、调整、迁移、重启、销毁等操作，配置 CPU、内存等信息规格
Amazon EC2	指	“Amazon Elastic Compute Cloud”的缩写，是一种 Web 服务，可在云中提供大小可调的计算容量。该服务旨在降低开发人员进行网络规模级云计算的难度
Amazon S3	指	“Amazon Simple Storage Service”的缩写，它提供了一种持久安全可扩展的云存储解决方案来备份、存储大量数据，为各种各样的使用案例提供低本高效的对象存储服务
Ceph	指	一个 Linux PB 级分布式文件系统
VLAN	指	“Virtual Local Area Network”的缩写，即虚拟局域网，是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样
GRE	指	“General Routing Encapsulation”的缩写, 是一个多协议承载协议
VxLAN	指	“Virtual eXtensible Local Area Network”的缩写，是一种将二层报文用三层协议进行封装的技术，可以对二层网络在三层范围进行扩展

Spark	指	UC Berkeley AMP Lab 所开源的类 Hadoop MapReduce 的通用并行框架
VPN	指	“Virtual Private Network”的缩写，虚拟专用网络的功能是：在公用网络上建立专用网络，进行加密通讯
Web 门户	指	将不同来源的信息以一种整齐划一的形式整理、储存并呈现的网站入口
APP	指	设计给智能手机、平板电脑和其他移动设备上运行的应用程序
OpenFlow	指	一种网络通讯协议，属于数据链路层，能够允许从远程控制网络交换器的数据包转送表，通过新增、修改与移除数据包控制规则与行动，来改变数据包转送的路径
SQL	指	“Structured Query Language”的缩写，即结构化查询语言

第一节 本次非公开发行股票方案概要

一、发行人基本情况

公司名称	北京神州绿盟信息安全科技股份有限公司
公司英文名称	Nsfocus Information Technology Co., Ltd.
上市地点	深圳证券交易所
股票代码	300369
股票简称	绿盟科技
注册资本	36,409.6355 万元
法定代表人	沈继业
上市时间	2014 年 1 月 29 日
注册地址	北京市海淀区北洼路 4 号益泰大厦 5 层
经营范围	许可经营项目：无。一般经营项目：货物进出口；技术进出口；代理进出口；开发计算机软硬件；销售自产产品；批发计算机硬件；提供技术开发、技术咨询、技术服务和计算机软硬件售后服务。

二、本次非公开发行的背景和目的

（一）本次非公开发行的背景

1、国家政策营造了信息安全、云计算和大数据产业健康发展的良好环境，信息安全成为国家和经济发展的重要保障

近年来，信息安全、云计算和大数据产业获得了国家战略层面的高度关注和重视。2014 年，中共中央网络安全和信息化领导小组成立；2015 年，《网络安全法（草案）》发布，体现出网络安全对维护国家利益、推动信息化发展的重要作用，有助于提高全社会和各行业对网络安全的重视程度。网络安全对国家安全、经济发展的保障作用得到广泛认可，关键信息基础设施和政府信息系统普遍加强了网络安全防护体系的建设。

2010 年，《国务院关于加快培育和发展战略性新兴产业的决定》将云计算纳入战略性新兴产业。2011 年，《国务院办公厅关于加快发展高技术服务业的指导意见》将云计算列入重点推进的高技术服务业。根据工信部电信研究院发布

的《2014 年云计算白皮书》，目前我国公共云服务市场仍处于低总量、高增长的产业发展初期阶段。2015 年，《国务院关于促进云计算创新发展培育信息产业新业态的意见》提出要加快发展云计算，打造信息产业新业态，推动传统产业升级和新兴产业成长，培育形成新的增长点，促进国民经济提质增效升级。

2014 年 3 月，中央《政府工作报告》提出设立新兴产业创业创新平台，在大数据等方面赶超先进，引领未来产业发展。2015 年 6 月，《国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见》要求以社会信用体系建设和政府信息公开、数据开放为抓手，充分运用大数据、云计算等现代信息技术，提高政府服务水平。2015 年 8 月，《国务院关于印发促进大数据发展行动纲要的通知》要求健全大数据安全保障体系，加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究。2015 年 10 月，《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》对大数据战略、利用大数据技术作出明确部署，指出“实施国家大数据战略，推进数据资源开放共享”、“运用大数据技术，提高经济运行信息及时性和准确性”。

2、网络安全威胁不断演化，迫切需要安全防护体系和产品服务进行更新换代

网络安全具备很强的对抗特征，安全防护体系、防护技术和产品、防护策略规则等都需要持续、及时升级换代，以应对不断演化的新型网络威胁。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，网络安全整体防护体系所涉及到的技术越来越复杂，有效安全防护和威胁响应所需的资源也越来越庞大。安全防护体系和产品服务需要更加智能、敏捷和开放，以使安全厂商能够具备快速、可靠和低成本的安全产品和服务的交付能力。

3、基于云计算和大数据的安全产品和服务具有广阔的市场空间

根据 IDC 研究报告预测，到 2019 年，国内信息安全市场总体规模有望达到 48.22 亿美元，2014 年到 2019 年的复合增长率为 16.6%。云计算、大数据技术的不断发展和应用给信息安全行业带来了广泛、深刻的影响。当前信息安全领域正在面临多种挑战。随着企业安全架构日趋复杂，各种类型的安全设备、安全数据

越来越多，传统的分析能力明显不足；为应对以高级持续威胁（APT）为代表的新型安全威胁，安全防护系统需要储存和分析更多的安全信息并且更加快速的做出判定和响应，大规模的安全数据需要被有效地关联、分析和挖掘，安全大数据分析重要性日益突显。根据 Gartner 研究显示，到 2015 年，10%的 IT 企业级安全产品功能将通过云服务提供，到 2017 年，全球基于云的安全服务市场产值将超过 40 亿美元。云计算、大数据技术的快速发展和应用也将促进信息安全行业的发展，并为基于云计算和大数据的安全产品和服务创造广阔的市场空间。

（二）本次非公开发行的目的

1、提升公司网络安全技术优势，深化公司战略布局

在公司成长过程中，技术创新和领先一直是公司的关键战略，公司持续加强产品研发和安全服务创新方面的投入，不断提升公司技术领先优势。“智慧安全防护体系”在公司原有安全云服务基础上，进一步提升安全云服务的大规模交付能力，以支持高效率的安全运营服务。“安全数据科学平台建设”通过对各类网络行为数据的记录、存储和分析，结合安全技术和防护经验，可以从更高的视野和角度、更广的维度上去发现异常、捕获威胁，实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对未来不断变化、日益增长的安全威胁。本次募集资金投资项目的成功实施，将是对公司现有主营业务和产品线的有力丰富与补充，可以极大提升公司的核心竞争力，帮助公司把握住包括云计算、大数据等先进技术变革带来的重大机遇，深化公司战略布局。

2、为行业客户提供更有针对性的安全解决方案，实现行业深耕

公司主要客户为运营商、政府、金融、能源、互联网、教育等领域的企业级用户。通过向客户提供差异化的产品和服务，公司一直走在行业创新发展的前列，是国内安全厂家中较早推出网络入侵防御系统、Web 应用防护系统等产品的创新型厂商，多项产品市场占有率位居国内前列。移动互联、云计算、下一代互联网和大数据等新兴技术的蓬勃发展，极大地促进了信息的共享，同时也给运营商、金融、能源、互联网等行业的信息安全带来更大挑战。近年来基于开放性网络的攻击入侵已经成为信息安全领域的一个关注焦点。本次募集资金投资项目的成功

实施，可以利用公司多年来在客户行业的深厚积累，结合客户行业大数据，进一步提升公司安全云服务的大规模交付能力，为行业客户提供更有针对性的安全解决方案，实现行业深耕。

3、紧跟行业趋势，提高公司盈利能力

公司在多年的发展中已经具备了较为完善、技术领先的产品线和解决方案，随着云计算、大数据、移动互联网、物联网等重大技术变革的逐步演化，安全行业也正在发生变革，公司需要建设并实施符合行业趋势的研发项目以保持技术领先地位，适应不断发展变革的产业环境。通过本次非公开发行，公司可以充实资本实力，推动业务模式创新，拓展业务规模和市场空间，巩固和提升公司的行业地位和核心竞争力，进一步提升公司价值，更好地回报上市公司全体股东。

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范围为符合中国证监会规定的证券投资基金管理公司、证券公司、保险机构投资者、信托投资公司、财务公司、合格境外机构投资者，以及符合中国证监会规定的其他法人、自然人或其他合格的投资者，发行对象不超过 5 名。最终发行对象将在本次发行申请获得中国证监会的核准文件后，根据发行对象申购报价情况，由董事会与本次发行的保荐机构（主承销商）协商确定。

目前公司尚未确定发行对象，因而无法确定发行对象与公司的关系。发行对象与公司之间的关系将在发行结束后公告的发行情况报告书中予以披露。

四、发行方案概要

（一）非公开发行股票的种类与面值

本次发行的股票为境内上市的人民币普通股（A 股），每股面值为人民币 1.00 元。

（二）发行方式及发行时间

本次发行的股票全部采取向特定对象非公开发行的方式，在中国证监会核准

后六个月内选择适当时机向特定对象发行。

（三）发行数量

本次非公开发行股票数量为不超过 2,600 万股。最终发行数量由董事会根据股东大会的授权、中国证监会相关规定及实际认购情况与保荐人（主承销商）协商确定。

若公司股票在关于本次非公开发行的董事会决议公告日至发行日期间有除权、除息行为，本次非公开发行的股票数量将做相应调整。

（四）发行对象

本次非公开发行股票的发行对象范围为符合中国证监会规定的证券投资基金管理公司、证券公司、保险机构投资者、信托投资公司、财务公司、合格境外机构投资者，以及符合中国证监会规定的其他法人、自然人或其他合格的投资者，发行对象不超过 5 名。最终发行对象将在本次发行申请获得中国证监会的核准文件后，根据发行对象申购报价情况，由董事会与本次发行的保荐机构（主承销商）协商确定。

（五）发行价格及定价原则

本次发行的定价基准日为发行期首日，定价原则为：发行价格不低于发行期首日前二十个交易日公司股票均价的百分之九十，或不低于发行期首日前一个交易日公司股票均价的百分之九十。最终发行价格由董事会根据股东大会授权在本次非公开发行申请获得中国证监会的核准文件后，按照中国证监会相关规则，根据竞价结果与本次发行的保荐人（主承销商）协商确定。

若发行人股票在定价基准日至发行日期间发生派息/现金分红、送红股、资本公积金转增股本等除权除息事项，本次非公开发行价格将按以下办法作相应调整：

假设调整前发行价格为 P0，每股送股或转增股本数为 N，每股派息/现金分红为 D，调整后发行价格为 P1，则：

派息/现金分红：P1=P0-D；

送股或转增股本：P1=P0/(1+N)；

两项同时进行：P1=(P0-D)/(1+N)。

（六）认购方式

发行对象应符合法律、法规规定的条件，均以人民币现金方式、以相同价格认购本次非公开发行股票。

（七）限售期

本次非公开发行股票完成后，特定投资者所认购的股份限售期需符合《创业板上市公司证券发行管理暂行办法》和中国证监会、深圳证券交易所等监管部门的相关规定：（1）发行价格不低于发行期首日前一个交易日公司股票均价的，本次发行股份自发行结束之日起可上市交易；（2）发行价格低于发行期首日前二十个交易日公司股票均价但不低于百分之九十，或者发行价格低于发行期首日前一个交易日公司股票均价但不低于百分之九十的，本次发行股份自发行结束之日起十二个月内不得上市交易。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。

（八）本次发行前公司滚存未分配利润的归属

本次非公开发行股票前公司的滚存未分配利润由本次发行完成后新老股东共享。

（九）上市地点

本次非公开发行股票将在深圳证券交易所上市交易。

（十）本次发行决议的有效期限

本次非公开发行决议的有效期为股东大会审议通过之日起 12 个月。

五、本次非公开发行的募集资金投向

公司本次发行募集资金总额不超过 80,121.58 万元，扣除发行费用后用于以下募投项目：

序号	项目名称	项目总投资额（万元）	拟投入募集资金数额（万元）
1	智慧安全防护体系建设项目	70,584.68	39,488.41
2	安全数据科学平台建设项目	30,045.42	20,633.17
3	补充流动资金	20,000.00	20,000.00
合计		**120,630.10**	**80,121.58**

若实际募集资金净额低于拟投入募集资金额，公司将根据实际募集资金净额，按照项目的轻重缓急等情况，调整并最终决定募集资金的具体投资项目、优先顺序及各项目的具体投资额，不足部分由公司以自有资金或自筹资金方式解决。在本次非公开发行募集资金到位之前，公司将根据项目进度的实际情况以自有资金或自筹资金先行投入，并在募集资金到位之后予以置换。

六、本次发行是否构成关联交易

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份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。

七、本次发行是否导致公司控制权发生变化

截至 2016 年 3 月 31 日，公司持股 5%以上的主要股东分别为 Investor AB Limited、联想投资有限公司、沈继业和雷岩投资有限公司，分别持有公司 20.77%、13.01%、12.43%和 9.73%的股份，公司无实际控制人。本次发行后，公司的股权结构将发生变化，本次非公开发行股票数量不超过 2,600 万股，本次非公开发行股票的数量占发行后总股本的比例不超过 6.67%。发行完成后，公司无控股股东和实际控制人的情况不会发生变化。

八、本次非公开发行的审批程序

公司第二届董事会第二十三次会议、2016 年第一次临时股东大会、第二届董事会第二十八次会议、第二届董事会第三十次会议、第二届董事会第三十四次会议审议通过了本次非公开发行股票相关事项。

根据《证券法》、《公司法》、《管理办法》等相关法律、法规和规范性文件的规定，公司已向中国证监会进行了申报。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发行和上市事宜，完成本次非公开发行股票全部呈报批准程序。上述呈报事项能否获得相关批准或核准，以及获得相关批准或核准的时间，均存在不确定性，提请广大投资者注意审批风险。

第二节 董事会关于本次募集资金使用的可行性分析

一、本次募集资金使用计划

公司本次发行募集资金总额不超过 80,121.58 万元，扣除发行费用后用于以下项目：

序号	项目名称	项目总投资额（万元）	拟投入募集资金数额（万元）
1	智慧安全防护体系建设项目	70,584.68	39,488.41
2	安全数据科学平台建设项目	30,045.42	20,633.17
3	补充流动资金	20,000.00	20,000.00
合计		**120,630.10**	**80,121.58**

若实际募集资金净额低于拟投入募集资金额，公司将根据实际募集资金净额，按照项目的轻重缓急等情况，调整并最终决定募集资金的具体投资项目、优先顺序及各项目的具体投资额，不足部分由公司以自有资金或自筹资金方式解决。在本次非公开发行募集资金到位之前，公司将根据项目进度的实际情况以自有资金或自筹资金先行投入，并在募集资金到位之后予以置换。

二、智慧安全防护体系建设项目—提供云安全产品和服务

（一）项目投资概算

该项目投资总额为 70,584.68 万元，拟募集资金 39,488.41 万元，项目投资概算如下：

编号	投资项目	投资金额（万元）	拟投入募集资金（万元）
1	固定资产投资	3,449.00	3,449.00
2	无形资产投资	149.00	149.00
3	实施费用	52,986.68	33,090.41
4	流动资金	14,000.00	2,800.00
合计		**70,584.68**	**39,488.41**

（二）项目实施主体

项目实施主体是绿盟科技。

（三）项目建设总体目标

本项目的建设包括云端能力和服务平台建设、客户侧部署解决方案两大领域。云端能力和服务平台是公司拟建设的安全技术运营平台，公司将负责云端能力和服务平台的建设和运营，并将协助客户完成客户侧部署解决方案的建设和实施。通过募投项目的建设和实施，公司可向客户同时提供云安全产品和服务。公司除可提供传统安全产品、服务外，还增强了云端安全服务能力，并可向客户提供基于安全产品结合安全云服务的一站式安全解决方案，使公司具备更强的市场竞争力和盈利能力。

1、云端能力和服务平台建设

（1）云基础设施建设，包括数据中心和计算存储等基础设施的建设；

（2）云运营平台建设，包括基础设施子平台、运行环境子平台、云服务子平台的建设；

（3）安全应用商店建设，包括用户管理、应用管理、应用编排、用户订阅订购管理等；

（4）云协同交付系统建设，包括智能升级系统、移动管家系统、线上线下协同系统等建设。

2、客户侧部署解决方案建设

（1）基于软件定义架构的控制平台，主要完成各种智能安全设备的管理、服务编排等功能；

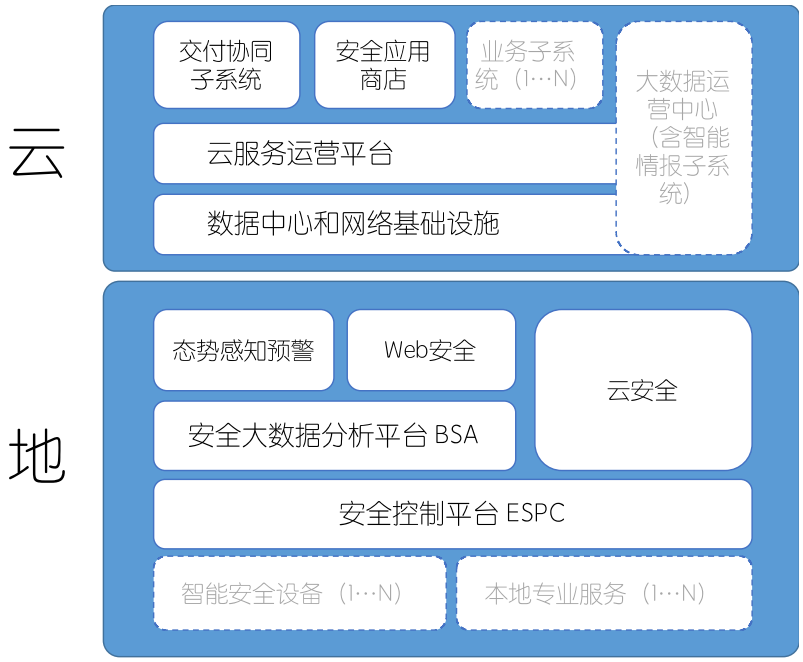
（2）安全大数据分析平台，主要完成安全数据收集和处理、大数据分析、数据可视化等功能；

（3）态势感知预警解决方案，主要完成安全威胁从感知到理解和预警的模型实现，以及相应的可视化；

（4）云安全解决方案，主要完成典型私有云和公有云环境下的网络安全解决方案相关的开发和测试；

（5）基于云运营的 Web 安全解决方案，主要完成用于 Web 网站的抗拒绝服务、Web 入侵检测防护，以及与云端系统的协同。

本项目的体系架构如下图所示：



（四）项目建设具体内容

1、云端能力和服务平台建设

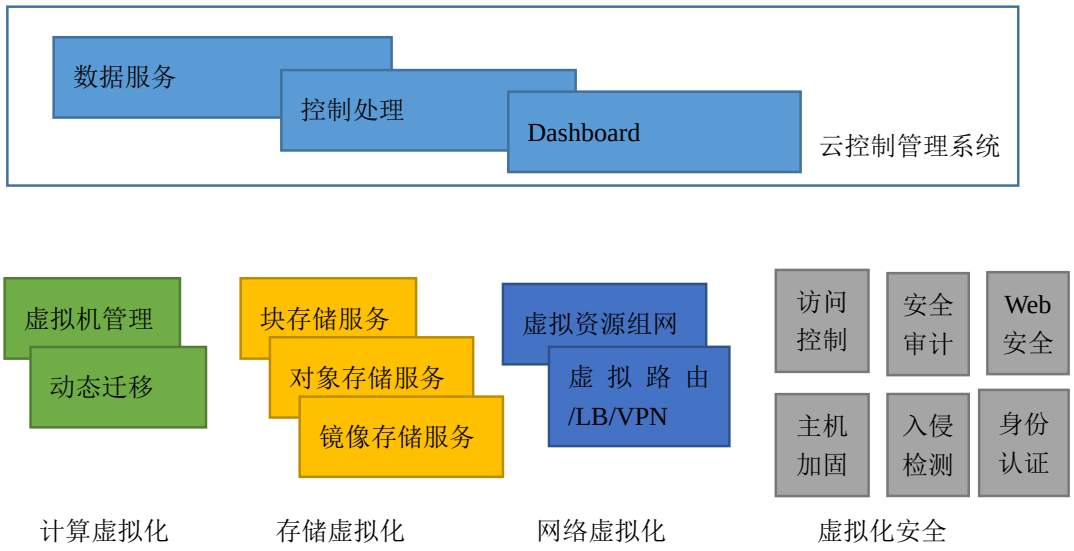
公司云端系统包括提供底层计算、存储和网络支持的基础设施系统，以及利用这些基础设施组件的中间件服务和运营平台。借助这些能力，安全业务部门可构建各种安全云服务，如安全应用商店、各类云端安全应用以及结合升级、协作和移动应用的协同交付体系等。

（1）云基础设施

云端基础设施包括数据中心和机房建设，以及云计算虚拟化系统的部署。

云计算虚拟化系统采用业界流行的设施虚拟化框架 Openstack，构建了完整的计算虚拟化、存储虚拟化和网络虚拟化组件，并针对每个组件的功能和业务需

求，部署了相应的虚拟化安全机制，如下图所示：



在计算虚拟化方面，采用了 Nova 组件，可支持租户虚拟机业务的自助开通，虚拟机可热迁移到其他计算节点，提供兼容 Amazon EC2 的接口。

在存储虚拟化方面，可支持不同操作系统的多种不同镜像。使用 Ceph 分布式存储技术，可提供面向对象存储的服务，兼容 Amazon S3 接口；可提供块存储服务，弹性地增加虚拟机磁盘挂载功能。

在网络虚拟化方面，提供灵活的虚拟资源进行组网，支持如 VLAN、GRE、VxLAN 等技术组建虚拟的覆盖网络，并支持虚拟路由器、负载均衡和 VPN 等服务。

在虚拟化安全方面，提供全生命周期的应用身份认证和授权机制，面向虚拟机和物理节点的主机加固机制，以及其他如访问控制、安全审计、入侵检测和 Web 安全等安全手段，对虚拟化系统中的虚拟资源或应用组件进行全方位的安全防护。

（2）云运营平台

云运营平台构建在云基础设施之上，在体系架构上可以纵向划分成基础设施/运行环境子平台和云服务子平台两部分。

运行环境为上层的云服务提供了所需的计算、数据和控制支撑，如分布式队列和调度服务、负载均衡和分布式存储服务、分布式计算服务，以及其他服务。

弹性的基础设施/运行环境子平台可实现安全业务快速部署和上线、业务规模的快速调整，使系统具备敏捷的安全事件响应能力和大规模的安全分析能力。为了实现云端海量数据的安全分析，运行环境子平台的分布式计算的模块需满足海量数据处理能力需求，建设由分布式日志收集系统、分布式消息系统、分布式实时流式计算、分布式文件系统、分布式批量计算系统、分布式数据查询引擎构成的分布式计算体系结构。

云服务子平台主要包括面向客户侧安全产品的设备托管服务模块，以及云端用户自助的安全云服务模块，所提供服务以统一的形式进行封装，以面向用户的Web 门户、移动应用等形态对外交付。

除了设备托管和云服务模块外，云服务子平台包括若干基础模块，例如客户管理、服务管理、事件管理、报表管理、设备管理和订单管理，向客户提供统一、高效的基础服务功能。一些新型的基础模块，如在线支付、支持第三方账户的客户管理，结合有强烈客户需求的安全业务，可有效地将业务拓展到更多传统行业和渠道外的中小型企业，大大降低边际成本。

（3）安全应用商店

安全应用商店可将云端安全应用通过互联网推送到客户侧，并完成应用的部署和启动；运行时可自动从云端获得更新和推送，实现应用和安全策略的升级。与传统的安全交付模式不同，这种模式无需长达数月的采购流程，可大大缩短安全能力从公司到客户的转移时间。

安全应用商店的功能主要包括：

1）云端安全应用管理，如应用存储、下载、创建和删除等；

2）用户管理，如用户注册、更新和认证等；

3）支持应用编排的部署模式，即多种应用可以叠加同时实现多种业务，如编排调度、任务增加、删除和执行等；

4）用户端应用管理，包括向云端注册、认证和购买，应用的搜索、更新、部署和操作。

（4）云协同交付系统

当云端具备了强大的海量数据分析和处理的能力，这些安全能力可以通过应用商店快速分发，可以辅助专家进行安全快速响应；同时，公司专家团队的分析报告、检测结果和响应方案，从云端和移动端的入口，将多方位、无缝的推送给广大的客户，有助于在小时级时间尺度防护绝大多数的恶意攻击。

云协同交付系统除了安全应用商店和云端平台支撑外，还包括以下部分：

1）智能升级系统

除了安全应用可通过安全应用商店进行在线升级外，具有安全检测和防护功能的安全设备也需要具备可更新的能力，特别是引擎、规则库等组件的更新，可使其性能和功能得到增强，具备快速响应的能力。

每次安全设备在新版本发布后，智能升级系统可推送给客户侧设备可用的更新，当设备完成更新后，其防护效率、防护性能都能得到进一步提升。

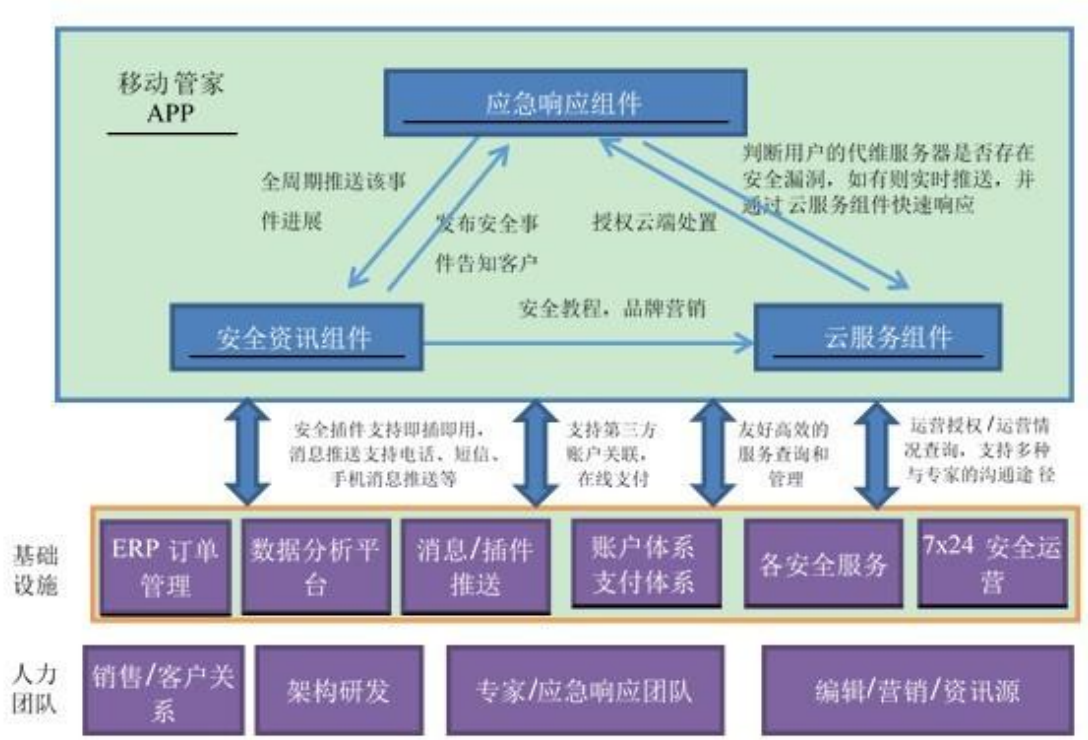
当突发安全事件发生时，经过专家团队协同配合后，智能升级系统可确认用户设备的规则或安全策略是否需要更新，如是则通知用户，并向设备推送相应的新规则和策略，在较短时间内即可对大规模的安全设备更新防护机制，从而抵御短时间内爆发的恶意攻击。

2）移动管家应用

与 Web 门户相比，移动端应用具有两个优点：第一，随时随地在线，推送及时。对于不能 7x24 小时在线的运维人员（如中小型企业）可及时获知其资产安全性，并授权公司云端运营人员进行维护；第二，视图直观，用户界面美观，方便操作。移动安全管家应用具有三大功能：安全资讯、应急响应端点、便携式的云服务。安全资讯包括安全事件介绍、安全教程，以及其他业界相关的安全新闻，可体现公司的经验积累、行业视野和态势感知能力。应急响应包括在安全事件出现后对客户的提醒功能，以及在安全事件全周期中给客户提供及时、透明的

展现功能。安全云服务可让客户在移动设备上随时方便地查看自己服务的状态和安全运营状态，可通过简单配置启用安全服务的功能；并可使公司云端运营团队通过用户授权进行安全运营。

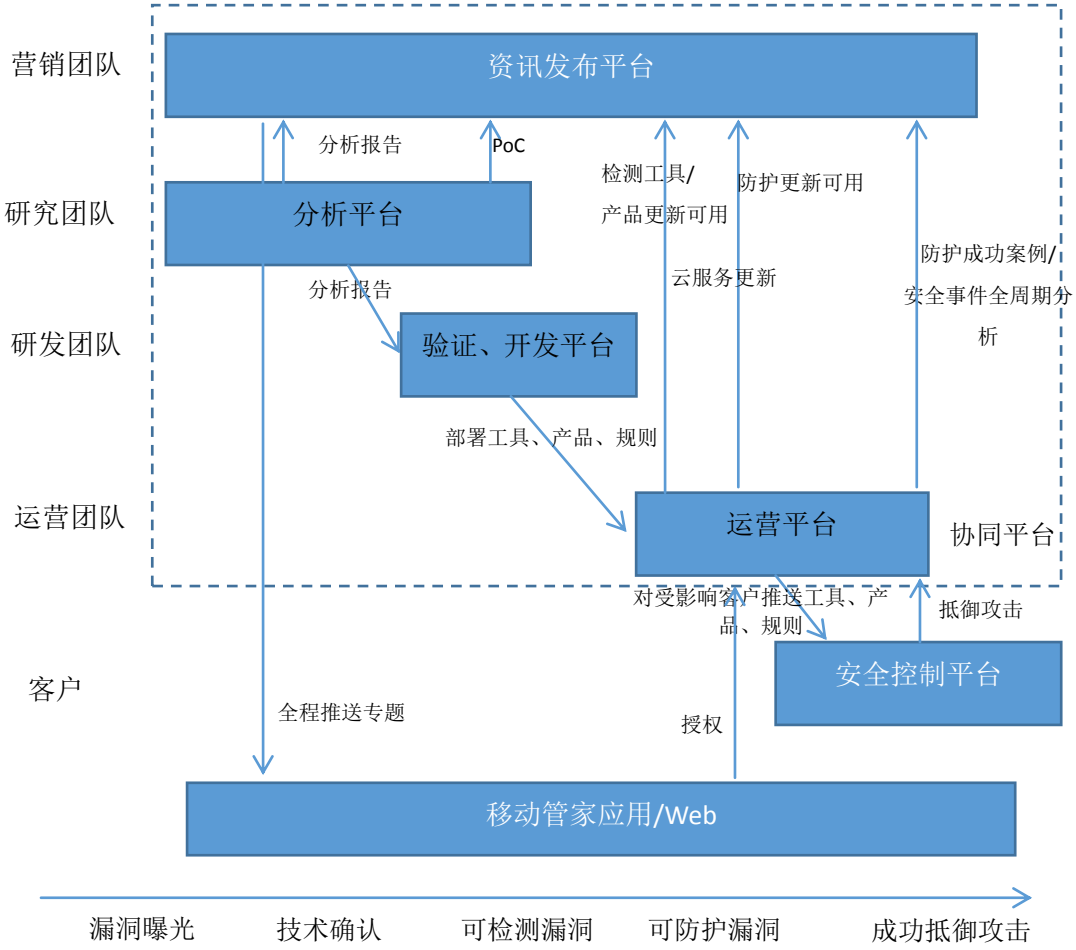
安全资讯组件、应急响应组件与云服务组件还可相互配合以使得服务更能体现价值。



3）线上线下协同系统

快速、完整的应急响应体系离不开安全专家团队，包括分析安全事件的研究团队，开发、测试和部署针对该事件的检测/防护规则、产品的研发运营团队，与客户对接的工程、销售和客服团队，面向市场宣传的营销团队。线上线下协同系统可将人力资源快速有序组织。

线上线下协同系统包括若干子系统，如资讯发布平台、研究分析平台、验证开发平台、运营平台和客户侧的安全控制平台。



安全事件的处理生命周期可分为：首先某漏洞被披露，然后研究人员从技术上确认可行，接着研发团队开发出相应的检测和防护工具、产品和规则更新，部署到运营平台。运营平台通过推送、通知等手段将上述更新部署到客户侧的安全控制平台，或直接将云服务升级，通过 Web 门户或移动管家应用使用户获知整个防护过程和当前状态。

线上线下协同系统可整合上述多个平台的功能，相关人员可在子平台上完成自己相应的工作，该系统可自动化地分配任务、协调资源和通知相关人员。

同时，通过开放的设计，使得整个协同平台可灵活调整，根据 Web 安全事件、移动端安全事件和高级持续威胁（APT）等典型场景设计相关的处理流程。并且在每次安全事件之后，分析整体的响应流程，根据事件特点进行调整，以缩短整体响应时间，改善客户体验。

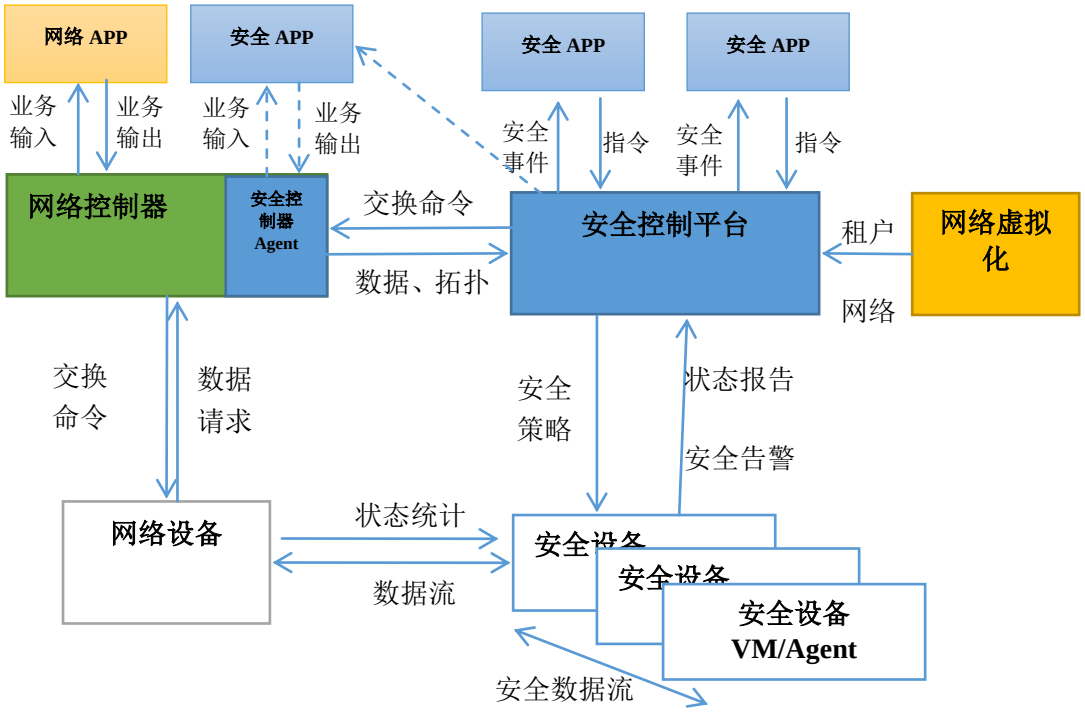
2、客户侧部署解决方案建设

虽然不同行业客户的应用场景和网络环境各不相同，但大部分客户的共性安全需求包括三点：保障 Web 应用的安全性与可用性；保护网络边界，及时发现网络中的异常行为，确保数据不被泄露；以及通过可管理可编排的自动化安全平台进行高效运营。针对这三种需求，需建设基于软件定义架构的控制平台、安全大数据分析平台，以及态势感知预警解决方案。

公司部分企业客户已经部署或计划在短期内部署云计算系统，但云计算系统安全一直困扰着企业的 IT 部门管理者和运营团队，并在很大程度上制约了关键业务的云化。云环境的底层支撑技术、网络部署方案也大不相同，故需根据客户的环境和安全需求，建设部署在客户侧的云安全解决方案或由公司运营的 Web 安全解决方案。

（1）基于软件定义架构的控制平台

公司构建了基于 Openstack 的软件定义安全的体系，其架构如下图所示。



1）安全控制平台架构

安全控制平台主要由若干核心模块和面向不同场景的定制模块组成。每个模

块可部署在不同节点，避免了单点失效的问题，且与安全控制平台内部的模块或外部的安全或网络主体进行交互，生成的数据保存到缓存或数据库中。

其中核心模块包含：

①分布式事件调度模块（Event Scheduler）：接受各模块注册事件，将需处理的事件分发给相应模块，触发事件处理机制；

②应用管理模块（APP Manager）：管理北向的安全应用信息，接受应用的可疑数据订阅，推送满足条件的可疑数据；

③设备管理模块（Device Manager）：管理南向的设备应用信息，在策略解析等模块中提供所需的安全设备；

④策略解析模块（Policy Resolver）：将安全 APP 的抽象策略分解为网络设备或安全设备可执行的具体命令。

此外，还有一些重要的定制模块（如数据收集、可疑数据监控和命令推送等）在不同场景有特定的实现。例如，在 OpenFlow/SDN 的环境中，还包括流表获取（Flow Polling）、流量监控（Flow Monitor）和流指令推送（Flow Pusher）三个模块。在具体场景中，可能会存在额外的安全模块，例如日志记录和分析等，工作流也可能存在一些差异。但每个模块实现自己的功能，相对独立。

2）安全设备资源池管理

若安全架构部署于云计算环境中，则可通过虚拟化技术实现安全设备的资源池化，并通过控制平台与 SDN 控制器的协同，对流量按需调度，实现服务链（Service Chain）。同时，根据应用所需的安全需求可以从资源池中找到相应资源，而无需关心安全设备的物理部署和如何布线划区。

3）安全设备重构

软件定义安全架构具有控制与数据分离的特点，使得安全设备可重构。

当安全设备完成资源池化后，对上层应用呈现出的只有安全能力，表现形式是向安全控制平台提供应用接口 API。当安全控制平台实现了策略管理、安全分析、安全状态机和各类知识库和资产库，上层应用就可以基于这些公共中间件实

现各种功能，调用安全设备的应用接口，满足客户的不同需求。

安全设备可重构使得安全设备的设计逻辑简单、处理高效，不容易出现影响系统稳定性的错误，同时避免了很多定制开发工作。

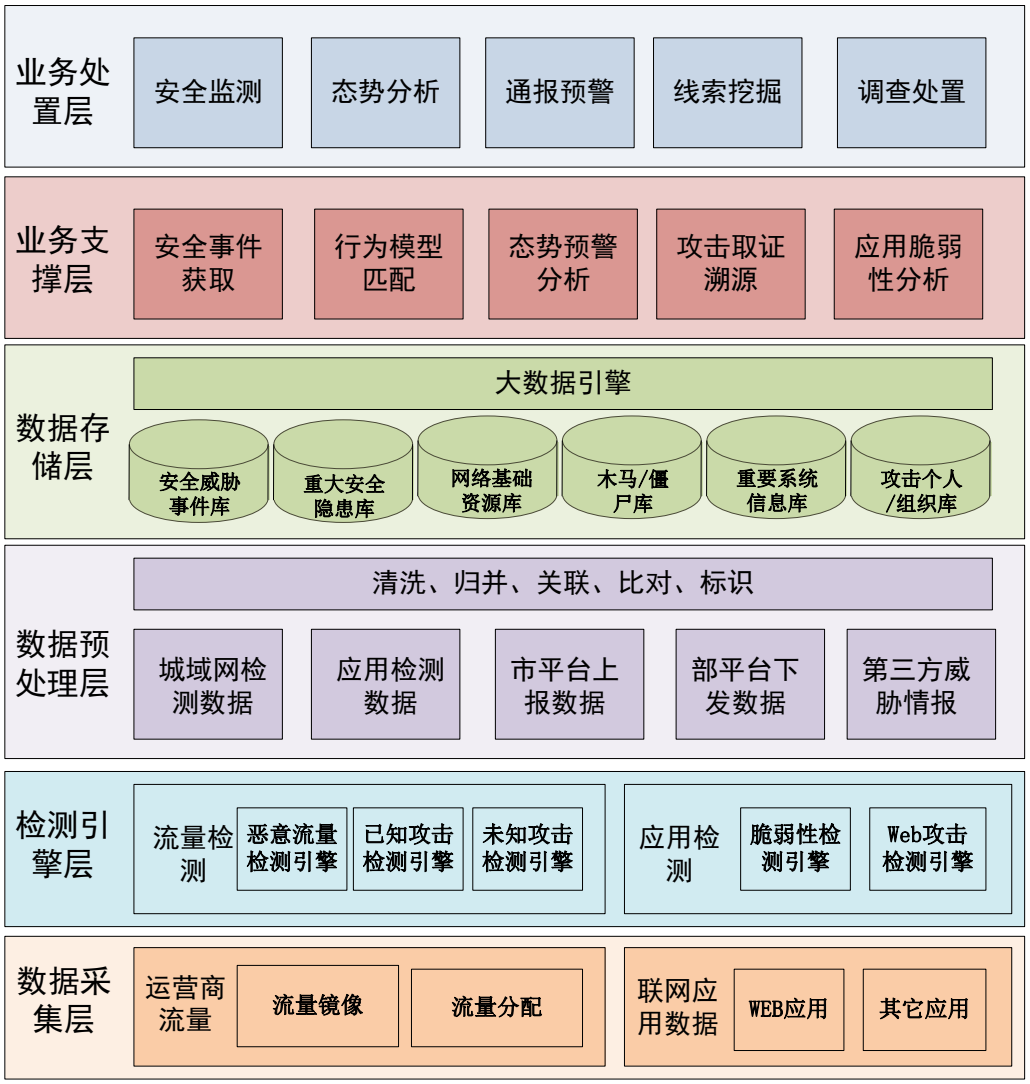
（2）安全大数据分析平台

网络中的所有攻击行为都会在网络或者系统中留有痕迹，且以多种方式表现，如网络流量、系统日志、安全设备告警等，故可通过较为复杂的安全分析方法，及时发现并阻止隐秘在企业内部的安全威胁。

安全大数据分析平台是基于云计算、分布式大数据处理等技术的新一代安全运营和支撑平台。该平台的建设使传统安全硬件产品通过虚拟化以软件或服务形式提供可定制、可管理的安全服务。安全大数据处理、分析和运营形成巨大的网络安全资源池，使安全产品可定制、信息可关联、数据可分析、攻击事件可溯源、威胁态势可展现。

（3）态势感知预警解决方案

态势感知预警解决方案系统总体架构自下向上可以分为数据采集层、检测引擎层、数据预处理层、数据存储层、业务支撑层和业务处置层等 6 个功能层，如下图所示：



其中，数据采集层是系统的基础数据源，包括了运营系统的出口流量镜像数据和互联网重要信息系统的数据。检测引擎层主要实现对基础数据的安全检测，包括对互联网流量的检测和对重要信息系统的检测。数据预处理层主要实现对攻击和脆弱性数据的预处理，为下一步数据应用打下基础。数据存储层主要实现对业务支撑的数据支持，一方面对预处理过的有效数据按照业务需求进行分类存储，另一方面通过大数据引擎为业务支撑提供数据存取和分析服务。业务支撑层主要实现对预警监控系统中各种安全应用的业务支撑。业务处置层主要实现预警监测工作中的各种业务流程。

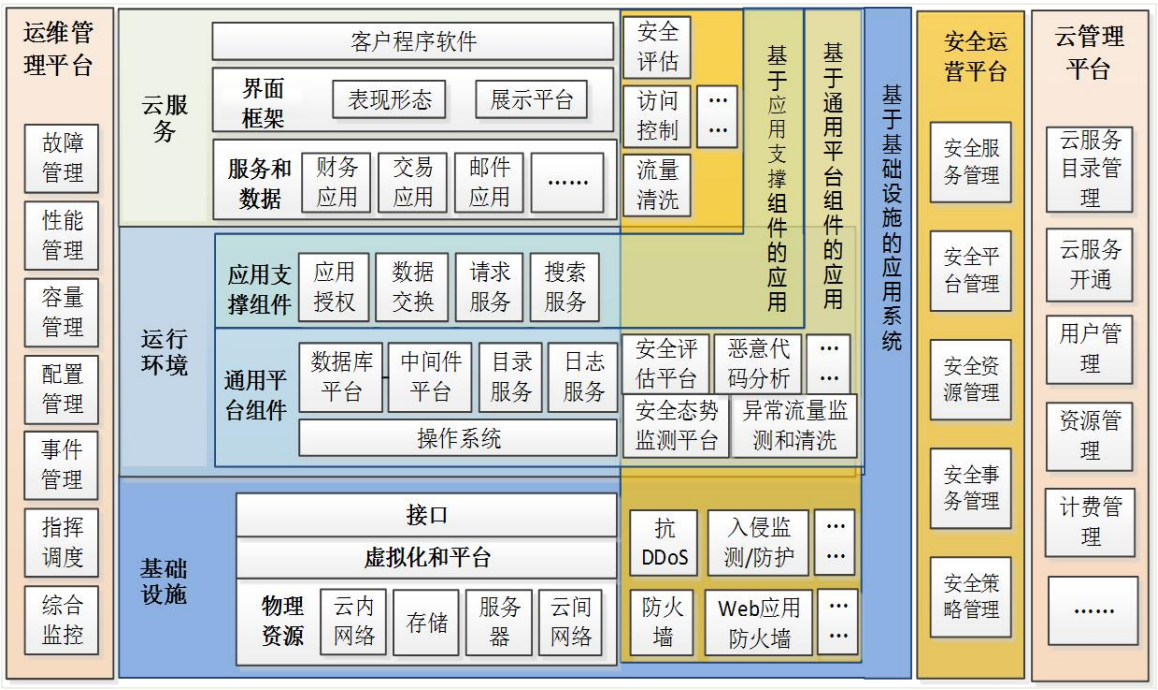
（4）云安全解决方案

在云计算系统的部署过程中，传统大企业因为数据安全、信任问题和合规性要求通常会部署私有云或混合云，而中小企业出于降低开支的考虑，越来越多迁

移到公有云上，搭建 Web 站点或虚拟私有云。

公司云安全解决方案充分挖掘云环境中的客户安全需求，综合考虑各种云环境中的网络拓扑和组网技术。云安全解决方案包括安全技术防护体系和安全技术服务。

安全技术防护体系的架构如下：



安全技术防护体系以用户风险为导向，将云计算系统网络划分为若干物理或虚拟安全域，在每个安全域内部部署安全机制，如网络异常流量分析、抗拒绝服务攻击、内网入侵检测、访问控制、Web 应用防护等。

安全技术服务包括虚拟化脆弱性评估、主机加固等，可有效解决客户在虚拟化环境中遇到的安全问题。

（5）基于云运营的 Web 安全解决方案

为帮助企业解决基于互联网的 Web 服务安全问题并节省购置多种安全设备的高昂费用，公司提出了基于云运营的 Web 安全解决方案。

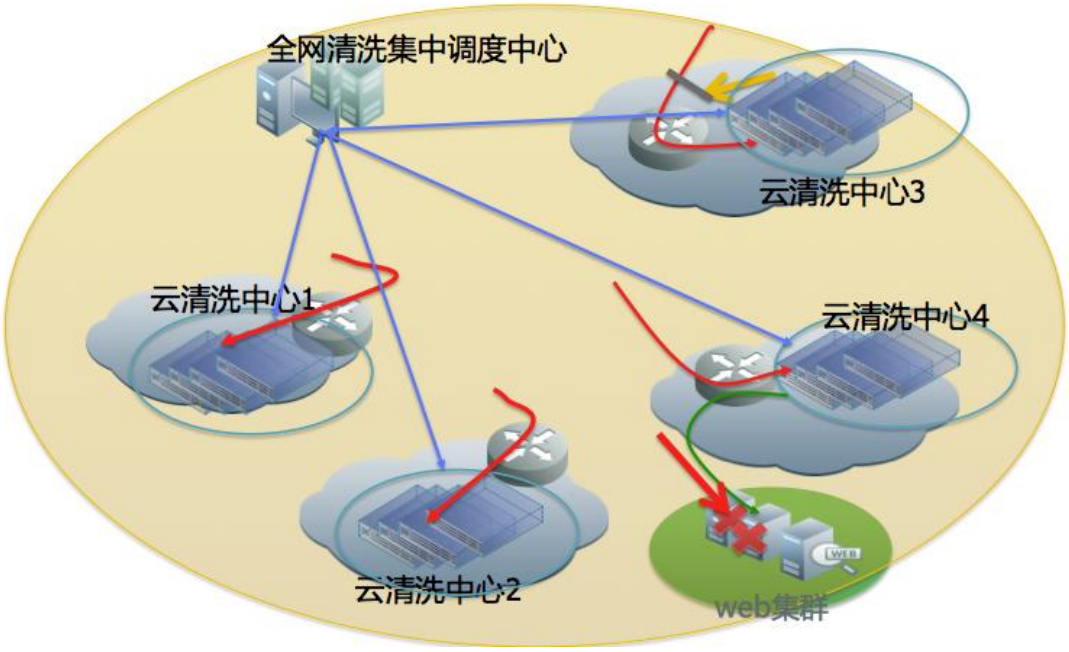
1）DDoS 云清洗中心建设方案

目前，国内运营商正在与安全厂商合作建设面向骨干网的清洗中心，以抵抗

大容量的攻击。公司拟通过与运营商、云服务商、数据中心合作的方式，建立容量为 100G+的独立云清洗中心和容量为 10G-40G 的分布式云清洗中心。

2）云清洗中心调度和集中运营方案

基于拟建立的分布式 DDoS 清洗中心，公司提出了云清洗中心调度和集中运营方案，如下图所示。当被攻击业务侧的清洗中心的容量无法应对大容量攻击时，可以基于主要攻击源的地理位置，调度各主要攻击源最近的多个分布式清洗中心协同清洗，可以大大提升整个云清洗中心的容量。



随着清洗中心的逐步建立和业务的发展，公司需要不断完善云安全服务相关的集中运营、攻击调度、大数据分析、API 等技术及客户自服务系统等平台。

（五）项目的服务对象和服务内容

公司主要客户为运营商、政府、金融、能源、互联网、教育等行业的企业级客户。本项目的服务对象包括公司目前现有客户群体。本项目的实施将使公司不但有能力为信息基础设施、超大型企业集团和大中型企业机构提供全新的安全产品和服务，还能为上述行业及上述行业以外的数量广泛的中小企业客户提供符合其信息安全保障需求的安全产品和服务，从而巩固并扩大公司客户群体和服务对象，提升公司盈利能力。

智慧安全防护体系建设项目提供的主要产品或服务情况如下：

序号	产品或服务	功能描述	与现有产品技术的关系	说明
1	基于软件定义架构的控制平台软件	一款新的软件产品，可以提升公司产品的智能性及协同效应。提供安全设备管理、安全应用开发接口、应用商店的支持、云中能力的集成互动等功能。	现有产品升级+新产品研发	基于现有软件产品企业安全中心进行研发升级和新产品研发
2	客户侧安全大数据分析平台软件	一款新的软件产品，用于处理安全大数据，具有更强的数据收集、分析、可视化能力。可以提供安全设备日志收集、安全大数据分析、安全应用开发接口应用商店的支持、云中能力的集成互动等功能。	现有产品升级+新产品研发	基于现有软件产品企业安全中心的日志管理模块，使用大数据技术进行重构和功能增强、新产品研发
3	安全威胁情报服务	一款新的安全云服务，帮助客户提升应急、运维、分析等安全管理水平。具体包括安全产品信誉输入、实时调查取证、攻击预测、安全态势展示等服务。	新产品研发	在现有威胁分析系统、网络入侵防御/检测系统、Web 应用防火墙等安全产品和网站照料等服务基础上开发的新服务
4	基于云运营的 Web 安全服务	一款新的安全云服务，主要向政府、大中型企业用户销售云端交付的抗拒绝服务和 Web 防入侵的云服务。主要提供用于 Web 网站的抗拒绝服务、Web 防入侵的检测和防护，以及与云端系统的协同。	现有产品、服务升级+新产品研发	在现有网站安全监测系统产品、网站照料服务的基础上进行升级、新产品研发
5	态势感知预警解决方案	一种集成多种安全软件、安全云服务的解决方案，满足政府、运营商、能源等行业用户不同应用场景需求。主要完成安全威胁的感知、理解和预警功能，以及相应的可视化功能。	现有产品、服务升级	利用安全控制平台软件、安全大数据分析平台软件，在远程安全评估系统、Web 应用漏洞扫描系统、网络入侵防御/检测系统、Web 应用防火墙等产品基础上进行集成、研发升级
6	云计算安全解决方案	一种集成多种安全软件、安全云服务的解决方案，主要完成云环境下网络安全产品	现有产品、服务升级	利用基于软件定义架构的控制平台软件，在现有远程安全评估系统、网络

		和服务的部署、开通、计费、运营支持等功能。主要进行多种公有云和私有云环境下的兼容性开发测试，开发相应的管理和运营接口，完成并提供打包方案。		入侵防御/检测系统、Web 应用防火墙、网络流量分析系统等产品的基础上进行虚拟化，以及云计算环境的适配和增强

目前，本项目尚处于建设初期且未达产。本项目提供的信息安全产品和服务主要是在公司现有安全产品和服务基础上，融合云计算、大数据、软件定义架构等技术进行的持续研发升级和新产品研发，在技术实现、市场销售等方面具备可行性。公司现有安全产品和安全服务的销售情况良好，公司近三年主营业务收入呈持续增长态势，预期本募投项目将取得良好的经济效益。

（六）项目必要性分析

1、网络安全、云计算、大数据已成为国家战略，本项目的建设和实施符合国家产业政策和行业发展规划

随着各国信息化建设的推进，网络安全已经上升到社会安全、经济安全甚至国家安全层面，成为国家安全、经济实力等综合国力的重要组成部分。为全面提高我国信息安全防护能力，保障重点基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化健康发展，《工业转型升级规划（2011-2015年）》指出，必须加快发展信息安全技术、产品及服务，构建自主可控的信息安全体系和架构，完善信息安全产品及服务认证制度，提高对国家安全和重大信息系统安全的支撑能力。

工信部发布的《软件和信息技术服务业“十二五”发展规划》中将信息安全软件与服务作为软件和信息技术服务业的发展重点，指出要加强网络安全、数据安全、可信计算、安全测评等关键技术的研发与产业化，重点发展安全可靠的安全基础产品、电子认证公共服务平台、网络与边界安全产品、信息安全支撑工具等，发展云计算、物联网等新一代信息技术应用环境下的安全技术产品。

近年来，我国不断推出支持和鼓励大数据产业发展的相关政策。2014 年 3 月，中央《政府工作报告》提出设立新兴产业创业创新平台，在大数据等方面赶超先进，引领未来产业发展。2015 年 6 月，《国务院办公厅关于运用大数据加

强对市场主体服务和监管的若干意见》要求以社会信用体系建设和政府信息公开、数据开放为抓手，充分运用大数据、云计算等现代信息技术，提高政府服务水平。2015 年 8 月，《国务院关于印发促进大数据发展行动纲要的通知》要求健全大数据安全保障体系，加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究。2015 年 10 月，《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》对大数据战略、利用大数据技术作出明确部署，指出“实施国家大数据战略，推进数据资源开放共享”、“运用大数据技术，提高经济运行信息及时性和准确性”。本项目的建设和实施符合国家产业政策和行业发展规划。

2、本项目的建设和实施有助于保持并加强公司技术领先优势，提升公司盈利能力

网络安全具备很强的对抗特征，安全防护体系、防护技术和产品、防护策略规则等都需要持续、及时升级换代，以应对不断演化的新型网络威胁。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”或“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，例如需要更加敏捷和开放的架构、需要更加友好的社区协同、需要支持威胁情报的共享。安全防护体系的变革进一步要求安全产品和服务进行变革，安全云和客户侧安全防护设备分工合作，在安全决策智能性、协同性和运营效率方面实现明显的提升。另外，网络安全整体防护体系涉及的技术越来越复杂多样，有效安全防护和安全应急响应所需的资源也越来越庞大。例如，作为安全对抗的基础，安全威胁情报的收集、分析处理、分发消费、评价反馈等各个环节都需要大量专业知识和系统建设，即使对规模化的专业团队也非常具有挑战性。由于威胁响应时效性的要求，7x24 小时的全天候高质量安全监控和运营非常关键，一般客户自行组建规模化的专业安全团队和搭建安全系统平台的成本将非常昂贵，这为专业化的安全运营服务提供了广阔的市场空间。

近年来，公司不断探索新型的在线服务业务模式并取得一定成果。本项目将

在公司原有安全云服务基础上，基于云计算和大数据技术的安全平台架构，致力于实现“云”（线上环境或云端）、“地”（线下环境或客户侧）、“人”（专家团队）、“机”（安全防护设备）协同体系，最大限度发挥安全云系统、客户侧安全设备、专家团队等的协同效应，进一步提升公司在云端的威胁情报感知能力、基于线上线下互动的安全应急响应能力、安全云服务的大规模交付能力，保证安全云业务的先进性和丰富性，并支持应急响应设备的在线升级改造，以提供高效率的安全运营服务，从而保持公司技术领先地位并提升公司盈利能力，使公司适应不断变革演化中的产业环境。

（七）项目可行性分析

1、智慧安全防护体系具有广阔的市场空间

信息安全行业正在进行变革，为了应对新的安全威胁，传统的基于安全硬件、相对封闭、大量手工孤立运维的安全防护技术架构，正在转向以智慧安全防护体系为代表的新架构。

一方面，安全防护系统越来越复杂，产生的海量日志和信息对采用传统 SQL 数据库架构的安全信息和事件管理系统的性能产生了巨大的挑战，迫使安全厂商开始采用大数据技术改造相关安全系统，大幅提高其数据处理能力和响应时效性。另一方面，随着攻防技术的发展，传统基于攻击手法的检测和防护模型遇到了挑战，安全厂商开始研究并采用异常检测、威胁情报和信誉库等技术来变革防护体系，带动了安全数据分析和安全数据可视化技术的发展，以优化安全决策、提高安全运维效率。上述安全业务应具备对海量数据的快速处理能力以及多种安全场景下的建模和自动化处理能力。

信息安全行业的以上变革必将带来大量的新市场需求，为公司业绩的持续增长创造有利条件。

2、公司在智慧安全防护体系相关领域具有丰富的技术积累和运营经验

本项目成功实施的关键技术包括安全攻防、云安全、大数据、安全运营服务等核心技术。

自公司成立以来，围绕安全攻防的研究、以及以攻防为主要特色的安全产品和技术服务一直是公司“技术领先”的核心内容。近年来，在以对抗高级持续威胁（APT）为主要方向的研究开发方面，公司研究开发了威胁分析中心（TAC）新产品以及下一代威胁防护（NGTP）解决方案，涵盖了动态检测、静态检测、信誉云、多引擎智能分析、威胁情报分享等先进攻防技术领域，并在政府、金融、运营商、能源等行业具有高等级安全需求的客户中成功部署，得到了市场认可。

公司自2009年启动云安全相关研究工作，公司是国际权威组织云安全联盟（CSA）在中国的第一个企业会员，参与和领导了一系列相关技术标准研究开发项目，已向客户提供基于云计算技术的网站照料服务。公司在2012年开展软件定义网络（SDN）相关技术的跟踪研究，成功提出和实现了业界领先的软件定义安全的框架，并开始对主要产品进行架构升级、虚拟化研发。公司还与多家业界领先的云计算服务提供商、云计算解决方案提供商展开了多层面的技术和商业合作。公司在云安全领域的技术积累将成为本项目成功实施的重要基础。

在关键技术环节之外，安全运营体系的高效与成熟也是本项目成功实施的关键。公司已开展多年网站照料服务，并成功推出了基于 OpenStack 架构的企业私有云、具备先进云安全服务架构的公司云端系统。这些云安全运营经验以及和多家业界领先的云计算提供商的合作，都将为本项目的成功实施提供保障。

（八）项目经济效益分析

经测算，本项目从实现收入年度起，预期可实现年均销售收入 56,366.67 万元，年均净利润 18,196.63 万元，静态回收期（含建设期）为 4.02 年，内部收益率为 39.59%。

通过本项目的建设和实施，公司可紧跟信息安全行业发展趋势，将十余年研发与创新过程中已经积累的核心技术、产品和服务用大数据、云计算、虚拟化等设计理念予以完善和改造，有助于彻底解决孤立防护带来的应急响应时间较长的缺点，为企业级客户提供及时、全天候的安全防护，在有效提升客户体验与粘性的同时推广公司新的产品和服务，稳步提升公司现有的盈利能力。另外，本项目有助于公司将服务于企业级客户的信息安全防护能力向更多客户推广。公司通过云端服务以较低的边际成本将安全服务提供给成本敏感的中小微企业，可以扩大

公司客户群体，拓展新的盈利渠道。

三、安全数据科学平台建设项目—提供基于大数据技术的云安全服务

（一）项目投资概算

该项目投资总额为 30,045.42 万元，拟募集资金 20,633.17 万元，项目投资概算如下：

编号	投资项目	投资金额（万元）	拟投入募集资金（万元）
1	固定资产投资	7,166.00	7,166.00
2	无形资产投资	189.00	189.00
3	实施费用	16,690.42	12,078.17
4	流动资金	6,000.00	1,200.00
合计		**30,045.42**	**20,633.17**

（二）项目实施主体

项目实施主体是绿盟科技。

（三）项目建设总体目标

安全数据科学平台建设项目是公司拟建设的安全大数据技术和运营平台，公司将负责平台的建设和运营。基于上述平台的建设和运营，公司可向客户提供基于大数据技术的云安全服务，全面提升现有安全服务的安全防护效果，还能够利用安全数据和大数据技术、通过云服务的方式为客户提供更多有价值的综合分析安全服务，从而为客户提供更好的安全保障。

本项目的总体建设目标是基于大数据平台技术，建立公司自身的安全大数据体系和标准，开发和实践安全大数据的商业价值与社会价值。

本项目计划建设的安全数据科学平台具有以下特点：

1、高性能、大容量：平台提供大容量安全数据的收集、处理、分析、存储功能，满足安全大数据的研究和使用需求。

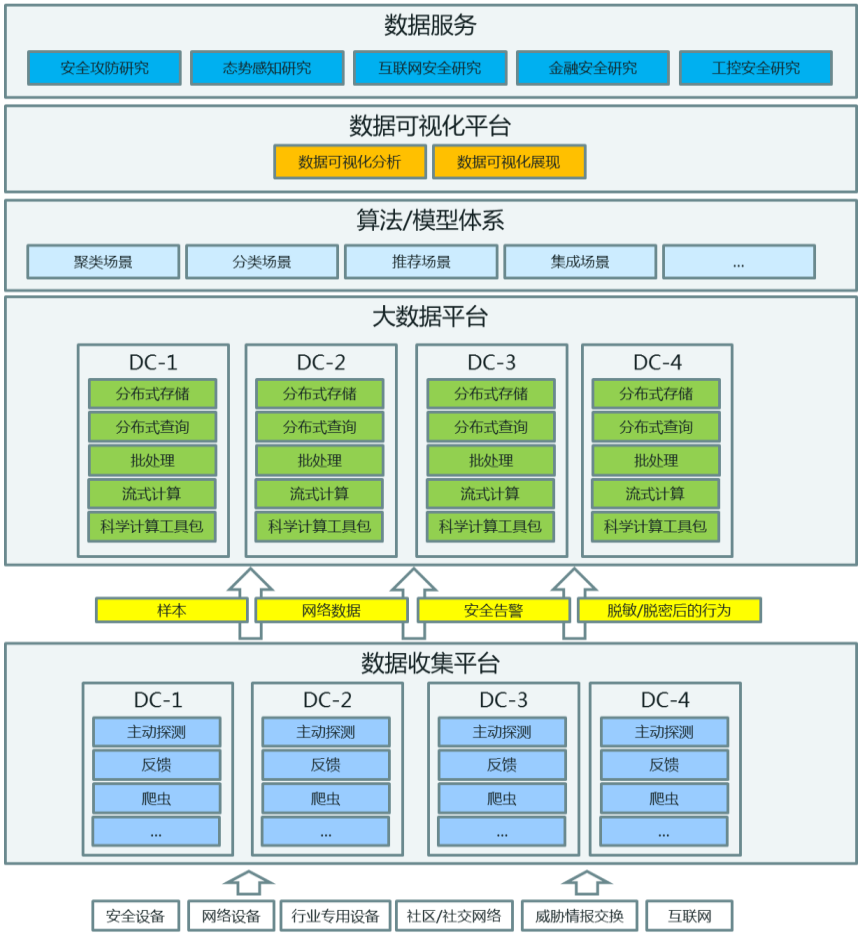
2、技术先进：使用先进的分布式计算、分布式存储等技术，紧跟互联网技术发展趋势，满足不同领域的应用需求。

3、易扩展：具有优秀的扩展能力，满足不断增大的服务需求。

4、高可用性：通过云计算技术，能够快速恢复故障系统，确保业务的连续性。

5、安全：依托公司在安全领域十几年的积累和持续创新，对大数据提供全面的安全保障。

本项目的体系架构如下图所示：



（四）项目建设具体内容

1、数据收集平台

数据收集平台通过主动探测、爬虫、反馈、威胁情况交换等多种方式，收集

安全设备、网络设备、行业专用设备、客户环境、社区/社交网络、互联网等多种环境下经授权的基础数据。基础数据经过清洗、脱密、脱敏等各种数据预处理，最终变成样本、网络数据、安全告警、行为等各种有意义的数据，并被传递、保存到大数据平台。

2、大数据平台

大数据平台需要满足大容量的数据处理能力需求。公司将基于当前业内流行的 Spark 生态圈技术，建设由分布式日志收集系统、实时流式计算系统、批量计算系统、分布式文件系统、分布式数据查询引擎、科学计算工具包等构成的大数据平台。

3、算法/模型体系

本项目面向国家经济建设和社会发展的重大需求，面向企业客户的安全大数据实际需求，将研究大数据技术在具体业务场景的应用，并开发典型的模型算法，形成自己独特的面向安全大数据的模型算法体系。例如，针对攻击识别场景，可以基于“神经网络”、“深度学习”等典型分类算法，配合“逻辑回归方法”、“贝叶斯方法”、“随机森林”、“支持向量机”等辅助算法，研发出不同攻击类型的识别模型。

4、数据可视化平台

数据可视化平台主要提供数据可视化分析、数据可视化展现的功能。

（1）数据可视化分析

依靠大数据平台和算法/模型体系，将需要分析的数据量降低到安全专家团队可以应对和处理的级别，在此基础上，结合可视化分析，使安全专家团队能够快速、有效地对安全事件进行响应，发现潜在的安全风险。

（2）数据可视化展现

数据可视化展现功能旨在将网络安全威胁可视化，从而有效帮助使用者理解复杂的安全问题和各种安全事件之间的内在联系。

5、数据服务

数据服务综合了大数据分析能力、算法模型能力、可视化能力、前沿攻防研究及十余年的安全经验积累，针对公司内外部提供不同层次的数据服务。

针对公司内部，安全数据科学平台可为公司的各个产品团队提供通用数据服务、算法模型支撑服务、特定行业深度安全解决方案，实现安全设备运维过程、安全服务过程的闭环管理，从而使用户具备小时级的安全应急响应能力。

针对外部客户，面向国家相关部门、行业主管机构等用户，安全数据科学平台提供的数据服务可以支持用户开展网络安全工作，使用户能够实时掌握安全态势，及时了解重要信息系统的安全威胁；面向安全厂商、安全服务商等用户，安全数据科学平台可提供威胁情报交互、推送服务；面向广大公众用户，安全数据科学平台可提供开放数据服务，帮助用户直观了解当前的网络安全威胁水平，提高用户网络安全意识，从而实践安全大数据的商业价值与社会价值。

安全数据科学平台数据服务主要进行以下研究：

（1）安全攻防研究

安全攻防研究通过安全大数据的挖掘、分析，对攻击的蛛丝马迹进行洞察，针对攻击链进行建模分析，挖掘、分析涵盖威胁尝试进入企业阶段、在企业内部进行扩散阶段、信息盗取阶段等，可显著提高企业对高级持续威胁（APT）的检测和防护能力。安全攻防研究通过建立数据模型，运用回归、聚类、语义模型等机器学习算法，提高不同攻防场景下的攻击检测的准确性和性能，是传统的基于特征的检测方法的重要补充。

（2）态势感知研究

态势感知研究致力于掌握实时网络安全态势，及时应对重要信息系统相关网络安全威胁风险，通过对漏洞、病毒、木马、网络攻击情况、主干网流量情况、DNS 数据进行挖掘分析，发现网络安全事件线索，及时通报预警重大网络安全威胁，帮助用户尽早发现安全威胁，提高用户安全防护能力。

（3）金融安全研究

金融安全研究旨在通过学术理论与行业实践的紧密结合，满足金融行业信息

安全的要求，开展针对金融应用的安全风险分析、安全应用的设计与开发、安全防御技术的研究，并提出符合金融行业需求的信息安全防控体系方案。

（4）工控安全研究

为适应工业控制领域全方位、智能化的发展趋势以及网络信息安全技术发展需求，工控安全研究致力于解决各行各业在工业控制过程中的信息安全问题。工控安全研究计划在仿真环境下建设攻防演练安全防护方案，并进行通信网、通信规约、工控终端安全性等的研究工作。

（5）互联网安全研究

互联网安全研究致力于从互联网的物理安全、网络拓扑结构安全、系统安全、应用系统安全和互联网管理安全等方面对互联网的安全体系进行全面的研究。涉及互联网信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是互联网安全研究的对象。

（五）项目的服务对象和服务内容

公司主要客户为运营商、政府、金融、能源、互联网、教育等行业的企业级客户。本项目的服务对象包括公司目前现有客户群体。本项目的实施将使公司不但有能力为信息基础设施、超大型企业集团和大中型企业机构提供全新的安全产品和服务，还能为上述行业及上述行业以外的数量广泛的中小企业客户提供符合其信息安全保障需求的安全产品和服务，从而巩固并扩大公司客户群体和服务对象，提升公司盈利能力。

安全数据科学平台建设项目提供的主要产品或服务情况如下：

序号	产品或服务	功能描述	与现有产品技术的关系	说明
1	网站安全监测服务	一款新的托管式云服务，向客户提供 7x24 小时远程网站安全监测服务，使客户能够第一时间了解网站的风险状况并获得绿盟专业团队的安全解决建议。可降低公司服务的交付成本、提高交付时效性。	现有服务升级	以现有网站照料服务、远程安全评估系统等产品为基础，结合云计算、大数据等技术进行研发升级
2	网站安	一款新的托管式云服务，向客户提	现有服务升	以现有 Web 应用防火墙、

	全防护服务	供 7x24 小时 Web 应用安全防护，最大限度提高 Web 网站安全防护能力。可降低公司服务的交付成本、提高交付时效性。	级+新产品研发	抗拒绝服务产品为基础；融合云计算、大数据等技术进行升级、新产品研发
3	漏洞自助扫描服务	一款新的云服务，提供自助式系统漏洞扫描、网站漏洞扫描、安全配置检查服务。可降低公司服务的交付成本、提高交付时效性。通过登录云端或通过手机应用，用户能够随时获知最新安全事件信息，并及时做出安全响应。	现有服务升级+新产品研发	基于现有远程安全评估系统、Web 应用漏洞扫描系统、自助扫描服务进行升级、新产品研发
4	移动应用安全检测服务	一款新的云服务，针对企业 APP 应用及其对应系统进行安全分析。在移动应用的测试阶段和运维阶段介入，通过上线前的整体应用安全测试和上线后随版本更新的增量测试，保证客户应用在整个生命周期中良好的安全性。可降低公司服务的交付成本、提高交付时效性、提升公司知识积累。	现有产品云服务化	以现有安全评估技术为基础，利用云计算技术对现有产品进行升级、改造
5	反垃圾邮件服务	一套将反恶意攻击、反垃圾邮件、病毒过滤、敏感信息智能过滤、邮件归档等功能进行整合的电子邮件安全云服务，帮助客户建立便于管理、不断升级的邮件病毒和垃圾邮件云监控防御体系，实现对邮件系统更加全面有效的保护。	现有产品云服务化	基于公司现有安全邮件网关产品，利用云计算技术对现有软件产品进行服务化升级、改造
6	软件行为分析服务	一款新的云服务，为安全研究和运维人员提供各类软件的安全性研究、分析、评估、测试等服务。	现有产品云服务化	以公司现有的威胁分析中心产品、安全评估服务为基础，利用云计算、大数据技术进行升级、改造
7	云清洗服务	一款新的云服务，提供防护海量复杂攻击的云端 DDoS 攻击防护。对客户的网络流量进行 7x24 小时全天候监控，并对攻击做出即时安全响应，有效保障客户业务安全性和连续性。	现有产品云服务化	以公司现有 ADS（抗拒绝服务）、NTA 等产品为基础；利用云计算、大数据技术进行升级、改造

目前，本项目尚处于建设初期且未达产。本项目提供的信息安全服务主要是在公司现有安全产品和服务基础上，融合云计算、大数据、软件定义架构等技术进行的持续研发升级和新产品研发，在技术实现、市场销售等方面具备可行性。公司现有安全产品和安全服务的销售情况良好，公司近三年主营业务收入呈持续

增长态势，预期本募投项目将取得良好的经济效益。

（六）项目必要性分析

1、本项目的建设和实施可以加强公司在网络安全检测、攻防对抗方面的技术优势

数据驱动安全是大数据时代安全行业的共识。通过对各类网络行为数据的记录、存储和分析，并结合安全技术和防护经验，可以使安全厂商从更广的维度发现异常、捕获威胁，实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对未来不断变化、日益频繁的安全攻击。

本项目通过大数据技术、挖掘、建模技术，帮助安全专家团队更好地洞察威胁，利用回归、聚类、语义模型等经典机器学习算法，使用分布式集群提供强大的计算、分析能力，更好地解决传统安全检测体系下难以处理的问题。例如，通过综合分析 DNS 日志、流量日志、各种攻击日志、用户访问行为等数据，实现攻击溯源、获取黑客信息；通过算法、模型补充传统的基于特征的检测方法，提高攻击检测的准确性和性能。

2、本项目的建设和实施可以为行业客户提供更有针对性的安全解决方案

公司主要客户为运营商、政府、金融、能源、互联网、教育等行业的企业级客户。上述行业都是涉及国计民生的重要领域或行业，其网络安全威胁防护重要性日益突显。例如，能源、高端制造等行业大量使用工业控制技术，部分工控设备存在信息安全漏洞和隐患，成为安全防护体系的薄弱环节，外部安全风险极易通过网络进入企业内部工业控制系统，进而形成巨大的安全风险。移动互联、云计算、下一代互联网和大数据等新兴技术的蓬勃发展，极大地促进了信息的共享，改变着经济社会的运行方式，但同时也给整个金融行业的信息安全带来更大挑战。

本项目的建设和实施可以为公司行业客户提供更有针对性的安全解决方案。例如，通过对工业控制领域的深刻研究，从海量数据中发现潜在安全风险，将危险消灭于无形；利用多年来在金融行业的深厚积累，结合金融行业大数据，可以从金融认证体系、征信体系、在线支付安全等方面提供有效的解决方案和建议等。

3、本项目的建设和实施可以提升公司的盈利能力，丰富公司的产品和服务类型

本项目在市场层面上可以为公司带来良好收益，依托大数据及数据挖掘、建模技术，既可以显著提高公司安全产品的检测能力，降低产品成本，又能通过云端大数据与客户侧设备、环境的联动，提高客户的安全防护效果，增强公司产品和服务的竞争力，从而提升公司盈利能力。本项目还可以丰富公司的产品和服务类型，如知识产权授权使用、提供分析预测报告、提供数据接口服务等。

（七）项目可行性分析

1、本项目的建设和实施符合国家产业政策和行业发展规划

2014 年 3 月，中央《政府工作报告》提出设立新兴产业创业创新平台，在大数据等方面赶超先进，引领未来产业发展。2015 年 6 月，《国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见》要求以社会信用体系建设和政府信息公开、数据开放为抓手，充分运用大数据、云计算等现代信息技术，提高政府服务水平。2015 年 8 月，《国务院关于印发促进大数据发展行动纲要的通知》要求健全大数据安全保障体系，加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究。2015 年 10 月，《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》，对大数据战略、利用大数据技术作出明确部署，指出“实施国家大数据战略，推进数据资源开放共享”、“运用大数据技术，提高经济运行信息及时性和准确性”。本项目的建设和实施符合国家产业政策和行业发展规划。

2、公司已经具备建设和实施本项目的技术基础

本项目的实施需要运用分布式存储、分布式计算，模型、算法研究，安全攻防等技术。其中，对于分布式存储、分布式计算技术，公司通过多年探索，已在相关领域拥有深入的积累，核心技术主要通过自主研发的方式取得；对于模型、算法研究技术，公司目前已经具备开展相关工作的基础，将主要通过自主培养和外部招聘相结合的方式，补充模型、算法方面的专业人员；对于安全攻防技术，公司是国内领先的、具有核心竞争力的企业级网络安全解决方案供应商，具有十

余年安全攻防方面的技术积累，能够满足本项目在安全领域方面的技术需求。

（八）项目经济效益分析

经测算，本项目从实现收入年度起，预期可实现年均销售收入 20,466.67 万元，年均净利润 6,104.25 万元，静态回收期（含建设期）为 4.22 年，内部收益率为 33.95%。

通过本项目的建设和实施，公司可深入挖掘大数据、分布式计算等技术在公司多年来积累的安全攻防、安全检测等核心技术、产品和服务上的应用。一方面，安全大数据平台的高性能、大容量、易扩展、高可用性，可以提升预测和处理能力，有效降低公司和客户的防护成本，提升客户体验和粘性。另一方面，安全大数据平台的海量数据、先进技术、开放接口等，也丰富了公司向客户提供的产品和服务类型，进而提高公司盈利能力。

四、补充流动资金

公司拟使用本次募集资金中的 20,000 万元用于补充流动资金，增强资金实力以支持公司的长远发展战略。

公司属于轻资产公司，公司资产主要由流动资产构成，非流动资产比例较小，轻资产的特点决定了公司日常经营较多涉及现金支付，折旧、摊销类的非现金支出相对较少，为了维持及拓展业务经营，须保有较多流动资金，对货币资金的需求较大。

公司所处行业为技术、人才密集型行业，强大的技术研发能力是公司保持市场竞争力与行业地位的关键。伴随本次募投项目的推进，未来公司将持续关注信息安全领域的最新科研成果在产业界的应用，加大高端人才培养与引进力度，拓展产学研合作范围，维持公司的核心技术优势。因此，公司需要持续高投入研发经费，公司运营资金需求会不断增长。

综上，公司拟使用部分募集资金补充流动资金，有利于增强公司资金实力，降低业务经营中的财务风险，促进公司研发实力的提升，支持公司的长远发展战略。

五、本次非公开发行对公司经营管理和财务状况的影响

（一）本次发行对公司经营管理的影响

本次非公开发行募投项目符合信息安全行业发展趋势。随着募投项目的建设和实施，公司将打造基于云计算和大数据技术的智慧安全防护体系，建立公司自身的安全大数据体系和标准，有利于公司加快实施发展战略，不断提高安全攻防、云计算、大数据等关键核心技术的水平，提升管理效率与人才聚集能力，满足不同客户差异化需求，增强公司综合竞争力，进一步巩固和增强公司在信息安全行业的优势地位。

（二）本次发行对公司财务状况的影响

本次发行募集资金投资项目实施后，公司资产规模、净资产规模将大幅增加，资本实力进一步提升，营运资金更加充裕，资本结构更加稳健，财务风险降低，偿债能力和后续融资能力增强。

六、募集资金投资项目涉及报批事项情况

本次非公开发行募集资金投资项目已经完成了相关报批备案手续。

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与资产整合计划，公司章程、股东结构、高管人员结构、业务结构的变化情况

（一）公司业务与资产整合计划

本次发行完成后，公司的主营业务保持不变，不存在与本次非公开发行相关的业务与资产整合计划。

（二）本次发行对公司章程的影响

本次发行完成后，公司注册资本和股本相应增加，公司将按照发行的实际情况完成对《公司章程》中与注册资本、股本等有关条款的修改，并办理工商变更登记。

（三）本次发行对股权结构的影响

公司无控股股东和实际控制人。公司股权较为分散，单个股东持股比例均未超过公司总股本 30%。截至 2016 年 3 月 31 日，公司持股 5%以上的主要股东分别为 Investor AB Limited、联想投资有限公司、沈继业和雷岩投资有限公司，分别持有公司 20.77%、13.01%、12.43%和 9.73%的股份。

本次发行后，公司的股权结构将发生变化，本次非公开发行股票数量不超过 2,600 万股，本次非公开发行股票的数量占发行后总股本的比例不超过 6.67%。发行完成后，公司无控股股东和实际控制人的情况不会发生变化。

（四）本次发行对高级管理人员结构的影响

公司不会因本次发行对高级管理人员进行调整，高级管理人员结构不会因本次发行而发生重大变动。

（五）对业务结构的影响

本次发行完成后，公司的业务结构不会因本次发行而发生重大变化。

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）本次发行对公司财务状况的影响

本次发行募集资金到位后，公司总资产和净资产将大幅增加，公司的资产负债率将会明显下降，公司财务状况得到改善，有利于降低公司财务风险。

（二）本次发行对公司盈利能力的影响

本次募集资金投资项目的盈利方式如下：1、向客户提供基于云计算、大数据技术的新一代信息安全软件产品、服务和解决方案，通过产品、服务和解决方案的销售实现盈利；2、通过募投项目的建设和实施，公司可在巩固现有客户的基础上扩大客户群体，从而增加新的盈利；3、通过提升现有安全产品的安全防护效果从而提升产品的市场竞争力，提升产品销量并实现盈利；4、通过募投项目的建设和实施，公司将具备向客户提供一系列新型安全即服务的能力，包括安全数据分析服务、威胁情报相关服务、风险评估和管理相关服务、Web 安全和抗拒绝服务相关等服务。

本次发行募集资金到位后，由于本次发行后公司净资产和总股本将有所增加，因此短期内可能会导致净资产收益率、每股收益等财务指标出现一定程度的下降。但随着公司业务规模的不断扩大、募集资金投资项目效益的实现，公司的盈利能力将会进一步增强。

（三）本次发行对公司现金流量的影响

本次非公开发行股票由特定对象以现金认购，待募集资金到位时，公司筹资活动现金流入将大幅增加。随着募投项目的逐步实施，用于募投项目投资活动现金的流出将相应增加。募投项目完成后，未来经营活动现金流入将逐步增加。

三、公司与主要股东及其关联人之间的业务关系、管理关系、同业竞争及关联交易等变化情况

公司与主要股东及其关联人之间的业务关系、管理关系、同业竞争及关联交易均不会因本次发行而发生变化。

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

本次发行完成后，公司不会存在资金、资产被主要股东及其关联人占用的情形，亦不会存在公司为主要股东及其关联人进行违规担保的情形。

五、公司负债结构是否合理，是否存在通过本次发行大量增加负债（包括或有负债）的情况，是否存在负债比例过低、财务成本不合理的情况

公司负债结构较为合理，本次募集资金到位后，将有效降低公司资产负债率，进一步提升抗风险能力；本次发行不会增加公司负债（包括或有负债），不存在发行后公司负债比例过低、财务成本不合理的情况。

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，除本预案提供的其他各项资料外，应特别认真考虑下述各项风险因素：

一、募集资金运用风险

（一）募集资金投资项目无法及时、充分实施的风险

公司对本次募集资金投资项目已经过慎重考虑、科学决策，募集资金计划投资项目的实施，有利于公司主营业务的发展，进一步提升公司的可持续盈利能力和核心竞争力。公司已就本次募集资金投资项目进行了充分的市场调研与严格的可行性论证，但是由于项目实施可能受国内外宏观经济状况、国家产业政策、政府宏观调控等诸多因素的影响，如上述因素发生不可预见的负面变化，本次募集资金投资项目将面临无法及时、充分实施的风险。

（二）市场开拓的风险

虽然信息安全行业具有良好的发展前景，市场潜力巨大，但是公司仍将面临较强的市场竞争压力。如果公司不能采取有效措施进行市场开拓，则公司可能无法将公司的产品、服务和技术转化为效益，从而无法取得相应市场份额，这将对公司发展产生不利影响。

（三）募投项目经济效益无法达到预期的风险

本次非公开发行募集资金投资项目经过了严格的科学论证，符合国家产业政策和行业发展趋势，具备良好的发展前景。但未来募集资金投资项目的实施过程、建设速度、运营成本、市场价格等可能与预测情况存在差异，本次发行完成后，所募集资金若在短期内未能运用于发展各项业务，可能在一定时期内出现闲置情形，不能立即形成收入和利润；公司本次非公开发行募投项目投资金额相对较大，智慧安全防护体系建设项目计划投资 70,584.68 万元，安全数据科学平台建设项目计划投资 30,045.42 万元，募投项目计划投资总额为 100,630.10 万元，而募集

资金投资项目需有一定的建设周期，募集资金投资项目在短期内难以全部产生效益；按照募集资金使用计划，所投入的固定资产、无形资产将在一定期限内计提折旧或摊销。募投项目投入建设前三年预计产生的固定资产折旧、无形资产摊销及项目其他成本费用的支出分别为 12,767.17 万元、30,285.38 万元和 40,965.14 万元，如募投项目不能产生预期收益，将对公司未来经营业绩产生不利影响，并导致公司净资产收益率和每股收益等盈利指标下降。因此，本次非公开发行的募集资金投资项目存在不能实现预期收益的风险。

二、本次非公开发行股票的审批风险

本次非公开发行股票尚需满足多项条件方可完成，包括但不限于中国证监会对本次非公开发行的核准。上述事项能否获得相关核准以及公司取得相关核准的时间存在一定的不确定性，因而本次非公开发行面临审批的风险。

三、管理风险

本次募集资金规模总体较大，随着募集资金的到位和公司业务的发展，公司资产规模和业务规模都将进一步扩大。为进一步满足公司发展需求，提升公司管理水平，公司应在运营管理、技术研发、市场开拓、人才引进、内部控制等方面采取具体的应对措施。如果公司管理团队人才建设及经营管理水平不能适应公司规模快速扩张的需要，公司的组织架构和管理体制未能及时调整、完善，将影响公司的市场应变能力和持续发展能力，进而削弱公司的市场竞争力。公司存在规模迅速扩张引致的经营管理风险。

四、产业政策风险

信息安全行业属于国家鼓励发展的重点产业，国家有关产业政策的大力支持为国内信息安全行业的发展创造了良好的条件。目前，产业政策为公司信息安全业务提供了良好的发展机遇和空间。但若未来国家对相关产业政策进行调整，公司的相关业务将可能会受到影响。

五、前瞻性技术创新风险

虽然本次募集资金投资项目是在对市场需求进行充分调研基础上结合行业经验确定的，但前瞻性技术研发以及行业发展趋势的不确定性仍然可能导致本公司前瞻性技术创新偏离行业发展趋势、研发出的新技术和新产品不能巩固和加强已有的竞争优势、客户市场认知度下降。公司存在一定的前瞻性技术创新风险。

六、核心人员流失与技术失密的风险

公司持续保持市场竞争优势，在较大程度上依赖于公司拥有的核心技术及培养、积累的一大批核心技术人员。本次募集资金投资项目的实施需要公司进一步进行技术研发，核心技术人员稳定及核心技术保密对公司的发展尤为重要。

如果在技术和人才的市场竞争中，出现技术外泄或者核心技术人员流失情况，可能会在一定程度上影响公司的技术创新能力。

七、每股收益和净资产收益率摊薄的风险

公司本次非公开发行募集资金数额相对较大，募集资金使用需要一定的周期。若监管政策等投资环境发生不利变化，将影响募投项目的进度。募投项目建设完成后，效益的显现需要一个过程，效果难以在短期内全部释放。

本次发行完成后，股本规模及净资产规模将明显扩大，募集资金购置的资产将在一定期限内计提折旧或摊销，上述因素将对公司经营业绩构成一定压力，可能导致公司的每股收益和净资产收益率被摊薄。

八、股价波动带来损失的风险

公司的股票价格不仅取决于公司的经营业绩、发展战略，还受到国际和国内宏观经济形势、资本市场走势、市场心理和各类重大突发事件等多方面因素的影响。投资者在考虑投资公司股票时，应预计前述各类因素可能带来的投资风险，并作出谨慎判断。

九、本次非公开发行导致原股东分红减少、表决权被摊薄的风险

本次非公开发行完成后，公司总股本和归属母公司股东所有者权益将有所增加。由于募集资金投资项目的实施需要一定时间，在募投项目实施期间，股东回报还是主要通过现有业务实现，因此公司原股东面临因股本增加而减少分红的风险。同时，原股东也将面临表决权被摊薄的风险。

第五节 发行人的股利分配情况

一、公司的股利分配政策

为完善和健全公司科学、持续、稳定的利润分配政策和机制，积极回报股东，按照《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）的相关要求，公司第一届董事会第十八次会议、2013 年第一次临时股东大会修改了《公司章程》对利润分配政策的有关规定。公司第二届董事会第二十三次会议、2016 年第一次临时股东大会审议通过了关于修订公司股利分配政策并相应修改《公司章程》的议案，进一步完善了公司股利分配政策。

公司《公司章程》中的利润分配政策如下：

“第一百八十一条 公司实施积极的利润分配政策，重视对股东的合理投资回报并兼顾公司的可持续发展，利润分配政策保持连续性和稳定性，健全现金分红制度。公司实施利润分配，应当遵循以下规定：

（一）公司可采取现金、股票或股票与现金相结合的方式分配股利。公司应每年至少进行一次利润分配。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股利分配；

（二）公司董事会根据既定的利润分配政策制定利润分配方案，公司的利润分配政策由董事会提出，并经股东大会表决通过。公司研究论证股利分配政策及利润分配方案应当充分考虑独立董事、监事和中小股东的意见。利润分配方案中应当对留存的未分配利润使用计划进行说明，独立董事应当就利润分配方案的合理性发表独立意见。在审议公司利润分配方案的董事会、监事会议上，需经全体董事过半数同意，并分别经公司 1/2 以上独立董事、1/2 以上监事同意，方能提交公司股东大会审议。公司独立董事在股东大会召开前可向公司社会公众股股东征集其在股东大会上的投票权，独立董事行使上述投票权应当取得全体独立董事 1/2 以上同意。

股东大会对利润分配具体方案进行审议前，公司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，及时答复中小股东关心的问题。公司利润分配方案应当由出席股东大会的股东（包括股东代理人）所持表决权的 1/2 以上表决通过。公司在召开审议分红的股东大会上应为股东提供网络投票方式。

公司对留存的未分配利润使用计划作出调整时，应重新报经董事会、股东大会批准，并在相关提案中详细论证和说明调整的原因，独立董事应当对此发表独立意见。

（三） 公司的利润分配条件及分配比例如下：

1.公司当年经审计净利润为正数且符合《公司法》规定的分红条件下，公司应当优先采取现金方式分配股利，如无重大投资计划或重大现金支出等事项发生，以现金方式分配的利润不少于当年实现的可分配利润的 30%；如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 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、购买资产等交易累计支出达到或超过公司最近一期经审计净资产的 50%，或超过 5,000 万元；

（2）公司未来十二个月内拟对外投资、购买资产等交易累计支出达到或超过公司最近一期经审计总资产的 30%。

2.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，并按照本章程规定的程序，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，现金分红在本次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，现金分红在本次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，现金分红在本次利润分配中所占比例最低应达到 20%；

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。

3.公司在确定以股票方式分配利润的具体金额时，应充分考虑以股票方式分配利润后的总股本是否与公司目前的经营规模、盈利增长速度相适应，并考虑对未来债权融资成本的影响，以确保分配方案符合全体股东的整体利益。

（四）公司的利润分配政策不得随意变更。公司重视对投资者的合理投资回报，并保持连续性和稳定性，如现行政策与公司生产经营情况、投资规划和长期发展的需要确实发生冲突的，可以调整利润分配政策，调整后的利润分配政策不得违反中国证监会和深圳证券交易所的有关规定。公司董事会在利润分配政策的修改过程中，需与独立董事、监事充分讨论。在审议修改公司利润分配政策的董事会、监事会会议上，需经全体董事过半数同意，并分别经公司 2/3 以上独立董事、1/2 以上监事同意，方能提交公司股东大会审议。公司应以股东权益保护为出发点，在提交股东大会的议案中详细说明修改的原因，独立董事应当就利润分配方案修改的合理性发表独立意见。

公司利润分配政策的修改需提交公司股东大会审议，应当由出席股东大会的股东（包括股东代理人）所持表决权的 2/3 以上表决通过，且应当经出席股东大会的社会公众股东（包括股东代理人）过半数以上表决通过。股东大会表决时，应安排网络投票。公司独立董事可在股东大会召开前向公司社会公众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当取得全体独立董事 1/2 以上同意。

公司按照章程确定进行现金分红，如需对现金分红政策进行调整或者变更，应重新报经董事会、股东大会批准，并在相关提案中详细论证和说明调整的原因，独立董事应当对此发表独立意见，并经出席股东大会的股东所持表决权的 2/3 以上通过。

（五）上市后五年内分红规划：公司当年经审计净利润为正数且符合《公司法》规定的分红条件下，应当优先采取现金方式分配股利，如无重大投资计划或重大现金支出等事项发生，以现金方式分配的利润不少于当年实现的可分配利润的 30%；如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 20%。”

二、最近三年现金分红及未分配利润使用情况

（一）最近三年现金分红情况

公司重视对投资者的合理回报，牢固树立回报股东的意识，并兼顾公司的可持续发展，保持连续、稳定的利润分配政策。

最近三年，公司的现金分红情况如下：

年度	现金分红金额（含税，万元）	分红年度合并报表中归属于上市公司普通股股东的净利润（万元）	占合并报表中归属于上市公司普通股股东的净利润的比率（%）
2013 年	2,284.20	11,052.88	20.67%
2014 年	3,007.07	14,450.35	20.81%
2015 年	4,004.97	19,432.39	20.61%

注：上表中 2013 年合并报表中归属于上市公司普通股股东的净利润为会计政策变更前的数据。

2014 年 1 月，公司首次公开发行股票并在创业板上市。根据公司上市后生效的《公司章程》规定，“公司当年经审计净利润为正数且符合《公司法》规定的分红条件下，公司应当优先采取现金方式分配股利，如无重大投资计划或重大现金支出等事项发生，以现金方式分配的利润不少于当年实现的可分配利润的 30%；如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 20%。”鉴于公司未来将有重大投资计划或重大现金支出等事项发生，公司 2013 年、2014 年、2015 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 20%。具体如下：

（1）根据公司 2014 年 1 月上市时披露的《招股说明书》中关于“未来资本性支出计划”等内容，“公司向海淀区申请在创新园建设 2.5 万平米的公司总部及研发中心，2010 年 10 月 12 日获得海淀区重点企业与重大项目评估委员会评估通过（评估意见书编号：2010029）。如公司能获得所需建设用地，将在未来五年内增加 2 亿元资本性支出用于总部及研发中心建设，具体投资额度以与海淀区创新园签订的协议为准。公司申请建设总部和研发中心项目获海淀区重点企业与重大项目评估委员会评估通过后，2011 年 6 月 28 日公司第一届董事会第六次会议审议并通过了《关于审议公司与北京实创科技园开发建设股份有限公司签署

<C-02 地块土地开发补偿框架协议>的议案》。”鉴于公司未来将有重大投资计划或重大现金支出等事项发生，公司 2013 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 20%。

2014 年 4 月 24 日，公司董事会审议通过了《2013 年年度利润分配预案和以资本公积金转增股本的议案》，以公司 2014 年 2 月 28 日末总股本 84,600,000 股为基数，每 10 股送红股 2 股（含税），合计送红股 1,692 万股；同时每 10 股派发现金股利 2.7 元（含税），合计派发现金股利 2,284.20 万元；同时以资本公积转增股本，每 10 股转增 4 股，合计转增股本 3,384 万股。

（2）根据公司 2015 年 1 月 20 日披露的《北京神州绿盟信息安全科技股份有限公司发行股份及支付现金购买资产并募集配套资金暨重大资产重组报告书》中关于“公司未来重大资本性支出”等内容，“为完成公司总部及研发中心建设计划，除土地开发补偿费用外，公司预计还将发生后续建设开发费用 1 亿元-1.2 亿元，总投资约 2 亿元；公司购建公司总部及研发中心项目总投资将根据取得土地的实际成本、后续建设开发支出进行调整”。根据公司《2014 年年度报告》中关于“公司未来发展规划”等内容，“2015 年公司将继续推进外延式扩张战略”，“今后还将继续寻找信息安全市场上可投资并购标的，特别是在一些新兴信息安全领域中，不断完善公司的战略布局”。2015 年公司通过对外投资或收购股权等方式取得了北京力控华康科技有限公司、北京金山安全管理系统技术有限公司、杭州邦盛金融信息技术有限公司等部分股权。鉴于公司未来将有重大投资计划或重大现金支出等事项发生，公司 2014 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 20%。

2015 年 4 月 24 日，公司董事会审议通过了《关于公司 2014 年度利润分配和以资本公积金转增股本预案的议案》，以公司 2015 年 4 月 23 日非公开发行完成后的总股本 143,193,882 股为基数，向全体股东每 10 股派发现金股利人民币 2.1 元（含税），共计派发现金股利 30,070,715.22 元（含税）。同时，以资本公积金向全体股东每 10 股转增 15 股，合计转增 214,790,823 股，转增后公司总股本为 357,984,705 股。

（3）根据公司《第二届董事会第二十九次会议决议公告》，根据《公司章

程》中的利润分配条件及分配比例之规定：“如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 20%”，鉴于公司尚处于发展阶段属成长期且预计未来十二月有重大资金支出安排；同时综合考虑公司目前的经营规模、盈利正常速度和未来发展前景，为使公司股本规模和经营规模的发展相匹配，公司 2015 年度利润分配预案为：以公司总股本 364,087,785 股为基数，向全体股东每 10 股派发现金红利 1.10 元（含税），向全体股东派发现金红利 40,049,656.35 元（含税）。

最近三年，公司累计现金分红为 9,296.24 万元，年均归属于上市公司股东的净利润为 14,978.54 万元，累计现金分红占年均归属于上市公司股东的净利润的 62.06%。

（二）最近三年未分配利润使用情况

公司历来注重股东回报和自身发展的平衡，报告期内公司将留存的未分配利润用于公司主营业务，以满足公司发展战略的需要。在合理回报股东的情况下，公司上述未分配利润的使用，有效降低了公司的筹资成本，同时增加了公司财务的稳健性。

三、未来股东回报规划

公司第二届董事会第二十三次会议、2016 年第一次临时股东大会审议通过了关于股东分红回报规划（2016 年-2018 年）的议案。具体内容如下：

“为进一步健全和完善北京神州绿盟信息安全科技股份有限公司（以下简称“公司”）对利润分配事项的决策程序和机制，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）的相关规定及要求，经综合考虑公司盈利能力、经营发展规划、股东回报、社会资金成本及外部融资环境等因素，公司制定了《北京神州绿盟信息安全科技股份有限公司股东分红回报规划（2016 年-2018 年）》（以下简称“本规划”）。

一、制定本规划所考虑因素：公司着眼于长远和可持续发展，综合考虑了公司实际情况、发展战略、建立对投资者持续、稳定、科学的回报机制，从而对股利分配做出制度性安排，以保证股利分配政策的持续性和稳定性。

二、股东分红回报规划制定原则：公司股东分红回报规划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，需与独立董事、监事充分讨论，坚持现金分红为主这一基本原则，公司当年经审计净利润为正数且符合《公司法》规定的分红条件下，公司应当优先采取现金方式分配股利，如无重大投资计划或重大现金支出等事项发生，以现金方式分配的利润不少于当年实现的可分配利润的 30%；如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 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、购买资产等交易累计支出达到或超过公司最近一期经审计净资产的 50%，或超过 5,000 万元；

2、公司未来十二个月内拟对外投资、购买资产等交易累计支出达到或超过公司最近一期经审计总资产的 30%。

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，并按照本章程规定的程序，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，现金分红在本次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，现金分红在本次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，现金分红在本次利润分配中所占比例最低应达到 20%；

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。

公司在确定以股票方式分配利润的具体金额时，应充分考虑以股票方式分配

利润后的总股本是否与公司目前的经营规模、盈利增长速度相适应，并考虑对未来债权融资成本的影响，以确保分配方案符合全体股东的整体利益。

公司董事会根据既定的利润分配政策制定利润分配方案，利润分配方案中应当对留存的未分配利润使用计划进行说明，独立董事应当就利润分配方案的合理性发表独立意见。在审议公司利润分配方案的董事会、监事会议上，需经全体董事过半数同意，并分别经公司 1/2 以上独立董事、1/2 以上监事同意，方能提交公司股东大会审议。公司独立董事在股东大会召开前可向公司社会公众股股东征集其在股东大会上的投票权，独立董事行使上述投票权应当取得全体独立董事 1/2 以上同意。

公司每五年重新审视一次分红回报规划和计划，如现行政策与公司生产经营情况、投资规划和长期发展的需要确实发生冲突的，经半数以上董事同意和半数以上独立董事同意，董事会可以对分红规划和计划进行调整；调整分红规划和计划应以股东权益保护为出发点，调整后的利润分配政策不得违反中国证监会、深圳证券交易所和公司章程的有关规定。

三、公司 2016-2018 年股东分红回报具体实施计划：公司当年经审计净利润为正数且符合《公司法》规定的分红条件下，公司应当优先采取现金方式分配股利，如无重大投资计划或重大现金支出等事项发生，应当采取现金方式分配股利，以现金方式分配的利润不少于当年实现的可分配利润的 30%；如有重大投资计划或重大现金支出等事项发生，公司以现金方式分配的利润不少于当年实现的可分配利润的 20%。公司在每个会计年度结束后，由公司董事会提出分红议案，并交付股东大会通过网络投票的形式进行表决。公司接受所有股东（特别是公众投资者）、独立董事、监事对公司分红的建议和监督。”

第六节 与本次发行相关的董事会声明及承诺事项

一、董事会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

除本次发行外，公司在未来十二个月内暂无其他股权融资计划。若未来公司根据业务发展需要及资产负债状况安排股权融资，将按照相关法律法规履行审议程序和信息披露义务。

二、本次发行对即期回报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

（一）本次募集资金到位当年每股收益相对上年度每股收益的变动趋势

1、最近三年公司每股收益情况

按照中国证券监督管理委员会《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），公司 2013 年度、2014 年、2015 年的每股收益如下表所示：

期间	报告期利润	每股收益（元/股）	
		基本每股收益	稀释每股收益
2015 年	归属于上市公司普通股股东的净利润	0.55	0.55
	归属于上市公司普通股股东的扣除非经常性损益后的净利润	0.46	0.46
2014 年	归属于上市公司普通股股东的净利润	0.43	0.43
	归属于上市公司普通股股东的扣除非经常性损益后的净利润	0.40	0.40
2013 年	归属于上市公司普通股股东的净利润	0.39	0.39
	归属于上市公司普通股股东的扣除非经	0.36	0.36

	常性损益后的净利润		

2、本次非公开发行股票对公司每股收益的影响

测算本次发行摊薄即期回报对公司每股收益影响的假设前提：

（1）假定本次发行方案于 2016 年 10 月底前实施完毕（该时间仅为估计，最终以中国证监会核准本次发行后的实际完成时间为准）；

（2）假定本次发行股票数量为 2,600 万股，募集资金总额为 80,121.58 万元，并且不考虑发行费用的影响；

（3）未考虑本次发行募集资金到账后，对公司生产经营、财务状况（如财务费用、投资收益）等的影响；

（4）假设公司 2016 年归属于上市公司股东的扣除非经常性损益后的净利润较 2015 年同比增长比例出现三种情形：-20%、0%、20%；

（5）假设 2016 年不存在因公积金转增股本或股票股利分配等增加股份数；

（6）未考虑本次发行前后因股权激励行权导致的股本变动；截至 2015 年 12 月 31 日公司总股本为 360,098,286 股，假设本次非公开发行股票数量为 2,600 万股，本次发行完成后公司总股本为 386,098,286 股。

上述假设仅为测算本次非公开发行股票摊薄即期回报对公司主要财务指标的影响，不代表公司对 2016 年盈利情况的承诺，亦不代表公司对 2016 年经营情况及趋势的判断。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。

基于上述情况，公司测算了本次非公开发行摊薄即期回报对主要财务指标的影响，具体情况如下：

项目	2015 年	2016 年	
		发行前	发行后
总股本（股）	360,098,286	360,098,286	386,098,286
假设情形 1：2016 年归属于上市公司股东的扣除非经常性损益后的净利润同比增长-20%。			
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	16,522.54	13,218.03	13,218.03

基本每股收益（扣除非经常性损益后）（元）	0.46	0.37	0.36
稀释每股收益（扣除非经常性损益后）（元）	0.46	0.37	0.36
假设情形 2：2016 年归属于上市公司股东的扣除非经常性损益后的净利润同比增长 0%。			
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	16,522.54	16,522.54	16,522.54
基本每股收益（扣除非经常性损益后）（元）	0.46	0.46	0.45
稀释每股收益（扣除非经常性损益后）（元）	0.46	0.46	0.45
假设情形 3：2016 年归属于上市公司股东的扣除非经常性损益后的净利润同比增长 20%。			
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	16,522.54	19,827.05	19,827.05
基本每股收益（扣除非经常性损益后）（元）	0.46	0.55	0.54
稀释每股收益（扣除非经常性损益后）（元）	0.46	0.55	0.54

根据测算，公司本次融资募集资金到位当年基本每股收益或稀释每股收益可能低于上年度，公司存在即期回报被摊薄的风险。

（二）关于本次发行摊薄即期回报的情况的风险提示

公司本次非公开发行募集资金数额相对较大，募集资金使用需要一定的周期。若监管政策等投资环境发生不利变化，将影响募投项目的进度。募投项目建设完成后，效益的显现需要一个过程，效果难以在短期内全部释放。

本次发行完成后，股本规模及净资产规模将明显扩大，募集资金购置的资产将在一定期限内计提折旧或摊销，上述因素将对公司经营业绩构成一定压力，可能导致公司的每股收益被摊薄。公司特别提醒投资者理性投资，关注本次非公开发行股票后即期回报被摊薄的风险。

（三）本次发行融资的必要性和合理性

1、提升公司网络安全技术优势，深化公司战略布局

在公司成长过程中，技术创新和领先一直是公司的关键战略，公司持续加强产品研发和安全服务创新方面的投入，不断提升公司技术领先优势。“智慧安全防护体系”在公司原有安全云服务基础上，进一步提升安全云服务的大规模交付能力，以支持高效率的安全运营服务。“安全数据科学平台建设”通过对各类网络行为数据的记录、存储和分析，结合安全技术和防护经验，可以从更高的视野

和角度、更广的维度上去发现异常、捕获威胁，实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对未来不断变化、日益增长的安全威胁。本次募集资金投资项目的成功实施，将是对公司现有主营业务和产品线的有力丰富与补充，可以极大提升公司的核心竞争力，帮助公司把握住包括云计算、大数据等先进技术变革带来的重大机遇，深化公司战略布局。

2、为行业客户提供更有针对性的安全解决方案，实现行业深耕

公司主要客户为运营商、政府、金融、能源、互联网、教育等领域的企业级用户。通过向客户提供差异化的产品和服务，公司一直走在行业创新发展的前列，是国内安全厂家中较早推出网络入侵防御系统、Web 应用防护系统等产品的创新型厂商，多项产品市场占有率位居国内前列。移动互联、云计算、下一代互联网和大数据等新兴技术的蓬勃发展，极大地促进了信息的共享，同时也给运营商、金融、能源、互联网等行业的信息安全带来更大挑战。近年来基于开放性网络的攻击入侵已经成为信息安全领域的一个关注焦点。本次募集资金投资项目的成功实施，可以利用公司多年来在客户行业的深厚积累，结合客户行业大数据，进一步提升公司安全云服务的大规模交付能力，为行业客户提供更有针对性的安全解决方案，实现行业深耕。

3、紧跟行业趋势，提高公司盈利能力

公司在多年的发展中已经具备了较为完善、技术领先的产品线和解决方案，随着云计算、大数据、移动互联网、物联网等重大技术变革的逐步演化，安全行业也正在发生变革，公司需要建设并实施符合行业趋势的研发项目以保持技术领先地位，适应不断发展变革的产业环境。通过本次非公开发行，公司可以充实资本实力，推动业务模式创新，拓展业务规模和市场空间，巩固和提升公司的行业地位和核心竞争力，进一步提升公司价值，更好地回报上市公司全体股东。

综上，本次非公开发行股票融资具有必要性和合理性。

（四）本次募投项目与公司现有业务的关系以及公司开展该等项目的准备情况

公司本次募集资金投资项目是在现有主营业务的基础上，结合未来市场发展的需求而对现有产品进行的升级换代或技术延伸。（1）“智慧安全防护体系”在公司原有安全云服务基础上，进一步提升安全云服务的大规模交付能力，以支持高效率的安全运营服务。（2）“安全数据科学平台建设”通过对各类网络行为数据的记录、存储和分析，结合安全技术和防护经验，可以从更高的视野和角度、更广的维度上去发现异常、捕获威胁，实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对未来不断变化、日益增长的安全威胁。（3）公司拟使用本次募集资金中的 20,000 万元用于补充流动资金，增强资金实力以支持公司的长远发展战略。综上，本次募集资金投资项目的成功实施，将是对公司现有主营业务和产品线的有力丰富与补充，可以极大提升公司的核心竞争力，帮助公司把握住包括云计算、大数据等先进技术变革带来的重大机遇，深化公司战略布局。

目前，公司在人员、技术、市场等方面已经具备了实施募集资金投资项目的各项条件，具体如下：

（1）人员方面，公司组建了高素质的核心管理团队和专业化的核心技术团队。公司核心管理团队长期致力于企业管理和市场拓展，具备丰富的管理经验和敏锐的市场眼光。公司核心技术团队长期致力于信息安全领域的研究开发，具备业界领先的技术能力。高学历、高素质、高技术的员工团队为公司未来经营业务的发展奠定了人才基础。公司建立了健全的内部控制体系，形成权责明确、相互制衡、科学规范的决策体系和制度，能够支撑本次募集资金投资项目的实施与运营。

（2）技术方面，关于“智慧安全防护体系”项目，公司自 2009 年启动云安全相关研究工作，公司是国际权威组织云安全联盟（CSA）在中国的第一个企业会员，参与和领导了一系列相关技术标准研究开发项目，已向客户提供基于云计算技术的网站照料服务。公司在 2012 年开展软件定义网络（SDN）相关技术的跟踪研究，成功提出和实现了业界领先的软件定义安全的框架，并开始对主要产品进行架构升级、虚拟化研发。公司还与多家业界领先的云计算服务提供商、云计算解决方案提供商展开了多层面的技术和商业合作。关于“安全数据科学平台

建设” 项目，公司通过多年探索，已在相关领域拥有深入的积累，核心技术主要通过自主研发的方式取得；对于模型、算法研究技术，公司目前已经具备开展相关工作的基础，将主要通过自主培养和外部招聘相结合的方式，补充模型、算法方面的专业人员；对于安全攻防技术，公司是国内领先的、具有核心竞争力的企业级网络安全解决方案供应商，具有十余年安全攻防方面的技术积累，能够满足本项目在安全领域方面的技术需求。公司目前的技术储备能够支撑募集资金投资项目实施和公司未来业务发展。

（3）市场方面，依托于技术领先、质量过硬的产品和专业、便捷的服务，公司逐步开拓并形成了以政府、电信运营商、金融、能源和互联网等领域优质客户为主的客户群体，并保持了长期稳定的合作关系。公司通过与客户的密切合作，积累信息安全项目实施经验，完善信息安全产品性能，满足其信息安全业务的发展规划及建设思路，动态把握主要领域客户对于信息安全的技术需求及发展趋势，为公司未来业务范围的扩展、募投项目的实施提供了良好支持。

综上，公司在人员、技术、市场等方面已经具备了实施募集资金投资项目的各项条件，募集资金到位后，预计募投项目的实施不存在重大障碍。

（五）填补被摊薄即期回报的措施

为保护投资者利益，公司应对本次发行可能摊薄即期回报采取的具体措施包括：

1、加强募集资金的管理，防范募集资金使用风险

公司制定了《北京神州绿盟信息安全科技股份有限公司募集资金使用管理制度》，对募集资金的专户存储、使用、用途变更、管理和监督进行了明确的规定。为保障公司规范、有效使用募集资金，本次非公开发行募集资金到位后，公司董事会将持续监督公司对募集资金专户存储、保障募集资金用于指定用途、定期对募集资金进行内部审计、配合保荐机构对募集资金使用的检查和监督，以保证募集资金合理规范使用，合理防范募集资金使用风险。

2、不断完善公司治理，为公司发展提供制度保障

公司将严格遵循《公司法》、《证券法》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力，确保公司股东大会、董事会、监事会、高级管理人员能够按照法律、法规和公司章程的规定行使职权，作出科学合理的决策，维护公司整体利益尤其是中小股东的合法权益。

3、严格执行公司分红政策，加强对股东的回报

公司已根据中国证监会《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）的相关要求并结合公司实际情况，在公司章程中对利润分配的相关条款进行了修订，并制订了股东分红回报规划（2016 年-2018 年），进一步明确了公司利润分配政策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，完善了公司利润分配的决策程序和机制以及利润分配政策的调整原则，强化了投资者回报机制。

本次发行完成后，公司将按照法律法规的规定和公司章程、股东分红回报规划（2016 年-2018 年）的约定，在符合利润分配条件的情况下，积极推动对股东的利润分配，有效维护和增加对股东的回报。

4、加强经营管理，提升经营效率和盈利能力

公司将努力提高资金的使用效率，完善并强化投资决策程序，设计更合理的资金使用方案，合理运用各种融资工具和渠道，控制资金成本，提升资金使用效率，全面有效地降低公司经营和管控风险。

公司将不断完善企业管理和内部控制制度，提高公司治理水平。同时，公司也将继续改善公司组织运营效率，合理控制成本费用支出，建立更加良好的成本管控体系，提高公司的财务管理及成本费用控制水平，不断提高公司的总体盈利能力。

公司声明：提醒投资者注意，公司制定的各项填补回报措施不等于对公司未来利润做出保证。

（六）公司董事、高级管理人员、主要股东对上述填补回报措施能够得到切实履行作出的承诺

公司董事、高级管理人员承诺如下：（一）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；（二）本人承诺对本人的职务消费行为进行约束；（三）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；（四）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；（五）本人承诺，如未来公司公布新的股权激励计划，其行权条件将与公司填补回报措施的执行情况相挂钩。

公司主要股东承诺如下：本公司/本人作为公司持股 5%以上的股东，根据中国证监会《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》的要求，就公司本次非公开发行 A 股股票摊薄即期回报采取填补措施的事宜，承诺如下：本公司/本人不会越权干预公司经营管理活动，亦不会侵占公司利益。

（七）对于本次非公开发行摊薄即期回报的审议程序及信息披露情况

公司第二届董事会第二十八次会议、2016 年第二次临时股东大会、第二届董事会第三十次会议审议通过了董事会对公司本次融资摊薄即期回报的分析、填补即期回报措施及相关承诺主体的承诺等事项的相关议案。

公司将在定期报告中持续披露填补即期回报措施的完成情况及相关承诺主体承诺事项的履行情况。

（以下无正文）

（本页无正文，为《北京神州绿盟信息安全科技股份有限公司非公开发行股票预案（三次修订稿）》之签章页）

北京神州绿盟信息安全科技股份有限公司

董　事　会

2016年8月23日