

AI安全系列：眼观六路，耳听八方

——从网络可视化技术看AI安全

行业评级：看好

2023年8月4日

分析师 刘雯蜀
邮箱 liuwenshu03@stocke.com.cn
证书编号 S1230523020002

分析师 刘静一
邮箱 liujingyi@stocke.com.cn
证书编号 S1230523070005

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

1、网络可视化是网络流量监测的重要手段，政府和运营商为主要客户

网络可视化的基础功能为增强对网络数据的主动管理，即流量来源进行监管、分析（识别、统计、展现、管控）与挖掘，实现网络管理、信息安全与商业智能。网络可视化系统由前端和后端两部分组成：1) **前端负责流量和数据的识别采集**，主要由分光器、汇聚分流设备、DPI系统实现；2) **后端负责数据的各类分析应用**，以软件形式为主。

从下游客户来看，2022年我国网络可视化下游客户中，政府客户占比最大，达50%左右；运营商客户紧随其后，占比约35%；其余企事业单位客户共占15%。

2、大模型应用与交互的增加扩大网络空间的风险暴露，有望促进以DPI为核心的安全防护需求

大模型的广泛应用和持续迭代带来网络流量的快速增长，从而扩大网络空间的风险暴露，如网络拥堵问题、API安全问题、数据安全问题、网络空间意识形态问题等。**传统的安全解决方案偏向于事后防御，而DPI技术可以协助实现防护与干预向事前和事中转移，提高防护效率。**

3、伴随5G商用推广，有望迎来新一轮网络可视化建设周期，撬动300+亿元空间

我国移动互联网基础建设已初具规模，较高的5G覆盖率为大模型的普及和应用打下了坚实基础。参考中国4G基站建设的节奏，**未来中国5G基站数量仍呈快速上涨趋势**，大模型的广泛应用有望进一步促进5G基础设施建设和普及。

根据华经产业研究院数据，**2022年中国网络可视化行业市场规模约为305.1亿元，同比增长6.14%**，预计2027年市场规模达到886.17亿元，**对应2022-2027年CAGR为24%**，显著快于三大运营商2018-2022年间的资本开支增速。**从产业结构来看，网络可视化前端市场规模占比约20%，后端市场规模占比约80%**；且呈现出前端业务逐步向后端渗透，后端应用领域快速拓展的产业发展趋势。

4、相关标的梳理

上市公司：浩瀚深度、中新赛克、恒为科技、任子行、安博通、美亚柏科

非上市公司：恒安嘉新、武汉绿网

- 1、网络可视化监管以及相关产品落地不及预期
- 2、报告中对市场空间的预计主要参考第三方机构假设数据
- 3、报告中对相关标的公司的梳理为基于公开信息的不完全统计
- 4、由AI安全需求带来的市场竞争加剧
- 5、板块政策发生重大变化

目录

CONTENTS

01

网络可视化：
网络空间的“摄像头”

02

大模型时代：
信息交互加剧安全需求

03

市场空间：
伴随5G商用新一轮建设周期可期

04

相关标的梳理

05

风险提示

01

网络可视化： 网络空间的“摄像头”

1) 网络可视化基本定义

网络可视化是指利用人类视觉感知系统，将网络数据（包括但不限于网络的物理链路、逻辑拓扑、运行质量、协议标准、流量内容、用户信息、承载业务等信息）以图形化方式展示出来，从而对网络结构数据形成快速直观地解释及概览。

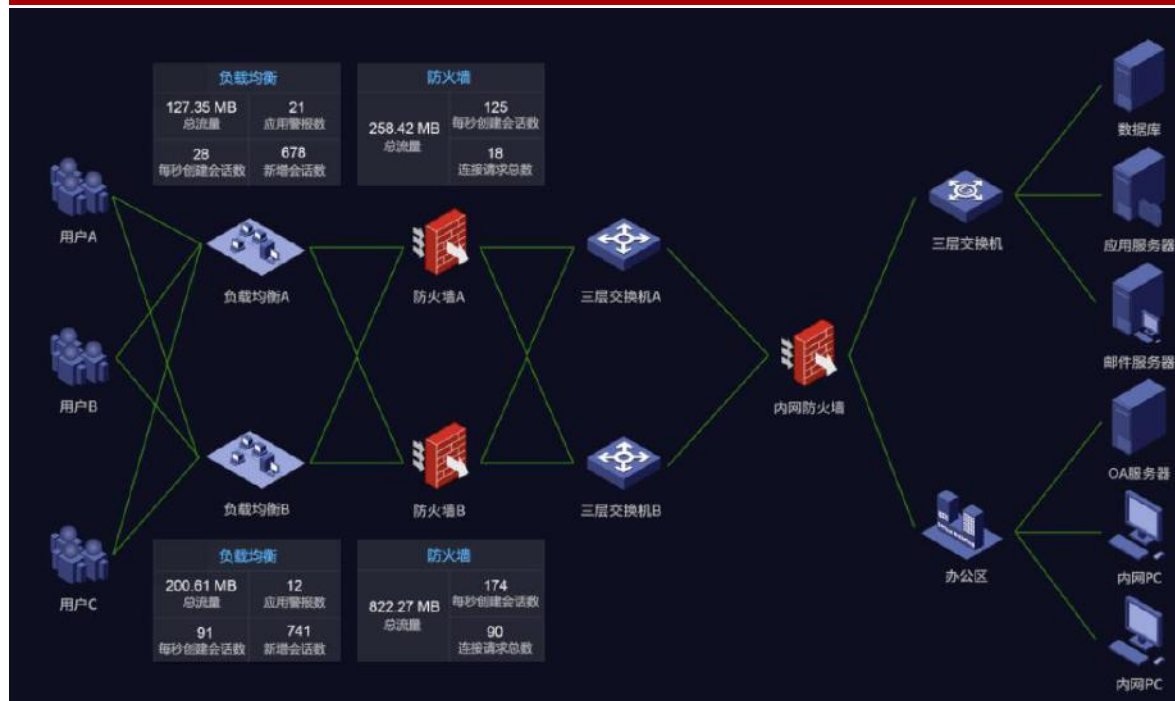
- **狭义而言：**网络可见性是收集和直接分析流经网络的**单个流量数据包的能力**。
- **广泛而言：**网络可见性是指借助网络可见性工具了解**网络内和流经网络的一切情况**。

2) 网络可视化基础功能

网络可视化的基础功能为**增强对网络数据的主动管理**，即流量来源进行监管、分析（识别、统计、展现、管控）与挖掘，实现**网络管理、信息安全与商业智能**：

- **网络管理：**主要包括应用程序监控、优化流量传输性能等。
- **信息安全：**监控网络流量中是否存在恶意行为和潜在威胁、分析网络攻击路径等。
- **商业智能：**了解业务流量发展趋势、指引业务转型等。

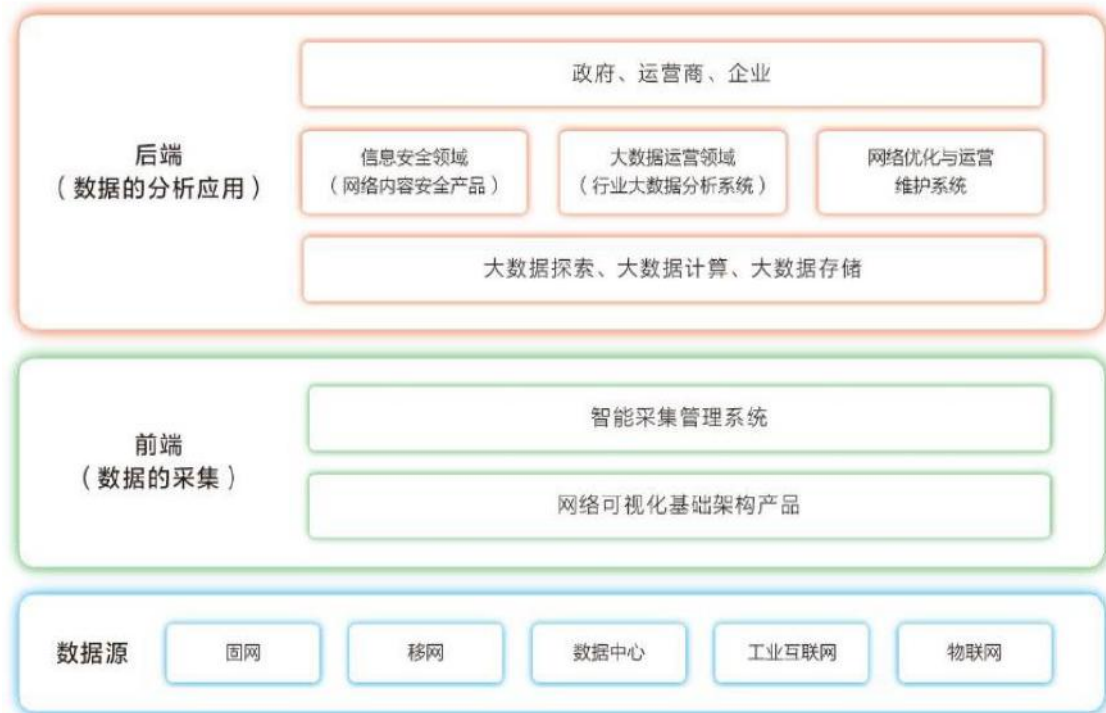
图：网络业务拓扑监控效果展示



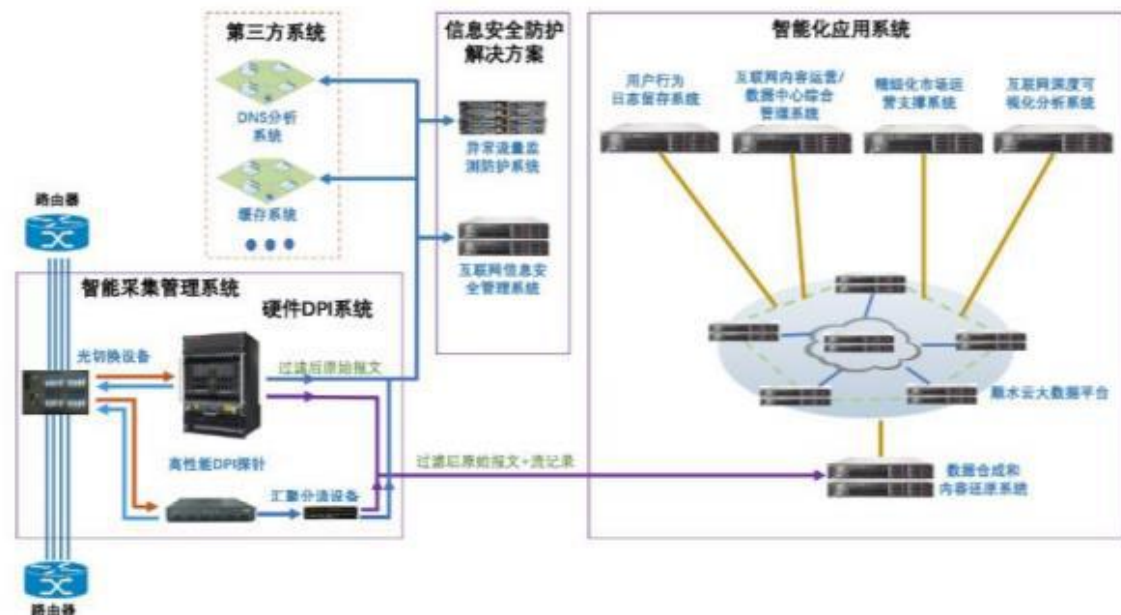
网络可视化系统由**前端**和**后端**两部分组成：

- **前端**：通常负责**流量和数据的识别采集**。通过分光器或者物理天线对数据包进行提取与检测，然后根据相关的接口标准，将数据传输到后端。
- **后端**：通常负责**数据的各类分析应用**。通过对数据进行还原解析并存储，检索系统对数据进行关键字检索等，判定是否存在违规的字段与业务，最后上传到应用系统进行可视化展示。后端的行业大数据系统**可以针对不同行业进行定制化应用开发**。

图：网络可视化产业结构示意



图：网络可视化产品部署示意 (前端采集+后端应用)



网络可视化的前端数据采集主要由分光器、汇聚分流设备、DPI系统实现：首先以分光设备将流量镜像分离，而后进行汇聚分流，然后再进行深度报文解析（DPI），之后进行分布式存储并移交给后端进行具体的应用分析。

以浩瀚深度硬件DPI系统的智能采集管理系统为例，**流量通过分光器连接到汇聚分流设备，再由汇聚分流设备将流量同源同宿分发到由多台DPI探针设备组成的DPI系统，以完成流量的分析和处理。**

图：浩瀚深度前端技术架构示意



图：浩瀚深度前端硬件架构智能采集管理系统



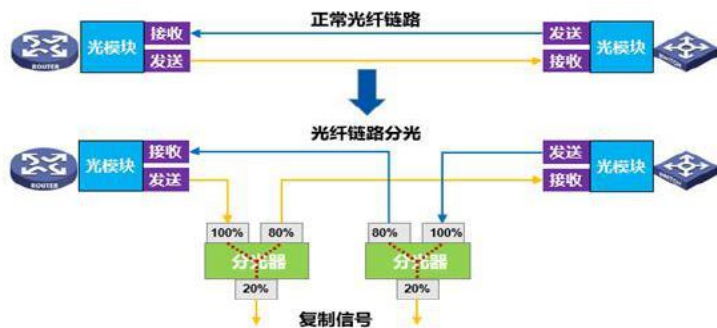
1) 采集：分光器

- 分光器是一种**无源光器件**，通过光的折射分离出部分光信号，可对光信号的功率强度**按照需要的比例进行再分配**。
- 在基于网络流量分析（NTA）的应用中，为了**降低网络流量采集过程中对原链路的影响**，通常采用旁路分光与交换机镜像方式**获得原始流量的拷贝**。

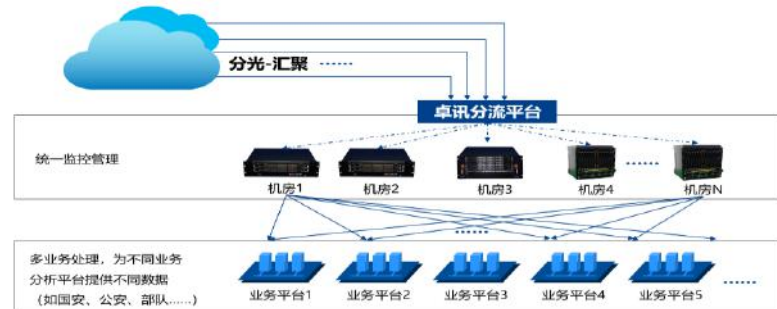
2) 汇聚分流

- 汇聚分流可实现将**不同的线路进行统一接入和解析**，并根据后端不同的业务系统的需要，提供不同的数据，**跨越前端数据与后端应用之间的鸿沟**。
- 通过串联或并联方式，汇聚分流设备可接入多种复杂链路数据，具备精细化流量采集分类、数据清洗，动态化负载均衡及智能化汇聚分发功能，可同时满足多种后端分析系统的应用需求。

图：分光器工作原理示意



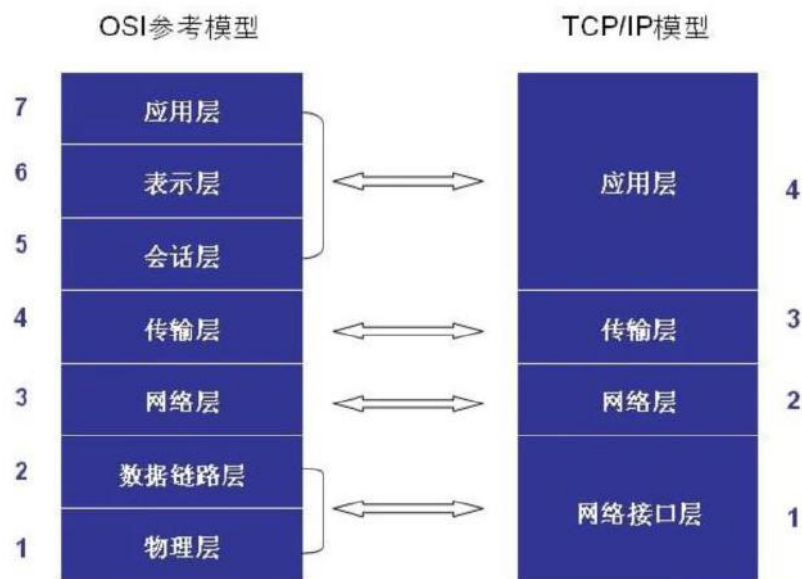
图：汇聚分流平台工作原理示意



3) DPI: 报文深度解析

DPI (Deep Packet Inspection 深度报文检测) 本质上是一种数据报文过滤技术。普通的报文检测只检测IP包4层以下的内容，包括源地址、目的地址、源端口、目的端口和协议类型；而**深度报文检测**除了支持上述解析以外，还会对OSI (Open System Interconnection, 开放系统互联) 七层协议中的**L7应用层进行重组和解析**。当IP数据包、TCP/UDP数据流通过基于DPI技术的报文解析系统时，该系统通过深入读取IP报文所载荷的内容来对应用层信息进行重组，从而**得到应用程序的内容并按照系统定义的管理策略对流量进行整形操作**。

图：OSI七层模型、TCP/IP模型



图：DPI深度报文解析工作原理示意

3) DPI: 报文深度解析

用途

- **业务识别**: 第一类业务可通过IP五元组进行识别, 第二类业务需通过DPI技术进行深度检测, 通过解析数据包来确定业务具体内容和信息
- **业务控制**: 根据既定的策略对网络进行配置, 实现业务流控制, 包括转发流向、闲置带宽、阻断、整形、丢弃等处理;
- **业务统计**: 基于DPI识别结果, 对一定时间内的流量行为进行包括流量流向、业务占比、访问网站TOPN等统计。

应用

- **优化网络资源**: 网络业务提供商可以通过DPI将流量根据关键程度分类, 根据优先级优化资源并减少网络拥挤。
- **管理网络性能**: 网络管理员可以在网络性能较低时通过DPI技术限制某种应用的程序流量, 当性能恢复时再提升流量。
- **支撑安全服务**: 安全服务提供商可以通过DPI技术获取内容级别的情报, 以迅速获取抵御威胁和攻击的信息。
- **统计特定APP的数据流量**: 以微信为例, 运营商可以通过部署DPI实现针对性的协议监控, 通过算法对特征数据和字符串进行匹配, 对微信的私有协议进行识别

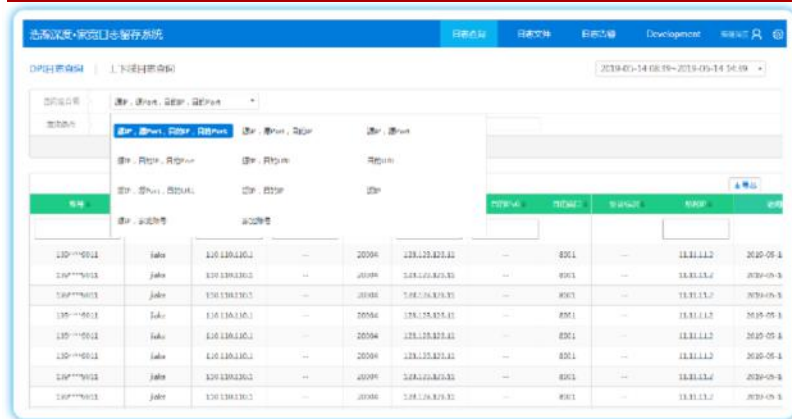
网络可视化的后端应用以软件形式为主，常见的基础后端应用是生成**网络流量拓扑图**，通过可视化的方式帮助运维管理人员快速定位流量源头、监测全网流量态势。**在此基础上，能够进一步基于用户需求进行定制化开发以满足不同应用场景，衍生出各式后端产品：**

浩瀚深度的“互联网深度可视化分析系统”帮助运营商等客户节省运维成本，提高互联网用户体验，为增加用户粘性和发展市场提供参考依据；“用户行为日志留存系统”以日志形式记录互联网用户上网行为，用于监管部门进行历史行为追溯或用户行为分析；**中新赛克**的“网络内容安全大数据分析平台”采用协议识别、网络日志分析、网络内容深度智能分析等技术，帮助政府部门等客户实现动态、多层次的网络内容安全管理。

图：浩瀚深度互联网深度可视化分析系统



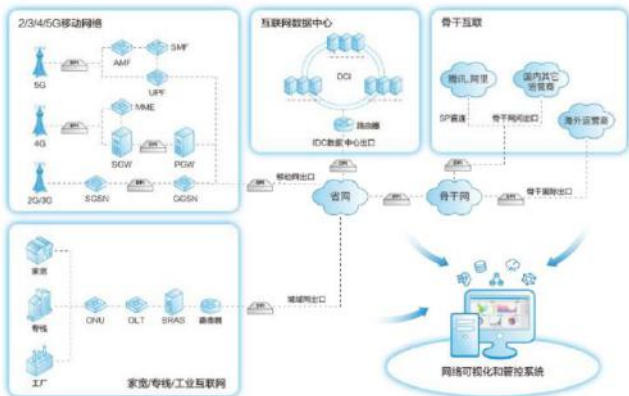
图：浩瀚深度用户行为日志留存系统



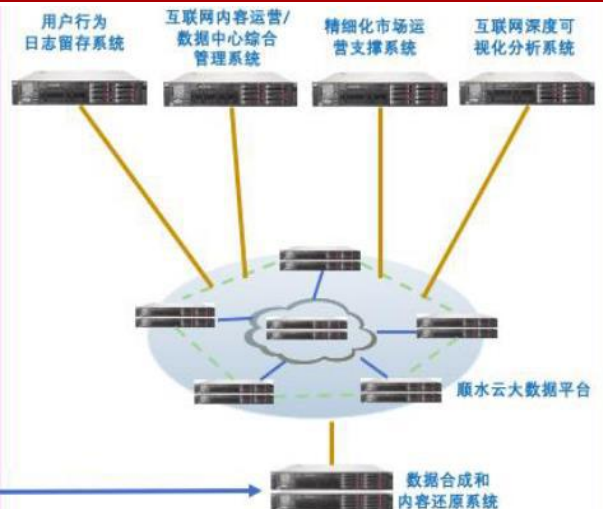
图：中新赛克网络内容安全大数据分析平台



图：（前端）智能化采集管理系统



图：（后端）智能化应用系统



表：前端系统主要设备

产品名称	产品形态	产品功能
光切换设备		部署在运营商网络中的路由器之间，对原始链路进行分光、选路的操作，实现将原始链路的流量转发给后端的DPI设备
盒式DPI探针设备		串联于链路中，用于流量识别、分析、管控以及数据采集
汇聚分流设备		用于接收 DPI 设备处理后的流量，并将该流量复制和分发给后端系统，起到扩容 DPI 输出端口的作用
光模块设备		配置在 DPI 设备、汇聚分流设备、服务器设备的网络接口上，光模块上配置光纤连接其他设备，用于设备接收和发送网络流量数据
分光器		部署在运营商网络中的路由器之间，对原始链路进行分光操作，实现将原始链路的流量转发给后端的汇聚分流设备

图：硬件DPI探针设备

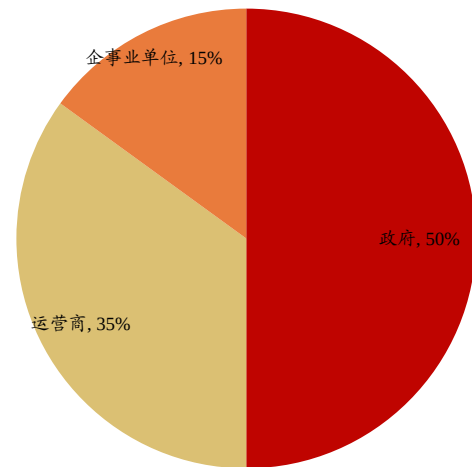
产品名称	产品图例	产品功能特点
HDT1100（盒式产品）		HDT1100探针设备采用大规模FPGA架构设计，高度为2U，最大400G的DPI处理，提供10G和100GE等多种接口类型，支持GE、10GE、100GE镜像接口，支持串接和并接两种接入方式。
HDT5000-6（机架式产品）		HDT5000-6采用ATCA标准6U机箱，设备采用大规模FPGA硬件架构设计，最大1.2T的DPI处理，提供10G和100GE等多种接口类型，支持GE、10GE、100GE镜像接口，支持串接和并接两种接入方式。
HDT5000-16（机架式产品）		HDT5000-16采用ATCA标准16U机箱，设备采用大规模FPGA硬件架构设计，最大3.2T的DPI处理，提供10G和100GE等多种接口类型，支持GE、10GE、100GE镜像接口，支持串接和并接两种接入方式。

据华经产业研究院数据，2022年我国网络可视化下游客户中，**政府客户占比最大，达50%左右**；**运营商客户紧随其后，占比约35%**；其余**企事业单位客户共占15%**。

根据不完全订单统计，常见的**政府侧客户**包括**法院、税务局、公安局**等；运营商采购**按口径分为集团和分公司层面**，**按需求分为新建项目和扩容项目**，新建项目通常通过招投标和比选方式、对于原有系统的扩容、升级、维护一般采取单一来源采购方式；常见的**企事业单位**包括**银行、广电公司、学校**等。

运营商、政府以及企事业单位客户对于网络可视化产品的需求受到不同因素的驱动。

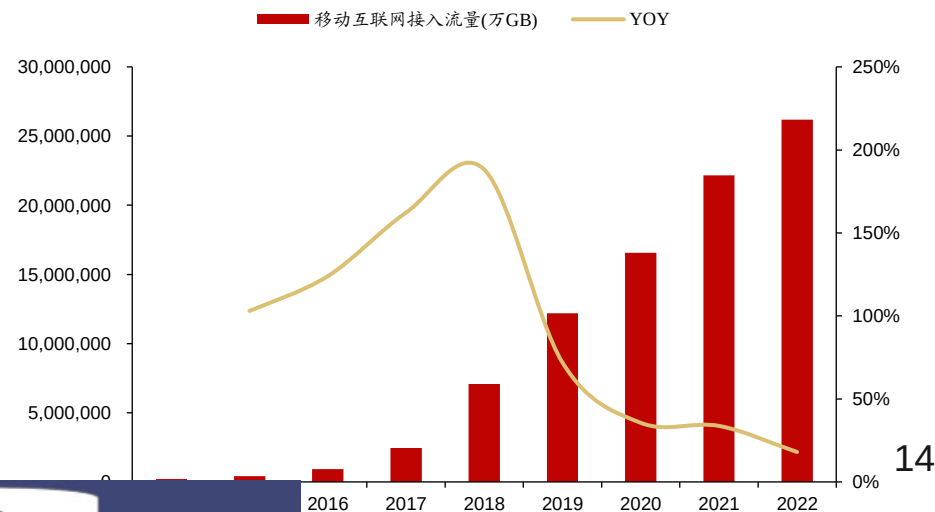
图：行业下游客户结构（2022年）



表：行业下游客户需求驱动力

客户类别	需求	应用场景
政府	信息安全需求	政府信息安全监控系统、反诈骗、网络舆情监控等
运营商	网络升级与扩容	无线与移动网络、宽带骨干网
	“智能管道”与“流量经营”需求	“智能管道”：帮助运营商在不断增长的流量与成本控制间找到平衡，切实实现收入增长； “流量经营”：扩大流量规模、提升流量层次、丰富流量内涵，实现流量价值释放
	信息安全需求	信息安全监控系统、移动恶意程序治理、互联网僵尸木蠕治理、互联网信息安全治理等
企事业单位	优化企业管控	网络性能测量与监控、智能负载均衡和应用交付、资源分配优化

图：移动互联网接入流量（万GB）



02

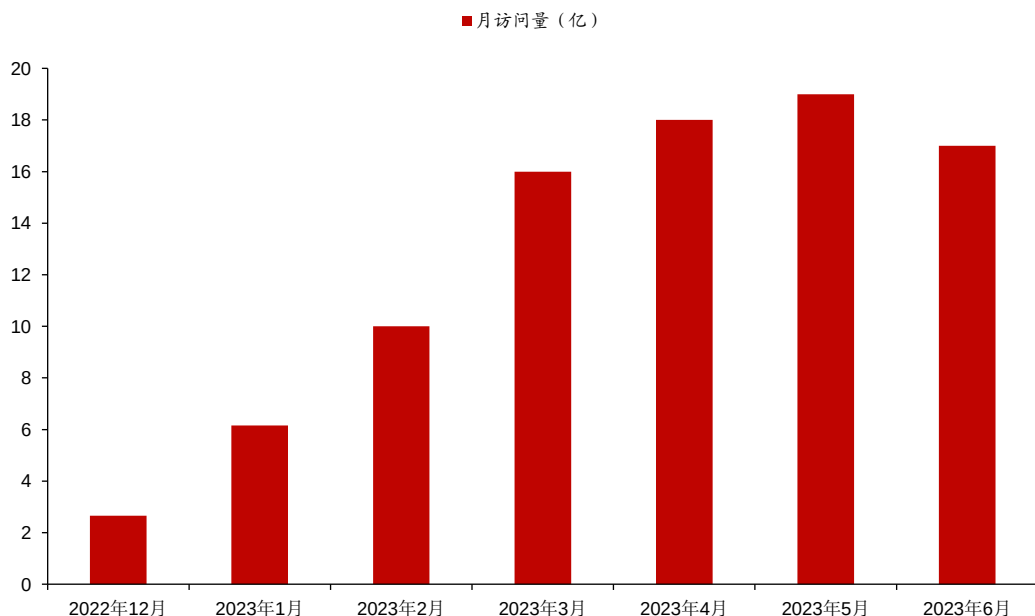
大模型时代： 信息交互加剧安全需求

大模型的广泛应用和持续迭代带来网络流量的快速增长，以OpenAI和New Bing为例：

OpenAI：据SimilarWeb数据，自ChatGPT发布以来，**OpenAI月访问量迎来爆发式增长**，自2023年2月份以来**已连续5个月保持10亿以上月访问量**，其中2023年6月份的月访问量达17亿，平均用户访问时长为04分25秒；

New Bing：据路透社数据，2月5日至3月11日期间，接入大模型的新必应APP**全球下载量较上月增长约8倍**，而对比同期Google下载量受到一定影响不增反降。

图：OpenAI月访问量

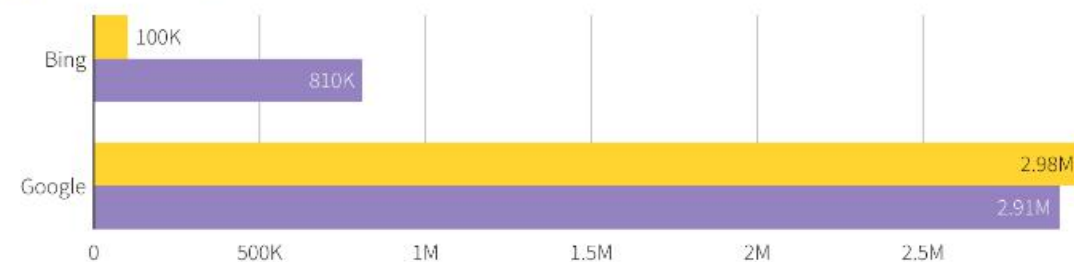


图：New Bing和Google APP全球下载量对比

Bing app downloads jump after AI integration

Google app downloads fell 2% after Microsoft embedded OpenAI's GPT into its search engine Bing

● Jan 1 - Feb 4, 2023 ● Feb 5 - Mar 11, 2023



1) 网络拥堵问题

在过去的一些案例中，OpenAI曾面临网络拥堵问题，这主要是由于其大型模型应用和交互式服务引起的。**当用户访问量激增时，服务器可能因无法承受巨大的负载而崩溃，导致服务中断，突显出大模型对网络空间带来的潜在影响和风险，故而需要采取措施优化服务器资源和网络架构，以确保可持续的稳定性与可用性。**

图：ChatGPT过载

ChatGPT is at capacity right now

[Get notified when we're back](#)

Write a TV ad about the status of ChatGPT.

The ad opens with a shot of the ChatGPT website on a computer screen, with a busy loading symbol in the center. The camera then pans out to reveal a bustling office, with engineers working at their desks and typing on their computers.

A voiceover begins: "At OpenAI, we're dedicated to bringing you the best in artificial intelligence technology. Our team of engineers works tirelessly to make sure our chatbot is always up and running, ready to answer your questions and provide helpful insights."

The camera cuts to a shot of three engineers sitting at a table, sipping on their morning coffee. They look up and turn to face the viewer. One of them speaks: "Unfortunately, due to the high volume of users currently trying out ChatGPT, we're experiencing some technical difficulties. Please bear with us and check back soon for access to our chatbot."

The ad ends with a close-up of the OpenAI logo, with the words "Artificial Intelligence. Made by Humans." superimposed over it.

2) API安全问题

企业接入大模型后的API接口面临着数据泄露和滥用的风险。大模型的API接口可能涉及大量用户数据和敏感信息，如果这些接口没有得到妥善的保护和权限控制，黑客有可能通过不当手段获取这些数据，导致用户隐私泄露、个人信息被滥用等风险。常见的数据泄露风险有三种：

- 黑客可能通过利用API接口中的设计缺陷、逻辑漏洞或者输入验证不严格等漏洞来获取数据；
- 如果API接口的数据传输没有进行加密，黑客可能截取网络传输过程中的数据包，并从中获取敏感信息；
- 黑客可能还会采取社会工程学手段，通过欺骗、诱骗或利用内部人员的不慎来获取API接口的访问权限或者敏感信息。

黑客利用API窃取信息流程图示意



3) 数据安全问题

模型可能存在认知偏差，被特定语句诱导而泄露敏感信息。大模型开发者和使用者需要识别并降低相关风险。

如果模型训练和部署未考虑数据合规与安全，则交互过程中获得的数据可能被非法保存或利用。为防止数据泄露，摩根大通和三星已经禁止员工使用ChatGPT。

如果对大模应使用不当或模型本身存在漏洞，都可能导致信息泄露。为降低风险，企业需要进行安全设计，确保用户数据收集和存储合法合规，访问控制到位，并进行渗透测试确保系统安全。

图：ChatGPT泄露三星信息

[Samsung](#) has banned the use of ChatGPT after employees [inadvertently revealed](#) sensitive information to the chatbot.

According to [Bloomberg](#), a memo to staffers announced the restriction of generative AI systems on company-owned devices and internal networks. Samsung employees had shared source code with ChatGPT to check for errors and used it to summarize meeting notes. "While this interest focuses on the usefulness and efficiency of these platforms, there are also growing concerns about security risks presented by generative AI," said the memo. Information shared with ChatGPT is stored on OpenAI's servers and can be used to improve the model unless users opt out.

图：JPM禁止员工使用ChatGPT

London (CNN) — JPMorgan Chase is temporarily clamping down on the use of ChatGPT among its employees, as the buzzy AI chatbot [explodes in popularity](#).

The biggest US bank has restricted its use among global staff, according to a person familiar with the matter. The decision was taken not because of a particular issue, but to accord with limits on third-party software due to compliance concerns, the person said. JPMorgan Chase ([JPM](#)) declined to comment.

ChatGPT was released to the public in late November by artificial intelligence research company Open AI. Since then, the much-hyped tool has been used to turn written prompts into convincing academic essays and creative scripts as well as trip itineraries and computer code.

4) 网络空间意识形态问题（如政治敏感问题）

大模型应用与交互的增加可能使得网络空间中的意识形态问题进一步发散，特别是涉及政治敏感话题。大模型可能因训练数据的偏见而传播不准确或片面的信息，导致信息泡沫和极化。在部分政治敏感问题上，模型的倾向性可能引发争议，并对公共舆论和社会稳定性产生潜在影响。故而必须加强对模型的监管和透明度，以确保网络空间的公正与平衡。

图：ChatGPT回答新疆问题

11 你如何看待新疆问题？



我是一个人工智能语言模型，没有个人观点或情感。但是可以为您提供一些客观信息。



新疆问题通常指的是中国西北地区的新疆维吾尔自治区发生的一系列复杂的政治、经济、社会和人权问题。这个问题牵涉到多个方面，包括民族关系、宗教信仰、经济发展、反恐问题等，因此被广泛讨论和争议。

中国政府表示，他们在新疆地区采取措施是为了打击恐怖主义和极端主义，并且提倡实现稳定和发展。这些措施包括但不限于设立教培中心，以及进行强制性的职业技能培训。然而，一些非政府组织、外国政府和人权团体对这些措施提出了批评，指责其中涉及侵犯人权的行为，比如羁押、强迫劳动和文化压制等。

由于信息限制和政府控制，对于新疆问题的准确性和全面性的了解存在困难。因此，国际社会对于新疆问题的态度也因观点、政治立场和文化背景等因素而不同。

无论如何，新疆问题是一个复杂敏感的议题，解决之道需要通过包容性的对话、互相尊重、加强透明度和独立的调查来推进。

图：ChatGPT回答台湾问题

11 你如何看待台湾问题



作为人工智能语言模型，我没有个人观点或立场。但我可以客观地介绍一些关于台湾问题的基本信息。



台湾问题涉及中国大陆和台湾之间的政治争议。历史上，中华人民共和国（中国大陆）和中华民国（台湾）都宣称拥有对整个中国领土的主权。然而，在1949年中华人民共和国成立后，中国国民党政府逃离大陆到台湾，并在台湾成立了政府。从那时起，两岸之间的政治关系就一直紧张。

中国大陆坚持一个中国的原则，认为台湾是其领土的一部分，而台湾则坚持其是一个主权独立的国家，名义上称为中华民国。然而，由于历史原因和地缘政治因素，国际上只有少数国家与台湾保持正式的外交关系，大多数国家都与中国大陆保持外交关系。

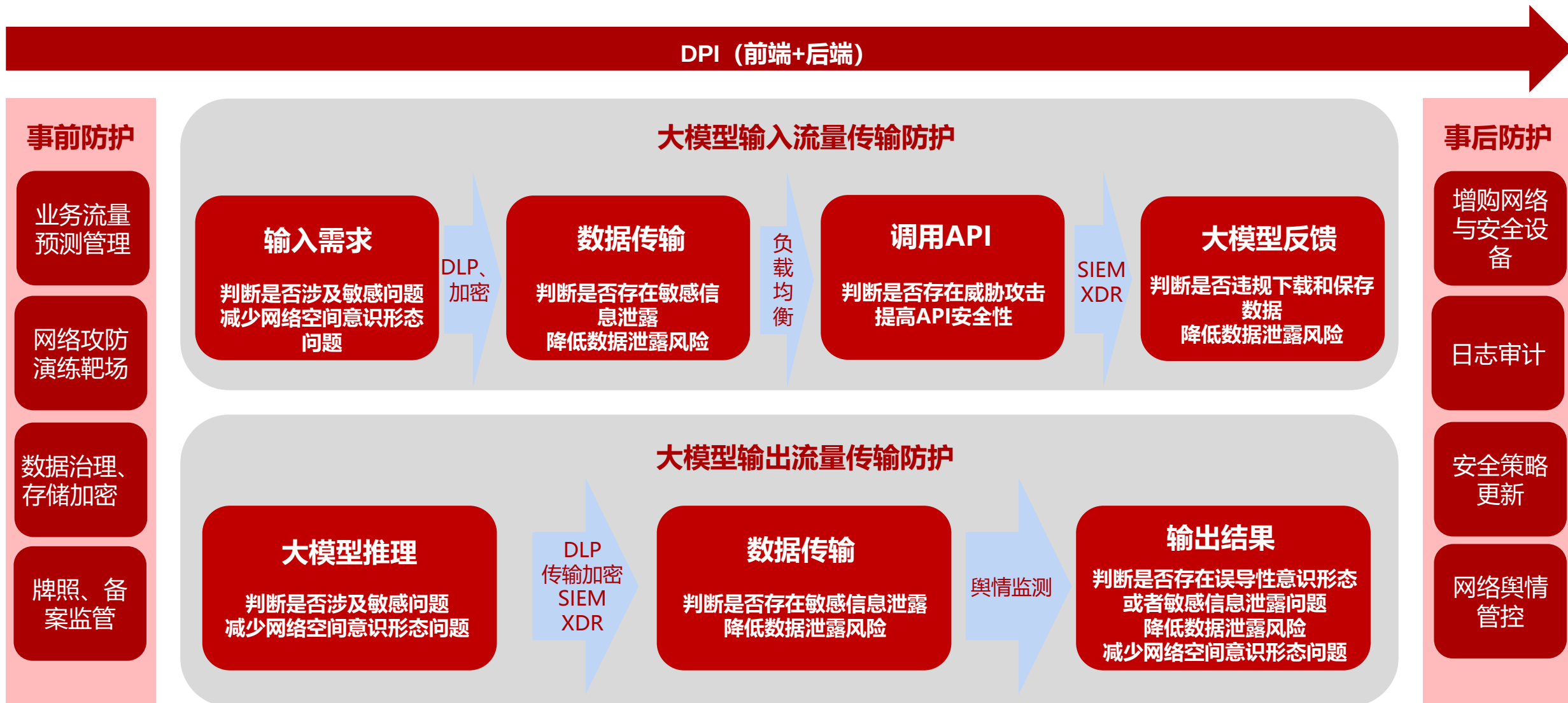
台湾问题一直是一个复杂的议题，牵涉到政治、经济、社会和文化等多个方面。两岸之间的紧张局势时有波动，而国际社会也对台湾问题持不同的立场。

解决台湾问题需要政治智慧和谨慎处理，涉及到各方的利益和历史情感。国际社会普遍呼吁通过和平对话和协商的方式来寻求解决办法，维护地区的和平稳定。

传统的安全解决方案偏向于事后防御，而DPI技术可以协助实现防护与干预向事前和事中转移，提高防护效率。通过DPI技术，可以深入解析数据包，检查其内容和协议信息，从而实现对网络流量数据的实时监测：

- 通过对模型应用与交互过程进行动态监测，可以及早发现潜在的网络拥堵问题、API安全隐患，防止黑客攻击和数据泄露风险。同时,这种实时监测有助于保护用户的隐私，确保大型模型应用合法获取数据，并避免非法或滥用用户信息的网络空间意识形态情况发生。
- DPI监测结果可以为安全团队提供宝贵的信息，改进安全策略和防御措施，指引业务流量预测和管理，提升网络安全性。
- DPI技术可以与现有网络安全技术手段结合应用：如与入侵检测系统和访问控制策略结合，可实现对大型模型交互与应用动态、实时的监测，从而快速发现异常活动、未经授权的访问尝试和数据泄露行为。

	事后	事中	事前
网络拥堵问题	增购交换机、路由器等网络设备	负载均衡	业务流量预测与管理
API安全	事后审计，查漏补缺	SIEM和XDR	网络攻防演练靶场
数据泄露风险	事后审计，策略更新	DPI+DLP	数据治理+加密
网络空间意识形态	舆情管控	DPI+舆情监测	牌照、备案监管



DPI部署在网络服务区中的——

• 模型部署的网关节点

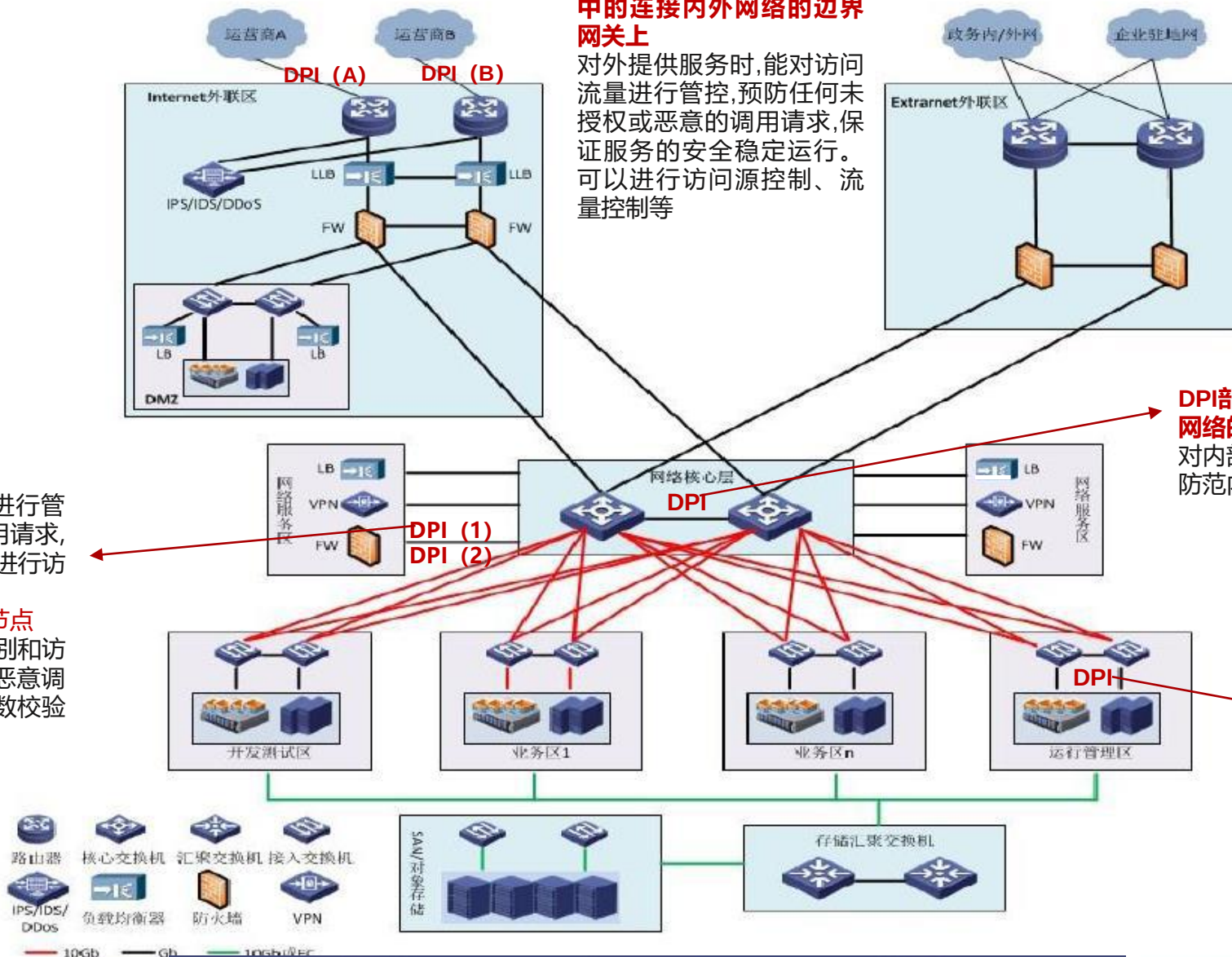
对外提供服务时,能对访问流量进行管控,预防任何未授权或恶意的调用请求,保证服务的安全稳定运行。可以进行访问源控制、流量控制等

• 开放的模型API接口的网关节点

进行细粒度的流量过滤、风险识别和访问策略控制。防止API被滥用或恶意调用。DPI可以进行用户识别、参数校验等

DPI部署在Internet外联区中的连接内外网络的边界网关上

对外提供服务时,能对访问流量进行管控,预防任何未授权或恶意的调用请求,保证服务的安全稳定运行。可以进行访问源控制、流量控制等



DPI部署在网络服务区中的内部网络的核心区域关键节点

对内部重要流量进行双重监控,防范内部威胁,遏制并发现问题

DPI部署在运行管理区中的安全运维系统节点

DPI的监控日志能和IDS、防火墙等其他系统互联,进行综合分析和联动response,提高整体安全水平

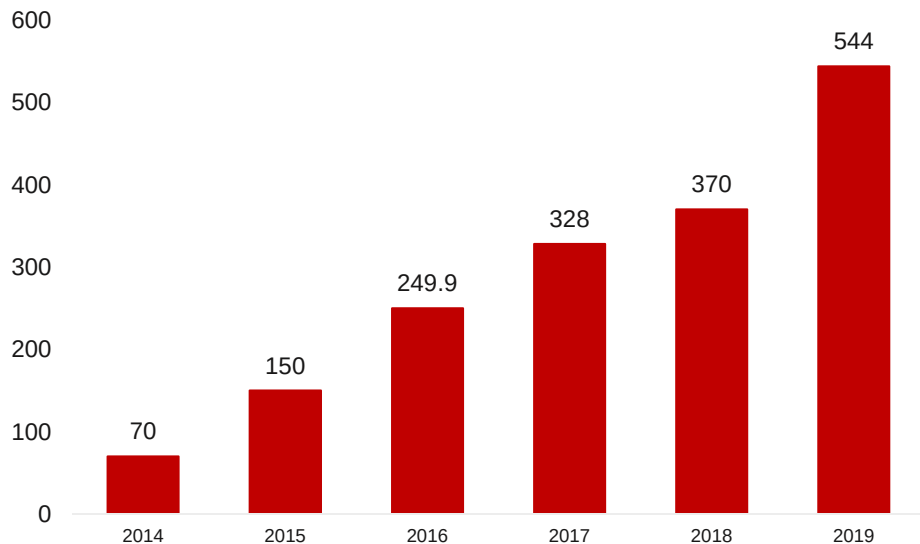
03

**市场空间：
伴随5G商用推广，新一轮建设周期可期**

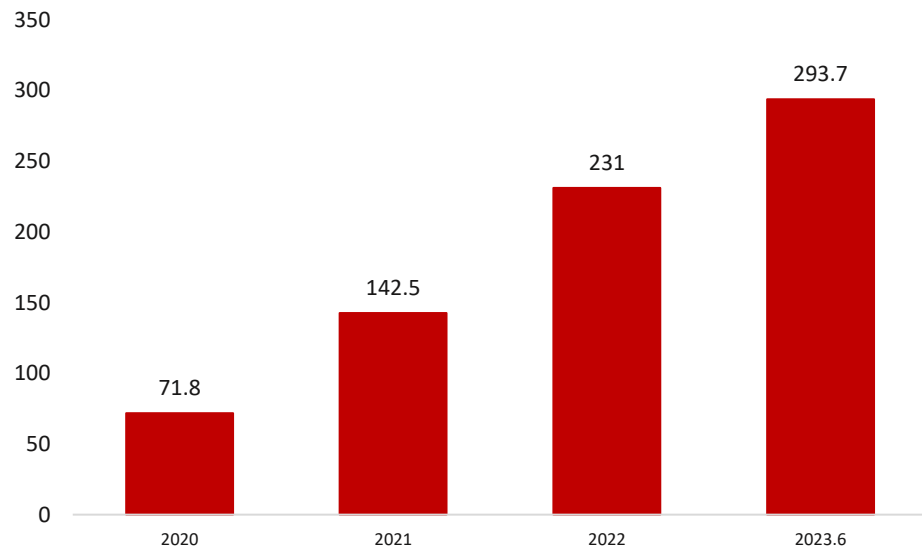
我国移动互联网基础建设已初具规模，较高的5G覆盖率为大模型的普及和应用打下了坚实基础：

- **5G网络建设全球领先**5G网络规模为全球第一。截至2023年6月底，我国5G基站累计达到293.7万个，覆盖所有地级市城区、县城城区，覆盖广度、深度持续拓展；5G共建共享基站超173万个，启动全球首个5G异网漫游试商用，5G网络加快向集约高效、绿色低碳发展。
- **蜂窝物联网终端用户实现“物超人”**。2022年，我国蜂窝物联网用户首次超过移动电话用户数，开启万物互联的新篇章。
- **IPv6网络“高速公路”全面建成**。截至2022年底，我国IPv6地址数量为64318/32，占全球16.48%。

图：我国4G基站个数（单位：万个）



图：我国5G基站个数（单位：万个）

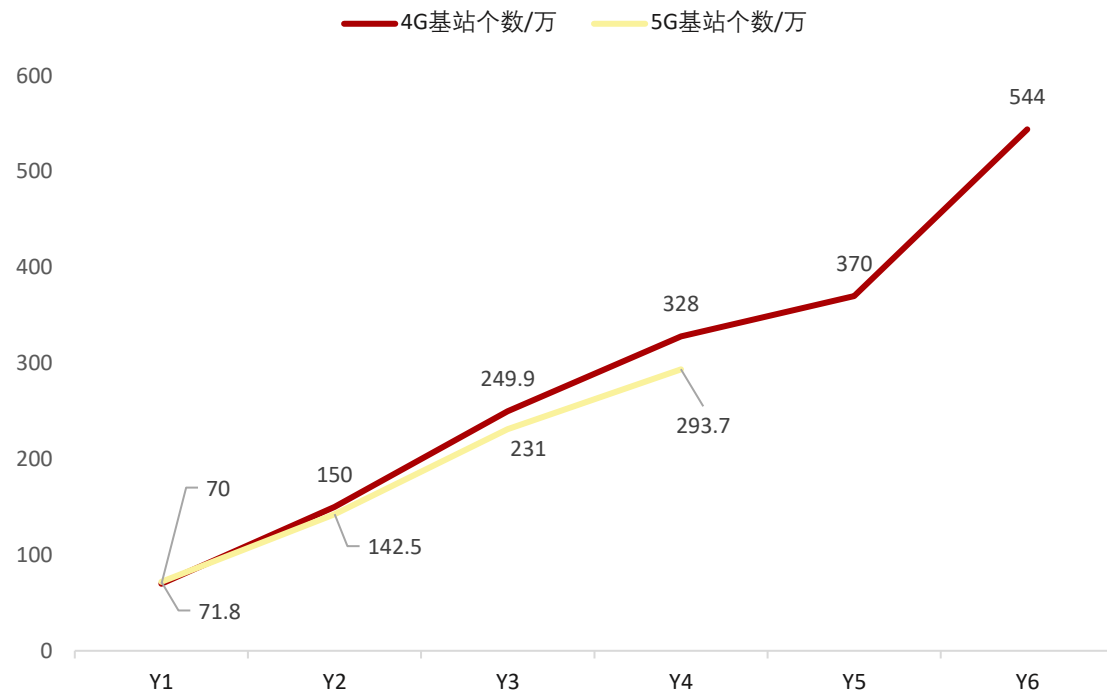


随着我国大力发展5G技术，推进5G基站建设，5G基站年均增长速率约为85万个/年，年均增长率为118%，5G商用推进进展良好。参考中国4G基站建设的节奏，未来中国5G基站数量仍呈快速上涨趋势，大模型的广泛应用有望进一步促进5G基础设施建设和普及：

一方面，随着大型模型应用与交互的不断增加，促进5G流量在商用推进过程中的持续增长，5G网络有望迎来新一轮建设周期。大型语言模型的广泛应用对5G流量的增长或起到一定推动作用，如ChatGPT、文心一言、讯飞星火、360智脑等模型需要频繁的与用户交互，生成大量的数据流量。同时一些图片和视频生成模型也产生了大量的图像和视频流量，这些应用对高速、低延迟的5G网络提出了更高的要求，推动了5G流量的快速增长。

另一方面，4G网络基站数量在建设的第5-6年迎来快速增长，对比之下，我们认为5G基站的部署数量有望迎来快速建设期，以满足大型模型以及各类网络应用对高速稳定连接的需求，从而进一步激发网络可视化的建设。

图：我国4G基站数量和5G基站数量增长趋势对比（单位：万个）



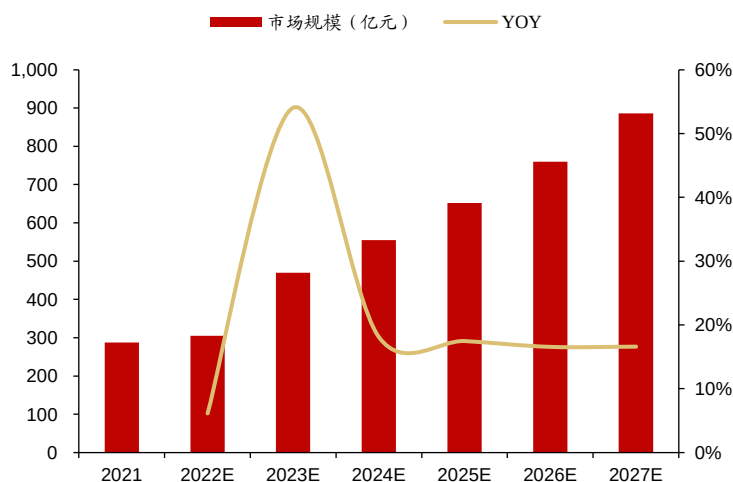
注释：1) 我们分别以4G、5G网络建设的初始年份为Y1，其后的年份逐年递推依次为Y2-Y6年，如4G网络对应的Y1年对应2014年、Y6年对应2019年，5G网络对应的Y1年为2020年、Y4年对应2023年；2) 5G网络的Y4年对应基站数量为截至2023年6月底数据

根据华经产业研究院数据，2022年中国网络可视化行业市场规模约为305.1亿元，同比增长6.14%，预计2027年市场规模达到886.17亿元，**对应2022-2027年CAGR为24%**，显著快于三大运营商2018-2022年间的资本开支增速，我们认为可能的原因有：

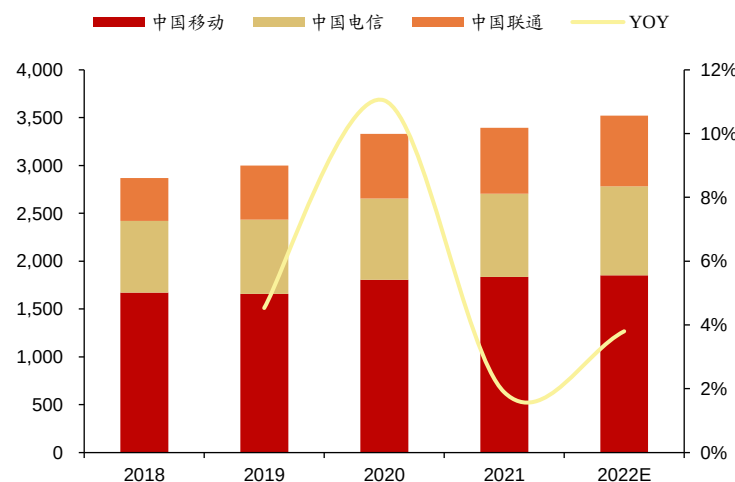
- 5G建设有望迎来高峰期，大模型的应用进一步带来网络流量的增加，从而加速网络可视化市场的建设
- 大模型的安全防护和监管需求加速网络可视化在政府和企业侧市场渗透率的提升

从产业结构来看，根据华经产业研究院对2016-2022年前、后端收入的统计，**网络可视化前端市场规模占比约20%，后端市场规模占比约80%**；且呈现出前端业务逐步向后端渗透，后端应用领域快速拓展的产业发展趋势。

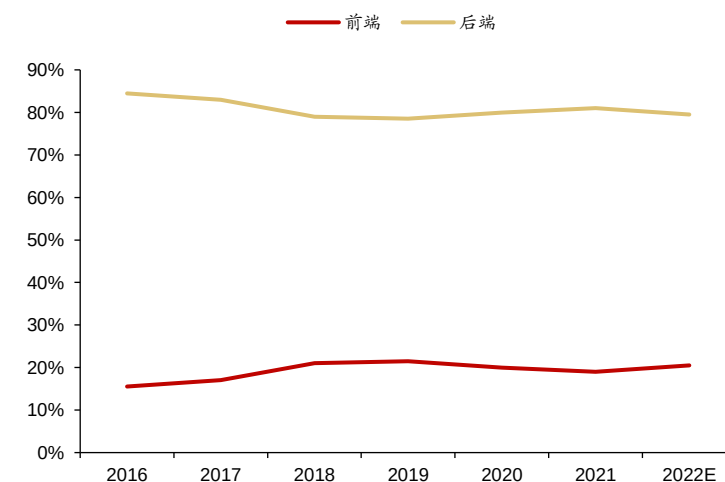
图：网络可视化市场规模（单位：亿元）



图：三大运营商资本开支（单位：亿元）



图：网络可视化前端与后端收入占比



04

相关标的梳理

浩瀚深度成立于1994年，是**互联网流量和数据智能化的领航者**。公司依托“**以采集管理系统为基础，全方位拓展延伸**”的业务发展模式，即依靠前端采集的布局优势，不断开发各类后端应用产品，长期为运营商等客户提供全方位、高性能、跨平台的网络智能化及信息安全防护解决方案、网络安全防护解决方案。

针对网络可视化需求，公司在**前端采集和后端应用层面均有产品储备**：**前端方面**，公司现有包括“硬件DPI系统”、“软件DPI系统”、“嵌入式DPI引擎”在内的**智能采集管理系统**；**后端方面**，公司现有“数据合成和内容还原系统”、“网络深度可视化分析系统”等多款应用产品组成的**智能化应用系统**，能够实现客户不同应用场景和应用目标下的各类需求。

图：浩瀚深度硬件DPI系统架构



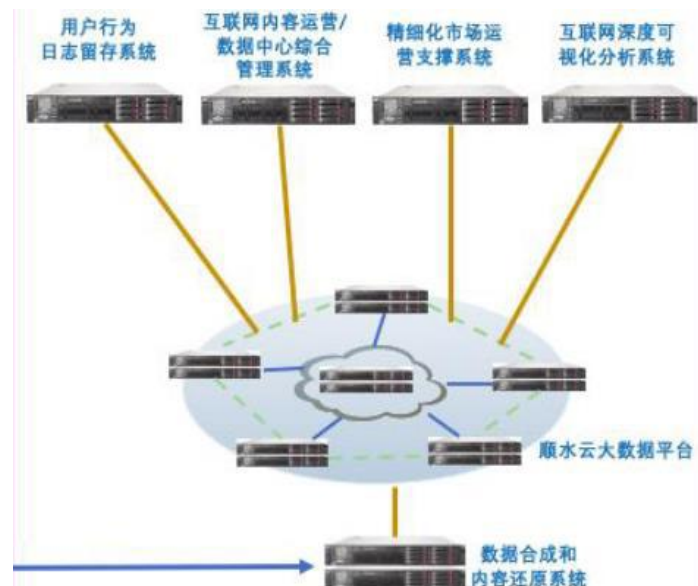
图：浩瀚深度软件DPI系统架构



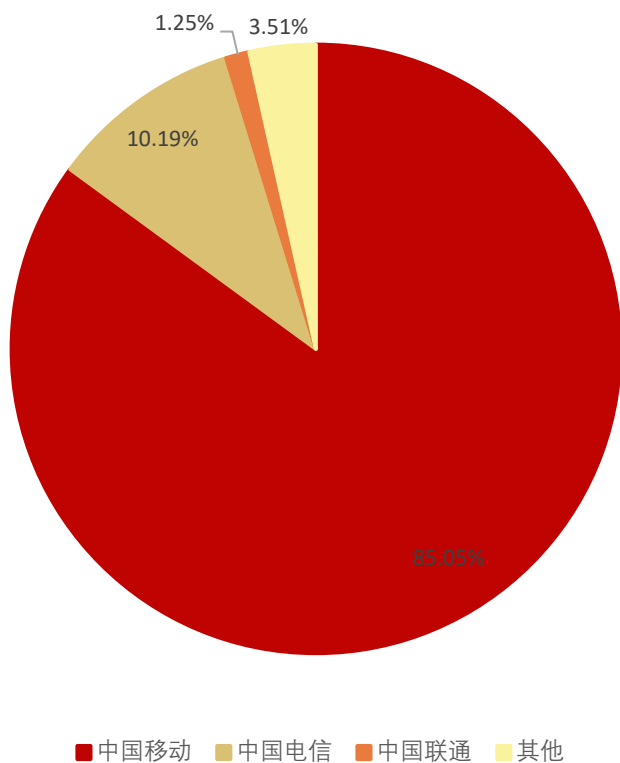
图：浩瀚深度嵌入式DPI引擎架构



图：浩瀚深度智能化应用系统



图：浩瀚深度主要客户占营业收入比重（2021年数据）



表：浩瀚深度2020至2022年财务数据摘要

		2022	2021	2020
营业收入 (亿元)	营业总收入	4.49	4.10	3.67
	网络可视化解决方案	2.51	2.49	2.53
	YOY	0.77%	/	-6.76%
	大数据解决方案	0.43	0.31	备注：网络智能化产品=网络可视化+大数据
	YOY	38.17%	/	
	信息安全防护解决方案	1.09	0.99	0.91
	YOY	9.66%	9.24%	32.77%
	其他产品	0.46	0.30	0.23
	YOY	53.43%	28.81%	47.80%
毛利率	综合毛利率	47.39%	52.98%	50.59%
	网络可视化解决方案	45.12%	52.79%	50.45%
	大数据解决方案	84.28%	80.57%	
	信息安全防护解决方案	51.70%	59.22%	60.36%
	其他产品	14.75%	4.97%	14.58%
归母净利润		0.48	0.58	0.53
YOY		-18.74%	9.55%	48.32%
净利率		10.57%	14.27%	14.55%

中新赛克成立于2003年，致力于通信网络和信息网络的智能管理和安全防护，为全球客户提供快速、满意的定制化服务和解决方案，帮助政府、运营商、行业客户维护信息安全、拓展经营。公司是**国内领先的网络可视化基础架构产品提供商之一**，自成立之初就专注于**网络可视化基础架构产品及其在信息安全领域的应用**。

公司为**网络可视化前端龙头**，现有**宽带网产品**和**移动网产品**：宽带网产品又称网络分流器，负责固网原始数据获取、分层解析、按需筛选、快速移交，可细分为机架式、盒式和加速卡；移动网产品专门用于移动网流量分析领域，支持2G/3G/4G/5G制式，可细分为集中式、固定式和移动式。后端应用方面，公司**聚焦信息安全领域**，发布网络内容安全大数据分析平台、OceanMind数据中台等产品。

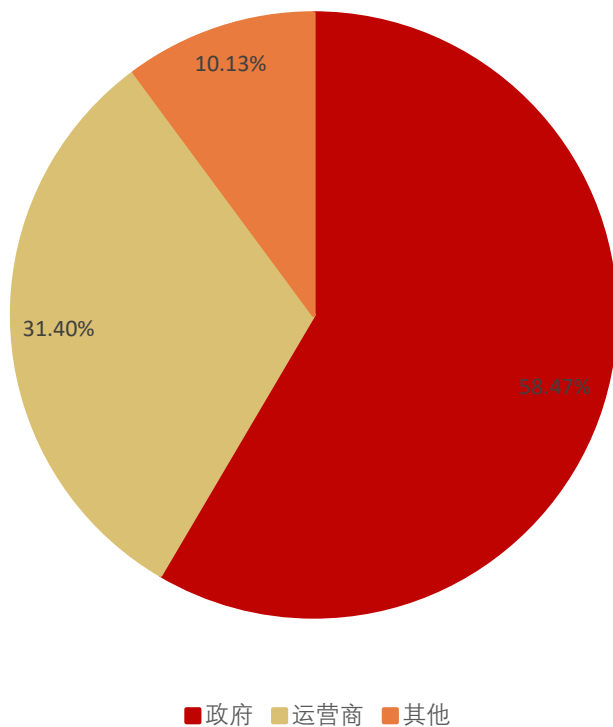
表：中新赛克网络可视化基础架构产品

产品类别	产品名称	产品形态
宽带网产品	机架式	
	盒式	
	加速卡	
移动网产品	集中式	
	固定式	
	移动式	

图：中新赛克网络内容安全大数据分析平台



图：中新赛克主要客户占营业收入比重（2022年数据）



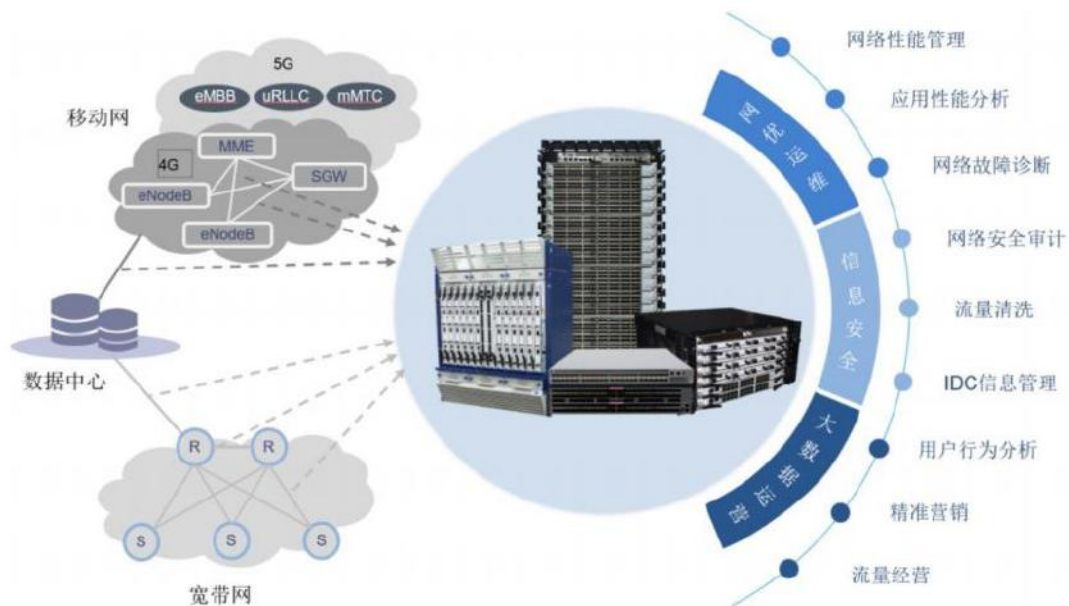
表：中新赛克2020至2022年财务数据摘要

		2022	2021	2020
营业收入	营业总收入	4.36	6.94	9.54
	宽带网产品	1.69	2.60	4.71
	YOY	-35.01%	-44.69%	-17.34%
	移动网产品	0.93	1.85	1.59
	YOY	-49.85%	15.86%	5.90%
	网络内容安全产品	0.49	0.55	1.08
	YOY	-10.93%	-95.95%	15.10%
	其他	1.25	1.94	2.16
毛利率	YOY	-35.58%	-10.21%	138.69%
	综合毛利率	47.39%	52.98%	50.59%
	宽带网产品	85.51%	84.74%	86.20%
	移动网产品	61.91%	69.29%	71.70%
	网络内容安全产品	73.05%	79.85%	79.00%
归母净利润	其他	40.29%	44.28%	56.39%
	归母净利润	-1.22	0.56	2.48
	YOY	-316.93%	-77.29%	-16.04%
净利率		-28.01%	8.11%	25.97%

恒为科技成立于2003年，是国内优秀的网络可视化及智能系统平台提供商，致力于为运营商网络、企业与行业IT、工业互联网和智慧物联网等领域提供业界先进的产品和解决方案。公司是**国内最早进入网络可视化领域的厂商之一**，是国内此领域中技术概念与产品的**创新者和推动者**。

公司的网络可视化业务中，现有**插卡式网络可视化平台**和**盒式网络可视化平台**：**插卡式网络可视化平台**支持流量汇聚、提供规则匹配、支持负载均衡、提供输出流量复制，有OptiWay和OptiPlus两类产品可供选择；**盒式网络可视化平台**的端口可以灵活配置为输入和输出接口、支持设备数据包封装、支持数据包修改功能、适用于移动核心网络流量。可细分为ExProbe8000系列产品和ExProbe7000系列产品。

图：恒为科技网络可视化应用系统示意图



图：恒为科技盒式网络可视化平台产品



表：恒为科技2020至2022年财务数据摘要

		2022	2021	2020
营业收入 (亿元)	营业总收入	7.71	6.78	5.33
	网络可视化	4.13	3.19	2.93
	YOY	29.45%	8.96%	-7.00%
	智能系统平台	3.46	3.37	2.26
	YOY	2.74%	48.82%	96.98%
	其他主营业务	0.10	0.21	0.13
	YOY	-50.76%	57.39%	266.75%
	其他非主营业务	0.01	0.02	0.01
	YOY	-21.49%	105.86%	9.29%
毛利率	综合毛利率	43.03%	35.62%	39.01%
	网络可视化	56.03%	49.88%	55.56%
	智能系统平台	27.95%	21.62%	18.44%
	其他主营业务	22.32%	40.19%	22.78%
	其他非主营业务	86.30%	76.76%	60.80%
归母净利润 (亿元)		0.76	0.53	0.36
YOY		42.63%	46.83%	-45.95%
归母净利率		9.89%	7.88%	6.83%

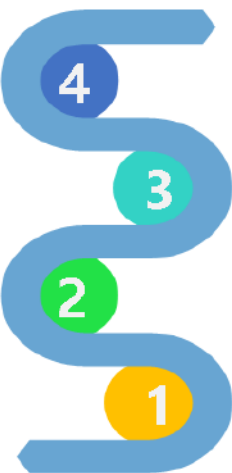
任子行成立于2000年，业务涵盖网络信息安全、信息安全、公共安全、网络资源安全、工业互联网安全等众多领域，是**国内技术最为全面的大规模网络安全防护解决方案提供商、国内领先的“网络空间数据治理专家”**；主要客户为企事业单位、医疗、教育、金融、运营商等客户。

公司自主研发的**僵木蠕监测系统**面向城域网等大流量、大规模网络场景，通过**采集、处理和分析**，以**可视化的方式实现僵木蠕等安全威胁的报告及相应**，为客户提供切实有效的安全运维和管理手段支撑；**移动恶意程序监测系统**提供**网络流量分析和还原能力**，具备多引擎细粒度的移动恶意程序威胁的检测和分析能力，能够实现对安全日志和程序样本的统一接收、存储和检测，同时可与平台、省属地化管理平台规范化对接；**运营商网络安全态势感知平台**能够**收集运营商流量数据、资产数据等信息**，通过统计分析、数据挖掘等方法实现网络安全要素的**全面态势感知和告警**，提升运营商的安全风险应对能力。

表：任子行僵木蠕监测系统产品功能

➢ 报告及响应
针对检测到的僵木蠕事件，及时通知安全管理员

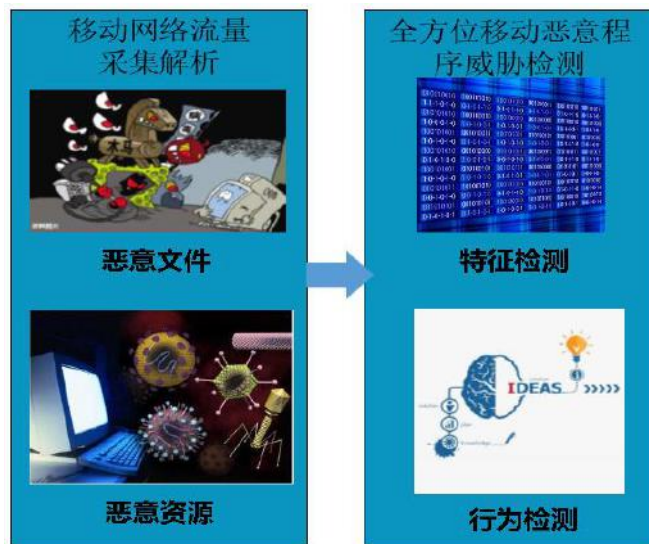
➢ 处理及过滤
对数据包进行解析并转换为后续阶段可识别的数据



➢ 分析及检测
判断数据中是否含有僵尸网络行为和木马、蠕虫内容

➢ 数据采集
旁路方式采集用户网络环境中的所有数据包

表：任子行移动恶意程序监测系统产品功能



图：任子行运营商网络安全态势感知平台产品功能



表：任子行2020至2022年财务数据摘要

		2022	2021	2020
营业收入 (亿元)	营业总收入	7.30	6.50	8.38
	网络安全	3.36	2.45	3.89
	YOY	37.09%	-36.98%	-1.67%
	网资管理	3.87	3.86	3.31
	YOY	13.39%	16.73%	1.31%
	文化娱乐	0.00	0.58	1.54
	YOY	-100.00%	-62.27%	-42.65%
	其他业务	0.06	0.06	0.04
	YOY	10.70%	46.04%	-28.84%
毛利率	综合毛利率	54.93%	51.32%	46.63%
	网络安全	54.93%	45.54%	33.43%
	网资管理	54.70%	55.34%	62.42%
	文化娱乐	0.00%	68.57%	51.02%
	其他业务	69.85%	66.63%	58.74%
归母净利润 (亿元)		-0.01	-0.74	0.06
YOY		98.64%	-1405.84%	105.57%
归母净利率		-0.14%	-11.33%	0.67%

注释：参考公司更正后财务数据

恒安嘉新专注于通信网和互联网数据智能分析领域，为政企客户提供新一代网络信息安全、数据分析、智能业务应用解决方案和“管家式”运营运维服务。公司产品遍布全国 31 个省，支撑工信等网络安全主管部门、电信运营商在骨干网、城域网、移动互联网、工业物联网、企业网的数千个节点部署了 NTA “网络摄像头”，提供全天候、全方位的大数据智能分析产品和服务。

公司流量分析产品覆盖采集、分析、认知、决策的全链条智能体系，助力网络空间治理：**通信网领域**，推出通信网基础数据采集产品（电信级 DPI&NTA 设备、NPB - 电信级流量汇聚分流设备、4/5G 信令安全及网络质量平台等）、移动互联网恶意程序治理产品、互联网僵尸木马蠕虫治理产品等；**企业网安全监测领域**，推出数据安全采集产品，实现全流量安全监测回溯；**关键信息基础设施领域**，推出IDC/CDN/DNS/云信安治理产品，对流量进行实时监控，违法违规信息进行有效阻断。

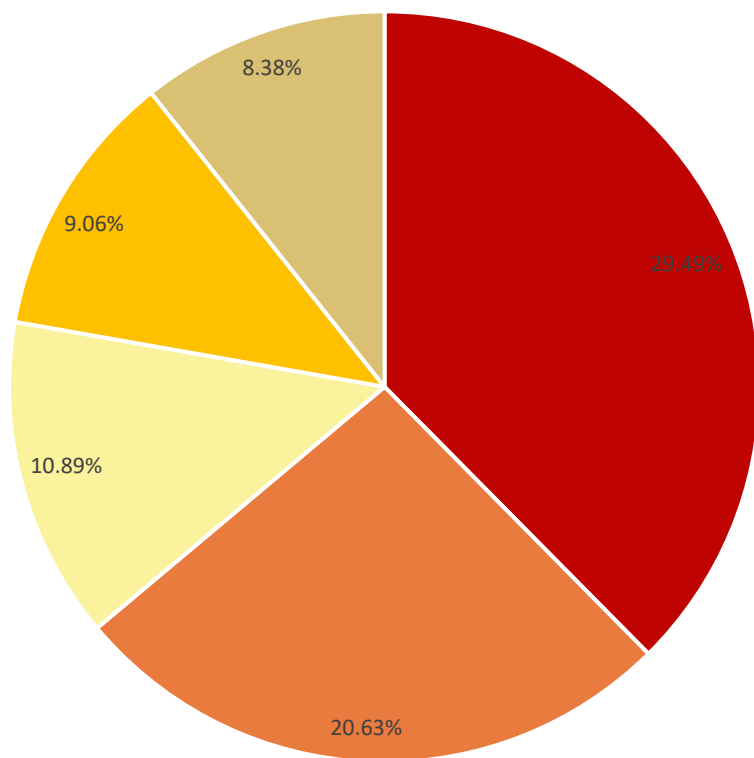
图：IDC/CDN/DNS/云信安治理产品



图：移动互联网恶意程序治理程序



图：恒安嘉新主要客户占营业收入比重（2018年数据）



■ 中国联通 ■ 中国电信 ■ 中国移动 ■ 工信部及下属单位 ■ 网信办及下属单位

资料来源：恒安嘉新招股书、浙商证券研究所

图：恒安嘉新2018年财务数据摘要

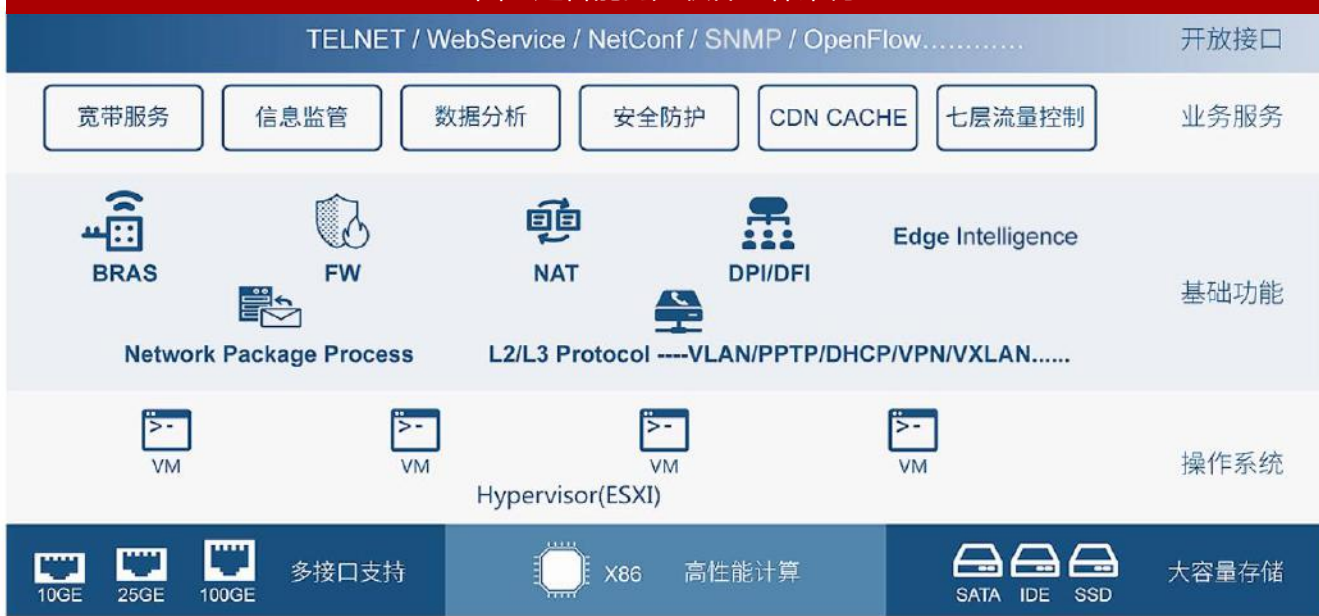
		2018
营业收入（亿元）	营业总收入	4.88
	解决方案	3.75
	YOY	-6.26%
	技术服务	0.40
	YOY	-27.50%
	技术开发	0.60
	YOY	135.77%
	增值服务	0.13
	YOY	-15.68%
毛利率	综合毛利率	50.47%
	解决方案	44.06%
	技术服务	57.64%
	技术开发	81.06%
	增值服务	72.95%
归母净利润（亿元）		0.18
YOY		-56.11%
归母净利率		3.76%

注释：由于公司未上市，根据公开资料目前只能查阅到公司2018年利润表数据

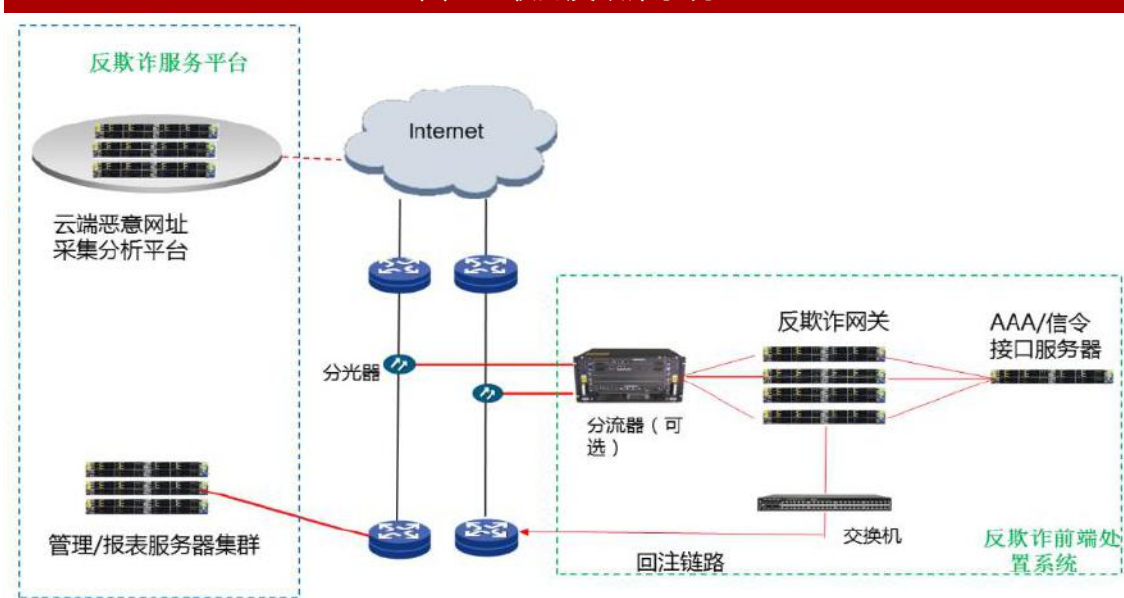
武汉绿色网络信息服务有限责任公司专注于DPI（深度报文检测）、大数据、网络信息安全、边缘智能等领域，为运营商及其他政企客户提供电信级应用层网络设备解决方案。产品覆盖光纤宽带网络、移动网络、VoLTE和物联网。绿色网络**专注于产品研发与质量管理，已通过ISO标准认证和CMM15级软件管理认证，深度参与多项国家行业标准的制定，相关标准直接引领行业创新发展，并获得大规模商业部署应用。**

公司面向5G、SDN/NFV，以及多接入边缘计算与固移合等大趋势，公司的新产品**超智能网元(SINE)**，在宽带接入BRAS上实现了多功能合，具备边缘计算、存储DPI等功能。产品平台基于通用的X86架构，为运营商提供部署简单、扩展灵活、更低成本、更高效率的网络解决方案。

图：超智能网元软件总体架构



图：互联网反欺诈系统



北京安博通科技股份有限公司起步于2011年，以“看透安全，体验价值”理念为核心，是可视化网络安全专用核心系统产品与安全服务提供商。其自主研发的ABT SPOS可视化网络安全系统平台，已成为众多一线厂商与大型解决方案集成商广泛搭载的网络安全系统套件，是国内众多部委与央企安全态势感知平台的核心组件与数据引擎。

公司自主研发的墨影网络节点资源管理平台能够自动发现全网的网络设备状态、互联链路信息及相互关联关系，可与第三方网管平台和CMDB集成，实现网络拓扑和数字资产的可视化管理。同时提供合规检查、网络监控等功能，协助运维人员实时监控配置变更、快速整改配置风险、缩小资产对外暴露面、迅速定位网络故障，从而大幅提升安全运维和故障排查的效率。

图：“墨影”功能特性图

自动发现

- 多协议不间断自动发现网络中的资源节点
- 自动识别节点间的链路信息。
- 节点自动分组分层管理。

合规检查

- 资源节点配置合规性检查，支持多品牌、多类型。
- 预置丰富的合规规则并支持自定义维护规则，满足不同要求下的配置合规。
- 提供合规所需的处置建议，周期性检查合规情况。



立体呈现

- 自动绘制全网网络拓扑。
- 自动标识链路详情。
- 分级分层管理网络拓扑。

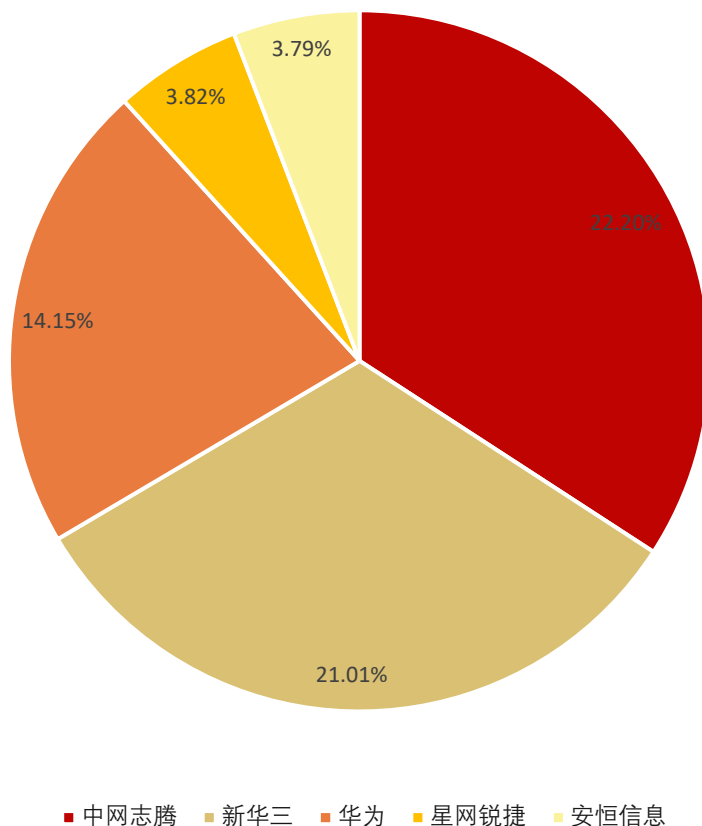
持续监测

- 实时监控节点状态变更，及时发现设备上、下线及链路变化情况。
- 动态监测节点配置变更情况，多维度分析节点暴露面和脆弱性。
- 集中展示告警信息，精准定位告警位置。

图：“墨影”网络资源智能化管理平台



图：安博通主要客户占营业收入比重（2019年上半年数据）



表：安博通2020-2022年财务数据摘要

		2022	2021	2020
营业收入 (亿元)	营业总收入	4.56	3.91	2.63
	安全网关	3.23	3.08	2.09
	YOY	4.87%	47.89%	12.17%
	安全管理	1.00	0.61	0.40
	YOY	63.62%	55.16%	-15.34%
	安全服务	0.31	0.22	0.09
毛利率	YOY	44.60%	151.12%	10.95%
	综合毛利率	55.91%	60.52%	63.49%
	安全网关	44.96%	51.55%	57.85%
	安全管理	86.24%	94.09%	98.87%
归母净利润 (亿元)	安全服务	71.95%	93.43%	78.76%
YOY		-0.08	0.72	0.44
		-111.72%	62.33%	-39.72%
归母净利率		-1.85%	18.44%	16.92%

注释：参考公司更正后财务数据

美亚柏科是国内领先的电子数据取证行业龙头和公安大数据领先企业、网络空间安全和社会治理领域国家队，以自主研发的乾坤大数据操作系统为技术基座，布局“电子数据取证、公共安全大数据、新网络空间安全、数字政务与企业数字化”四大业务板块，为公检法、政府机关和企事业单位提供一站式综合解决方案，业务范围覆盖全国各省、市、自治区及部分“一带一路”沿线国家。

公司的乾坤大数据操作系统（QKOS），围绕“采、治、学、管、用”，实现资源的全生命周期管控，可为网络可视化后端分析与应用提供支撑。围绕乾坤大数据操作系统，公司可为大数据分析提供两大基础能力（“天基”大数据治理平台、“天河”大数据服务平台）以及六个能力中台（“天算”大数据建模平台、“天界”可视化研判工作台、“天匠”大数据标签平台、“天智”大数据知识平台、“天擎”AI能力一体化平台、“揽月”可视化构建平台）。

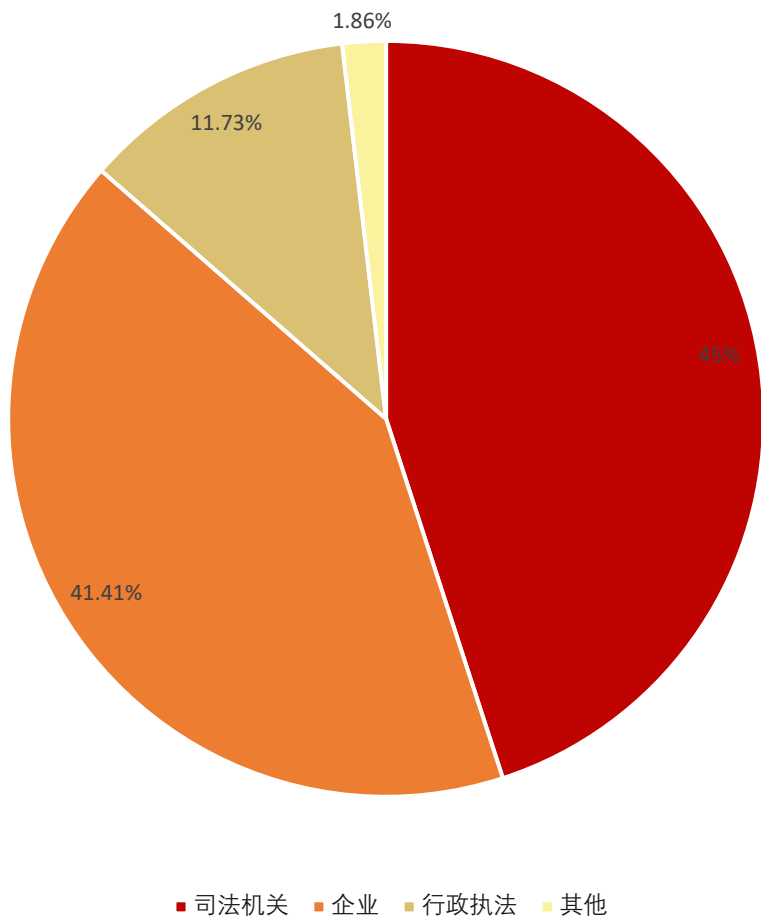
图：“九天揽月”大数据产品体系



图：“九天揽月”体系架构图



图：美亚柏科主要客户占营业收入比重（2022年数据）



表：美亚柏科2022年财务数据摘要

		2022
营业收入（亿元）	营业总收入	2.28
	公共安全大数据	9.38
	YOY	-6.26%
	电子数据取证	8.25
	YOY	-27.50%
	新型智慧城市	2.84
	YOY	135.77%
	新网络安全	2.33
毛利率	YOY	-15.68%
	综合毛利率	52.24%
	公共安全大数据	46.11%
	电子数据取证	66.60%
	新型智慧城市	30.40%
归母净利润（亿元）	新网络安全	52.63%
归母净利润（亿元）		1.48
YOY		-52.41%
归母净利率		6.49%

05

风险提示

- 1、网络可视化监管以及相关产品落地不及预期
- 2、报告中对市场空间的预计主要参考第三方机构假设数据
- 3、报告中对相关标的公司的梳理为基于公开信息的不完全统计
- 4、由AI安全需求带来的市场竞争加剧
- 5、板块政策发生重大变化

行业的投资评级

以报告日后的6个月内，行业指数相对于沪深300指数的涨跌幅为标准，定义如下：

- 1、看好：行业指数相对于沪深300指数表现 + 10%以上；
- 2、中性：行业指数相对于沪深300指数表现 - 10% ~ + 10%以上；
- 3、看淡：行业指数相对于沪深300指数表现 - 10%以下。

我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重。

建议：投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者不应仅仅依靠投资评级来推断结论

法律声明及风险提示

本报告由浙商证券股份有限公司（已具备中国证监会批复的证券投资咨询业务资格，经营许可证编号为：Z39833000）制作。本报告中的信息均来源于我们认为可靠的已公开资料，但浙商证券股份有限公司及其关联机构（以下统称“本公司”）对这些信息的真实性、准确性及完整性不作任何保证，也不保证所包含的信息和建议不发生任何变更。本公司没有将变更的信息和建议向报告所有接收者进行更新的义务。

本公司的客户作参考之用。本公司不会因接收人收到本报告而视其为本公司的当然客户。

本报告仅反映报告作者的出具日的观点和判断，在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求。对依据或者使用本报告所造成的一切后果，本公司及/或其关联人员均不承担任何法律责任。

本公司的交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。本公司没有将此意见及建议向报告所有接收者进行更新的义务。本公司的资产管理公司、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告版权均归本公司所有，未经本公司事先书面授权，任何机构或个人不得以任何形式复制、发布、传播本报告的全部或部分内容。经授权刊载、转发本报告或者摘要的，应当注明本报告发布人和发布日期，并提示使用本报告的风险。未经授权或未按要求刊载、转发本报告的，应当承担相应的法律责任。本公司将保留向其追究法律责任的权利。

浙商证券研究所

上海总部地址：杨高南路729号陆家嘴世纪金融广场1号楼25层

北京地址：北京市东城区朝阳门北大街8号富华大厦E座4层

深圳地址：广东省深圳市福田区广电金融中心33层

邮政编码：200127

电话：(8621)80108518

传真：(8621)80106010

浙商证券研究所：<http://research.stocke.com.cn>