中信建投证券股份有限公司

关于

杭州迪普科技股份有限公司

首次公开发行股票并在创业板上市

之

发行保荐书

保荐机构

二〇一九年三月

保荐机构及保荐代表人声明

中信建投证券股份有限公司及本项目保荐代表人赵军、谢思遥根据《中华人民共和国公司法》、《中华人民共和国证券法》等有关法律、法规和中国证监会的有关规定，诚实守信，勤勉尽责，严格按照依法制订的业务规则、行业执业规范和道德准则出具本发行保荐书，并保证发行保荐书的真实性、准确性和完整性。

目 录

释 义

在本发行保荐书中，除非另有说明，下列词语具有如下特定含义：

一般词语		
本保荐机构、保荐机构、保荐人、主承销商、中信建投、中信建投证券	指	中信建投证券股份有限公司
公司、发行人、迪普科技、股份公司	指	杭州迪普科技股份有限公司
迪普有限	指	杭州迪普科技有限公司，发行人的前身
方广创投	指	苏州方广创业投资合伙企业（有限合伙）
中移创新	指	中移创新产业基金（深圳）合伙企业（有限合伙）
伯乐圣赢	指	杭州伯乐圣赢股权投资合伙企业（有限合伙）
杭州哲创	指	杭州哲创投资合伙企业（有限合伙）
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
IDC	指	International Data Corporation，国际数据公司
Frost & Sullivan	指	弗若斯特沙利文咨询公司
Gartner	指	高德纳咨询公司
证监会	指	中国证券监督管理委员会
《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》
《公司章程》	指	公司现行有效的《杭州迪普科技股份有限公司章程》
股东大会	指	杭州迪普科技股份有限公司股东大会
董事会	指	杭州迪普科技股份有限公司董事会
监事会	指	杭州迪普科技股份有限公司监事会
发行人律师、锦天城律师	指	上海市锦天城律师事务所
发行人会计师、立信会计师	指	立信会计师事务所（特殊普通合伙）
股票、A 股	指	发行人本次发行的每股面值人民币 1 元的普通股股票
本次发行	指	发行人首次公开发行 A 股并在创业板上市
报告期	指	2016 年、2017 年及 2018 年
最近三年	指	2016 年、2017 年及 2018 年
最近两年	指	2017 年、2018 年

“十三五”	指	2016 年至 2020 年
元、万元、亿元	指	人民币元、万元、亿元
专业术语		
FW	指	Firewall，防火墙
IPS	指	Intrusion Prevention System，入侵防御系统
WAF	指	Web Application Firewall，Web 应用防火墙
Guard	指	迪普科技异常流量清洗产品
Probe	指	迪普科技异常流量检测产品
DAC	指	迪普科技物联网设备应用控制系统产品
DPI	指	Deep Packet Inspection，深度包检测
Scanner	指	迪普科技漏洞扫描系统产品
ADX	指	迪普科技应用交付平台产品
UAG	指	迪普科技上网行为管理及流控系统产品
DeepCache	指	迪普科技高速缓存加速系统产品
UMC	指	迪普科技统一管理中心产品
DPX	指	迪普科技深度业务路由交换网关产品
LSW	指	迪普科技盒式交换机产品
WLAN	指	Wireless Local Area Networks，无线局域网
AC	指	Access Controller，无线接入控制器
AP	指	Access Point，无线访问接入点
XR	指	迪普科技路由器产品
UTM	指	Unified Threat Management，统一威胁管理
ConPlat	指	迪普科技 L2~7 融合操作系统
APP-X	指	迪普科技高性能硬件架构
APP-ID	指	迪普科技应用识别与威胁特征库
DP xFabric	指	迪普科技技术解决方案架构
OVC	指	OS-Level Virtual Context，操作系统级虚拟化
VSM	指	Virtual Switching Matrix，虚拟交换矩阵
VEM	指	Virtual Extension Matrix，虚拟扩展矩阵
FPGA	指	Field Programmable Gate Array，即现场可编程门阵列
Web	指	网络、互联网，表现为三种形式，即超文本（hypertext）、超媒体（hypermedia）、超文本传输协议（HTTP）等
URL	指	Uniform Resource Locator，统一资源定位符

DNS	指	Domain Name System，域名系统
HTTP	指	HyperText Transfer Protocol，超文本传输协议
IPv4	指	Internet Protocol version 4，互联网协议第四版
IPv6	指	Internet Protocol version 6，互联网协议第六版
L2~7	指	网络系统结构的二层至七层。网络系统结构的七层参考模型将整个网络通信的功能划分为七个层次，由低到高分别是物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。每层完成一定的功能，每层都直接为其上层提供服务，并且所有层次都互相支持。四层到七层主要负责互操作性，而一层到三层则用于创造两个网络设备间的物理连接
VLAN	指	Virtual Local Area Network，虚拟局域网
漏洞	指	在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，使攻击者能够在未授权的情况下访问或破坏系统
病毒	指	编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码
蠕虫	指	通过网络和电子邮件进行复制和传播的计算机病毒
木马	指	有隐藏性的、自发性的可被用来进行恶意行为的程序
间谍软件	指	从计算机上搜集信息，并在未得到该计算机用户许可时便将信息传递到第三方的软件
僵尸网络	指	一组被植入恶意程序的可控主机以及若干控制它们的主机所组成的网络，攻击者可以用来发动 DDoS 攻击、发送垃圾邮件或窃取用户信息等
网页挂马	指	把恶意代码嵌入到正常的网页中，使 PC 终端中木马，达到盗取用户信息、控制 PC 等非法目的
跨站脚本	指	利用网站漏洞把恶意的脚本代码注入到网页之中，当其他用户浏览这些网页时，就会执行其中的恶意代码，对受害用户可能采取 Cookie 资料窃取、会话劫持、钓鱼欺骗等各种攻击
SQL 注入	指	通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意 SQL 命令的攻击手段
Webshell	指	一种 web 入侵的脚本攻击工具
DDoS 攻击	指	分布式拒绝服务（Distributed Denial of Service）攻击，借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动攻击，使计算机或网络无法提供正常的服务
APT 攻击	指	高级持续性威胁（Advanced Persistent Threat）攻击，利用先进的攻击手段对特定目标进行长期持续性网

		络攻击
黑客	指	Hacker，利用安全漏洞对网络或系统进行攻击破坏或窃取资料的人
负载均衡	指	Load Balance，将工作任务分摊到多个网络设备和服务器，增加吞吐量、加强网络数据处理能力
NAT	指	Network Address Translation，网络地址转换
VPN	指	Virtual Private Network，虚拟专用网络
SSL	指	Secure Sockets Layer，安全套接层协议层
CVE	指	Common Vulnerabilities & Exposures，公共漏洞和暴露
MPLS	指	Multi-Protocol Label Switching，多协议标签交换
Cookie	指	网站为了辨别用户身份、进行跟踪而储存在用户本地终端上的数据
TCP	指	Transmission Control Protocol，传输控制协议
P2P	指	Peer-to-Peer，对等计算机网络，在对等者之间分配任务和工作负载的分布式应用架构
IPv4/IPv6 双栈	指	一台路由器上同时运行 IPv4 和 IPv6 路由协议
CLOS 架构	指	多级交换网架构
“交钥匙”工程	指	通过完备的产品线、以及针对各行业特点设计的完善的解决方案体系，为用户交付可以完整满足需求并可直接使用的整个网络，而不再需要用户自己进行复杂的网络设计与实施工作，可以有效降低用户工作复杂度

本发行保荐书若出现合计数尾数与各分项数字之和尾数不一致的情况，均为四舍五入原因造成。

第一节 本次证券发行基本情况

一、本次证券发行具体负责推荐的保荐代表人

中信建投证券指定赵军、谢思遥担任本次迪普科技首次公开发行股票并在创业板上市项目的保荐代表人。

上述两位保荐代表人的执业情况如下：

赵军先生：保荐代表人，硕士学历，现任中信建投证券投资银行部执行总经理，曾主持或参与的项目有：王府井可转换公司债券、三元股份非公开发行、隧道股份公司债券、京东方非公开发行、王府井非公开发行、隧道股份重大资产重组、中恒电气重大资产重组、中国国旅非公开发行、航天通信非公开发行、中华企业公司债、上实发展公司债、华西股份非公开发行、仙琚制药非公开发行、银河电子非公开发行、永和智控首次公开发行、新文化公司债、黑牛食品非公开发行等。作为保荐代表人现在尽职推荐的项目有：上海锦和商业经营管理股份有限公司首次公开发行。

谢思遥先生：保荐代表人，硕士学历，现任中信建投证券投资银行部副总裁，曾主持或参与的项目有：润建通信首次公开发行、新泉股份首次公开发行、仙琚制药非公开发行、黑牛食品非公开发行、迪马股份公开发行公司债、中华企业非公开发行公司债、上实发展公开发行公司债、黑牛食品重大资产出售等。

二、本次证券发行项目协办人及项目组其他成员

（一）本次证券发行项目协办人

本次证券发行项目的协办人为洪敏，其保荐业务执行情况如下：

洪敏先生：硕士学历，现任中信建投证券投资银行部副总裁，曾主持或参与的项目有：友利控股重大资产重组、海伦哲发行股份购买资产、中国商用飞机有限责任公司非公开发行公司债券等。

（二）本次证券发行项目组其他成员

本次证券发行项目组其他成员包括吴继平、杨浩。

吴继平先生：硕士学历，现任中信建投证券投资银行部副总裁，曾主持或参与的项目有：杉杉股份非公开发行、黑牛食品非公开发行、春光股份首次公开发行、浙商银行 2016 年二级资本债、华西股份 2016 年公开发行公司债、华西股份 2016 年非公开发行公司债等。

杨浩先生：硕士学历，现任中信建投证券投资银行部高级经理，曾主持或参与的项目有：新文化公司债、黑牛食品重大资产出售、黑牛食品非公开发行、维信诺重大资产购买及重大资产出售等。

三、本次保荐发行人证券发行的类型

首次公开发行人民币普通股股票（A 股）并在创业板上市。

四、发行人基本情况

（一）发行人概览

公司名称：杭州迪普科技股份有限公司

英文名称：Hangzhou DPtech Technologies Co.,Ltd.

注册资本：人民币 36,000 万元

法定代表人：郑树生

成立日期：2008 年 5 月 28 日

股份公司设立日期：2016 年 12 月 12 日

公司住所：杭州市滨江区通和路 68 号中财大厦 6 楼（邮政编码：310051）

联系电话：0571-2828 1966

联系传真：0571-2828 0900

互联网网址：http://www.dptech.com

电子信箱：public@dptech.com

负责信息披露和投资者关系管理部门和负责人：证券事务与投资者关系部、

董事会秘书邹禧典

经营范围：生产：计算机软硬件、数据通信产品、网络安全产品、应用交付产品及网络产品。研究、开发、销售：计算机软硬件、网络安全产品、应用交付产品及网络产品、通信设备；货物进出口（法律、行政法规禁止经营的项目除外，法律、行政法规限制经营的项目取得许可后方可经营）。（依法须经批准的项目，经相关部门批准后方可开展经营活动）。

（二）发行人主营业务发展情况

公司主营业务为从事企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务。主要产品包括网络安全产品、应用交付产品及基础网络产品。公司提供基于创新的统一软件平台和高性能硬件平台下，以网络安全为核心，融合企业通信领域中网络安全、应用交付、基础网络各功能模块的整体解决方案。

公司推出了包括应用防火墙（FW）、入侵防御系统（IPS）、异常流量清洗（Guard/Probe）、Web 应用防火墙（WAF）、物联网应用安全控制系统（DAC）、DPI 流量分析设备、漏洞扫描系统（Scanner）、应用交付平台（ADX）、上网行为管理及流控（UAG）、高速缓存加速系统（DeepCache）、统一管理中心（UMC）、深度业务路由交换网关（DPX）、盒式交换机（LSW）等在内的十余类上百款产品，形成了以“简单、智能、安全”为特色的完备产品线。公司建立了覆盖全国的市场销售与技术支援体系，产品广泛运用于运营商、政府、电力能源、教育、医疗、金融和其他大型企业，公司已成为具备核心技术与竞争力、国内领先的企业级网络通信产品及解决方案提供商。

公司在北京、杭州设有研发中心，拥有专业的软件开发及硬件逻辑开发团队，公司拥有一系列具有自主知识产权的核心技术，自主开发了基于多核 CPU、FPGA 芯片以及分布式转发技术的高性能硬件平台“APP-X”，全面融合网络、安全、应用交付功能的 L2~7 融合操作系统“ConPlat”，将应用特征库、攻击特征库以及病毒库三库合一的应用识别与威胁特征库“APP-ID”，以及将应用支持能力从单设备扩展到整网的技术解决方案架构“DP xFabric”。截至 2018 年 12 月 31 日，公司拥有已获授权的专利 193 项（其中发明专利 105 项）、申请中的专利 983 项（其中发明专利 981 项）、已登记的软件著作权 34 项。

公司已通过中国信息安全认证中心信息安全服务资质认证（信息安全风险评估一级、信息安全应急处理一级）、中国信息安全测评中心信息安全服务资质认证（安全工程类二级）、公安部信息安全等级保护安全建设服务机构认证、中国通信企业协会安全建设服务机构能力认证（通信网络安全风险评估一级），以及质量管理体系认证（GB/T 19001、ISO 9001、TL 9000、GJB 9001）、信息安全管理体系认证（GB/T 22080、ISO/IEC 27001）、环境管理体系认证（GB/T 24001、ISO 14001）等。2017 年，公司获得美国软件工程学会软件能力成熟度模型集成最高等级认证（CMMI 5 级），标志着公司在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列。

公司是国家信息安全漏洞库技术支撑单位、中国互联网网络安全威胁治理联盟成员单位、二级保密资格单位、商用密码产品生产定点单位、中国保密协会会员单位、中国网络安全产业联盟理事单位、中国网络空间安全协会会员单位，也是北京“APEC 峰会”、杭州“G20 峰会”、乌镇“世界互联网大会”、厦门“金砖国家峰会”、南宁“中国-东盟商务与投资峰会”、青岛“上海合作组织峰会”、上海“中国国际进口博览会”等重大国际会议和展览的网络安全保障和应急响应工作的技术支撑单位。公司是国家信息中心在电子政务安全领域的战略合作伙伴，公司高性能高可靠的下一代应用防火墙、面向云计算的高性能入侵防御系统、面向云计算和大数据应用的高性能异常流量检测和清洗产品入选发改委国家信息安全专项，基于下一代互联网的高性能入侵防御系统入选科技部国家重点新产品计划项目，自主可控核心交换机入选 2019 年度浙江省重点研发计划项目。公司“转发与控制分离技术及应用”获 2016 年浙江省技术发明一等奖，公司被浙江省经济和信息化委员会评为 2017 年及 2018 年“浙江省电子信息 50 家成长性特色企业”，被浙江省经济和信息化委员会、省财政厅、省国家税务局、省地方税务局、杭州海关认定为“浙江省省级企业技术中心”，被浙江省科学技术厅、省财政厅、省国家税务局、省地方税务局认定为“高新技术企业”，被国家知识产权局认定为“国家知识产权优势企业”。2017 年 8 月，公司“浙江省迪普网络信息安全研究院”被浙江省科学技术厅、浙江省发展和改革委员会和浙江省经济和信息化委员会认定为省级企业研究院。

五、保荐机构与发行人关联关系的说明

（一）中信建投证券或其控股股东、实际控制人、重要关联方不存在持有迪普科技或其控股股东、实际控制人、重要关联方股份的情况；

（二）迪普科技或其控股股东、实际控制人、重要关联方不存在持有中信建投证券或其控股股东、实际控制人、重要关联方股份的情况；

（三）中信建投证券本次具体负责推荐的保荐代表人及其配偶，董事、监事、高级管理人员不存在拥有迪普科技权益、在迪普科技任职等情况；

（四）中信建投证券的控股股东、实际控制人、重要关联方不存在迪普科技控股股东、实际控制人、重要关联方相互提供担保或者融资等情况；

（五）除上述情形外，中信建投证券与迪普科技之间亦不存在其他关联关系。

六、保荐机构内部审核程序和内核意见

（一）保荐机构关于本项目的内部审核程序

本保荐机构在向中国证监会推荐本项目前，通过项目立项审批、内核部门审核及内核小组审核等内部核查程序对项目进行质量管理和风险控制，履行了审慎核查职责。

1、项目的立项审批

本保荐机构按照中信建投证券《投行相关业务立项规则》（2015 年 4 月修订）的规定，对本项目执行立项的审批程序。

本保荐机构投行项目立项委员会（下称“立项委员会”）于 2016 年 11 月 30 日做出准予本项目立项的决定，并确定了本项目的项目组成员。

2、内核部门的审核

本保荐机构在投行管委会下设立运营管理部，负责投行保荐项目的内部审核。2017 年 3 月 13 日至 2017 年 3 月 16 日，运营管理部对本项目进行了现场核查。本项目的项目负责人于 2017 年 3 月 14 日向运营管理部提出内核申请，运营管理部组织相关人员对本项目的发行申请文件进行了审核。运营管理部在完成内

核初审程序后，于 2017 年 3 月 20 日出具了关于本项目的内核初审意见。

3、内核小组的审核

运营管理部在收到本项目的内核申请后，于 2017 年 3 月 16 日发出内核会议通知，并于 2017 年 3 月 23 日召开内核会议对本项目进行了审议和表决。

参加本次内核会议的内核成员共 8 人。内核成员在听取项目负责人和保荐代表人回答内核初审意见及内核成员现场提出的相关问题后，以记名投票的方式对本项目进行了表决。根据表决结果，内核会议审议通过本项目并同意向中国证监会推荐。

项目组按照内核意见的要求对本次发行申请文件进行了修改、补充和完善，并经全体内核成员审核无异议后，本保荐机构为本项目出具了发行保荐书，决定向中国证监会正式推荐本项目。

（二）保荐机构关于本项目的内核意见

本保荐机构本着诚实守信、勤勉尽责的精神，针对发行人的实际情况充分履行尽职调查职责，在此基础上，本保荐机构内核部门对本项目的发行申请文件、保荐工作底稿等相关文件进行了严格的质量控制和审慎核查。

通过履行以上尽职调查和内部核查程序，本保荐机构认为迪普科技本次发行发行申请符合《证券法》及中国证监会相关法规规定的发行条件，同意作为保荐机构向中国证监会推荐迪普科技首次公开发行股票项目。

七、保荐机构对私募投资基金备案情况的核查

（一）核查对象

根据中国证监会于 2015 年 1 月 23 日发布的《发行监管问答—关于与发行监管工作相关的私募投资基金备案问题的解答》的规定，本保荐机构对发行人股东中是否有私募投资基金及其是否按规定履行备案程序情况进行了核查。

（二）核查方式

本保荐机构履行的核查方式包括查阅股东方广创投、中移创新、杭州哲创和

伯乐圣赢的工商登记资料、营业执照、公司章程、合伙协议、基金备案证书、财务报表等。

（三）核查结果

经核查，方广创投已于 2014 年 4 月 29 日取得了中国证券投资基金业协会颁发的《私募投资基金备案证明》，基金编号为 SD2095，其私募基金管理人上海方广投资管理有限公司已于 2016 年 10 月 19 日在中国证券投资基金业协会进行了登记，登记编号为 P1034285。

经核查，中移创新已于 2016 年 8 月 31 日取得了中国证券投资基金业协会颁发的《私募投资基金备案证明》，基金编号为 SM2498，其私募基金管理人中移国投创新投资管理有限公司已于 2016 年 8 月 29 日在中国证券投资基金业协会进行了登记，登记编号为 P1033245。

经核查，伯乐圣赢已于 2016 年 9 月 30 日取得了中国证券投资基金业协会颁发的《私募投资基金备案证明》，基金编号为 SK0582，其私募基金管理人浙江赛伯乐科创股权投资管理有限公司已于 2014 年 5 月 4 日在中国证券投资基金业协会进行了登记，登记编号为 P1001886。

经核查，杭州哲创已于 2017 年 3 月 24 日取得了中国证券投资基金业协会颁发的《私募投资基金备案证明》，基金编号为 SM0991，其私募基金管理人浙江赛伯乐科创股权投资管理有限公司已于 2014 年 5 月 4 日在中国证券投资基金业协会进行了登记，登记编号为 P1001886。

八、保荐机构关于评估机构签字人员离职情况的说明

发行人聘请的评估机构银信资产评估有限公司出具的《杭州迪普科技有限公司股份支付涉及的股东全部权益价值评估项目评估报告》（银信财报字（2016）沪第 134 号）、《杭州迪普科技有限公司股份制改制净资产价值评估项目评估报告》（银信评报字（2016）沪第 1304 号）、《杭州迪普科技有限公司股份支付涉及的股东全部权益价值追溯评估项目评估报告》（银信财报字（2017）沪第 109 号）和《杭州迪普科技有限公司股份支付涉及的股东全部权益价值追溯评估项目评估报告》（银信财报字（2018）沪第 032 号）的经办资产评估师为程永海、周强。

2018 年 10 月 24 日，程永海因工作变动已从银信资产评估有限公司离职。

2019 年 2 月 18 日，银信资产评估有限公司出具了《银信资产评估有限公司关于承担离职签字评估师责任的声明及承诺函》，承诺：“1.本机构确认已从本机构离职的签字评估师程永海签署的杭州迪普科技股份有限公司相关文件均真实、准确、完整，不存在虚假记载、误导性陈述和重大遗漏。

2.本机构承诺将一直对已从本机构离职的签字评估师程永海所签署的杭州迪普科技股份有限公司相关文件的真实性、准确性、完整性承担法律责任。”

九、保荐机构关于 2018 年度发行人净利润较快增长的主要原因的分析

2016-2018 年度，发行人净利润分别为 6,861.74 万元、15,399.06 万元及 20,100.69 万元，扣除非经常性损益后归属于母公司所有者的净利润分别为 6,836.95 万元、14,711.76 万元和 19,542.22 万元，最近三年呈现增长趋势，其中 2018 年，发行人净利润较上年增长 30.53%，扣除非经常性损益后归属于母公司所有者的净利润较上年增长 32.83%。

报告期内，发行人主营业务突出，形成了以网络安全产品为主导，应用交付、基础网络及服务类业务等各业务相互促进，协调发展的业务格局，各业务的稳步增长、应用领域的不断拓展。报告期内，发行人业务规模不断扩大，盈利能力总体趋好。2018 年，发行人业务规模持续增长，毛利率保持相对稳定，在毛利率及期间费用整体规模较为稳定的情况下，发行人净利润保持较快增长趋势。

十、保荐机构关于发行人财务报告审计基准日后的主要经营状况的说明

公司预计 2019 年 1-3 月营业收入在 14,900 万元至 16,300 万元之间，同比变动幅度为 5.00%至 15.00%，归属于母公司股东的净利润在 3,900 万元至 4,700 万元之间，同比变动幅度为 6.00%至 27.00%，扣除非经常性损益后归属于母公司股东的净利润在 3,900 万元至 4,700 万元之间，同比变动幅度为 6.90%至 27.80%。

2019 年 1-3 月财务数据为发行人初步测算结果，未经审计机构审计，预计数不代表发行人最终可实现收入和净利润，亦不构成发行人盈利预测。

财务报告审计基准日（2018 年 12 月 31 日）后，发行人的整体经营环境未

发生较大变化，经营状况良好，经营模式未发生重大变化。财务报告审计基准日后，发行人的主要原材料采购、技术研发、生产及销售等业务运转正常，不存在将导致发行人业绩异常波动的重大不利因素。

第二节 保荐机构承诺事项

一、中信建投证券已按照法律、行政法规和中国证监会的规定，对迪普科技进行了尽职调查、审慎核查，同意推荐迪普科技首次公开发行股票并在创业板上市，并据此出具本发行保荐书。

二、通过尽职调查和对申请文件的审慎核查，中信建投证券作出以下承诺：

（一）有充分理由确信发行人符合法律法规及中国证监会有关证券发行上市的相关规定；

（二）有充分理由确信发行人申请文件和信息披露资料不存在虚假记载、误导性陈述或者重大遗漏；

（三）有充分理由确信发行人及其董事在申请文件和信息披露资料中表达意见的依据充分合理；

（四）有充分理由确信申请文件和信息披露资料与证券服务机构发表的意见不存在实质性差异；

（五）保证所指定的保荐代表人及本保荐机构的相关人员已勤勉尽责，对发行人申请文件和信息披露资料进行了尽职调查、审慎核查；

（六）保证保荐书、与履行保荐职责有关的其他文件不存在虚假记载、误导性陈述或者重大遗漏；

（七）保证对发行人提供的专业服务和出具的专业意见符合法律、行政法规、中国证监会的规定和行业规范；

（八）自愿接受中国证监会依照本办法采取的监管措施；

（九）中国证监会规定的其他事项。

三、中信建投证券按照《关于进一步提高首次公开发行股票公司财务信息披露质量有关问题的意见》（证监会公告[2012]14 号）和《关于做好首次公开发行股票公司 2012 年度财务报告专项检查工作的通知》（发行监管函[2012]551 号）的要求，严格遵守现行各项执业准则和信息披露规范，勤勉尽责、审慎执业，对

发行人报告期内财务会计信息的真实性、准确性、完整性开展全面自查，针对可能造成粉饰业绩或财务造假的 12 个重点事项进行专项核查，同时采取切实有效的手段核查主要财务指标是否存在重大异常，并以必要的独立性走访相关政府部门、银行、重要客户及供应商。

中信建投证券就上述财务专项核查工作的落实情况，作出以下专项说明：

（一）通过财务内部控制情况自查，确认发行人已经建立健全财务报告内部控制制度，合理保证财务报告的可靠性、生产经营的合法性、营运的效率和效果；

（二）通过财务信息披露情况自查，确认发行人财务信息披露真实、准确、完整地反映公司的经营情况；

（三）通过盈利增长和异常交易情况自查，确认发行人申报期内的盈利情况真实，不存在异常交易及利润操纵的情形；

（四）通过关联方认定及其交易情况自查，确认发行人及各中介机构严格按照《企业会计准则》、《上市公司信息披露管理办法》和证券交易所颁布的相关业务规则的有关规定进行关联方认定，充分披露了关联方关系及其交易；

（五）通过收入确认和成本核算情况自查，确认发行人结合经济交易的实际情况谨慎、合理地进行收入确认，发行人的收入确认和成本核算真实、合规，毛利率分析合理；

（六）通过主要客户和供应商情况自查，确认发行人的主要客户和供应商及其交易真实；

（七）通过资产盘点和资产权属情况自查，确认发行人的主要资产真实存在、产权清晰，发行人具有完善的存货盘点制度，存货真实，存货跌价准备计提充分；

（八）通过现金收支管理情况自查，确认发行人具有完善的现金收付交易制度，未对发行人会计核算基础产生不利影响；

（九）通过可能造成粉饰业绩或财务造假的 12 个重点事项自查，确认如下：

1、发行人不存在以自我交易的方式实现收入、利润的虚假增长；

2、发行人不存在发行人或其关联方与其客户或供应商以私下利益交换等方

法进行恶意串通以实现收入、盈利的虚假增长；

3、发行人不存在发行人的关联方或其他利益相关方代发行人支付成本、费用或者采用无偿或不公允的交易价格向发行人提供经济资源；

4、发行人不存在发行人的保荐机构及其关联方、PE 投资机构及其关联方、PE 投资机构的股东或实际控制人控制或投资的其他企业在申报期内最后一年与发行人发生大额交易从而导致发行人在申报期内最后一年收入、利润出现较大幅度增长；

5、发行人不存在利用体外资金支付货款，不存在少计原材料采购数量及金额，不存在虚减当期成本和虚构利润；

6、发行人不存在采用技术手段或其他方法指使关联方或其他法人、自然人冒充互联网或移动互联网客户与发行人（即互联网或移动互联网服务企业）进行交易以实现收入、盈利的虚假增长等；

7、发行人不存在将本应计入当期成本、费用的支出混入存货、在建工程等资产项目的归集和分配过程以达到少计当期成本费用的目的；

8、发行人不存在压低员工薪金、阶段性降低人工成本粉饰业绩；

9、发行人不存在推迟正常经营管理所需费用开支，不存在通过延迟成本费用发生期间增加利润和粉饰报表；

10、发行人不存在期末对欠款坏账、存货跌价等资产减值可能估计不足；

11、发行人不存在推迟在建工程转固时间或外购固定资产达到预定使用状态时间等，不存在延迟固定资产开始计提折旧时间；

12、发行人不存在其他可能导致公司财务信息披露失真、粉饰业绩或财务造假的情况。

（十）通过未来期间业绩下降信息风险披露情况自查，确认发行人对于存在未来期间业绩下降情形的，已经披露业绩下降信息风险。

经过财务专项核查，本保荐机构认为，发行人的财务管理、内部控制、规范运作等方面制度健全，实施有效，报告期财务报表已经按照企业会计准则的规定

编制，财务会计信息真实、准确、完整，如实披露了相关经营和财务信息。

第三节 对本次发行的推荐意见

中信建投证券接受发行人委托，担任其本次公开发行的保荐机构。本保荐机构遵照诚实守信、勤勉尽责的原则，根据《公司法》、《证券法》和中国证监会颁布的《证券发行上市保荐业务管理办法》等法律法规的规定，对发行人进行了审慎调查。

本保荐机构对发行人是否符合证券发行上市条件及其他有关规定进行了判断、对发行人存在的主要问题和风险进行了提示、对发行人发展前景进行了评价，对发行人本次公开发行履行了内部审核程序并出具了内核意见。

本保荐机构内核小组及保荐代表人经过审慎核查，认为发行人本次公开发行符合《公司法》、《证券法》等法律、法规、政策规定的有关首次公开发行的条件，募集资金投向符合国家产业政策要求，同意保荐发行人本次公开发行。

一、发行人关于本次发行的决策程序合法

（一）2017 年 5 月 2 日，迪普科技第一届董事会第七次会议审议并通过了《关于公司首次公开发行股票并在深圳证券交易所创业板上市的议案》等关于首次公开发行股票并在创业板上市的相关议案，并决定提交公司 2017 年第二次临时股东大会讨论决定。2017 年 6 月 2 日，公司召开 2017 年第二次临时股东大会，审议通过了《关于公司首次公开发行股票并在深圳证券交易所创业板上市的议案》等议案。2019 年 1 月 25 日，迪普科技第一届董事会第十二次会议审议并通过了《关于修改杭州迪普科技股份有限公司首次发行人民币普通股（A 股）股票募集资金投资项目部分内容的议案》等议案。

根据上述决议，发行人本次发行上市方案的主要内容如下：

1、发行股票的种类：境内上市人民币普通股（A 股）。

2、发行股票的每股面值：每股面值为人民币 1 元。

3、发行数量：本次发行不超过 4,001 万股，占发行后总股本的比例为 10.00%；全部为发行新股，原股东不公开发售股份。

4、发行方式：本次发行将采用网下向配售对象询价配售与网上向社会公众

投资者定价发行相结合的方式，或者采用经国务院证券监督管理机构认可的其他发行方式。

5、发行定价原则：本次发行定价采用询价方式，最终发行价在向询价对象询价基础上由公司与主承销商（保荐机构）协商确定。

6、发行对象：符合资格的询价对象和在深圳证券交易所开立 A 股股东账户并已开通创业板市场交易账户的投资者（国家法律、法规禁止购买者除外）。

7、上市地点：本次发行完成后，公司股票将申请在深圳证券交易所创业板上市交易。

8、议案有效期：本次发行上市方案决议有效期为二十四个月，自股东大会审议通过本议案之日起计算。

9、授权董事会办理杭州迪普科技股份有限公司首次公开发行股票并在创业板上市有关具体事宜。

10、公司本次公开发行股票募集的资金用于以下项目：

（1）安全威胁态势感知平台项目；

（2）新一代高性能云计算数据中心安全平台项目；

（3）新一代高性能应用交付平台项目；

（4）网络安全产品及相关软件开发基地项目。

11、如果公司首次公开发行股票的申请获得批准并成功发行，则公司首次公开发行股票并上市前的滚存利润由发行后的新老股东按照持股比例共同享有。

（二）经本保荐机构核查，发行人第一届董事会第七次会议、2017 年第二次临时股东大会的召集、召开方式、与会人员资格、表决方式及决议内容，符合《证券法》、《公司法》等有关法律、法规、规范性文件以及《公司章程》规定。发行人 2017 年第二次临时股东大会已依法定程序做出批准公司股票首次发行上市的决议。

（三）发行人 2017 年第二次临时股东大会授权董事会办理有关发行上市事

宜的授权程序合法、内容明确具体，合法有效。

经核查，迪普科技已就首次公开发行股票履行了《公司法》、《证券法》及中国证监会规定的决策程序。

二、本次发行符合相关法律规定

（一）依据《证券法》对发行人符合发行条件进行逐项核查情况

1、发行人具备健全且运行良好的组织机构；

2、发行人具有持续盈利能力，财务状况良好；

3、发行人最近三年财务会计文件无虚假记载，无其他重大违法行为；

4、符合经国务院批准的国务院证券监督管理机构规定的其他条件。

（二）依据《管理办法》对发行人符合发行条件进行逐项核查情况

1、发行人系依法设立且持续经营三年以上的股份有限公司

2016 年 9 月 30 日，迪普有限召开股东会，同意由有限公司整体变更为股份有限公司，以 2016 年 11 月 30 日为审计、评估基准日。

2016 年 12 月 9 日，杭州迪普科技有限公司召开股东会，由迪普有限全体股东作为发起人，以发起设立方式将迪普有限整体变更为股份有限公司，公司名称为“杭州迪普科技股份有限公司”：公司以截至 2016 年 11 月 30 日经审计的净资产 270,131,314.60 元为基础，按照 1：0.370190328 的比例折合股份 100,000,000 股，每股面值 1 元，其余净资产计入股份公司的资本公积，各发起人以各自在有限公司拥有的权益所对应的净资产作为出资。

2016 年 12 月 12 日，公司在杭州市市场监督管理局完成工商变更登记手续，并领取了统一社会信用代码为 91330108673990352B 的《营业执照》，注册资本为 10,000.00 万元。

2016 年 12 月 14 日，立信会计师事务所（特殊普通合伙）出具了信会师报字[2016]第 610943 号《验资报告》，审验确认拟设立股份公司的注册资本已缴足。

发行人系由迪普有限整体变更设立的股份有限公司，迪普有限成立于 2008

年 5 月 28 日。根据《管理办法》第十一条的规定，发行人的持续经营时间可以从迪普有限成立之日起计算，已经持续经营三年以上。

2、发行人符合下列条件：

（1）2017 年度和 2018 年度，发行人的归属于母公司股东的净利润分别为 15,399.06 万元和 20,100.69 万元，扣除非经常性损益后的归属于母公司股东的净利润分别为 14,711.76 万元和 19,542.22 万元。发行人最近两年连续盈利，净利润以扣除非经常性损益前后较低者为计算依据，累计为 34,253.98 万元，不少于 1,000 万元。

（2）截至 2018 年 12 月 31 日，发行人的净资产为 103,330.03 万元，不少于 2,000 万元；发行人的未分配利润为 32,678.98 万元，不存在未弥补亏损。

（3）发行前，发行人的股本总额为 36,000 万股，本次拟发行不超过 4,001 万股，为发行后总股本的 10.00%。

3、发行人股本缴纳及财产转移手续情况

发行人是整体变更设立的股份有限公司，承继了迪普有限的全部资产及负债，财产转移手续办理完毕，发行人的主要资产不存在重大权属纠纷。

4、发行人生产经营的合法合规性

发行人主要经营网络安全产品、应用交付产品以及基础网络产品的研发、生产、销售及提供专业安全服务。发行人生产经营活动符合法律、行政法规和《公司章程》的规定，符合国家产业政策及环境保护政策。

5、最近两年内，发行人的主营业务和董事、高级管理人员没有发生重大变化，实际控制人没有发生变更

最近两年，发行人主要经营网络安全产品、应用交付产品以及基础网络产品的研发、生产、销售及提供专业安全服务，主营业务最近两年未发生重大变化。

最近两年，公司控股股东及实际控制人均为郑树生先生，未发生变更。

最近两年，公司董事、高级管理人员未发生重大变化。

6、发行人的股权清晰，控股股东和受控股股东、实际控制人支配的股东所持发行人的股份不存在重大权属纠纷。

7、发行人的独立性

（1）发行人的资产完整

发行人为依法整体变更设立的股份有限公司，继承了迪普有限所有的资产、负债和权益。发行人拥有独立完整的研发及产、供、销系统，合法拥有与生产经营有关的商标及专利的所有权、设备、软件著作权和业务资质等。发行人目前业务和生产经营所必需资产的权属完全由发行人独立享有，不存在与股东共用的情况。发行人对所有资产拥有完全的控制权和支配权，不存在资产、资金被股东和其他关联方占用而损害发行人利益的情况。

（2）发行人的人员独立

发行人董事、监事及高级管理人员均按照《公司法》、《公司章程》规定的条件和程序产生，发行人的总经理、副总经理、财务总监等高级管理人员未在控股股东、实际控制人及其控制的其他企业中担任除董事、监事以外的其他职务，未在控股股东、实际控制人及其控制的其他企业领薪。发行人的财务人员未在控股股东、实际控制人及其控制的其他企业中兼职。

（3）发行人的财务独立

发行人按照《中华人民共和国会计法》、《企业会计准则》等有关法律法规的要求建立了独立的财务核算体系，能够独立做出财务决策，具有规范的财务会计制度，不存在财务决策等依赖于控股股东、实际控制人及其控制的其他企业的情况。发行人所有银行账户均独立使用，不存在与控股股东、实际控制人及其控制的其他企业共用银行账户。

（4）发行人的机构独立

发行人根据《公司法》、《公司章程》的要求建立了较为完善的法人治理结构，股东大会、董事会、监事会严格按照《公司章程》规范运作，并建立了独立董事制度。发行人建立了适应自身业务发展的组织结构，内部经营管理机构健全，各机构职能明确并配备了相应人员，不存在与控股股东、实际控制人及其控制的其

他企业间机构混同的情况。

（5）发行人的业务独立

公司主营业务为从事企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务。发行人拥有从事上述业务完整、独立的研发及产、供、销系统和人员，不存在对股东和其他关联方的依赖，具备独立面向市场、独立承担责任和风险的能力。发行人与控股股东、实际控制人及其控制的其他企业间不存在同业竞争或者显失公平的关联交易。

经核查，发行人严格按照《公司法》、《证券法》等有关法律、法规和《公司章程》的要求规范运作、独立经营，在资产、人员、财务、机构、业务等方面独立于控股股东、实际控制人及其控制的其他企业，具有独立完整的经营资产、业务体系及面向市场自主经营的能力。发行人与控股股东、实际控制人及其控制的其他企业间不存在同业竞争，以及严重影响发行人独立性或者显失公平的关联交易。

8、发行人的规范运行

发行人已经依法建立了股东大会、董事会、监事会、独立董事、董事会秘书、审计委员会制度，相关机构和人员能够依法履行职责。发行人已经依法建立了健全股东投票计票制度，建立发行人与股东之间的多元化纠纷解决机制，切实保障投资者依法行使收益权、知情权、参与权、监督权、求偿权等股东权利。

9、发行人会计基础工作规范，财务报表的编制符合企业会计准则和相关会计制度的规定，在所有重大方面公允地反映了发行人的财务状况、经营成果和现金流量，并由立信会计师事务所（特殊普通合伙）出具了“信会师报字[2018]第ZF10576 号”标准无保留意见的审计报告。

10、发行人的内部控制制度健全且被有效执行，能够合理保证发行人运行效率、合法合规和财务报告的可靠性，并由立信会计师事务所（特殊普通合伙）出具了“信会师报字[2019]第 ZF10015 号”无保留意见的《内部控制鉴证报告》。

11、发行人的董事、监事和高级管理人员忠实、勤勉，具备法律、行政法规和规章规定的任职资格，且不存在下列情形：

（1）被中国证监会采取证券市场禁入措施尚在禁入期；

（2）最近三年内受到中国证监会行政处罚，或者最近一年内受到证券交易所公开谴责；

（3）因涉嫌犯罪被司法机关立案侦查或者涉嫌违法违规被中国证监会立案调查，尚未有明确结论意见。

12、发行人及其控股股东、实际控制人最近三年内不存在损害投资者合法权益和社会公共利益的重大违法行为。

发行人及其控股股东、实际控制人最近三年内不存在未经法定机关核准，擅自公开或者变相公开发行证券，或者有关违法行为虽然发生在三年前，但目前仍处于持续状态的情形。

13、发行人募集资金的运用

（1）募集资金使用方向

发行人募集资金将用于主营业务，并有明确的用途。根据发行人 2017 年第二次临时股东大会通过的决议，发行人拟公开发行不超过 4,001 万股普通 A 股股票，本次募集资金运用计划在扣除发行费用后按项目轻重缓急顺序投向下列项目：

序号	项目名称	项目总投资（元）	拟投入募集资金（元）
1	安全威胁态势感知平台项目	115,369,800.00	115,369,800.00
2	新一代高性能云计算数据中心安全平台项目	171,568,100.00	171,568,100.00
3	新一代高性能应用交付平台项目	79,442,500.00	79,442,500.00
4	网络安全产品及相关软件开发基地项目	200,000,000.00	46,410,600.00
合计		**566,380,400.00**	**412,791,000.00**

（2）募集资金项目的合理性

发行人的募集资金数额和投资项目与发行人现有生产经营规模、财务状况、技术水平、管理能力及未来资本支出规划等相适应。

三、发行人的主要风险提示

（一）技术风险

1、技术创新风险

公司通过持续的技术创新，已经拥有一系列具有自主知识产权的核心技术。但是公司所处的行业在技术与产品上更新换代很快，企业需要随时判断行业发展方向，预测技术发展趋势，并根据判断及预测的结果不断调整相应的研发和创新，然后将研发和创新成果转换为成熟产品推向市场，才能够使自身的产品贴合市场需求，并保持持续的竞争力和领先优势。

虽然公司拥有很强的研发创新能力，在研发方向的选择上也是基于长期行业实践积累的经验以及对市场需求充分调研的基础上综合决定的，但是由于行业发展趋势的不确定性，可能会导致公司选择及投入的研发方向、创新成果与未来的行业发展趋势存在差异，使公司新产品无法满足未来的行业需求，从而降低公司产品体系的整体竞争力。另外，各种原因造成的研发创新及相应产品转化的进度拖延，也有可能造成公司未来新产品无法及时投放市场，对公司未来的市场竞争造成不利影响。

综上，公司在技术创新方面存在一定的风险。

2、技术失密和核心技术人员流失风险

公司主营产品科技含量较高且在核心关键技术上拥有自主知识产权，技术研发与创新依赖于所拥有的核心技术以及培养、积累的核心技术人员。截至 2018 年 12 月 31 日，公司研究开发部员工 458 人，占公司员工总数 41.86%；截至 2018 年 12 月 31 日，公司拥有 193 项已获授权的专利、34 项软件著作权；此外，当前公司多项产品和技术处于研发阶段，因此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的情况，可能会在一定程度上影响公司的技术创新能力。

（二）市场风险

1、市场竞争的风险

（1）信息安全行业

我国信息安全行业市场空间已颇具规模。根据 IDC《中国 IT 安全市场预测，2017-2021》报告预测，2017 年中国信息安全硬件、软件、服务市场的规模为 41.56 亿美元，同比增长 23.91%，保持了快速增长态势。在整体信息安全硬件、软件、服务市场中，安全硬件市场的占比最大，为 56.47%，安全软件市场占比 17.18%，安全服务市场占比 26.35%。

市场机遇也带来了较多参与者，市场竞争较为激烈。目前国内信息安全行业厂商众多，主营业务涵盖在信息安全的物理安全、网络安全、系统安全、应用安全、数据安全等多个细分领域中。在公司主要产品集中的网络安全领域，国内已有数家企业登陆资本市场。未来，随着信息安全市场空间进一步拓展，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧。

（2）应用交付行业

应用交付行业产品技术复杂、研发难度高，过去市场一直由国外企业主导。近年来，在国内信息产品国产化政策的背景下，随着国内企业技术、自主创新实力的不断增强，国内企业在国内应用交付市场的份额逐渐增加。根据 IDC《中国应用交付市场份额》统计，2017 年度中国应用交付平台产品市场国内企业份额占比已超过 49.15%，其中公司市场份额为 11.64%，位居业内第三。

虽然国内厂商在应用交付市场发展势头很好，但与国外竞争对手相比，在品牌影响力、资金实力、专业人才水平、产品技术积累等方面仍存有差距。随着公司产品进入中高端市场，必将面临与国外厂商的直接竞争。另一方面，随着未来国内应用交付企业的不断崛起与发展，公司也可能会面临来自国内企业的挑战与竞争。

2、主营业务收入增速下滑风险

2016-2018 年度，公司的主营业务收入分别为 53,172.51 万元、61,555.34 万元和 70,369.43 万元，同比增长 18.02%、15.77%和 14.32%，报告期内公司主营

业务收入持续增长，增长态势趋于平缓。尽管目前公司主营业务所属行业的国家政策、发展状况、技术前沿，公司的销售、经营和管理模式，均未发生较大的变化。但是，如果未来出现行业竞争加剧、市场需求萎缩、重要客户流失或经营成本上升等不利因素，或者公司出现不能巩固和提升市场竞争优势、跟不上产品技术更新换代的速度、市场开拓能力不足、募集资金投资项目的实施达不到预期效果等情形，公司业绩增长速度将可能会有所降低，亦可能出现业绩下滑。

3、经营业绩季节性波动风险

公司的营业收入有一定的季节性，主要原因是公司业务的下游客户群体主要来源于运营商、政府、公共事业（电力能源、教育、医疗）等领域，这些客户大多在上半年对全年的投资和采购进行规划，下半年再进行项目招标、项目验收和项目结算。因此，公司下半年（尤其是第四季度）的业务收入显著高于上半年（或其他季度），使得公司整体的销售收入在上、下半年呈现不均衡性。

最近三年，公司营业收入和净利润（剔除股份支付）按季度分布情况如下：

项目	2018 年度		2017 年度		2016 年度	
	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比
第一季度	20.12%	18.44%	19.82%	17.43%	20.29%	23.78%
第二季度	23.35%	19.83%	22.89%	23.07%	24.04%	15.40%
上半年小计	**43.47%**	**38.27%**	**42.70%**	**40.49%**	**44.34%**	**39.18%**
第三季度	24.72%	27.73%	24.32%	27.13%	23.21%	18.43%
第四季度（剔除股份支付）	31.82%	34.01%	32.98%	32.38%	32.45%	42.39%
下半年小计	**56.53%**	**61.73%**	**57.30%**	**59.51%**	**55.66%**	**60.82%**
合计（剔除股份支付）	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**

注：各季度收入和利润数据未经审计，其中净利润为剔除股份支付影响后数额。

从公司各季度营业收入和净利润占全年的比重来看，最近三年公司下半年营业收入占比均显著高于上半年，公司的营业收入呈现的季节性特征导致公司利润也呈季节性分布。公司营业收入在全年实现的不均衡性，可能对公司生产经营活动造成一定不利影响。由于费用在年度内较为均衡的发生，而收入主要集中在下半年，因此可能造成上半年净利润低于全年的 50%的情况。公司收入和盈利有一

定的季节性波动，投资者不宜以半年度或者季度报告的数据推测全年盈利情况。

4、销售渠道风险

由于信息安全行业最终用户分散、用户具体需求各有差异，报告期内，公司的产品销售采用渠道销售和直签销售相结合的方式，并以渠道销售为主。报告期内，公司渠道销售占主营业务收入的比重分别为 67.78%、64.83%和 70.89%。报告期内，公司销售渠道主要包括一级渠道代理商（含总代理商和一级代理商）及二级渠道代理商。截至 2018 年末，发行人总代理商数量为 2 家，一级代理商为 1 家，二级渠道代理商为 1,776 家，公司在全国设有 27 个办事处。而公司产品通过代理商渠道销售的最终用户大部分属于运营商、政府、金融、电力能源、教育、医疗等领域，这些用户通常采用招投标的方式进行信息安全产品与服务的采购。因此，若最终用户项目招投标竞争激烈，而渠道代理商综合能力下滑或不具优势，可能会导致渠道代理商在最终招投标过程中不能中标或中标份额下降，导致其向公司采购金额下滑，存在公司渠道销售收入下滑的风险。

5、外协加工风险

出于购置焊接机等生产设备利用率较低且投资回报期长、焊接及装配等环节委外加工模式在业内较为成熟等因素考虑，公司将产品生产的 PCBA 阶段全部外协加工，装配与测试阶段根据业务量弹性外协加工，公司自身负责原材料采购、部分产品的组装、软件灌装、整机测试、高温老化、验证测试等环节的加工或控制。随着未来募投项目的实施以及公司生产规模的扩大，外协加工的规模必然随之增长，如果现有外协厂商出现加工任务饱和、加工能力下降或是公司出现突发大额订单等情况，有可能会影响公司产品生产进度，从而影响产品及时供货，导致客户满意度下降，甚至存在丢失客户和订单的风险。另外，如果外协加工厂加工的产品存在重大质量问题，并且因为产品质量问题引致丢失客户、纠纷、索赔或诉讼，均将对公司的市场信誉、市场地位甚至对公司销售造成重大不利影响。

6、原材料采购风险

公司产品生产所用的芯片、内存条、光模块等原材料，其高端款型的核心技术垄断，市场集中度较高，主要由美国、韩国、中国台湾等国家或地区的知名厂商生产，最终供应商采取渠道销售模式，授权专业代理商向 IT 基础设备厂商销

售。公司研发和生产部门选定产品所需原材料原厂品牌后，采购部门向交付迅速、价格具有竞争优势、能够满足公司相应采购需求的贸易供应商采购该等原材料。报告期内，该等原材料供给较充分，价格总体趋势相对稳定。同时，随着国内电子元器件厂商的发展，国产电子元器件的竞争力不断增强，公司对该等原材料的国产替代产品进行了较深入的技术研究，已经部分实现产品化，并计划持续加大采用替代原材料产品的比重。然而公司目前芯片、内存条、光模块等原材料的高端款型的采购，在整体上仍存在一定进口供应风险。若国际市场供需变化导致进口原材料价格波动，或因为国际贸易环境变化导致进口原材料供应限制，而公司不能采取有效应对措施，短期内公司可能会遇到生产成本升高、客户供货紧张等问题，将会对公司的产品生产、销售及经营业绩产生一定的不利影响。

7、总代理商变化风险

公司为保持公司业务发展稳定性和持续性，减少特定总代理商集中度过高的风险，报告期内一直保持两家及以上总代理商的合作关系。基于行业特性及行业分工，行业内出现了较多具有总代理商能力的知名代理商，随着公司经营规模的增长，公司具备更换总代理商的能力。2018 年 6 月，公司主动与北京方正终止了总代理商合作关系，并通过考察代理商的综合实力，与新科佳都建立了总代理商合作关系。新科佳都系佳都新太科技股份有限公司（600728）的全资子公司，2017 年度，新科佳都的营业收入为 87,652.06 万元，净利润为 2,339.35 万元。尽管公司总代理商基本不参与最终用户招投标，对公司获取商业机会基本无影响，但是在公司总代理商发生变化后，如果新的总代理商不能充分发挥其物流服务、资金管理、下级代理商的管理培训等作用，公司的产品销售、渠道管理和运营效率仍可能受到不利影响。

8、主要客户的招投标风险

基于行业特性，公司业务主要以解决方案提供商的模式进行，并以项目招投标的方式实现销售，招投标过程通常受公司不能控制的若干因素影响，包括市场情况、客户招投标计划、招投标条件、标书所规定的竞标者的资质及其他竞标者所提供的条款等，因此，公司销售情况受到项目招投标结果的直接影响，从而导致公司向主要客户的销售数量、金额和毛利水平等方面会有所波动。以公司主要客户之一中国移动为例，2016-2018 年度，公司向中国移动的销售收入分别为

10,158.62 万元、5,419.89 万元、11,356.92 万元，在报告期内存在一定波动，主要系报告期内公司中标中国移动的项目在金额及时间分布上存在一定波动，其中 2017 年中标中国移动的项目主要发生在第四季度，发货和收入确认在 2017 年度较少。截至本发行保荐书签署日，公司中标了中国移动 2018 年硬件防火墙产品集采的第一标段第二名及第三标段第二名、中国移动 2018 年至 2020 年 Web 应用防火墙（WAF）设备集采第一名以及中国移动 2018 年至 2019 年负债均衡集采第二标段第三名，中标情况整体保持平稳。

若未来年度公司主要客户招投标竞争激烈而公司不能中标、中标份额下降或入围产品价格较大幅度下降，或招投标计划调整而项目规模、数量、时间等情况发生较大变化，将影响公司当年或下一年度的销售情况，可能存在公司向主要客户销售收入波动或经营业绩下滑的风险。

（三）管理风险

1、实际控制人控制的风险

郑树生先生直接持有公司 53.78%的股份，为公司控股股东及实际控制人。本次发行后，公司实际控制人仍将处于绝对控股地位。虽然公司已经建立了较为完善的内部控制制度和公司治理结构，包括制订了《公司章程》、《股东大会议事规则》、《董事会议事规则》、《监事会议事规则》、《独立董事工作制度》和《关联交易决策制度》等规章制度，但并不能排除实际控制人利用其控制地位从事相关活动，对公司和中小股东的利益产生不利影响。

2、公司规模扩张的管理风险

报告期内，公司的资产规模持续扩大，总资产从 2016 年末的 91,566.92 万元增长到 2018 年末的 135,513.36 万元，公司在杭州、北京均设立研发中心，并在全国设有 27 个办事处。

随着募集资金投资项目的实施，公司资产规模、人员规模将有一定的增长，需要公司在资源整合、市场开拓、产品研发与质量管理、财务管理、内部控制等诸多方面进行调整，对各部门工作的协调性、严密性、连续性也提出了更高的要求。如果公司管理层素质及管理水平不能适应公司规模扩张的需要，组织模式和管理制度未能随着公司规模的扩大而及时调整、完善，公司的市场竞争力将因此

受到削弱。

（四）政策风险

1、财税优惠政策风险

根据国家有关税收的法律法规，报告期内，公司享受的税收优惠主要包括增值税退税和企业所得税优惠。

根据财政部、国家税务总局《关于软件产品增值税政策的通知》（财税[2011]100 号），公司销售自行开发生产的软件产品，按 17%税率（根据财政部、税务总局《关于调整增值税税率的通知》（财税[2018]32 号），2018 年 5 月 1 日起税率调整为 16%）征收增值税后，对其增值税实际税负超过 3%的部分实行即征即退政策。2016-2018 年度，公司增值税退还金额分别为 4,402.62 万元、6,504.99 万元和 6,663.63 万元。如果公司享受的增值税税收优惠政策发生不利变化或取消，或者未能如期收到增值税返还款项，也会对公司经营成果产生较大不利影响。

根据浙江省科学技术厅、浙江省财政厅、浙江省国家税务局和地方税务局于 2013 年 9 月 26 日联合颁发的《高新技术企业证书》（证书编号：GF201333000439），认定公司为国家高新技术企业，认证有效期为 3 年，公司在 2015 年度可享受企业所得税 15%的优惠税率。

根据财政部、国家税务总局发布的财税[2012]27 号文件《关于进一步鼓励软件产业和集成电路产业发展企业所得税政策的通知》的规定以及财政部、国家税务总局、发改委、工信部于 2016 年 5 月 4 日发布的《关于软件和集成电路产业企业所得税优惠政策有关问题的通知》（财税[2016]49 号）对于重点软件企业申请税收优惠申请方式的补充规定，公司符合国家规划布局内重点软件企业的要求，公司在 2016-2018 年度可享受企业所得税 10%的优惠税率；公司获得浙江省科学技术厅、浙江省财政厅、浙江省国家税务局和地方税务局于 2016 年 11 月 21 日联合颁发的《高新技术企业证书》（证书编号：GR201633001578），认定公司为国家高新技术企业，认证有效期为 3 年。如果国家税收优惠政策发生不利变化，或如果公司以后年度不能被认定为“国家规划布局内重点软件企业”或“高新技术企业”，公司需按 25%的税率缴纳企业所得税，将对公司的经营成果产生不利影响。

综上所述，公司存在税收优惠政策变化风险。

2、财政补贴变化产生的风险

报告期内，政府一直重视高新技术企业，并给予重点鼓励和扶持。2016-2018年度，公司除增值税退税外政府补助形成的营业外收入分别为 1,037.53 万元、365.63 万元和 630.87 万元。补助项目包括国家高技术产业发展项目财政配套补助资金、浙江省专利保护与管理专项资金、杭州市工业统筹资金重点项目区财政配套资金等。

但是，如果政府对公司所处行业及高新技术企业的扶持政策发生变化，将对公司的发展产生一定的影响。

3、产品和服务不能获得相关认证的风险

信息安全及网络设备厂商从事研发、生产、销售和提供安全服务等经营活动，通常需取得计算机信息系统安全专用产品销售许可证等产品认证，并具备信息安全服务资质等业务资质。截止本发行保荐书出具日，公司拥有 IT 产品信息安全产品认证证书、中国国家信息安全产品认证证书、信息技术产品安全测评证书、涉密信息系统产品检测证书、军用信息安全产品认证证书、计算机信息系统安全专用产品销售许可证、信息安全服务资质认证证书、中国通信企业协会通信网络安全服务能力评定证书、信息安全等级保护安全建设服务机构能力评估合格证书等信息安全行业的主要产品和服务资质证书。

虽然公司内部有专人负责产品和服务认证的申请、取得和维护，且未曾出现过已取得认证或资质被取消的情况，但如果未来国家关于产品和服务认证的政策或标准出现重大变化，公司无法为过期证书续证，产品和服务存在不能获得相关认证的风险。

（五）财务风险

1、应收账款金额较大及发生坏账的风险

2016-2018 年末，公司应收账款账面价值分别为 10,886.79 万元、8,592.35 万元和 7,813.75 万元，应收账款金额较大。

项目	2018-12-31	2017-12-31	2016-12-31
账面价值（万元）	7,813.75	8,592.35	10,886.79
账面价值较上期末增长	-9.06%	-21.08%	44.52%
占期末总资产比例	5.77%	7.90%	11.89%
应收账款周转率（次）	7.91	6.04	5.67
应收账款余额前 5 名之和占比	89.49%	94.64%	96.25%

2016-2018 年末，公司应收账款占期末总资产的比例分别 11.89%、7.90%和 5.77%，应收账款周转率分别为 5.67、6.04 和 7.91。2016-2018 年末，应收账款余额前五名之和占比分别为 96.25%、94.64%和 89.49%。

公司应收账款主要以政府事业单位，以及运营商、电力能源、金融等领域的企业客户为主。虽然客户资信状况良好，应收账款较少发生坏账，应收账款总体状况良好，但随着公司经营规模的扩大，应收账款金额较大，如出现客户信用发生变化等情况，公司存在应收账款坏账损失增大的风险。

2、期间费用较高的风险

报告期内公司期间费用主要由销售费用、研发费用和管理费用组成。

报告期内，为提高公司的市场占有率，建立完善的营销体系，公司加大对市场拓展的投入，2016-2018 年度，公司销售费用总额分别为 16,344.93 万元、17,155.27 万元和 18,482.70 万元，销售费用率分别为 30.69%、27.81%和 26.25%。最近三年，销售费用金额逐年增加，与营业收入的增长趋势相同，因营业收入增幅更大，导致销售费用率有所降低。

报告期内，为保持技术领先优势，提高公司的核心竞争力，公司持续加大研发投入，提高研发员工的薪酬待遇水平，储备研发技术人才，2016-2018 年度，公司研发费用总额分别为 13,404.59 万元和、14,355.20 万元和 15,792.33 万元，研发费用率分别为 25.17%和、23.27%和 22.43%。

2016-2018 年度，公司管理费用总额分别为 3,392.99 万元、2,422.33 万元和 2,347.89 万元，管理费用率分别为 6.37%、3.93%和 3.33%，2016 年度公司管理费用较高，主要系公司进行股权激励确认了 1,467.56 万元股份支付费用。

销售费用、研发费用和管理费用的投入，推动了市场渠道的建设，巩固、提

高了公司的行业地位，培养了研发人才、管理团队，为公司持续发展提供了动力。

未来几年内，为了进一步巩固公司的行业地位和竞争优势，公司将继续增加研发和销售等投入，相关期间费用可能持续增加。这些投入给公司技术创新能力、品牌价值和新产品开发能力所带来的提升效应将会在未来一定时间内逐步显现。期间费用投入与效益产生之间会有时间差，若短期内大规模投入未能产生预期效益，公司的经营业绩将会受到不利影响。

3、发行后净资产收益率下降的风险

2016-2018 年度，公司扣除非经常性损益后加权平均净资产收益率分别为 28.89%、19.48%和 20.95%。预计本次发行完成后，公司净资产将有较大幅度的增长。由于募集资金投资项目须有一定的建设周期，募集资金产生经济效益存在一定的不确定性和时间差。因此，短期内公司净资产收益率可能有一定幅度的下降，从而存在净资产收益率下降的风险。

4、经营活动产生的现金流量净额波动风险

2016-2018 年度，公司经营活动产生的现金流量净额分别为 9,183.67 万元、17,567.08 万元和 22,244.95 万元。基于对行业前景和公司发展的信心，公司业务规模持续增长，员工规模持续增长，产品的研发投入持续增加，导致公司支付给员工的工资及费用和采购支出增长。随着公司业务规模的不断增长，资金支出与销售回款之间存在一定的时间差异，从而影响经营活动产生的现金流量净额，导致资产流动性风险。

（六）募集资金投资项目的风险

本次发行募集资金，拟全部用于以下项目：

序号	项目名称	项目总投资（元）	拟投入募集资金（元）
1	安全威胁态势感知平台项目	115,369,800.00	115,369,800.00
2	新一代高性能云计算数据中心安全平台项目	171,568,100.00	171,568,100.00
3	新一代高性能应用交付平台项目	79,442,500.00	79,442,500.00
4	网络安全产品及相关软件开发基地项目	200,000,000.00	46,410,600.00
合计		**566,380,400.00**	**412,791,000.00**

公司本次发行募集资金投资项目是依据公司发展战略制定的，并进行了详尽的可行性分析。该等项目的实施有利于进一步提升公司核心竞争力、丰富产品线、扩大服务规模、降低运营成本，在开拓新业务和增强市场风险抵御能力等方面都具有重要的意义。但本次发行募集资金投资项目可能存在以下风险：

1、募投项目实施的风险

本次募集资金拟投资的项目是公司主营业务产品的技术改造和升级，并加强公司的研发能力。项目的可行性分析是基于目前的国家产业政策、国内外市场条件作出的。若国家产业政策发生变化或随着时间的推移，在项目实施时如果募集资金不能及时到位，或因市场环境突变、行业竞争加剧、项目建设过程中管理不善导致募集资金投资项目不能如期实施，都将会导致项目不能如期完成或不能实现预期收益，从而影响公司的经营业绩。

2、技术研发的风险

本次募集资金拟投资的安全威胁态势感知平台项目、新一代高性能云计算数据中心安全平台项目和新一代高性能应用交付平台项目，均是在公司原有技术基础上的进一步开发和升级，公司在相关项目中对诸多关键技术难点进行了预研和攻关，有效降低了项目整体风险。但技术的升级开发具有不确定性，如未能按期完成研发计划，可能会导致新产品推出时间延后。

另一方面，目前我国包括信息安全、网络应用在内的 IT 行业仍处于快速发展阶段，高级人才较为缺乏，行业内对高端技术人才的竞争非常激烈。公司上述拟投资项目中关键性技术和产品的研发均依赖于公司核心技术人员的专业知识、技术及经验。如果核心技术人员流失，将对募集资金项目的顺利实施造成一定的不利影响。

3、产品市场变化的风险

公司本次募投项目多为在原有技术和产品的基础上进行的技术升级和拓展开发，一方面可以更好的满足市场用户的差异化需求，提高公司产品的性能，保持并提高公司的市场占有率；另一方面，技术的更新开发有利于公司紧跟信息安全行业的技术发展趋势，提高公司的核心竞争力。

尽管公司已对上述募集资金投资项目产品的市场前景进行了充分的调研和论证，公司现有的客户可以成为上述募集资金投资项目产品的潜在客户，但公司在开拓新市场、推销新产品的过程中依然会面临一定的不确定性。如果本次募投项目所推出的新产品、新服务的未来市场空间低于预期，或公司推广新产品、新服务的效果与预测产生较大偏差，将会导致募集资金投资项目投产后达不到预期效益的风险。

四、发行人的发展前景评价

安全需求的提升一直是推动信息安全行业增长的一大因素。随着我国不断完善网络安全保障措施，网络安全防护水平进一步提升。根据 IDC《中国 IT 安全市场预测，2017-2021》报告预测，2017 年，中国信息安全硬件、软件、服务市场的规模为 41.56 亿美元，同比增长 23.91%，2012 年至 2017 年的年复合增长率为 20.10%，保持了快速增长态势。在整体信息安全硬件、软件、服务市场中，安全硬件市场的占比最大，为 56.47%，安全软件市场占比 17.18%，安全服务市场占比 26.35%。根据 IDC 研究报告预测，中国信息安全市场将保持快速增长，预计到 2021 年将达到 95.81 亿美元，2017 年至 2021 年的年复合增长率将为 23.22%。

如何构建可信的网络环境，加强信息安全防护水平，受到了国家以及企业的前所未有的关注和重视，发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。在此需求的推动下，各类信息安全产品和安全服务的市场空间得到了进一步增长，信息安全产品国产化替代趋势日益显著。除了政府政策的驱动，IT 第三平台的新兴技术云计算、大数据、移动以及社交网络的发展给信息安全市场带来了严峻挑战，同时这些技术热点也将是引领未来安全领域市场增长的主要方向。

基于对网络安全发展趋势及用户需求的深刻理解，公司致力于“让网络更简单、智能、安全”，持续专注于企业级网络通信领域的研发与创新。公司凭借先进的技术实力和完备的产品体系，通过持续不懈的市场及服务体系组织建设、客户及渠道拓展以及公司品牌建设，实现了市场的快速增长。公司产品广泛运用于运营商、政府、电力能源、教育、医疗、金融等众多行业。目前，公司已在北京

和杭州建立了研发中心，设立了 27 个办事处，同时在国内各个市场区域建立起广泛的渠道体系，实现各区域市场的深耕细作。未来，公司将充分受益于行业的高速发展，继续在企业级网络通信领域进行持续投入，进一步完善产品与解决方案，为社会和投资者创造更大价值。

本次募集资金拟投资项目为：（1）安全威胁态势感知平台项目、（2）新一代高性能云计算数据中心安全平台项目、（3）新一代高性能应用交付平台项目、（4）网络安全产品及相关软件开发基地项目。上述募投项目论证充分，项目符合国家产业政策，项目实施后，发行人将进一步提升在行业内的竞争力和品牌影响力。

综上，本保荐机构认为发行人未来发展前景良好。

五、保荐机构对本次证券发行的推荐结论

受发行人委托，中信建投证券担任本次迪普科技首次公开发行股票的保荐机构。中信建投证券本着行业公认的业务标准、道德规范和勤勉精神，对发行人的发行条件、存在的问题和风险、发展前景等进行了充分尽职调查、审慎核查，就发行人与本次发行有关事项严格履行了内部审核程序，并已通过保荐机构内核部门的审核。保荐机构对发行人本次发行的推荐结论如下：

本次公开发行股票符合《公司法》、《证券法》等法律、法规和规范性文件中有关首次公开发行股票的条件；募集资金投向符合国家产业政策要求；发行申请材料不存在虚假记载、误导性陈述或重大遗漏。

根据《中信建投证券股份有限公司投资银行类业务内核规则（试行）》，中信建投证券同意作为迪普科技本次公开发行股票的保荐机构，并承担保荐机构的相应责任。

（以下无正文）

（本页无正文，为《中信建投证券股份有限公司关于杭州迪普科技股份有限公司首次公开发行股票并在创业板上市之发行保荐书》之签字盖章页）

项目协办人签名：

洪　敏

保荐代表人签名：

赵　军　　谢思遥

保荐业务部门负责人签名：

吕晓峰

内核负责人签名：

林　煊

保荐业务负责人签名：

刘乃生

保荐机构总经理签名：

李格平

保荐机构法定代表人签名：

王常青

中信建投证券股份有限公司

2019年 3月 15日

附件一：

保荐代表人专项授权书

本公司授权赵军、谢思遥为杭州迪普科技股份有限公司首次公开发行股票并在创业板上市项目的保荐代表人，履行该公司首次公开发行股票并在创业板上市的尽职推荐和持续督导的保荐职责。

特此授权。

保荐代表人签名：赵军　谢思遥

赵　军　　谢思遥

保荐机构法定代表人签名：

王常青

中信建投证券股份有限公司

2019年 3月 11日

中信建投证券公司文件

中建证发〔2019〕261号　　签发人：吕晓峰

关于保荐代表人申报的在审企业情况及承诺事项的说明

中国证券监督管理委员会：

中信建投证券股份有限公司就担任杭州迪普科技股份有限公司首次公开发行股票并在创业板上市项目的保荐代表人赵军、谢思遥的相关情况作出如下说明：

保荐代表人	注册时间	在审企业情况（不含本项目）	承诺事项	是/否	备注
赵军	2013 年 8 月 13 日	主板（含中小企业板）1 家（上海锦和商业经营管理股份有限公司首发项目）	最近 3 年内是否有过违规记录，包括被中国证监会采取过监管措施、受到过证券交易所公开谴责或中国证券业协会自律处分	否	
		创业板 0 家	最近 3 年内是否曾担任过已完成的首发、再融资项目签字保荐代表人	是	江苏银河电子股份有限公司非公开发行项目于 2016 年 10 月在中小企业板上市、黑牛食品股份有限公司非公开发行项目于 2018 年 3 月在中小企业板上市
谢思遥	2018 年 4 月 23 日	主板（含中小企业板）0 家	最近 3 年内是否有过违规记录，包括被中国证监会采取过监管措施、受到过证券交易所公开谴责或中国证券业协会自律处分	否	
		创业板 0 家	最近 3 年内是否曾担任过已完成的首发、再融资项目签字保荐代表人	否	

中信建投证券股份有限公司

2019 年 3 月 14 日

（联系人：杨浩 15201927889）

中信建投证券股份有限公司综合管理部 2019 年 3 月 14 日印发

中信建投证券股份有限公司

关于杭州迪普科技股份有限公司成长性的专项意见

中国证券监督管理委员会：

杭州迪普科技股份有限公司（以下简称“迪普科技”、“发行人”或“公司”）拟申请首次公开发行 A 股股票并在创业板上市（以下简称“本次证券发行”或“本次发行”），并已聘请中信建投证券股份有限公司（以下简称“中信建投”）作为首次公开发行 A 股股票并在创业板上市的保荐机构。

中信建投本着诚实守信、勤勉尽责的原则，认真比照《首次公开发行股票并在创业板上市管理办法》、《公开发行证券的公司信息披露内容与格式准则第 29 号——首次公开发行股票并在创业板上市申请文件（2014 年修订）》等法律法规和规范性文件的规定，对发行人进行了审慎调查，认为迪普科技符合首次公开发行股票并在创业板上市有关成长性方面的要求。现就发行人成长性出具专项意见，具体内容如下：

（本专项意见中如无特别说明，相关用语具有与《杭州迪普科技股份有限公司首次公开发行股票并在创业板上市招股说明书（申报稿）》中相同的含义）

一、发行人经营业务开展情况

（一）公司主营业务和主要产品情况

公司以“让网络更简单、智能、安全”为愿景，专注于企业级网络通信领域，致力于为用户提供完备的产品和解决方案。通过持续的研发与创新，公司推出了全面覆盖企业级网络通信主要应用领域的共十余类上百款产品，形成了有较强竞争力的完备产品线。主要产品和服务如下表所示：

业务分类		具体产品和服务	简要说明
网络安全产品	安全防护产品	应用防火墙（FW）	实现网络边界安全防护，对进、出不同网络安全域的数据访问行为进行安全控制，确保网络访问的合法性。
		入侵防御系统（IPS）	深度检测与智能防御系统漏洞攻击、病毒蠕虫、DDoS 攻击、网页篡改、间谍软件、恶意攻击、流量异常等网络应用层威胁。

业务分类		具体产品和服务	简要说明
		Web 应用防火墙（WAF）	为 Web 应用提供保护，对来自 Web 客户端的各类请求进行检测和验证，对非法的请求和内容予以实时阻断，防护 SQL 注入、跨站脚本、网页挂马等常见 Web 攻击。
		异常流量清洗系统（Guard、Probe）	Probe 用于实时检测 DDoS 攻击，Guard 用于对 DDoS 攻击流量进行实时阻断，配合形成异常流量清洗系统，自动发现网络中的 DDoS 攻击并进行实时阻断。
		物联网应用安全控制系统（DAC）	对物联网、视频监控网等场景使用的白名单准入控制及应用控制，实现对物联网全网范围内前端 IP 设备和传输的流量进行精确管控，防范非法私接、设备仿冒、非法扫描、DDoS 攻击等。
	安全分析产品	DPI 流量分析设备	对网络中的流量进行采集，同时针对流量中的业务应用以及报文内容进行深度识别与分析，与第三方应用系统配合，实现网络流量分析、网络优化及安全管控。
		漏洞扫描系统（Scanner）	及时发现网络设备、主机、应用等系统的漏洞隐患，提供漏洞通告、自动修复、安全基线检查、资产风险管理等功能，实现对网络中各种资产全方位、高效的漏洞检测与管理，对黑客攻击的主动防御。
应用交付产品		应用交付平台（ADX）	提高用户业务应用稳定性和质量，避免服务器宕机或链路故障对业务应用的影响，确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展。
		上网行为管理及流控（UAG）	对网络中的用户上网行为进行分析控制，保障网络资源合理使用，保证关键应用和关键用户的网络服务质量。
		高速缓存加速系统（DeepCache）	网络内容的自动缓存与访问加速，将高速缓存加速系统部署到局域网中，自动缓存用户频繁访问的网络内容，后续访问时通过局域网提供，提升用户访问速度、改进上网体验，有效节约出口带宽，降低带宽成本。
		统一管理中心（UMC）	对网络中各类安全设备、网络设备的统一管理，对网络日志事件信息的统一收集、过滤、归并和关联性分析，实现对整网用户上网行为、应用访问行为、流量应用组成、网络及应用质量、安全和攻击状态等全方位的监控，为用户直观呈现网络运行中各维度的实时状态和历史状态。
基础网络产品		深度业务路由交换网关（DPX）	公司各产品线通用的多业务核心平台，采用分布式高性能的框式架构，提供与业界

业务分类	具体产品和服务	简要说明
		主流核心交换机相匹敌的网络功能和大容量交换能力，可作为高端交换机使用，也可单独插入各类安全和应用交付业务板，作为高端安全产品和应用交付产品使用，也支持一起插入多类安全和应用交付业务板，作为融合网络、安全以及应用交付等各类业务功能于一体的高性能综合网关使用。
	盒式交换机（LSW）	针对企业级园区网、数据中心、工业网络等网络场景使用的网络接入交换机，在提供完善的传统网络特性和数据中心特性的同时，在网络接入边缘加强了对接入用户和接入流量的安全管控。
	WLAN 产品（AC、AP）	在公共场所、校园、酒店、写字楼等各类需要无线覆盖的场景提供 WIFI 无线网络的信号覆盖与控制，为用户提供无线上网功能。
	路由器产品（XR）	城域网、企业广域网、企业园区互联和数据中心网络出口等广域网络场景使用的互联互通设备。
服务类业务	安全服务	通过为用户提供安全技术服务，帮助用户完善信息系统安全防护能力，提升安全运维水平。服务内容包含安全风险评估、渗透测试、等保差距分析、安全技术体系规划、安全管理咨询、等保差距整改、安全巡检、安全加固、安全应急响应、安全通告、安全攻防演练等。
	维保服务	远程及现场技术支持、软件升级、备件先行更换、网络运行管理支持，帮助客户维护安全、高效、稳定的 IT 环境，提高网络生产力。

1、网络安全产品

公司基于具有自主知识产权的一系列攻击检测与防护技术、自主研发的高性能软硬件平台、以及网络与安全融合的产品设计理念，推出了一系列在安全防护能力、性能、组网能力等方面具有较强竞争力的网络安全产品，主要分为安全防护、安全分析两类产品。安全防护产品体系主要包括应用防火墙（FW 系列产品）、入侵防御系统（IPS 系列产品）、Web 应用防火墙（WAF 系列产品）、异常流量清洗（Guard、Probe 系列产品）、物联网应用安全控制系统（DAC 系列产品）等，安全分析产品体系主要包括 DPI 流量分析设备、漏洞扫描系统（Scanner 系列产

品）等。

（1）应用防火墙（FW 系列产品）

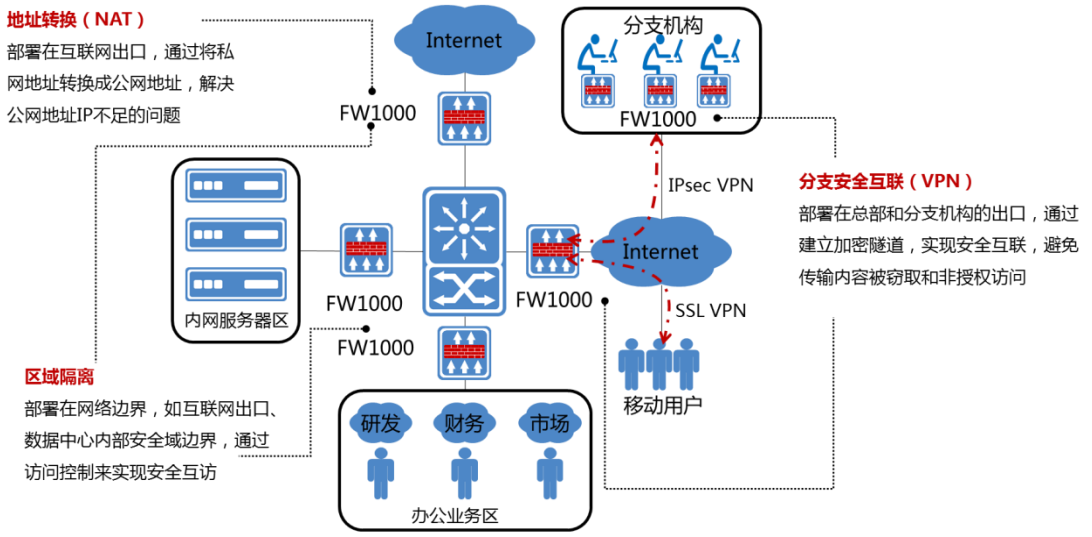
FW 系列应用防火墙用于实现网络边界安全防护，对进、出不同网络安全域的数据访问行为进行安全控制，确保网络访问的合法性。

产品基于高性能硬件架构，提供基于用户及应用的访问控制功能，支持入侵防御、URL 过滤等特性。产品配备由专业安全研究团队维护的 APP-ID 特征库，能够识别应用程序，无需考虑协议以及端口，并以此为基础匹配安全策略，实现对于网络行为的管控；通过识别和匹配用户而非仅识别 IP 地址，实现无论用户位于何处，均可保证安全策略能够始终作用于对应的用户；能够根据不同业务系统特点，配置对应安全策略的有效时间，保障业务运行安全、高效。产品主要技术特点如下表所示：

技术特点	简要说明
丰富的安全功能	支持应用控制、入侵防御、URL 过滤等安全功能，实现深入的应用层攻击防护；专业漏洞库团队提供实时可灵活升级的攻击特征库；内置专业防病毒引擎，可有效防止病毒威胁。
基于用户及应用的访问控制	基于用户部署应用访问控制策略，保证不论用户物理位置如何变化，使用什么种类的应用程序，只要其用户权限不变，安全策略就始终紧跟用户。
丰富的 NAT 能力	支持源地址 NAT、目的地址 NAT、一对一 NAT、端口块 NAT、对称 NAT、NAT64 等 NAT 方式；支持多种应用协议；支持组播 NAT。
强大的网络特性	支持 IPv4/IPv6，支持静态路由、策略路由、RIP v1/2、OSPF、BGP 等多

技术特点	简要说明
	种路由协议，支持 MPLS VPN，支持组播协议。
支持虚拟化防火墙，应用能力按需调度	支持 N:M 虚拟化，可将 N 台设备虚拟成一个资源池，再将资源池按需分成 M 台逻辑设备，实现云计算环境下资源池的动态调度。
全内置 VPN	支持 IPSec VPN、L2TP VPN、GRE VPN、SSL VPN，并且全内置硬件加密芯片，减少安全建设投入。
性能优异	基于自主研发的硬件架构 APP-X，保证高带宽以及多策略下稳定运行，并可通过 N:M 虚拟化进行多设备性能聚合，实现性能的倍增。
智能运维模块	通过统计会话日志，自动生成安全策略模拟业务处理过程，及时发现故障并解决。

FW 系列应用防火墙可广泛应用于园区网、数据中心网络区域隔离、网络出口及边界 NAT 地址转换、分支机构安全互联等场景。产品主要应用场景如下图所示：



（2）入侵防御系统（IPS 系列产品）

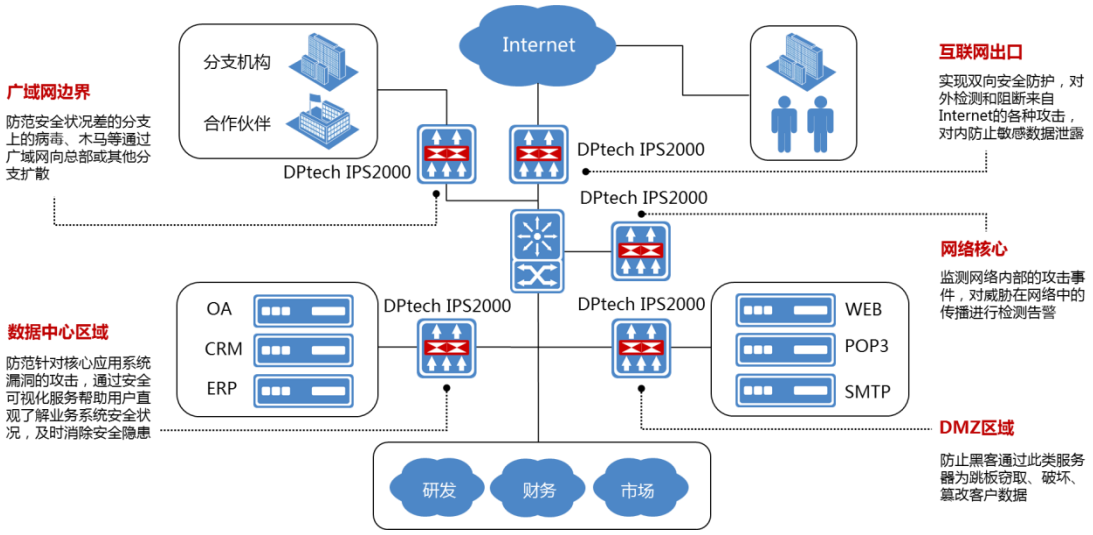
IPS 系列入侵防御系统用于深度检测与智能防御系统漏洞攻击、病毒蠕虫、DDoS 攻击、网页篡改、间谍软件、恶意攻击、流量异常等网络应用层威胁。

产品增加了敏感数据保护能力、未知威胁防御能力以及深度应用感知能力，提供了更精准的检测、更优化的管理能力，实现了对网络基础设施、服务器等用户关键设施的全面保护。产品主要技术特点如下表所示：

技术特点	简要说明

技术特点	简要说明
威胁检测引擎	具备防逃逸检测引擎、协议智能推导引擎、协议语义解析引擎和虚拟环境检测引擎，全面实现多种安全威胁的发现与检测。
深度应用层攻击检测与防御	具备全面的 L4~7 应用检测与防御能力，支持对缓冲溢出攻击、蠕虫、木马、病毒、SQL 注入、网页篡改、恶意代码、网络钓鱼、间谍软件、DoS/DDoS、流量异常等攻击的防御。
敏感数据保护能力	具备应用识别、敏感数据识别能力，可以基于时间生效相应的防护策略，对用户的关键数据进行保护。
防高级逃逸攻击能力	基于智能数据包重组技术对逃逸攻击进行深度检查，避免黑客绕过安全检测。
专业病毒防护能力	内置专业病毒库，支持新一代虚拟脱壳和行为判断技术，支持防御文件型、网络型和混合型等各类病毒。
变种攻击防护能力	支持对分片逃逸、乱序逃逸、编码变形逃逸等变种攻击进行检测及防御。
专业特征库团队	实时跟踪国内外最新安全技术，提供集漏洞库、病毒库、协议库于一体的专业特征库，特征库完全兼容 CVE。
虚拟化能力	具备多租户环境下的资源统一划分、策略统一管理能力，不同租户之间可以实现转发隔离及安全自主监控。
深度报文检测能力	支持丰富的网络特性，可以识别并检测 QinQ、PPPoE、MPLS、GRE 等特殊封装的网络报文。
安全可视化能力	对用户整体安全风险进行评级 ，针对攻击级别较高的攻击事件提供安全解决方案。

IPS 系列入侵防御系统可应用于互联网出口攻击防护及敏感数据防泄漏、网络核心内部攻击及病毒防护、DMZ（demilitarized zone，隔离区）区域及数据中心业务系统保护、广域网边界病毒木马防扩散等使用场景。产品主要应用场景如下图所示：



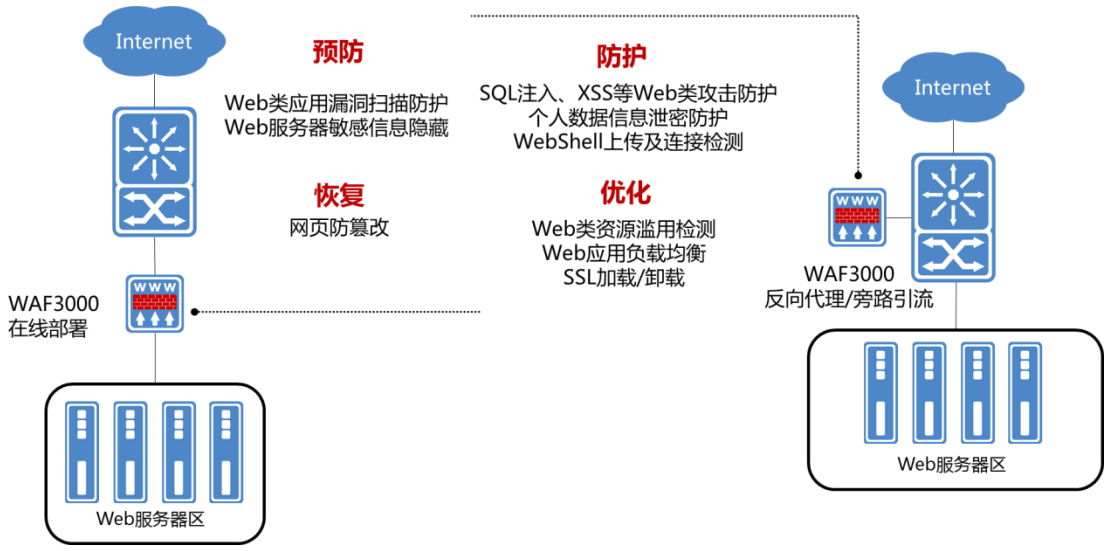
（3）Web 应用防火墙（WAF 系列产品）

WAF 系列 Web 应用防火墙为 Web 应用提供保护，对来自 Web 客户端的各类请求进行深度内容检测和验证，对非法的请求和内容予以实时阻断，防护 SQL 注入、跨站脚本、网页挂马等常见 Web 攻击。

产品具有高效、完备的 Web 威胁深度防护、Webshell 检测、协议语义解析引擎、Web 类漏洞扫描防护、网页防篡改、Web 应用优化等能力，可以全面保证用户 Web 应用的安全，随时应对最新的 Web 安全威胁。产品主要技术特点如下表所示：

技术特点	简要说明
实时 Web 漏洞扫描防护	基于指纹识别及行为分析引擎，对主流扫描工具、异常探测行为进行实时阻断，可对 SQL 注入、跨站脚本攻击、会话劫持等攻击进行防护。
自主研发 WebShell 检测	采用自主研发的 WebShell 风险分值检测引擎，准确阻断 WebShell 上传及连接行为。
针对性的网页防篡改能力	通过采用自主研发的页面指纹技术和白名单技术，对动态及静态页面提供针对性防篡改方案。
OWASP TOP10 攻击防护	深入分析 OWASP TOP10 及各种最新 Web 攻击原理，提供针对性检测方法，确保防护策略及时有效。
Web 服务器敏感信息隐藏	可对服务器版本号、操作系统类型等敏感信息进行隐藏，避免被攻击者收集、利用，保护 Web 服务器敏感信息不泄露。
Web 层 DDoS 防护	支持拒绝服务攻击防御，抵御针对 Web 的应用层 DDoS 攻击，比如 CC 攻击、慢速 DDoS 等。
HTTP 协议加固	支持 HTTP 协议加固：非标准协议过滤、Cookie 正规化、缓冲区溢出保护。
Web 服务器加固	支持 Web 服务器加固：服务器信息隐藏、网络爬虫检测和阻止。
Web 流量优化	对 Web 类应用进行 SSL 加载/卸载、负载均衡，提升用户应用体验，保障业务可靠性。

WAF 系列 Web 应用防火墙针对各类 Web 服务器的安全威胁事前预防、Web 攻击事中防护、Web 页面事后恢复、以及 Web 应用优化等使用场景提供服务。产品主要应用场景如下图所示：



（4）异常流量清洗系统（Guard、Probe 系列产品）

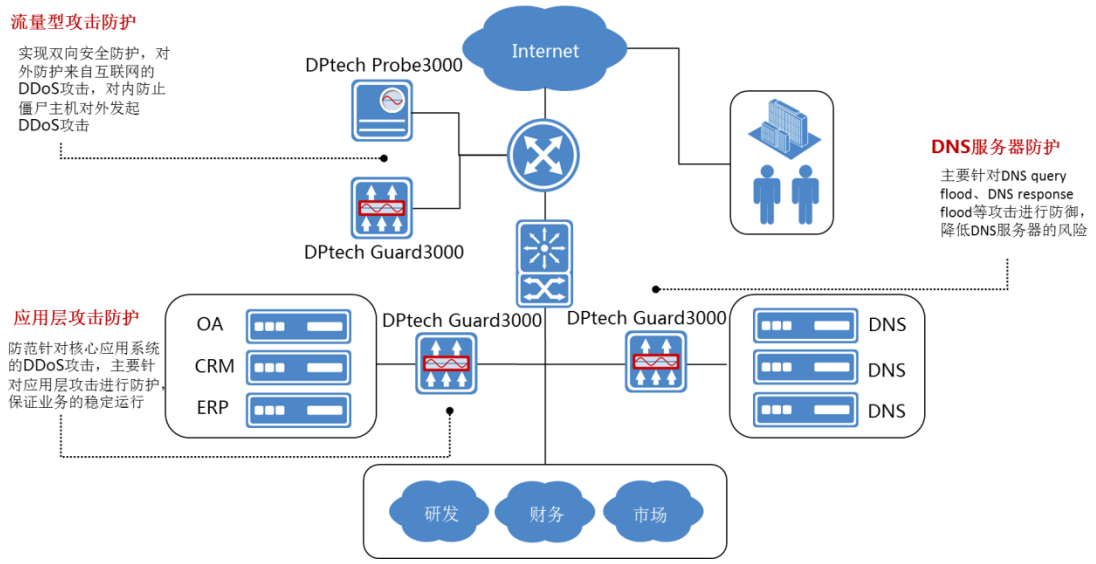
异常流量清洗系统用于专门防御 DDoS 攻击，包括异常流量检测 Probe、异常流量清洗 Guard、异常流量清洗业务管理平台，Probe 用于实时检测 DDoS 攻击，Guard 用于对 DDoS 攻击流量进行实时阻断，配合形成异常流量清洗系统，自动发现网络中的 DDoS 攻击并进行实时阻断。

产品具备精确有效的 DDoS 攻击智能检测与防御技术，支持全方位的 DNS 攻击防护、智能自学习防护模型、自动流量牵引和灵活的流量回注，具备很好的扩容性，完整支持主流路由协议，具备领先的路由组网能力。产品主要技术特点如下表所示：

技术特点	简要说明
全面 DDoS 攻击防范	支持基于 IPv4/v6 双栈下的 SYN/ACK Flood、ICMP Flood、UDP Flood、DNS Query Flood、HTTP Get Flood、CC、Connections Flood 等常见 DDoS 攻击手段的防护。
可对双向流量进行检测及防护	Guard 支持在线部署，支持异常流量检测和防护一体化，可以对双向流量进行实时清洗防护。
模糊攻击检测能力	在攻击源、防护对象不确定的情况下，通过全局检测方式统计 TOPN 攻击，基于 TOPN 信息配置精细防护策略。
内部集成溯源分析能力	平台内部集成一套抓包溯源与攻击自动分析工具，帮助用户对 DDoS 攻击追踪溯源，并支持一键提取攻击特征。
未知攻击自学习能力	支持流量突变检测、应用行为突变检测、报文信息突变检测能力建立自动学习模型，可实现未知攻击防护。
协议漏洞威胁防护	支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，比如 Land、Smurf、Fraggle、Tear Drop、Winnuke。

技术特点	简要说明
多种异常流量检测方式	基于 NetFlow/NetStream/SFlow 协议的流量检测方式（DFI）、深度数据包检测方式（DPI）。
攻击取证	支持抓包溯源功能，支持抓取清洗前、清洗后、清洗丢弃的报文进行分析；针对抓包文件可以进行攻击源 IP 溯源，并提取攻击报文中的攻击特征下发到清洗设备过滤。
多租户自服务能力	多租户环境下，支持租户账号分配、检测清洗策略自配置、租户管理权限划分以及报表单独导出。
复杂网络适应能力	旁路部署模式下，支持通过 BGP 技术进行流量牵引，流量回注技术可使用 GRE、策略路由、MPLS 等技术。

异常流量清洗系统可应用于互联网出口双向 DDoS 攻击防护、业务系统前端应用层 DDoS 攻击防护、DNS 服务器前端 DDoS 攻击防护等场景。产品主要应用场景如下图所示：



（5）物联网应用安全控制系统（DAC 系列产品）

DAC 系列物联网应用安全控制系统用于准入控制及应用控制物联网、视频监控网等场景使用的白名单，实现对物联网全网范围内前端 IP 设备和传输的流量进行精确管控，只有通过认证的设备才允许接入，只有合法的应用才允许在网络中传输，防范非法私接、设备仿冒、非法扫描、DDoS 攻击等。

产品主要技术特点如下表所示：

技术特点	简要说明
物联网应用识别能力	可以比较全面的识别物联网常用应用和协议，可以准确识别国标 GB28181 和主流监控厂商私有的各类视频应用、各类常用的管理协

技术特点	简要说明
	议及数据采集协议，可以比较完整的覆盖视频监控网的常见应用。
准入认证功能	支持 IP/MAC 绑定、IP 过滤、MAC 过滤、MAC 认证、1X 认证、DHCP option82 认证等准入认证功能。
基于白名单的安全控制功能	只有通过认证的设备才允许接入，只有合法的应用才允许在网络中传输，从而防范非法私接、设备仿冒、非法扫描、DDoS 攻击等问题。
资产管理功能	通过主动探测和监听识别，准确监测网络中接入终端的类别、数量以及在线情况，为用户提供有效的资产管理手段。
透明可视的网管功能	通过统一的网管中心，对物联网中所有接入终端的类别、数量、在线情况、流量大小、应用组成以及各种非法接入的告警和阻断日志进行集中展现，实现整个网络业务情况的透明可视。

DAC 系列物联网应用安全控制系统可应用于平安城市、智能交通、电力能源、医疗、生产自动化等行业。特别对于视频监控应用场景，产品能够解决海量 IP 摄像机及其他前端 IP 设备的接入认证和安全管控问题，帮助用户构建一张安全可控的物联网。

（6）DPI 流量分析设备

DPI（Deep Packet Inspection）流量分析设备用于对网络中的流量进行采集，同时针对流量中的业务应用以及报文内容进行深度识别与分析，并将满足其它系统所需的流量或分析统计数据分发给各第三方应用系统。与第三方应用系统配合，实现网络流量分析、网络优化以及安全管控。

产品完成数据采集、流量分析统计、日志合成，并执行由第三方应用系统下发的流量管理策略，第三方应用系统主要完成针对 DPI 设备上报数据的进一步分析处理、存储以及统一呈现，同时负责流量管理策略的统一管理与维护。产品主要技术特点如下表所示：

技术特点	简要说明
丰富的接口类型	支持 GE、10G、40G、100G 以太口以及 2.5G、10G、40G POS 口等丰富的接口类型，适应各类组网。
高精度的应用识别能力	内置高精度的应用识别引擎，能准确识别各类网络应用。
全面的报文解析能力	除了常规的 IPv4/IPv6 报文，同时支持对 PPPoE、MPLS、GRE、VxLAN 等各类隧道封装报文的解析功能。
高性能深度报文内容识别能力	通过高性能的关键字和特征匹配算法，实现针对深度报文内容的精准识别功能。

技术特点	简要说明
性能优异	产品采用分布式高性能的框式架构，利用 FPGA 作为业务处理单元，具备高性能、低时延的特点，整机最高支持 3.2Tbps 的业务处理能力。

（7）漏洞扫描系统（Scanner 系列产品）

Scanner 系列漏洞扫描系统用于及时发现网络设备、主机、应用等系统的漏洞隐患，实现漏洞通告、自动修复、安全基线检查、资产风险管理，对网络中各种资产全方位、高效的漏洞检测与管理，对黑客攻击的主动防御。

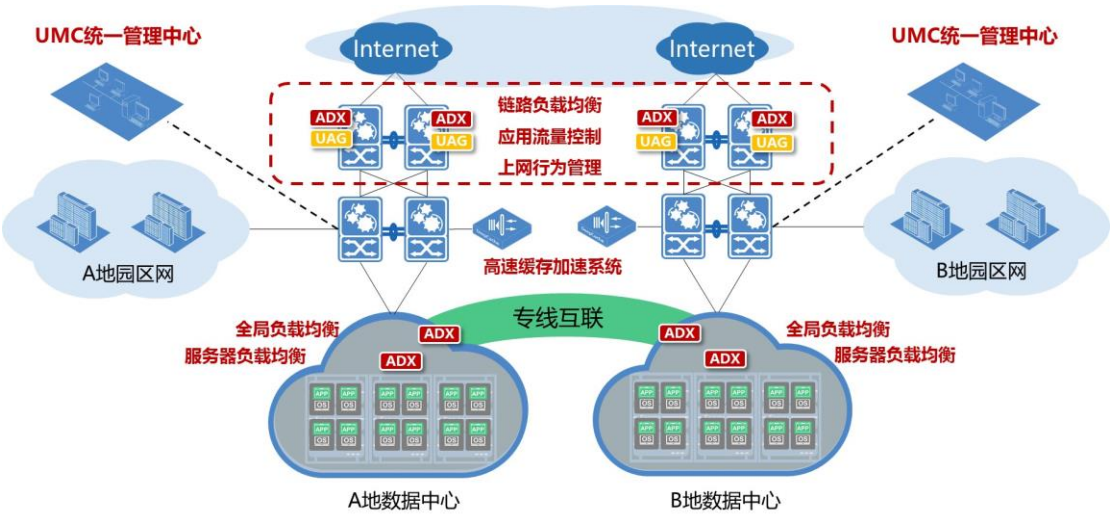
产品同时具备主机漏洞扫描、Web 漏洞扫描和安全基线检查三个功能模块，可应对超大规模的扫描目标，满足等级保护中安全管理方面的要求；支持主动防御，智能联动；支持自动补丁管理，及时解决潜在风险；支持漏洞库自动更新，持续安全防护。产品主要技术特点如下表所示：

技术特点	简要说明
支持多种网络资产	支持终端设备、服务器、路由/交换设备等网络资产，支持多种操作系统（Windows/Linux/Unix）、应用服务、数据库。
支持大规模目标扫描	支持超过 1000 以上的扫描目标对象，支持批量导入 IP 地址、域名 URL 混合的目标对象。
深度 Web 漏洞扫描	Web 服务器检测、插件检测、配置检测、注入攻击漏洞检测、注射攻击漏洞检测、远程文件检索漏洞检测、文件上传检测、FORM 弱口令检测、数据窃取检测、GOOGLE-HACK 检测、中间人攻击检测、Web2.0 AJAX 注入检测、Cookies 注入检测、弱口令扫描。
网页木马检测	支持各种类型木马检测、木马分析、木马溯源。
应用漏洞扫描	SMTP/POP3、FTP、SNMP、端口扫描、弱口令扫描。
多种扫描方式	支持定时扫描、手动扫描等多种扫描方式。
支持网络爬虫方式	可自定义扫描深度、预定义用户登录参数、提供交互式用户登录参数设置、支持并发扫描。
安全基线检查	支持根据不同行业不同等级的安全要求，灵活地调整基线标准，主动发现和提出安全管理方面的整改意见。
自动漏洞修复能力	自动补丁管理，可与微软 WAUS 联动。
丰富的报表功能	可提供扫描结果对比、漏洞报告、统计分析等多种报表类型。

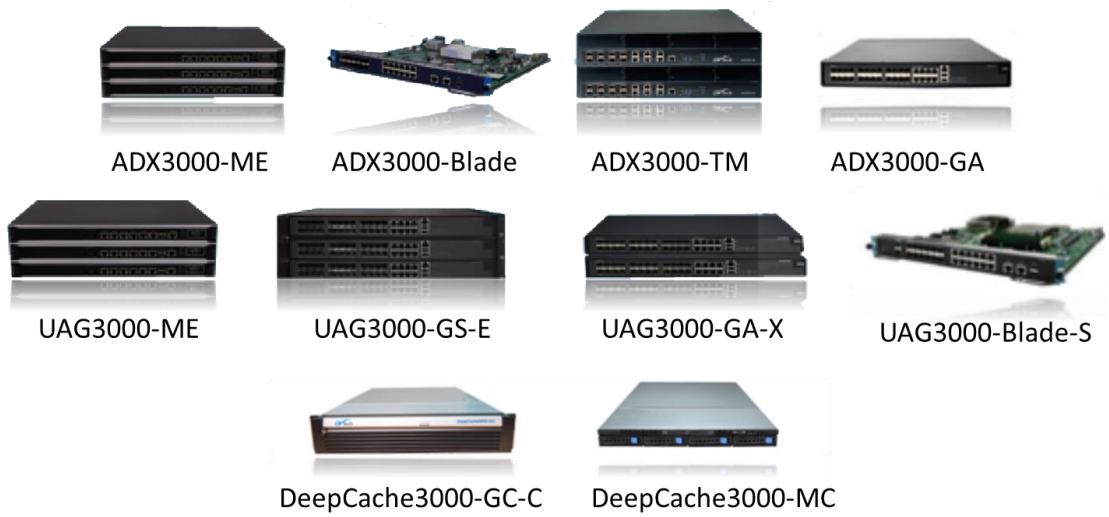
Scanner 系列漏洞扫描系统可应用于安全合规、业务系统漏洞发现及管理、Web 漏洞发现、木马检测、安全基线检查等场景。

2、应用交付产品

公司基于应用智能识别、应用访问控制、用户/应用带宽保障与控制、上网行为管理与审计、应用智能负载均衡、应用加速等一系列核心技术，推出了一系列应用交付产品，主要提供应用识别及流量控制、安全审计、优化网络应用的访问体验、提升应用可靠性、提高网络资源的利用效率等功能，实现网络中各应用可视可控、确保各应用安全高效交付的目标。应用交付产品体系主要应用场景如下图所示：



公司的应用交付产品体系主要包括应用交付平台（ADX 系列产品）、上网行为管理及流控（UAG 系列产品）、高速缓存加速系统（DeepCache 系列产品）、统一管理中心（UMC 系列产品）。



（1）应用交付平台（ADX 系列产品）

ADX 系列应用交付平台用于提高用户业务应用稳定性和质量，避免服务器宕机或链路故障对业务应用的影响，确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展。

产品通过链路负载均衡、服务器负载均衡、全局负载均衡、服务器性能优化、SSL 卸载、应用加速等多种技术，在不中断业务的情况下按需扩展链路和服务器。产品主要技术特点如下表所示：

技术特点	简要说明
多功能融合全面覆盖应用需求	融合链路负载均衡、服务器负载均衡、全局负载、SSL 加速、HTTP 压缩、Best TCP 优化、深度健康检查、温暖上下线等各类应用交付技术，确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展，有效改善用户体验。
深入的应用积累	在众多行业有深入积累，对各行业主流应用有深入的理解，同时能及时响应用户新型行业应用相关应用交付特性的开发需求。
应用适应能力	支持开发编程脚本语言（ADL），可快速匹配并满足用户个性化需求。
广域虚拟化技术	将广域异地多出口链路资源整合为一体，异地带宽也能均衡利用。
基于应用的调度	针对应用选择链路的调度方法，可精确实现业务资源的调配，能对 P2P、视频等流量进行调度，让关键业务的传输质量得到保障。
丰富的网络特性	支持 IPv4/IPv6、OSPF、RIP、MPLS 等协议，满足复杂网络环境的组网要求。
优异的性能	基于自主研发的硬件架构 APP-X，保证大带宽以及多策略下仍然稳定运行，并可通过 N:M 虚拟化进行性能聚合，实现性能的倍增。

ADX 系列应用交付平台全面支持服务器应用负载均衡与应用优化、链路负载均衡及优化、多数据中心全局负载均衡三大功能，可全面服务于数据中心应用可用性保障、应用访问性能优化、跨数据中心访问调度以及互联网出口多链路流量调度等场景。

（2）上网行为管理及流控系统（UAG 系列产品）

UAG 系列上网行为管理及流控系统用于对网络中的用户上网行为进行分析控制，保障网络资源合理使用，保证关键应用和关键用户的网络服务质量。

产品利用自主开发的深度应用特征智能识别技术，实现对网络应用的高精度识别和网络内容的透明可视；利用高性能的访问控制和行为审计技术，实现用户

上网行为的安全可控；利用特有的质量感知技术，为用户提供网络排障和应用优化的准确指导；利用自主开发的低带宽损耗流控技术，有效优化网络应用的传输质量和最终用户体验。产品主要技术特点如下表所示：

技术特点	简要说明
高应用识别率	可识别超过 4300+以上协议，让网络应用清晰可见。
基于用户实名审计	支持与主流认证系统对接，实现用户上网行为实名制。
多功能融合	上网行为管理、流量控制、行为审计、流量分析、NAT、负载均衡、访问控制等多功能合一。
低带宽损耗流控技术	通过应用速率抑制技术，在进行流量管理时，将带宽消耗降低到5%以内。
丰富的网络特性	支持 IPv4/IPv6、OSPF、RIP、MPLS 等协议，满足复杂网络环境的组网要求。
终端用户认证	多终端，多场景、多种认证方式接入，支持本地认证、Portal 认证、短信认证、微信认证等多种认证方式。
应用虚拟化	支持 N:M 虚拟化，可将多台虚拟成一个资源池，再将资源池按需分成多台逻辑设备，实现云计算环境下资源池的动态调度。
优异性能	可提供超过 200G 单设备性能，并可通过 N:M 虚拟化进行性能聚合，实现性能的倍增。

UAG 系列上网行为管理及流控系统可应用于互联网出口流量优化、网络使用者行为管理及上网行为安全审计等场景。

（3）高速缓存加速系统（DeepCache 系列产品）

DeepCache 系列高速缓存加速系统用于网络内容的自动缓存与访问加速，将高速缓存加速系统部署到局域网中，自动缓存用户频繁访问的网络内容，后续访问时通过局域网提供，提升用户访问速度、改进上网体验，有效节约出口带宽，降低带宽成本。

产品主要技术特点如下表所示：

技术特点	简要说明
多种内容格式全面缓存	支持视频、音乐、HTTP 下载、P2P 下载、APP 应用等多种文件缓存。
热点资源提前主动预缓存	主动获取热门资源，“提前”提供加速服务。
可实现高性能集群部署	采用高度集成的模块化设计方案，可按需平滑扩容升级，支持万兆网络环境的缓存服务。

技术特点	简要说明
智能自定义缓存策略	允许用户自主制定缓存策略，主动选择下载缓存资源的时段。与应用交付系统智能联动，避免缓存下载抢占网络流量高峰时段带宽资源。
移动终端加速	支持手机等移动终端的缓存服务，包括移动终端应用、网页、视频 ，为用户提供全面的网络加速。
实时分发机制	缓存资源实时下载、实时分发，无需内容全部下载完毕即可为用户提供服务。
精确的服务策略	支持配置服务网络地址段，只对来自已配置的地址段的互联网访问进行监听并提供缓存服务。
异常流量告警	支持对异常流量的告警功能，当网络中出现流量突增突降等异常情况时会给予提示。
加速引擎	具有 Web Acc 加速引擎，采用高度优化的协议处理和转发框架，可以提供高性能大并发的处理能力，并支持多设备集群管理。

DeepCache 系列高速缓存加速系统主要应用在互联网出口。

（4）统一管理中心（UMC 系列产品）

UMC 系列统一管理中心用于对网络中各类安全设备、网络设备的统一管理，对网络日志事件信息的统一收集、过滤、归并和关联性分析，实现对整网用户上网行为、应用访问行为、流量应用组成、网络及应用质量、安全和攻击状态等全方位的监控，为用户直观呈现网络运行中各维度的实时状态和历史状态。

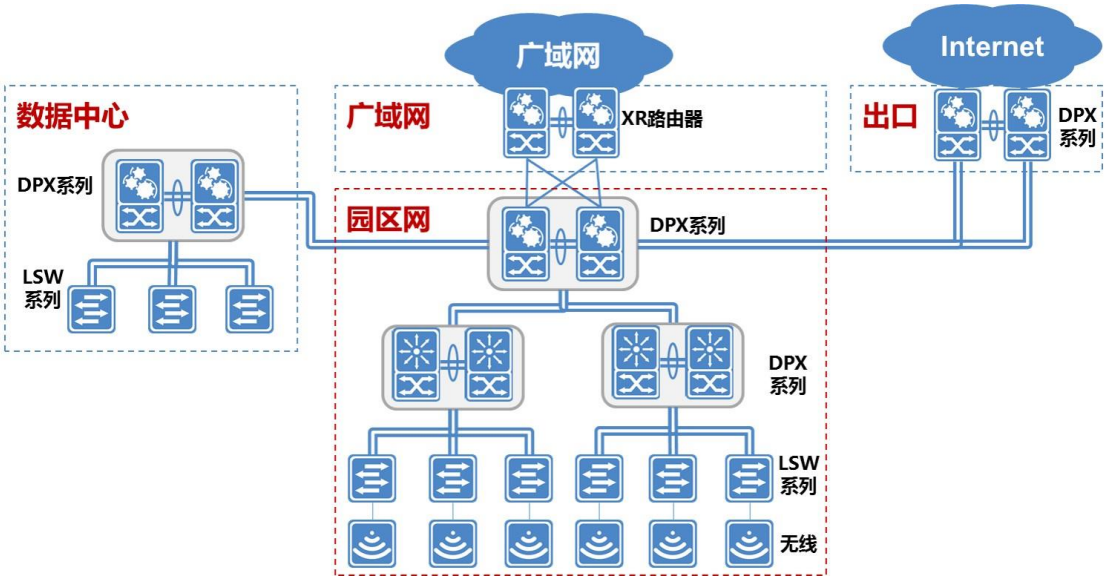
产品可对网络资源提供网络拓扑、性能图表展示、故障分级报警、策略配置统一分发和系统分级分域等功能，可对公司全系列产品进行组件化管理，各组件之间能够深度智能关联，将隔离、分散的不同系统整合为一体化管理平台，降低网络运维成本，提升网络管理效率。产品主要技术特点如下表所示：

技术特点	简要说明
统一的管理能力	通过对网络中各类日志事件信息的统一收集、过滤、归并和关联性分析，实现对整个网络中用户上网行为、应用访问行为、流量应用组成、网络及应用质量、安全和攻击状态等全方位的监控功能，同时具备安全预警、日志留存、集中配置等功能，可为用户直观的呈现网络运行中各维度的实时状态和历史状态，实现针对整网的安全智能管理。
角色权限管理	提供操作员角色分配的功能，为不同管理角色分配相应操作和日志查看等权限，同时还提供操作员分权限管理功能，可以根据设备和用户单独进行分权限管理，不同操作员管理指定设备，或者查看指定用户的日志等权限功能。

技术特点	简要说明
系统分级管理	支持 UMC 分级配置，即可设置为独立管理的 UMC，也可对 UMC 进行上下级分配，符合用户网络分级管理需求。
拓扑管理	可对管理范围内的设备进行自动发现，支持多种自动生成拓扑的算法，可自动生成完整准确的拓扑，支持链路超负载等告警功能。
深度智能关联分析	实现各类产品数据之间的深度智能关联，将隔离、分散的不同系统整合为能够一体化联动的综合系统平台。
安全分析与预警	对安全信息与事件进行分析，关联聚合常见的安全问题，过滤重复信息，发现隐藏的安全问题，使管理员能够轻松了解突发事件的起因、发生位置、被攻击设备和端口，并能根据预先制定的策略做出快速的响应，保障网络安全。配合公司的专业安全评估服务，可为用户网络安全建设提供专家级的管理平台。

3、基础网络产品

公司推出了覆盖园区网、数据中心等常见组网场景的一系列基础网络产品。产品体系主要应用场景如下图所示：



公司的基础网络产品体系主要包括深度业务路由交换网关（DPX 系列产品）、盒式交换机（LSW 系列产品）、WLAN 产品（AC、AP 系列产品）以及路由器产品等（XR 系列产品）。

（1）深度业务路由交换网关（DPX 系列产品）

DPX 系列深度业务路由交换网关是公司各产品线通用的多业务核心平台，采用分布式高性能的框式架构，提供与业界主流核心交换机相匹敌的网络功能和大容量交换能力，支持插入应用防火墙、入侵防御、异常流量清洗、Web 应用防火墙、物联网应用安全控制、流量分析、上网行为管理及流控、应用交付等一系列业务板以及各类接口板，既可作为高端交换机使用，也可单独插入各类网络安全和应用交付业务板，作为高端网络安全产品和应用交付产品使用，也支持一起插入多类安全和应用交付业务板，并且通过业务流定义、云板卡等核心技术，实现网络、安全以及应用交付等各类业务功能的“一体化部署、一体化配置、一体化防御、一体化管理”，为用户提供高性能一体化的融合网关解决方案，简化用户部署运维的工作量和复杂度。

产品主要技术特点如下表所示：

技术特点	简要说明
丰富的接口类型	支持 GE、10G、40G、100G 以太口以及 2.5G、10G、40G POS 口等丰富的接口类型，适应各类组网。
完善的网络特性	支持 OSPF、ISIS、BGP、PIM、LDP 等各类 IPv4/IPv6 单播、组播、MPLS VPN 路由协议，MSTP、FRRP 等环网协议，可以全面覆盖核心交换机组网需要的网络特性，可作为高端交换机应用于企业级园区网、数据中心核心或汇聚节点等网络场景。

强大的交换性能	整机最大提供 204.8Tbps 交换容量。
灵活扩展各类业务板	通过扩展各类安全和应用交付业务板，既可以作为独立的高端安全产品和应用交付产品使用，也可以作为融合网络、安全以及应用交付等各类业务板卡于一体的高性能综合网关使用，整机最高可以支持 3.2Tbps 安全和应用交付业务处理性能。
资源池化能力	创新的 N:M 虚拟化技术，可将多个同类设备虚拟为一个逻辑设备，再将这个大的逻辑设备虚拟成多个互相独立的虚拟设备，实现业务平台资源“颗粒化”，极大地提升资源使用效率，用户可以为应用灵活配置所需的资源。
核心级高可靠性保障	业内领先的 CLOS 架构设计，主控引擎和交换网板硬件相互独立，在大幅提高设备可靠性的同时，为后续平滑扩容整机的业务处理能力提供保证。

DPX 系列深度业务路由交换网关可部署在园区网核心、数据中心核心、互联网出口、城域网、大型云数据中心核心等关键位置。

（2）盒式交换机（LSW 系列产品）

LSW 系列盒式交换机是针对企业级园区网、数据中心、工业网络等网络场景使用的网络接入交换机，在提供完善的传统网络特性和数据中心特性的同时，在网络接入边缘加强了对接入用户和接入流量的安全管控。

产品可对网内用户的状态进行标识与记录，可针对网内用户的异常行为进行及时告警与阻断，并具备行为回溯能力，具有安全威胁阻止扩散、安全事件有据可查的功能。产品主要技术特点如下表所示：

技术特点	简要说明
完整的网络特性	支持完整的网络特性。支持 MCE 功能，实现了不同 VPN 用户在同一台设备上的隔离，为网络中多业务安全隔离提供可靠和经济的解决方案。支持 IGMP、IGMP Snooping、GMRP、PIM 等协议。支持大规模组播表项，充分满足 IP 高清视频监控和其他组播业务的需求。支持 FRRP 快速环网恢复协议和 FLRP 快速链路恢复协议，可以实现网络故障的快速检测与收敛。
丰富的 QoS 策略	支持端口流量识别，支持基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 端口号、协议类型、VLAN 等多种方式的流分类。支持基于硬件的优先级队列，提供 SP、WRR、SP+WRR 等多种队列调度算法。支持拥塞管理和端口速率限制。
全面的 IPv6 特性	硬件支持 IPv4/IPv6 双栈和 IPv6 over IPv4 隧道（包括手工 Tunnel，6to4 Tunnel，ISATAP Tunnel），支持 IPv6 三层线速转发。
完备的安全控制策略	支持 MAC 地址认证、802.1x 认证、PORTAL 认证，内置认证服务器。支持用户帐号、IP、MAC、VLAN、端口等用户标识元素的动态或静态绑定，同时实现用户策略的动态下发。提供增强的 ACL 访问控

	制，支持超大容量的入端口和出端口 ACL。
用户异常行为智能检测与阻断能力	为每个用户基于总流量大小、报文大小构成、单目的地址流量大小，总体新建会话速率以及并发会话数等各维度建立模型，对于行为发生异常突变的用户判定为异常用户，进行自动告警并阻断，并留存相关证据，实现安全威胁阻止扩散、安全事件有据可查的目标。

此外，公司的 AC、AP 系列 WLAN 产品可以在公共场所、校园、酒店、写字楼等各类场所提供 WIFI 覆盖，为用户提供无线上网功能，XR 系列路由器产品可以满足城域网、企业广域网、企业园区互联和数据中心网络出口等广域网络场景的组网需求，与深度业务路由交换网关、盒式交换机、网络安全以及应用交付产品一起配合，可以为用户提供以“简单、智能、安全”为核心价值的整网解决方案。

4、服务类业务

公司的服务类业务针对不断发展变化的用户需求，设计适用的解决方案，包括安全策略的制定、技术和管理体系的构建，选取匹配的产品集成，实现咨询服务、解决方案、产品集成三位一体的信息安全价值链。

（1）安全服务

公司拥有一支高水平的专业安全服务团队，负责安全服务的相关技术研究和实施。公司具备中国信息安全认证中心信息安全服务资质认证（信息安全风险评估一级、信息安全应急处理一级）、中国信息安全测评中心信息安全服务资质认证（安全工程类二级）、公安部信息安全等级保护安全建设服务机构认证、中国通信企业协会安全建设服务机构能力认证（通信网络安全风险评估一级）；公司建有独立的安全研究院和安全攻防实验室，跟踪最新安全攻防技术，持续进行漏洞分析与挖掘、APT 攻击分析、攻击工具分析、黑客行为画像、僵尸网络等课题研究。基于以上技术积累，公司依照信息系统安全工程方法论推出安全评估、安全规划、安全运维、安全培训共四大类服务，解决用户在安全建设及运维过程中的风险发现、风险评估、安全改进及持续检查等问题，涵盖信息系统生命周期整个阶段。

安全评估服务：通过资产识别、脆弱性识别、风险分析、威胁识别、黑盒测试等规范化流程，专业的渗透测试检测（完全模拟黑客可能使用的攻击技术和漏

洞发现技术，对目标系统的安全情况做深入的探测），以及行业安全规范合规性检查等手段，对网络和应用系统的安全漏洞、安全隐患、安全风险，进行系统性探测、识别、控制与消除。该服务从风险管理角度，运用科学的方法和手段，系统地分析网络与应用系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。

安全规划服务：提供新建网络设计、安全防护设计的安全建设规划服务，以及辅助定级、等级改造建设、辅助通过测评的等级保护咨询服务。根据用户网络和应用系统的安全现状和安全风险，结合用户的安全需求，提供系统的信息安全建设规划方案。

安全运维服务：针对用户网络提供安全策略日常维护以及重要时期安全保障服务；对系统整体安全加固情况、安全预警情况、用户各类信息资产以及敏感信息管理系统提供安全巡检与审计服务；根据安全评估及渗透测试结果，对用户资产提供安全加固服务；针对突发安全事件，提供应急响应处置以及回溯调查服务。通过各维度的加固和保障，确保用户网络及业务系统平稳安全的运行。

安全培训服务：结合业务搭建相应的攻防平台，为用户提供一个理论结合实际、可上机进行系统演练实践的网络安全攻防实验环境，针对不同角色客户提供对应的培训课程，并定期向用户发布互联网安全趋势报告以及安全通告，为用户培养合格的网络信息安全技术人才。

（2）维保服务

产品维保服务：远程及现场技术支持、软件升级、备件先行更换、网络运行管理支持，帮助客户维护安全、高效、稳定的 IT 环境，提高网络生产力。

（二）公司主营业务收入及构成情况

报告期内，公司主营业务收入分产品的构成情况如下表所示：

单位：万元

业务	2018 年度		2017 年度		2016 年度	
	金额	占比	金额	占比	金额	占比
网络安全产品	42,503.46	60.40%	37,596.92	61.08%	33,088.20	62.23%

业务	2018 年度		2017 年度		2016 年度	
	金额	占比	金额	占比	金额	占比
其中：安全防护产品	30,117.01	42.80%	23,617.14	38.37%	26,030.38	48.95%
安全分析产品	12,386.45	17.60%	13,979.78	22.71%	7,057.82	13.27%
应用交付产品	14,132.99	20.08%	12,970.79	21.07%	10,524.94	19.79%
基础网络产品	12,021.13	17.08%	10,236.00	16.63%	9,012.42	16.95%
服务类业务	1,711.85	2.43%	751.63	1.22%	546.94	1.03%
合计	**70,369.43**	**100.00%**	**61,555.34**	**100.00%**	**53,172.51**	**100.00%**

报告期内，公司各业务收入情况的具体分析如下：

（1）网络安全产品

网络安全产品主要包括安全防护产品和安全分析产品。2016-2018 年度，网络安全产品的营业收入分别为 33,088.20 万元、37,596.92 万元和 42,503.46 万元，占公司主营业务收入的比重分别为 62.23%、61.08%和 60.40%。其中，2016-2018 年度，公司安全防护产品营业收入的比重最高，分别为 48.95%、38.37%和 42.80%。安全分析产品的营业收入金额及占比呈现一定的波动性。

2016-2018 年度，公司网络安全产品收入年均复合增长率为 13.34%，主要原因系：①随着对网络安全防范意识的提升，网络信息安全受到了企业的高度重视，随着公司在相关领域的技术积累和品牌效应，公司网络安全产品的应用行业领域不断拓展，用户数量持续增长；②公司建立了完善的销售和服务网络，为用户提供便捷的售前售后服务，报告期内，公司陆续在全国重要省市设立了 27 个办事处，为客户提供全方位的服务；③公司通过与渠道商合作推广业务取得积极成效，与渠道商的合作带动了多领域、多区域用户群体的增长。

报告期内，公司网络安全产品收入销售模式具体构成及占比情况如下：

单位：万元

项目	2018 年度		2017 年度		2016 年度	
	金额	占比	金额	占比	金额	占比
直签销售	14,527.53	34.18%	16,080.26	42.77%	14,738.51	44.54%
渠道销售	27,975.93	65.82%	21,516.66	57.23%	18,349.69	55.46%
合计	**42,503.46**	**100.00%**	**37,596.92**	**100.00%**	**33,088.20**	**100.00%**

2016-2018 年度，公司网络安全产品收入以渠道销售为主，占比分别为 55.46%、57.23%和 65.82%。

（2）应用交付产品

2016-2018 年度，公司应用交付产品的营业收入分别为 10,524.94 万元、12,970.79 万元和 14,132.99 万元，占公司主营业务收入的比重分别为 19.79%、21.07%和 20.08%。 2016-2018 年度，公司应用交付产品营业收入年均复合增长率为 15.88%，主要原因系：一方面，公司建立了完善的销售和服务网络，为用户提供便捷的售前售后服务，同时公司通过与渠道商合作推广业务取得积极成效，与渠道商的合作带动了多领域、多区域用户群体的增长；另一方面，在国内信息产品国产化政策的背景下，应用交付产品的国产化替代进一步加强，随着公司在应用交付领域的技术积累和产品性能的提高，公司应用交付产品持续入围重要客户采购，导致收入持续增长。

（3）基础网络产品

2016-2018 年度，公司基础网络产品的营业收入分别为 9,012.42 万元、10,236.00 万元和 12,021.13 万元，占公司主营业务收入的比重分别为 16.95%、16.63%和 17.08%。

2016-2018 年度，公司基础网络产品营业收入年均复合增长率为 15.49%，主要系：①公司产品及服务以“让网络更简单、智能、安全”为主要目标，并在网络与安全融合的产品设计理念指导下研发和生产，随着对网络安全防范意识的提升，网络安全受到了企业的高度重视，随着公司在相关领域的技术积累和品牌效应，公司网络安全业务的不断拓展，用户数量持续增长，带动了公司基础网络业务的发展；②公司建立了完善的销售和服务网络，为用户提供便捷的售前售后服务，报告期内，公司陆续在全国重要省市设立了 27 个办事处，为客户提供全方位的服务；③公司通过与渠道商合作推广业务取得积极成效，与渠道商的合作带动了多领域、多区域用户群体的增长。

（4）服务类业务

公司服务类业务主要包括安全服务和维保服务两大块，其中安全服务主要包

括安全评估服务、安全规划服务、安全运维服务、安全培训服务等服务；维保服务主要系与产品升级、产品维护等相关的服务。2016-2018 年度，发行人服务类业务的营业收入分别为 546.94 万元、751.63 万元和 1,711.85 万元，最近三年呈现不断上涨的趋势，主要系：①随着网络安全环境的多样化和复杂化，传统、功能单一的信息安全产品越来越无法满足客户的安全保障需求，与此同时客户自身的信息安全技术人员解决相关问题的能力有限，使得风险发现、风险评估、安全改进及持续检查等相关的安全服务的作用越来越受到用户重视，客户对安全服务的需求日渐增强。同时，公司以安全服务运营模式，通过全方位的安全解决方案，实现咨询服务、解决方案、产品集成三位一体的信息安全价值链，随着网络安全产品的销售增长，公司安全服务收入相应增长；②公司维保服务主要系公司产品升级、产品维护等相关的服务，随着公司经营状况的提升，公司各产品销量的增加，与产品相关的服务也随之相应增加。

综上所述，公司报告期内营业收入主要来自主营业务，公司主营业务突出。公司主要产品具备良好市场优势、技术优势、品牌优势，公司营业收入保持良好的增长态势。

二、发行人未来成长的可持续性

（一）发行人所处行业前景分析

1、信息安全行业发展概况

（1） 全球信息安全行业发展概况

当前，世界各国信息化快速发展，信息技术的应用促进了全球资源的优化配置和发展模式的创新，互联网对政治、经济、社会和文化的影响更加深刻，信息化渗透到国民生活的各个领域，网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，围绕信息获取、利用和控制的国际竞争日趋激烈，保障信息安全成为各国重要议题。

近年来，全球频现重大安全事件，2013 年曝光的“棱镜门”事件、“RSA 后门”事件、2017 年爆发的新型“蠕虫式”勒索软件 WannaCry 等更是引起各界对信息安全的广泛关注。网络攻击从最初的自发式、分散式的攻击转向专业化的有

组织行为，呈现出攻击工具专业化、目的商业化、行为组织化的特点。随着获利成为网络攻击活动的核心，许多信息网络漏洞和攻击工具被不法分子和组织商品化，以此来牟取暴利，从而使信息安全威胁的范围加速扩散。个人信息及敏感信息泄露的信息安全事件，可能引发严重的网络诈骗、电信诈骗、财务勒索等犯罪案件，并最终导致严重的经济损失；而政府机构、工业控制系统、互联网服务器遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。全球整体网络安全形势不容乐观，国际间网络空间竞争形势日益紧张。

面对日益严峻的网络空间安全威胁，美国、德国、英国、法国等世界主要发达国家纷纷出台了国家网络安全战略，明确网络空间战略地位，并提出将采取包括外交、军事、经济等在内的多种手段保障网络空间安全。2011 年 4 月，美国发布了《网络空间可信身份国家战略》，首次将网络空间的身份管理上升到国家战略的高度，并着手构建网络身份生态系统。这一战略的出台表明美国已高度认识到网络身份安全在保障网络空间安全中的重要战略地位。从各国的战略规划的内容来看，一方面政府希望通过顶层安全战略的制定来引导本国安全产业的发展，另一方面对于网络空间的保护逐渐上升到和传统疆域保卫同等的地位上来，通过成立网络安全部队以加速军队信息安全攻防的研发，积极应对未来有可能发生的网络战争。

严峻的网络安全形势驱动安全市场的快速增长。根据 Gartner 的数据显示，2017 年全球网络安全产业规模达到 989.86 亿美元，较 2016 年增长 7.9%，数字化企业的多个要素日益推动全球关注信息安全，尤其是云计算、移动计算和物联网等，而错综复杂、影响重大的高级针对性攻击同样起到了推动作用。

（2）我国信息安全行业发展概况

①信息安全成为我国国家战略的重要组成部分

我国一直高度重视信息安全产业的发展，早在 2003 年，中共中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》，党的十六届四中全会将信息安全上升到国家安全的战略层面，明确提出“确保国家的政治安全、经济安全、文化安全和信息安全”。面对日益复杂的全球信息安

全形势和国内信息安全现状，2012 年，党的十八大报告中强调，要高度关注网络空间安全，并将网络空间安全、海洋安全、太空安全置于同一战略高度。2013 年，党的十八届三中全会也再次指出，“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全”。2014 年，中央网络安全和信息化领导小组成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，充分体现了国家对信息安全的重视程度。2015 年 7 月，全国人民代表大会常务委员会通过《中华人民共和国国家安全法》，并于 2015 年 7 月 1 日开始实施，首次将网络空间正式上升成为我国继陆、海、空、天后的第五疆域。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》指出“实施网络强国战略，加快构建高速、移动、安全、泛在的新一代信息基础设施”。2016 年 4 月，习近平总书记主持召开网络安全和信息化工作座谈会并发表重要讲话，强调“加快构建关键信息基础设施安全保障体系”、“增强网络空间安全防御能力”。2016 年 11 月，全国人民代表大会常务委员会通过《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日开始实施，提出“国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”，强调了金融、能源、交通、电子政务等行业在网络安全等级保护制度的建设。2016 年 12 月，国家互联网信息办公室发布《国家网络空间安全战略》，是我国第一次向全世界系统、明确地宣示和阐述对于网络空间发展和安全的立场和主张。2017 年 1 月，工业和信息化部制定印发了《软件和信息技术服务业发展规划（2016－2020 年）》，对信息安全产品明确提出了到 2020 年收入达到 2,000 亿元，年均 20%以上增速的目标。2017 年 1 月，工业和信息化部制定印发了《信息通信网络与信息安全规划（2016-2020 年）》，紧扣“十三五”期间行业网络与信息安全工作面临的重大问题，对“十三五”期间行业网络与信息安全工作进行统一谋划、设计和部署。2017 年 7 月，国家互联网信息办公室起草《关键信息基础设施安全保护条例（征求意见稿）》，提出顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。2018 年 6 月，公安部会同有关部门起草《网络安全等级保护条例（征求意见稿）》，以贯彻落实《中华人民共和国网络安全法》，深入推进实施国家网络安全等级保护制度。信息安全产业作为信息安全技术、产品和服务提

供者和实施者，承担着国家信息安全防御和保障的历史使命。发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

②信息安全产品国产化替代趋势日益显著

近年来，国内信息安全厂商快速发展，依托本地布局的产品和研发团队，对用户需求理解更为透彻，对新需求的响应更为迅速，产品性价比更高，部分功能特性已超过国外厂商，但在高端产品市场的竞争力仍相对较弱。以应用交付产品为例，根据 IDC 报告，2017 年度，F5 网络（美国）在中国应用交付的市场份额达到 30.87%，国外厂商在中国应用交付的市场份额合计超过 47.89%，信息安全产品国产化替代空间仍然较大。

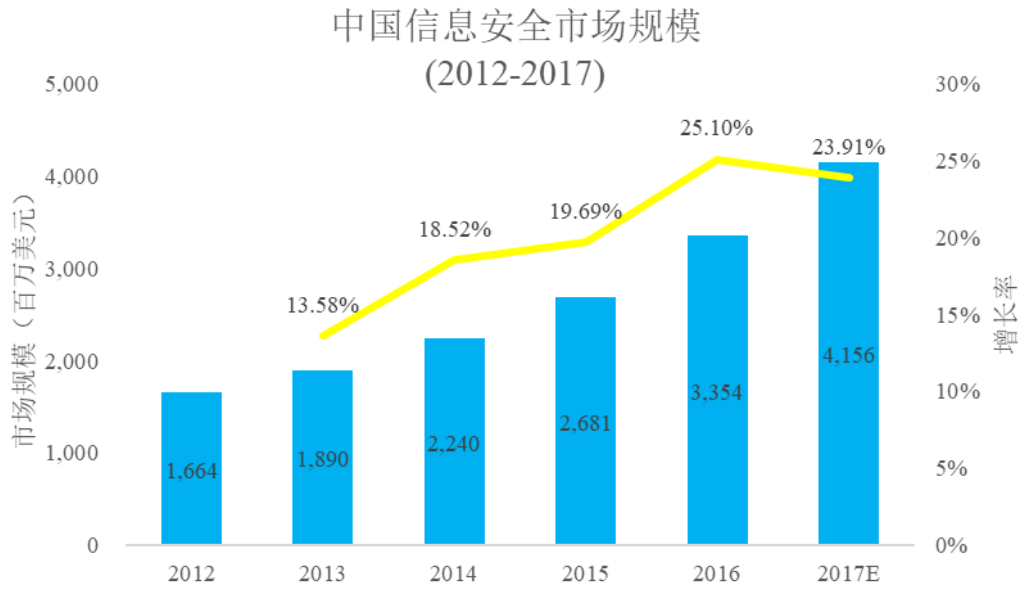
“十三五”时期，我国将大力实施网络强国战略，要求网络与信息安全有足够的保障手段和能力，通过切实推进自主可控和国产化替代，政策化培养和市场化发展双向结合，信息安全市场国产化脚步逐步加快。拥有自主可控的标准、技术、产品的信息安全厂商，将在对公业务，为政府、行业服务的大背景下，充分应用包括云计算、大数据等技术，把握产业发展机遇，不断扩大市场份额，实现对国外信息安全产品的规模性替代，在核心应用领域和国内产业转型升级的变革中发挥重要作用，在国家网络信息安全领域中担当核心角色。

③我国网络安全事件多有发生

随着我国不断完善网络安全保障措施，网络安全防护和网络安全事件应急响应水平进一步提升，网络安全国际合作进一步加强。但随着互联网应用的深化、网络空间战略地位的日益提升，网络空间已经成为国家或地区安全博弈的新战场。。国家互联网应急中心报告，2017 年，我国面临的安全问题日益复杂，敲诈勒索病毒盛行，分布式拒绝服务攻击事件峰值流量持续突破新高，联网智能设备面临的安全威胁加剧，工业控制系统安全风险在加大，网络攻击“武器库”泄露给网络空间安全造成严重的潜在安全威胁，APT 攻击组织依然活跃等问题，对我国实现建设成为网络强国目标不断提出新的挑战。。日益复杂严峻的网络安全形势、国家网络强国战略推进建设迫切要求创新安全技术、增强综合安全保障能力。

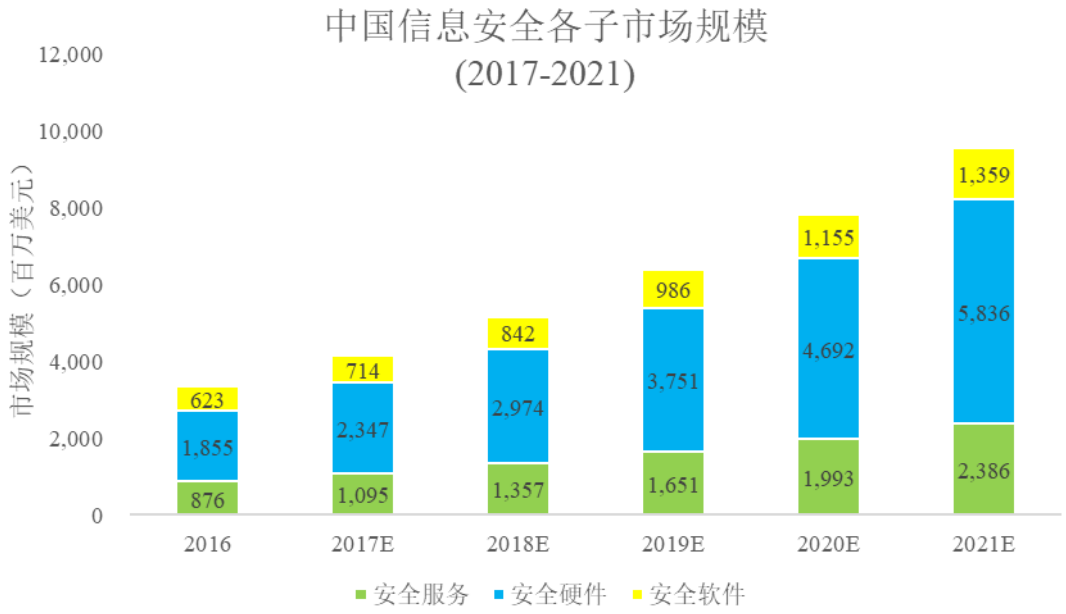
④我国信息安全产业规模快速增长

根据 IDC《中国 IT 安全市场预测，2017-2021》报告预测，2017 年，中国信息安全硬件、软件、服务市场的规模为 41.56 亿美元，同比增长 23.91%，2012 年至 2017 年的年复合增长率为 20.10%，保持了快速增长态势。



数据来源：IDC China

2017 年，在整体信息安全硬件、软件、服务市场中，安全硬件市场的占比最大，为 56.47%，安全软件市场占比 17.18%，安全服务市场占比 26.35%。2017 年中国信息安全软件市场的规模为 7.14 亿美元，同比上升 14.61%，得益于企业级用户对安全软件需求的提升及云应用带来的刚需。2017 年中国信息安全硬件市场的规模为 23.47 亿美元，同比增长 26.52%，保持了快速增长势头，得益于政府、军队、金融以及电信行业对防火墙和统一威胁管理等产品的采购。2017 年中国安全服务市场规模为 10.95 亿美元，同比增长 25.00%，随着云与大数据技术的快速发展，将刺激安全服务市场持续快速增长。



数据来源：IDC China

根据 IDC 研究报告预测，中国信息安全市场将保持快速增长，预计到 2021 年将达到 95.81 亿美元，2017 年至 2021 年的年复合增长率将为 23.22%。根据中国信息通信研究院的数据，全球安全产业规模从 2016 年至 2019 年有望保持超过 8%的增长速率。国内信息安全产业增速高于全球增速。

⑤国内信息安全市场以硬件产品为主

根据上海社会科学信息研究所、中国信息通信研究院安全研究所《中国网络空间安全发展报告（2016）》，2015 年，全球信息安全产业中安全服务、安全软件与安全硬件占比分别达到 60.1%、24.5%和 15.4%。而国内的产业结构与之有所不同，安全硬件的占比达到 54.2%，国内信息安全行业以安全硬件为主的特点与全球以安全服务为主的特点有着明显的差异。安全硬件市场中防火墙硬件市场的占比为 37.8%，依然是中国安全硬件市场中最大的子市场，统一威胁管理硬件市场和安全内容管理硬件市场，分别占整体安全硬件市场的 25.9%和 13.1%，入侵检测与防御硬件市场占比为 17.0%。

⑥信息安全投入有待提高

与美国、日本等发达国家相比，我国信息安全投入的绝对数量以及相对 IT 总投入的占比都明显偏小。国内安全投入占信息产业总规模较低的占比说明国内信

息安全发展程度与发达国家相比尚存在差距。这与国内信息安全产业起步较晚，普遍重视程度不够有关系。而根据经验，随着发展阶段的变化，对于信息安全的投入会从产品为主逐渐过渡到服务为主。目前国内处在信息安全发展较为初级的阶段，国内信息安全产品偏高的占比也体现了这点。信息安全产业的快速发展将逐渐降低国内外信息安全领域投入的差距，国内逐渐增长的信息安全投入也将成为信息安全厂商发展的原动力。

2、行业发展的影响因素及趋势

（1）信息安全行业发展影响因素

我国信息安全行业近年来快速发展的主要驱动因素有以下几个方面：

①基础信息网络和重要信息系统设备国产自主水平关乎国家网络安全形势，信息安全设备自主可控和国产化替代是大势所趋。随着国家对信息安全愈加重视而上升到国家战略层面，国产化替代不可逆转，随着技术能力提升及政策推动，我国信息基础设备会沿着外围到核心、从党政军企特殊市场到消费者市场，国产替代率会逐渐提高。

②信息安全需求的提升是推动行业快速发展的根本因素。随着我国整体信息化水平持续提升，经济和社会对信息化的依赖程度日益提高，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益，而随着身份盗用、交易诈骗、资源滥用、网络钓鱼等安全事件频繁发生，政府、企业、个人对信息安全的关注程度日益增强，社会对信息安全的需求与日俱增，政府部门、重点行业在信息安全产品和服务上的投入也不断增加，促进了信息安全行业的持续增长。

③国家政策支持是信息安全行业发展的重要因素。近年来，国家有关部门相继出台了一系列法律法规和鼓励行业发展的产业政策，为信息安全行业的发展营造了良好的政策环境。我国的信息安全工作提高到国家战略高度。信息安全形势的日益严峻，国家对信息安全产业的重视程度日益提高，随着政府及行业政策法规的推动，促使我国信息安全市场空间日益扩大。

④信息安全标准化工作的推进促进了信息安全行业的发展。近年来，我国相继制定了一系列信息安全国家标准，进一步规范了行业的发展，为信息安全产品

的选用和研发提供了标准和依据，对信息安全行业的发展起到了积极的引导作用。

⑤信息技术不断发展革新。近年来，云计算、大数据、移动以及社交网络的快速发展给信息系统架构带来了巨大变化，信息安全也随之迎来挑战。例如云计算技术，使得数据中心的基础设施由原来的各业务系统独立建设模式转变为资源池建设模式，服务器、存储、网络设备的部署方式相应改变。基础架构的变化要求信息安全建设能够适应新的 IT 基础架构，从而满足新的安全需求，这同时为信息安全建设带来了新的发展空间。

（2） 信息安全行业发展趋势

①安全威胁态势智能感知将成为一个重要方向

目前各种各样的安全产品被用于检测网络中的攻击威胁，维护网络的安全运行。但这些安全手段一般只能在一定范围内发挥特定的作用，互相之间缺乏有效的数据融合和协同管理机制。面对众多分散的信息，用户无法全面直观地了解系统安全脆弱点、整体攻击状况以及安全防护效果，无法满足预判系统安全脆弱点并提前实施防御措施的需求，另一方面，随着攻击手段的不断变化，目前部分高级攻击隐蔽性很强，通过单独的安全产品很难检测和防护，需要汇总用户网络中所有安全事件信息、威胁信息以及相关数据，结合知识库和网络情报库，快速准确地发现网络异常和高级威胁，同时通过通知用户或与网络中安全设备进行联动，实现针对高级威胁进行智能检测与防护的目的。

安全威胁态势感知平台可以有效解决以上问题，其融合了基于大数据的安全分析技术、威胁情报和可视化技术，可以更加系统的分析整体漏洞和风险，呈现整体安全状态，同时能够实现针对攻击风险的预判和预防，并且可以与传统网络安全产品一起联动配合，整体形成网络安全威胁“全局可视、提前预判、主动预警、立体防护”的全新安全解决方案，有效提升安全防护效果和客户体验，因此将成为未来几年安全建设的重要方向。

②云安全和物联网安全市场将会成为下一个高速增长点

随着云计算的普及，大量数据和业务都集中在云计算数据中心中，云计算数

据中心面临着巨大的安全风险，其对安全的需求达到了全新的高度，安全在云计算领域将成为与计算、存储、网络并列的四大基础设施之一，云计算的快速发展给网络安全行业带来了巨大的市场空间和商业价值。

另外近几年来，物联网发展也非常迅猛，物联网技术不仅仅在家庭及消费级设备上取得发展，还在制造业、物流、矿业、石油、公用设施和农业等拥有大型资产的行业也开始大量得到应用。但是物联网的安全性非常薄弱，各类物联网终端很容易成了被入侵和控制的对象，黑客通过入侵物联网设备，再逐步渗透到整个网络，窃取大量机密信息，甚至通过操控物联网设备对企业、国家产生直接攻击和威胁。近几年来物联网安全事故频发，物联网的安全问题正在被日益重视，后续几年物联网安全市场将会取得快速发展。

③应用交付市场将持续快速发展

随着各类互联网业务的高速发展，网络应用不断增多，各类网络应用的安全和质量管理也日益复杂，同时用户业务随着访问用户量、业务流量的逐渐增大，链路、服务器的负载均衡以及按需平滑扩容变得非常重要，并且由于服务器宕机、链路故障、应用程序故障时有发生，故障智能检测与自愈也迫在眉睫。用户急需一类能智能识别应用，让网络中各应用可视可控，同时能智能检测各类故障并平滑自愈，支持业务处理能力按需平滑扩容，确保各应用安全高效交付的智能产品和解决方案。

基于以上需求，信息安全行业衍生了一个新型的应用交付领域，目前该领域需求旺盛，存在较大的市场空间和商业价值，并且随着用户需求的日益强烈，在未来几年也将会持续快速发展。

④高端产品需求快速增长

随着各行各业信息化和各类互联网应用的蓬勃发展，尤其视频、游戏、移动互联网的快速发展，网络流量急剧增长，用户对网络安全产品的性能需求将会快速提高，市场对高端产品的需求将会快速增长。

⑤安全产品向多功能融合方向发展

业界现有的信息安全和应用交付类设备通常组网能力较弱，需要与网络设备

一起配合部署，并且基本上每一种业务功能都是单一品类，例如防火墙、IPS 入侵防御设备、WEB 防火墙、DDoS 防护设备、流控审计设备等，导致用户网络中设备种类繁多，配置和维护工作都比较复杂。用户急需一类能融合所有功能、开启全部功能后仍然保持较高性能的产品，从而有效降低用户运维管理的复杂度。因此多功能融合的安全产品需求日益强烈，相关产品将会加速发展。

⑥网络安全由“注重防外”向“内外兼顾”转变

过去业界认为网络攻击通常来自于外网，而内网相对比较安全，因此网络安全产品通常部署在网络出口和重要区域边界，对内网攻击却疏于防护，但近些年由内网发起的攻击日益增多，例如各类蠕虫病毒一旦感染某台主机后，就会在局域网内部快速扩散攻击全网，从而给用户造成重大损失，另外从内网非法窃取数据资料的行为时有发生，尤其随着云计算多租户模式的快速发展，内网云租户之间的安全防护不可或缺，因此，内网安全防护变得日益重要。用户不仅需要重视外部安全，更要对内网安全做配套建设，对接入用户、网络应用、用户行为、网络异常流量进行严格管控，做到“内外兼顾、立体防护”，才能实现真正意义上的安全。

⑦整体解决方案能力将变得日益重要

目前安全产品可分为防火墙、IPS、DDoS 防护、Web 应用防火墙、上网行为管理与审计、漏洞扫描等产品，各类产品配置方法和监控日志形式各异，运维管理非常复杂，另外，随着网络安全的威胁来源和攻击手段不断变化，仅采购和部署几类安全产品无法完全保障网络长期、系统的安全，而对网络进行系统规划、构建全面的安全防护体系、制定完善的安全管理策略、落实日常专业的安全管理显得尤为重要。但是大量中小企业安全技术人员匮乏，并不具备这样的能力，另外随着信息安全环境日益复杂，即使是大型企业和机构也越来越难以独自应对，用户普遍期望安全厂商能够提供全面应对各类安全威胁的整体解决方案，从而降低用户安全管理复杂度。所以在未来的安全市场中，整体解决方案能力将变得日益重要。

（二）发行人的发展战略和目标

1、整体发展战略

公司以“让网络更简单、智能、安全”为愿景，坚持产品和技术的创新，采取“以科技创新赢得未来，以产品质量赢得市场”的发展方式，致力于成为一家具有优秀企业文化、可持续发展的企业级网络通信领域领军企业。

未来公司除了保持已有的鲜明技术特点和领先技术优势之外，将抓住企业级网络通信市场的发展机遇，凭借公司在行业方面的核心技术优势、丰富的专家资源、多年沉积的专业化解决方案，依托公司自主研发的集网络、安全及应用交付功能于一体的软硬件平台，紧跟企业级网络通信领域的用户需求与发展趋势，加大研发力度，研发出能更好的满足用户需求、更具竞争力的产品和解决方案。同时公司将不断扩大产业链深度和广度、发挥规模化经营效应、加强品牌建设力度、拓展客户及营销渠道，大力提升公司核心竞争力，成为企业级网络通信领域的领导者。

2、公司未来三年发展目标

根据上述发展战略，未来三年内公司将继续保持在企业级网络通信领域的研发投入，不断深化产品及服务结构，持续提升公司自身的技术研发能力和服务能力，并将物联网、移动互联、大数据、云计算等新技术、新理念与公司产品进行深度结合，重点针对安全威胁态势感知平台、新一代高性能云计算数据中心安全平台、新一代高性能应用交付平台等项目进行研发攻关，满足行业不断向深度发展以及未来扩展业务的需要，有效提升公司在企业级网络通信市场的核心竞争力，巩固公司的行业领先地位。

三、发行人竞争优势分析

（一）领先的技术

公司具有一支业界领先的研发队伍，并通过一系列有效的聘用、培训和激励机制保障团队稳定。截至 2018 年 12 月 31 日，公司在北京和杭州设有研发中心，一共拥有研发员工 458 名，占公司员工总数的 41.86%，其中核心技术团队在企业级网络通信领域拥有丰富的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法、安全研究和安全服务相关技术等方面具有深厚积累。公司拥有专业的安全攻防实验室、一流

的安全研究团队以及各类业界高等级的安全服务资质，相关研究成果能够迅速转化为产品能力，为持续提升公司安全产品的防护能力、确保公司在市场竞争中保持技术领先性提供了有力保障。

通过持续的技术创新，公司形成了一系列具有自主知识产权的核心技术。截至 2018 年 12 月 31 日，公司拥有已获授权的专利 193 项（其中发明专利 105 项）、申请中的专利 983 项（其中发明专利 981 项）、已登记的软件著作权 34 项，并以这些核心技术为基础，推出了全面覆盖企业级网络通信主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线。

围绕“让网络更简单、智能、安全”的核心目标，公司在相关产品和解决方案上已经形成鲜明技术特点和领先技术优势，同时，通过完备的产品布局和系统的安全服务能力，可以为用户提供完善的整网解决方案，真正实现“交钥匙”工程。目前公司相关产品和解决方案已经在众多行业获得广泛应用，较好地满足了用户需求，受到用户的广泛认可。

（二）客户与行业经验的积累

通过持续的市场拓展，目前公司产品及服务已经全面进入了包括运营商、政府、电力能源、金融、教育、医疗、交通等在内的众多行业，积累了大量客户，并长期保持着深入稳定的合作关系，这些客户自身具有雄厚的实力并在业界拥有良好的信誉，极大降低了公司的经营风险和财务风险。

公司通过在上述行业的长期耕耘与积累，与行业内的大量客户达成了紧密合作，积累信息化建设及信息安全建设项目的实施经验，完善产品功能，满足客户信息化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化建设的技术需求及发展趋势，可以进一步提高公司产品、解决方案及服务的竞争力。此外，公司已经在各大行业建立了数量众多的样板点，可以对更大范围的用户起到较好的辐射和示范效应，为公司实现持续快速发展、进一步扩大领先优势打下了坚实基础。

（三）业内知名的品牌

公司产品和服务的用户已经遍及全国各个省份以及众多行业，通过优质的产

品质量、领先的解决方案以及专业的服务，公司在客户中树立了良好的企业形象，并且建立起了良好口碑和品牌。

公司获得了 Frost & Sullivan 颁发的“2016 中国区网络安全技术领导奖”、中国高科技产业化研究会和品牌战略专家工作委员会联合颁发的“2015 中国计算机信息安全产品创新•质量创优•消费者放心品牌”。除此之外，公司还是由中国信息安全测评中心认定的国家信息安全漏洞库技术支撑单位、国家互联网应急中心和中国互联网协会联合认定的中国互联网网络安全威胁治理联盟首批成员单位、以及中国网络安全产业联盟理事单位、中国保密协会会员单位和中国网络空间安全协会会员单位。在北京“APEC 峰会”、杭州“G20 峰会”、乌镇“世界互联网大会”、厦门“金砖国家峰会”、南宁“中国-东盟商务与投资峰会”、青岛“上海合作组织峰会”、上海“中国国际进口博览会”等重大国际会议和展览活动期间，公司都是重要的网络安全保障单位。广大用户、行业同仁以及国家相关部门对公司的认可，体现出公司在信息安全行业的品牌已得到广泛认可。

（四）完备的营销和服务体系

公司在营销体系方面的竞争力主要体现在建立了全国性的营销团队和技术支持中心，以及广泛的渠道体系两个方面。

公司在全国设有 27 个办事处，通过持续的市场拓展，公司已建立起覆盖全国的市场销售与技术支援体系，公司对行业价值客户的信息化建设和网络安全需求的理解和把握能力，使公司针对价值客户所提供的产品及服务赢得了广泛认同。公司拥有专业的安全服务与研究团队，能够自行挖掘安全漏洞，提供安全评估、安全应急等服务；具有本地化服务能力，能保证对用户突发事件的及时响应。

公司广泛发展渠道合作伙伴，现拥有 1,700 余家认证代理商，公司已经建立了覆盖众多细分行业市场的完备的营销和服务渠道体系。目前，公司的办事处、售后服务机构与渠道合作伙伴之间形成了良好的互动，使得公司的产品和服务能得到快速推广。

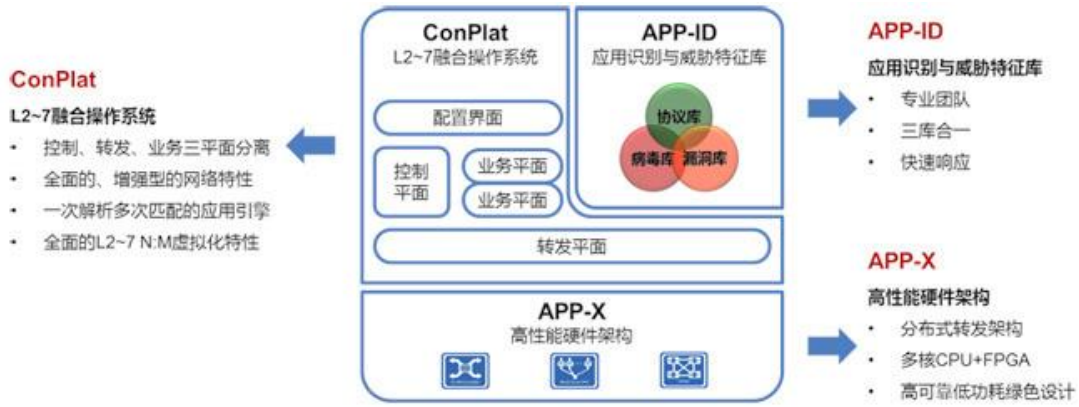
四、发行人的自主研发能力

（一）公司核心技术情况

1、 公司产品核心技术简介

基于对网络安全发展趋势及用户需求的深刻理解，公司以“让网络更简单，智能，安全”为愿景，持续专注于企业级网络通信领域的研发与创新。通过高性能硬件平台，融合网络、安全、应用交付功能于一体的软件平台，FPGA 系统设计、信息安全和应用交付领域相关核心技术等方面的一系列创新，形成了一系列具有自主知识产权的核心技术。截至 2018 年 12 月 31 日，公司拥有已获授权的专利 193 项（其中发明专利 105 项）、申请中的专利 983 项（其中发明专利 981 项）、已登记的软件著作权 34 项。

其中公司产品核心架构如下：



（1）L2~7 融合操作系统 ConPlat：将网络特性与安全和应用交付特性融合在一起，具有全面的操作系统级虚拟化能力，以及下一代网络操作系统的高可靠特性。

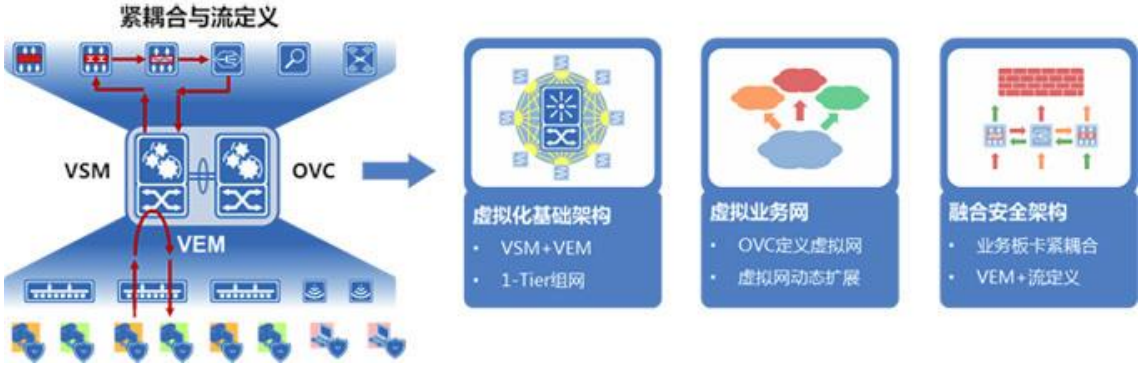
（2）高性能硬件架构 APP-X：基于多核 CPU、FPGA 以及分布式转发技术，是高性能网络和应用处理的硬件基础。

（3）应用识别与威胁特征库 APP-ID：创新性的将应用特征库、攻击特征库以及病毒库三库合一，是设备应用层业务处理能力的基础。APP-ID 由公司专家团队维护，具有专业的分析能力和快速的响应能力，保证了 APP-ID 的有效性和更新的及时性。

通过 ConPlat、APP-X 和 APP-ID，公司构建了网络、安全和应用交付融合的产品体系，形成了颇具特色的产品和解决方案，与业界同类产品相比具有比较明显的差异化竞争优势，并以这些核心技术为基础，推出了全面覆盖企业级网络通信主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线，成为业内领先的企业级网络通信设备提供商。

2、 公司解决方案核心架构简介

在先进的产品技术基础之上，公司推出了“DP xFabric”技术解决方案架构，将应用支持能力从单设备扩展到整网。“DP xFabric”技术解决方案架构包括四个核心技术：



（1）VSM（Virtual Switching Matrix）虚拟交换矩阵：L2~7 层 N：1 虚拟化技术，可以将多台设备虚拟为一台逻辑设备。VSM 不仅实现了网络资源的虚拟化，还实现了安全和应用交付资源的虚拟化，提高整网性能、可靠性与弹性。

（2）VEM（Virtual Extension Matrix）虚拟扩展矩阵：将核心设备与接入设备虚拟化为一台逻辑设备。核心设备对所有接入设备进行统一的管理和控制，接入设备相当于核心设备的扩展接口，所有接口流量都上行至核心设备进行处理。与 VSM 结合使用，可以将整网虚拟为一台逻辑设备，实现 1-Tier 组网。

（3）OVC（OS-level Virtual Context）操作系统级虚拟化：将一台设备虚拟成多台逻辑设备（虚拟系统），每个虚拟系统拥有独立的资源和管理界面，不同虚拟系统间实现操作系统级隔离。通过 OVC，可以实现网络、安全与应用交付资源的 1：M 虚拟化。

（4）紧耦合与流定义：紧耦合是指业务板卡与机框的紧耦合，业务板卡可

以提供丰富的安全与应用交付功能，并实现一键配置。流定义则可以让数据流按需通过指定的业务板，针对不同应用提供不同的安全防护和应用交付能力。结合 VEM 技术，可以将安全与应用交付能力推广至整网每个接口。

3、 公司核心技术具体情况

公司核心技术具体情况如下：

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
1	APP-X 硬件平台	采用 CLOS 分布式架构，利用 FPGA 实现 L2 到 L7 的全业务处理引擎，利用 PCIE DMA 技术实现超高速控制通道。	自主研发	集成创新	201110040242.X、201110456737.0、201310129304.3、201310129568.9、201510148704.8 等多项发明专利授权专利申请号包括 201410150125.2、201510466404.4、201510633157.2、201610169489.4、201710273938.4、201710651939.8、201810077043.8、201811160054.9 等	DPX 系列产品及各类业务板
2	Conplat 软件平台	采用多平面和组件化设计，融合网络、安全、应用交付所有特性，适用于盒式、框式等多种产品形态，每个功能模块都可以单独加载和裁剪，实现分布式产品一体化管理与业务处理的软件平台。	自主研发	原始创新	200910176725.5、200910259323.1、201210271588.5、201210419293.8、201210522682.3、201210523851.5、201310469518.5、201410451693.6 等多项发明专利授权专利申请号包括 201510373353.0、201510478716.7、201610171111.8、201610819828.9 、201610864312.6、201710179363.X、201710188655.X、201810241442.3、	公司全系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
					201811067022.4 等	
3	流定义技术	在分布式设备中实现不同业务模块间流量灵活调度的引流技术，可实现基于接口、IP 地址、协议和端口的业务引流功能，对用户提供业务功能自动编排的能力。	自主研发	原始创新	201410264274.1 发明专利授权 专利申请号包括 201410415045.5、201510023360.8、201510050678.5、201610017953.8、201811062881.4 等	DPX 系列产品及各类业务板
4	VSM 技术	将多台物理设备虚拟成为一台逻辑设备，实现多台设备统一管理、简化组网、业务自动分流、故障自动切换以及性能按需扩展等功能。	自主研发	原始创新	200910250570.5、201310198456.9、201410229710.1 发明专利授权 专利申请号包括 201510869068.8、201610807967.X、201710034837.1、201710821372.4、201810786378.7、201811003623.9 等	公司全系列产品
5	云板卡技术	将同一台框式设备以及多台堆叠设备上的多块物理板卡虚拟成一块逻辑板卡，实现多板卡统一管理、业务自动分流、故障自动切换以及性能按需扩展等功能。	自主研发	原始创新	201410116447.5 发明专利授权 专利申请号包括 201310094780.6、201510512485.7、201710403498.X 等	DPX 系列产品及各类业务板
6	OVC（OS-Level Virtual Context，操作系统级虚拟环境）技术	将一台物理设备虚拟成多台逻辑设备。经过 OVC 虚拟化之后，同一台物理设备上的多个逻辑设备都拥有独立的硬件、软件、转发表项、管理平面和日志，各逻辑设备的运行互不影响，有效地解决了多业务安全隔离和资源按需分配的问题，为网络和安全向动态、弹性的云服务模式转变创造了基础条件。	自主研发	原始创新	专利申请号包括 201510191335.0、201610162220.3、201610846530.7、201710393583.2、201710476004.0 等	公司全系列产品
7	大容量策略高速匹配技术	在安全策略、NAT 策略、会话数限制等策略的配置达到百万级的情况	自主研发	原始创新	专利申请号包括 201510967791.X、201511032058.5、	FW 系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
		下，通过核心算法优化，实现报文转发性能无损失。			201610581346.4、201710113606.X、201710008116.3 等	
8	大容量 NAT 地址转换技术	通过空闲端口分配和会话管理算法优化，高性能的实现了对称 NAT、圆锥 NAT、静态/动态端口块 NAT，DS-Lite/6RD 等各种 NAT 地址转换技术，很好的满足了运营商城域网部署大容量 NAT 地址转换网关的需求。	自主研发	原始创新	201010508058.9、201210223888.6、201210461711.X 、201210477060.3 等多项发明专利授权专利申请号包括 201310185284.1、201510340183.6 、201510500555.7 、201610293183.X 等	FW 系列产品
9	高性能 Ipsec VPN/SSL VPN 技术	通过对 Ipsec/SSL 协议加密过程和内网资源管理机制的优化，实现了高性能的 Ipsec VPN/SSL VPN 功能。	自主研发	原始创新	201210146021.5、201210272081.1、201210512666.6、201410072361.7 等多项发明专利授权专利申请号包括 201510434327.4 、201510530221.4 、201610335493.3、201610545144.4、201710606272.X、201710827200.8、201810093891.8、201810829794.0 等	FW 系列产品
10	应用识别技术	通过应用特征和行为模型识别技术，能够准确、有效、快速地完成应用的识别。	自主研发	原始创新	200910143613.X、201210477026.6、201210477357.X、201510077179.5 等多项发明专利授权专利申请号包括 201510220668.1 等	IPS 系列产品
11	IPS 入侵检测技术	通过攻击特征高速匹配算法以及攻击智能识别技术，实现对 IPS 攻击的精确检测。	自主研发	原始创新	201110227812.6 发明专利授权 专利申请号包括 201510320652.8、201510489691.0、201610398605.X、201610837577.7、201710079177.9、201710754886.2、201810279466.8 等	IPS 系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
12	IPS 入侵防御技术	支持串接/旁路阻断、邮件删除、黑名单、网络设备联动等各类防御手段，实现对 IPS 攻击的精准防御。	自主研发	原始创新	专利申请号包括 201410653834.2、201510690099.7、201610018371.1、201610150250.2 、201710210829.8、201710277205.8、201810106237.6 等	IPS 系列产品
13	DDoS 攻击检测与防护技术	支持各种 Flood 攻击以及应用层资源耗尽攻击，包括 SYN Flood 攻击、ACK Flood 攻击、HTTP CC 攻击等，有效提高了 DDoS 攻击检测准确度和防御效果。	自主研发	原始创新	201110219058.1、201110219066.6、等多项发明专利授权 专利申请号包括 201510040601.X 、201510874597.7 、201610203948.6 、201610474049.X、201710170344.0、201710769285.9、201811031383.3 等	Guard 系列产品
14	DNS 攻击防护技术	针对 DNS 缓存攻击、DNS 放大攻击、DNS Flood 攻击等多种常见 DNS 攻击提供了多维度的检测和防护手段，有效提高了 DNS 攻击检测准确度和防御效果。	自主研发	原始创新	201110219060.9、201110337375.3、201210226566.7、201210418881.X、201310209362.7 等多项发明专利授权 专利申请号包括 201610134542.7、201610297054.8 等	Guard 系列产品
15	链路负载智能均衡技术	包括均衡调度、过载调度、DNS 智能解析调度、异地调度、应用调度等多项关键技术，实现链路负载的智能均衡和灵活调度。	自主研发	原始创新	201210270710.7、201210418301.7、201310522849.0、201410007930.X 等多项发明专利授权 专利申请号包括 201510252769.7、201510535511.8、201610274530.4、201710147015.4、201710005553.X 等	ADX 系列产品
16	服务器负载智能均衡技术	包括均衡调度、连接拆分/复用、TCP 加速、SSL 卸载、全局负载均衡等多项关键技术，实现服务器负载的智能均衡和灵活加速功能。	自主研发	原始创新	201210226876.9、201310525163.7、201610460465.4 等发明专利授权 专利申请号包括、201310700265.8、	ADX 系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
					201510552450.6、201510836542.7、201610465959.1、201710114921.4、201710492909.7、201810035257.9 等	
17	健康检查技术	包括 ICMP/TCP/UDP/HTTP/DNS 等全方位的网络层、应用层健康检查功能，快速检测网络或服务器故障，实时进行流量迁移和调度，实现业务无缝切换功能。	自主研发	原始创新	201210227793.1、201210272077.5 等多项发明专利授权专利申请号包括 201510535755.6、201610716650.5、201610850767.2、201710236434.5、201710076590.X 等	ADX 系列产品
18	高性能行为审计技术	支持对用户行为进行审计，包括网页浏览、邮件、论坛、文件传输等，并通过应用协议分离、特征独立等优化算法，有效提高了行为审计系统的效率和准确性。	自主研发	原始创新	201010255359.5 发明专利授权专利申请号包括、201510085516.5、201610035084.1、201710087242.2、201810067601.2 等	UAG 系列产品
19	流控技术	通过用户/私网 IP 精准识别技术以及流控算法和技术，实现对流量进行按用户/应用等各维度的精准控制。	自主研发	原始创新	201210148153.1、201210419277.9、201210517179.9、201210539673.5 等多项发明专利授权专利申请号包括 201610018340.6、201610826697.7、201710161589.7 等	UAG
20	环网快速收敛技术	通过对 FRRP、MSTP 等环网协议的优化，有效提高了环路抑制的准确性以及网络故障收敛的灵敏性。	自主研发	引进消化吸收再创新	201110139605.5、201210418810.X、201210455293.3 等多项发明专利授权专利申请号包括 201410240812.3、201510612286.3、201510833898.5、201610053801.3、201610601349.X、201710008701.3、201710362345.5 等	LSW 系列产品
21	大容量 IP 地址动态分配	通过对 DHCP 地址分配算法以及防攻击算法的	自主研发	引进消化	201210271957.0、201210444579.1、	LSW 系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
	管理技术	优化，有效提高了 DHCP 的性能和容量，确保大规模网络 IP 地址动态分配的稳定性和安全性。		吸收再创新	201310633030.1 等多项发明专利授权 专利申请号包括 201510241158.2、201610281948.8、201610941632.7、201611040872.6、201710522668.6、201810712739.3 等	
22	大容量 ACL 管理技术	通过对 ACL 资源管理算法以及 ACL 下发通道的优化，实现了大容量 ACL 的高效管理和高速下发。	自主研发	原始创新	201210417824.X、201410370043.9 发明专利授权 专利申请号包括 201610145013.7、201610865869.1、201611250006.X、201710384699.X、201710891489.X、201810931112.7 等	LSW 系列产品
23	Web 攻击检测与防御技术	通过指纹识别、行为分析、Webshell 检测、Web 类漏洞扫描防护、网页防篡改等关键技术，实现针对 Web 攻击的精准检测与防御。	自主研发	原始创新	201210437105.4、201210450653.0、201310423483.1、201410100797.2 等多项发明专利授权 专利申请号包括 201410308572.6 、201510531757.8、201610811816.1、201610919494.2、201710090683.8、201710505947.1、201810043611.2、201811203799.9 等	WAF 系列产品
24	高性能认证技术	包括大容量 Portal 认证、MAC 认证等技术，有效提升了认证的容量和性能。	自主研发	原始创新	201210228247.X 发明专利授权 专利申请号包括 201510535329.2、201510152605.7、201610111404.7、201610326700.9、201610354956.0、201710236449.1、201710813541.X、	DAC 系列产品

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	相关产品和服务
					201810082592.4 等	
25	漏洞扫描技术	在精确识别跨站脚本攻击、SQL 注入、网页挂马等漏洞威胁的同时，有效提高了扫描效率，缩短了扫描时间，并降低了系统成本，有效的提升了产品竞争力。	自主研发	原始创新	201410032006.7、201610122286.X 发明专利授权 专利申请号包括 201410498518.2、201610483894.3、201810105641.1 等	Scanner 系列产品
26	高性能资源缓存与分发技术	通过压缩、热点识别、自动热点更新、视频文件本地转换、存储空间优化、高速查找算法优化等技术，在实现高性能内容查找与分发的同时，大幅节省缓存空间和出口带宽开销，有效减少了用户建设成本。	自主研发	原始创新	201410127034.7 发明专利授权 专利申请号包括 201410140158.9、201610485051.7、201610494338.6、201610915061.X 等	DeepCache 系列产品
27	智能网管技术	包括设备实时监控、集中管控以及网络状态智能分析等技术，能够实现对各类设备的有效监控和管理，同时能精确识别网络异常攻击、链路质量异常等网络异常事件，并与相关产品形成联动处置，有效提高整体网络的可维护性。	自主研发	原始创新	201210418840.0 发明专利授权 专利申请号包括 201510130782.5、201510467498.7、201610304982.2、201610591223.9 、201610837924.6、201710064475.0、201710674731.8、201810504999.1 等	UMC 系列产品

公司拥有的核心技术均来源于长期的技术投入和自主创新，拥有独立的知识产权，针对核心技术，公司制定了严格的知识产权保护措施和制度，对各项核心技术均申请了发明专利和软件著作权等知识产权保护，同时在公司与员工签署的劳动合同中规定，有关作品的所有知识产权或其他相关专利均归公司所有，不存在知识产权方面的潜在纠纷。

公司核心技术不涉及公司的董事、监事、高管及主要发明人员在原单位的职务成果，不存在违反竞业禁止的有关规定，不存在违反保密协议的情形。

以上核心技术均在公司的产品和服务中有效应用，得到了市场和客户的普遍认可。报告期内，公司核心技术产品收入占营业收入的比例如下：

单位：万元

项目	2018 年度	2017 年度	2016 年度
核心技术产品收入	**65,939.41**	**56,242.32**	**49,594.70**
营业收入	70,405.56	61,696.30	53,264.92
核心技术产品收入占营业收入比例	**93.66%**	**91.16%**	**93.11%**

（二）公司核心技术人员情况

1、研发人员及核心技术人员整体情况

公司现有研发团队具有专业的技术能力，丰富的项目经验，公司已经形成了新老结合、技术层次全面的研发团队，形成了人才、技术和业务相互促进的发展模式。截至 2018 年 12 月 31 日，公司有专业研发人员 458 人，占公司员工总数的 41.86%。

2、核心技术人员简介

公司核心技术人员包括周顺林、钱雪彪、李治、关巍等，周顺林先生的具体情况如下：

周顺林先生，1970 年出生，中国国籍，无境外永久居留权。1992 年毕业于北京科技大学流体控制专业，获学士学位；1995 年毕业于北京航空航天大学自动控制专业，获硕士学位。1995 年至 1999 年，任中国科学院空间中心工程师；1999 年至 2003 年，任华为技术有限公司产品研发经理；2003 年至 2011 年，任职于杭州华三通信技术有限公司，历任研发副总监、软件部部长；2011 年起，历任公司首席技术官、公司副总裁，2016 年至今，任公司董事、副总经理。

钱雪彪先生，1978 年出生，中国国籍，无境外永久居留权。2000 年毕业于陕西师范大学物理学专业，获学士学位；2003 年毕业于电子科技大学光学工程专业，获硕士学位。2003 年至 2012 年，任职于杭州华三通信技术有限公司，历任软件工程师、项目经理、系统工程师；2012 年起，任公司软件开发部部长，2016 年至今，任公司副总经理。兼任杭州迪普信息技术有限公司总裁。

李治先生，1977 年出生，中国国籍，无境外永久居留权。1999 年毕业于南京大学计算机应用专业，获学士学位。1999 年至 2003 年，任职于华为技术有限

公司，历任软件工程师、产品开发代表、质量工程师、项目经理；2003 年至 2012 年，任职于杭州华三通信技术有限公司，历任产品开发团队经理、项目经理；2012 年起，历任公司交换机产品部部长、技术支援部总监，2016 年至今，任公司副总经理。

关巍先生，1978 年出生，中国国籍，无境外永久居留权。2001 年毕业于南开大学信息科学专业，获学士学位。2001 年至 2002 年，任华为技术有限公司软件工程师；2002 年至 2003 年，任港湾网络有限公司测试工程师；2003 年，任三一通讯技术有限公司测试工程师；2003 年至 2013 年，任职于杭州华三通信技术有限公司，历任测试工程师、测试经理、软件开发部项目经理、测试中心测试系统工程师；2013 年起，历任公司测试中心部长、北京运作支撑部部长，2016 年至今，任公司监事会主席。

3、核心技术人员变动情况

公司核心技术人员保持稳定，最近两年未发生变动。

五、发行人未来成长的不确定性

（一）尽管公司在国内同行业内具有一定的技术优势，且成长性良好，但较国内外知名企业相比，仍存在规模较小、资金实力不足等弱点，面对市场的快速增长，全国快速拓展的模式和手段单一。

（二）行业随着技术进步，所需要突破的技术难题将会不断产生，要求公司不断对前瞻性技术研究、产品升级换代、服务能力优化等关系公司核心竞争力的重点领域加强研发投入，提升研发水平，以保持和提升公司在行业的领先地位。

（三）信息安全行业属于知识密集型行业，技术、知识的更新换代迅速，新技术、新产品的研究、开发需要大量专业技术人员，特别是能够深刻把握信息安全领域发展趋势、具有核心技术的高端人才。同时，随着公司的发展和业务规模的不断扩大，公司也需要大量营销人才和项目管理人才。人才结构的调整、人才数量的增加能否与公司的发展相匹配可能会影响到公司发展目标的实现。

（四）公司自成立以来，经营规模和业务范围不断扩大，组织结构日益复杂，对公司管理的要求越来越高，公司的人员也有较大规模的扩充。这些变化将对公

司的管理将提出新的和更高的要求。虽然公司的管理层在经营和管理快速成长的企业方面有着丰富的经验，但是仍需不断调整，以适应资本市场要求和公司业务发展需要。

六、保荐机构的专项意见

（一）尽职调查及审慎核查过程

保荐人对发行人的成长性进行了尽职调查，通过审慎核查发行人公司治理、内部控制等制度建设，确保发行人制度建设已逐步得到有效执行；审慎核查发行人的研发生产制度、研发投入、研发成果、生产质量管理状况等，确保发行人具有健全的生产质量管理能力和可持续的自主研发能力；审慎核查发行人采购、生产、销售、研发及管理各环节的工作，确保发行人经营工作的有序运作；与律师、会计师保持密切沟通，确保发行人在法律、财务方面的合法合规性。同时，根据发行人目前的业绩和发展现状，结合可能存在的风险因素，保荐人对发行人的主营业务、行业发展前景、自主研发能力、生产质量管理能力、未来发展与规划以及募集资金运用计划等影响发行人持续成长的各方面进行了尽职调查、审慎核查和独立分析判断。

（二）结论

本保荐机构认为：发行人在报告期内主营业务突出，专注于企业级网络通信领域，致力于为用户提供以“简单、智能、安全”为核心价值的网络安全产品、应用交付产品、基础网络产品和相关专业服务，所处行业未来具有较好的发展前景；通过持续的创新与研发，发行人拥有一系列具有自主知识产权的核心技术，已成为具备核心技术与竞争力、国内领先的网络安全、应用交付以及基础网络产品及解决方案提供商；发行人建立了覆盖全国的市场销售与技术支援体系，相关产品已经进入了包括运营商、政府、电力能源、金融、交通、教育、医疗等在内的众多行业，发行人主营业务具有良好的业绩成长性；发行人在高性能硬件平台，融合网络、安全、应用交付功能于一体的软件平台，FPGA 系统设计、信息安全和应用交付领域相关核心技术等方面的一系列创新，为发行人未来业绩增长奠定了较为坚实的基础。发行人已建立了未来发展战略和具体发展举措，有利于保证

发行人持续的核心技术优势和市场竞争优势，发行人具有良好的发展前景和成长性。

（以下无正文）

（本页无正文，为《中信建投证券股份有限公司关于杭州迪普科技股份有限公司成长性的专项意见》的签字盖章页）

保荐代表人签名：

赵　军　　谢思遥

中信建投证券股份有限公司

2019 年 3 月 19 日