

2024年中国云安全行业概览

打破“云威胁”阴霾，筑牢安全“生命线”

企业标签：奇安信、绿盟科技、深信服

China Cloud Security Industry

中国クラウドセキュリティ産業

撰写人：林若薇

报告提供的任何内容（包括但不限于数据、文本、图表、图像等）均系头豹研究院独有的高度机密性文件（在报告中另行标明出处者除外）。未经头豹研究院事先书面许可，任何人不得以任何方式擅自复制、再造、传播、出版、引用、改编、汇编本报告内容，若有违反上述约定的行为发生，头豹研究院保留采取法律措施、追究相关人员责任的权利。头豹研究院开展的所有商业活动均使用“头豹研究院”或“头豹”的商号、商标，头豹研究院无任何前述名称之外的其他分支机构，也未授权或聘用其他任何第三方代表头豹研究院开展商业活动。

团队介绍

头豹是国内领先的行企研究原创内容平台和创新的数字化研究服务提供商。头豹在中国已布局3大研究院，拥有近百名资深分析师，头豹科创网(www.leadleo.com)拥有20万+注册用户，6,000+行业赛道覆盖及相关研究报告产出。

头豹打造了一系列产品及解决方案，包括数据库服务、行企研报服务、微估值及微尽调自动化产品、财务顾问服务、PR及IR服务，研究课程，以及分析师培训等。诚挚欢迎各界精英与头豹交流合作，请即通过邮件或来电咨询。

报告作者



袁栩聪
首席分析师
oliver.yuan@Leadleo.com



林若薇
行业分析师
ruwei.lin@leadleo.com

头豹研究院

咨询/合作

网址：www.leadleo.com

电话：15999806788（袁先生）

电话：18916233114（李先生）

深圳市华润置地大厦E座4105室

摘要

随着云计算的广泛应用，云安全工具逐渐崭露头角，头部云厂商也逐步将安全防护服务云化。当前，云安全市场规模已达到171亿元，并预计在2027年将迎来更为显著的增长，达到979亿元。产业链上游主要涵盖硬件和软件供应商，其中行业标准的制定、技术的不断发展以及构建生态系统成为发展的关键要点。云安全行业的细分市场分析表明，中小企业更倾向于使用公有云服务，而大型企业则更注重数据安全，倾向于选择私有云或混合云模式。商业模式上，云安全厂商主要采用订阅、授权和定制等多样化商业模式。在各行各业中，云安全在身份与访问控制、基础架构防护、监控与检测以及合规审计等场景中的应用渗透率均超过50%。目前，云安全行业仍面临一些制约因素，包括技术创新、性能扩展性、可扩展性、合规性以及人才培养等挑战，预计在未来3-5年内，中国云安全将努力迎头赶超国际水平。发展趋势上，技术升级、零信任和云原生等方向将主导行业，同时云安全行业也将朝向C端市场拓展，更好地满足合规需求。

- 2022年中国云安全市场规模达到171亿元，预计到2027年将进一步扩大至979亿元。云原生、人工智能、物联网等技术的不断推进，将引发更多细分安全场景的需求

中国云安全市场在2022年达到了171亿元的规模，同比增长41.72%。这一迅猛增长受到多方面因素的推动。首先，中国数据安全法规不断完善，为市场提供了引导和规范。其次，企业对云安全的需求进入高峰期，工业设备上云率提升至17.7%，企业业务上云普及率为41.4%。随着云原生技术的成熟和安全架构升级，以及客户安全意识的提高，云安全市场需求有望持续释放。预计到2027年，市场规模将达到979亿元，复合增速为42%。

- 在云安全领域，身份与访问控制、基础架构防护、监控与检测以及合规审计等方面应用渗透率均超50%。其中，身份与访问控制达95%，基础架构防护为80%，监控与检测为70%，合规审计为60%

在云安全应用场景中，身份与访问控制、基础架构防护、监控与检测和合规审计等方面的应用渗透率均较高，均超50%。身份与访问控制场景中，应用渗透率高达95%，体现了在云计算环境确保授权访问的关键性。基础架构防护场景中，应用渗透率为80%，强调了在云基础架构各组件上全面覆盖防护的重要性。监控与检测场景中，应用渗透率达70%，符合云安全零信任模型对验证和监控的高要求。在合规审计场景中，云安全同样具有高应用渗透率，为60%，强调了对符合法规的数据处理和存储进行审计的重要性。

内容目录

1 云安全行业综述 05页

- 定义
- 发展历程
- 架构体系
- 市场规模

2 云安全产业链分析 10页

- 产业链图谱
- 产业链上游—发展概述
- 产业链中游--细分市场分析
- 产业链中游--商业模式
- 产业链下游--行业场景
- 产业链下游--业务场景

3 云安全行业分析 18页

- 政策分析
- 制约因素
- 发展趋势
- 竞争格局

4 云安全典型厂商分析 23页

- 奇安信
- 绿盟科技
- 深信服

研究目标

研究目的

了解云安全的技术演变、预测市场规模、探析产业链生态图谱，洞察厂商商业模式并探析云安全行业、业务场景以判断行业发展趋势。

研究目标

- 了解中国云安全的背景、定义、演变
- 预测中国云安全市场规模
- 探析中国云安全行业产业链情况
- 分析中国云安全的行业、业务应用场景
- 预判中国云安全行业发展态势

本报告的关键问题

- 中国云安全行业市场规模情况如何？未来增长情况如何？
- 竞争格局：中国打造云安全的企业有哪些？哪些企业更具备发展潜力与优势？
- 发展趋势：中国云安全发展面临哪些机遇与挑战？发展驱动力有哪些？

名词解释

- ◆ **零信任网络访问 (ZTNA)**：是一种网络安全模型，它基于一个简单的理念：不信任任何人或设备，即使它们在组织的网络内。零信任模型认为内部和外部都可能存在威胁，因此每个用户、设备或应用程序都应该在其尝试访问网络资源时进行身份验证和授权。
- ◆ **云原生应用保护平台 (CNAPP)**：云原生应用保护平台是指一类工具和服务，旨在为基于云原生架构构建的应用程序提供全面的安全性、可观测性和治理支持。
- ◆ **安全访问服务边缘 (SASE)**：是一种网络安全架构，旨在提供强大、综合的安全性和网络访问服务。SASE 将网络安全与广域网络 (WAN) 服务集成到一个统一的云服务平台上，以便更好地支持分布式、移动的工作方式和云原生应用的需求。
- ◆ **云基础设施权限管理 (CIEM)**：是指在云计算环境中有效管理和控制用户、服务或应用程序对云基础设施资源的访问权限的过程。
- ◆ **云安全态势管理 (CSPM)**：云安全态势管理是一种综合性的安全管理方法，旨在实时监控、分析和应对云环境中的各种安全威胁和事件。
- ◆ **Serverless安全**：Serverless安全是指在Serverless计算架构中实施的一系列安全性措施和最佳实践，以确保Serverless应用程序和其依赖的云服务的安全性。
- ◆ **云工作负载保护平台 (WAAP)**：指的是一类解决方案或平台，用于提供云环境中工作负载的安全性、可视性和治理。云工作负载通常包括在云基础设施上运行的应用程序、服务、虚拟机、容器等。
- ◆ **Web应用程序和API保护 (WAAP)**：Web应用程序和API保护是一组安全措施和最佳实践，旨在确保Web应用程序和API (Application Programming Interface) 在互联网上的安全性，防范各种网络攻击和威胁。
- ◆ **可扩展检测响应平台 (XDR)**：是一种安全性平台，专注于检测和响应网络安全事件。该平台旨在提供一种可扩展性强、适应性好的解决方案，以有效地监控、检测和应对各种安全威胁和攻击。
- ◆ **云数据备份**：云数据备份是指将数据存储于云服务提供商的服务器上，以便在发生数据丢失、损坏、意外删除或其他灾难性事件时，能够迅速还原和恢复数据。
- ◆ **公有云**：指的是云服务提供商向公众开放其计算资源、存储和服务，使用户能够按需访问和使用这些资源。在公有云中，这些计算资源是在互联网上提供的，用户可以通过互联网连接来使用这些资源，而不必在本地拥有或维护物理硬件。
- ◆ **私有云**：与公有云不同，私有云通常在组织的内部数据中心或由第三方提供专用基础设施的环境中部署。私有云提供了云计算的核心特征，如可伸缩性、虚拟化、自助服务等，但其资源和服务仅供特定组织使用。
- ◆ **混合云**：是指将公有云和私有云相结合的云计算环境。在混合云模型中，组织可以同时使用本地数据中心的私有云和公有云服务提供商的云服务，通过这种方式实现资源的灵活共享和管理。

Chapter 1

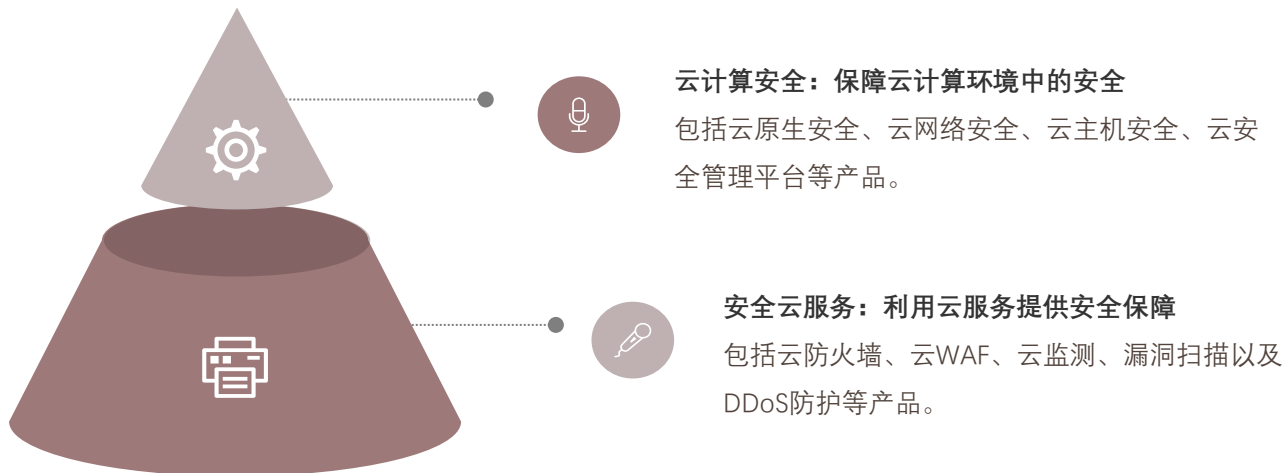
行业综述

- **定义与关键词：**云安全具有“云计算安全”和“安全云服务”等两层含义，而零信任网络访问、云原生应用保护平台、安全访问服务边缘等是云安全2023年的关键词
- **架构体系：**云安全平台架构包括基础设施、能力支撑、安全服务和服务与运营四层
- **发展历程：**2009年被称为中国云计算元年，2015年云计算市场快速发展。随着云计算普及，云安全问题凸显，云安全工具兴起，头部云厂商逐渐实现安全防护服务云化
- **市场规模：**2022年中国云安全市场规模达171亿元，预计2027年将达到979亿元。云原生、人工智能、物联网等技术将推动更多细分安全场景需求

中国云安全行业综述——定义与关键词

- 云安全具有“云计算安全”和“安全云服务”等两层含义，而零信任网络访问、云原生应用保护平台、安全访问服务边缘、云基础设施权限管理、云安全态势管理等是云安全2023年的关键词

中国云安全分类及关键词



- 云安全涵盖云计算环境的数据和网络保护，同时指云服务提供商提供的安全功能。2023年云安全的关键词包括零信任网络访问、云原生应用保护、云安全态势管理

云安全具有两层含义，一个是“云计算安全”，这是指在云计算环境中保护数据和网络不受未经授权的访问、使用、泄露、破坏和干扰的一系列措施，另外一层含义是“安全云服务”，是指利用云服务提供安全能力。例如，云服务提供商可以利用其基础设施提供安全服务，包括防火墙、入侵检测和防御系统、反病毒和恶意软件检测等。当前，以云计算为代表的数字技术正在全面渗透各行业，与此同时，云端威胁的问题成为云计算发展最为关键的保障。2023年，零信任网络访问、云原生应用保护平台、安全访问服务边缘、云基础设施权限管理、云安全态势管理和Serverless安全成为云安全行业的关键词。

来源：专家访谈、头豹研究院

中国云安全行业综述——架构体系

- 云安全平台架构包括基础设施、能力支撑、安全服务和运营平台层。基础设施涵盖底层设备，能力支撑提供关键技术支持，安全服务层核心保护数据和网络，运营平台层关注整体平台运作与管理

云安全管理平台架构



- 云安全平台四层架构：基础设施层涵盖底层设备，能力支撑层提供关键技术支持，安全服务层核心防护数据和网络，运营平台层关注整体运作与管理

云安全管理平台架构模式可分为四个层级，分别为基础设施、能力支撑层、安全服务层和服务与运营平台层。在基础设施层，涉及云计算环境的底层基础设施，包括服务器、网络设备等。能力支撑层则提供了必要的技术支持，包括身份认证、网页防篡改和负载均衡等关键能力，为上层安全服务提供基础支持。安全服务层是云安全管理平台的核心，包括防火墙、入侵检测与防御系统、恶意软件检测等安全服务，旨在保障云计算环境中数据和网络的安全。这一层级的工具和服务致力于防范未经授权的访问、使用、泄露、破坏和干扰。最上层是服务与运营平台层，该层级关注整体的平台运营和管理，包括安全事件监测、日志管理、合规性审计等功能，以确保整个云安全管理平台的高效运作。

来源：新华三、头豹研究院

中国云安全行业综述——发展历程

- 中国云安全行业经历萌芽、起步到发展阶段。2009年被称为中国云计算元年，2015年云计算市场快速发展。随着云计算普及，云安全问题凸显，云安全工具兴起，头部云厂商逐渐实现安全防护服务云化

中国云安全行业的发展历程

发展期（2019-2020年）

云上的安全工具开始大量出现，如云防火墙、云上身份管控和认证、云上终端安全检测等。

高速发展期（2021年-至今）

云平台大面积普及，安全事故频发，行业发展开始进入合法合规的阶段。

起步期（2015-2018年）

云服务应用逐渐广泛，一些企业尝试将云计算技术应用于企业内部系统的建设，安全隐患愈发凸显。

萌芽期（2008-2014年）

在这个阶段中国云行业开始起步，2009年，阿里云正式成立。之后，华为云、腾讯云、百度智能云相继成立。

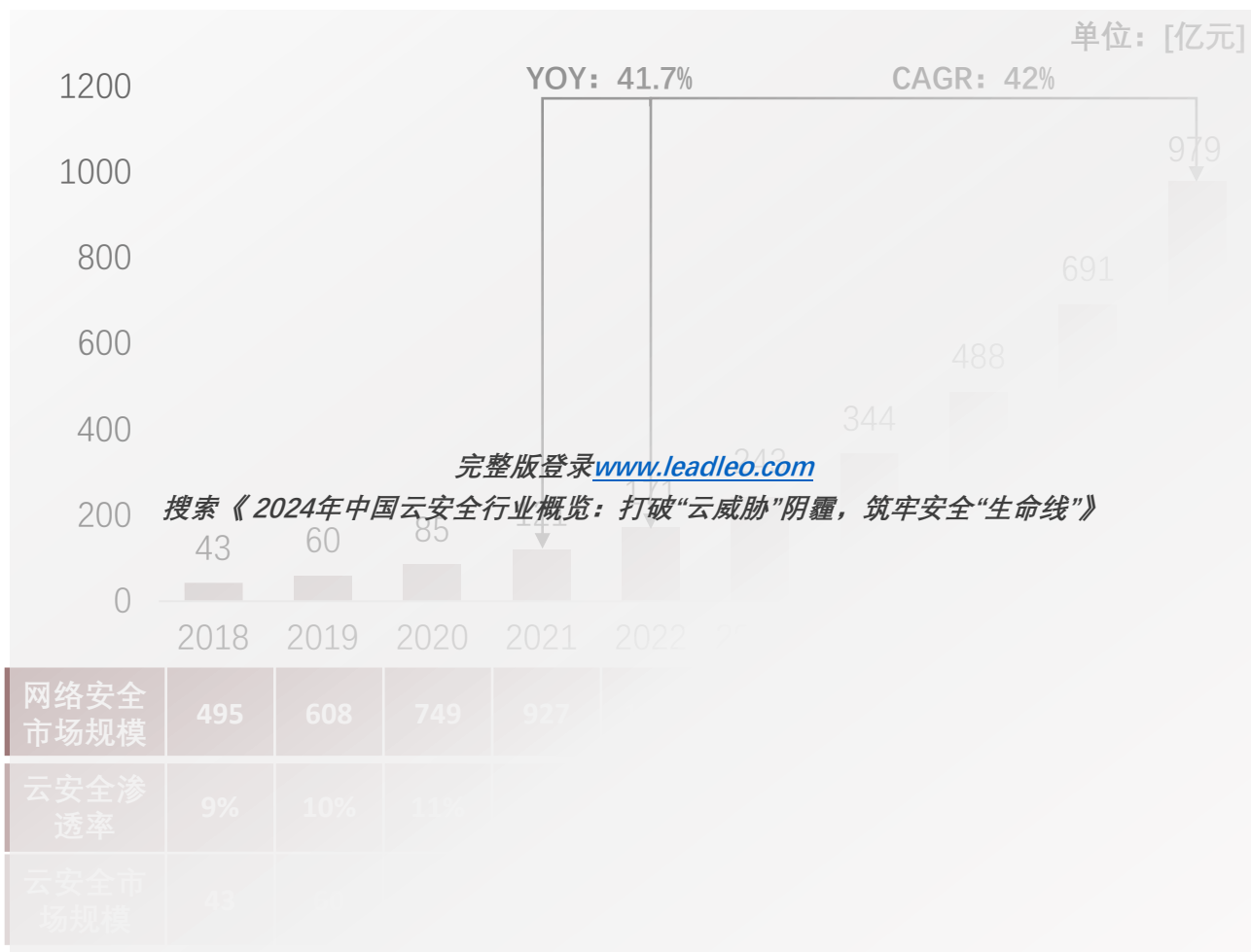
- 萌芽阶段：**2009年5月，中国电子学会主办了第一届中国云计算大会。同年，阿里软件建立首个“电子商务云计算中心”，随后阿里云正式成立，2009年也被称为中国的云计算元年。2010年，浪潮实施第一个落地行业云项目。
- 起步阶段：**2015年，中国云计算市场全面盛开，国内IT企业纷纷转向云计算。随着移动互联网对传统行业的颠覆性影响，中国用户对“云化”需求迅速增长。2017年4月，工信部发布了《云计算发展三年行动计划（2017-2019年）》，支持积极发展工业云服务，搭建面向制造业特色领域的工业云平台。
- 发展阶段：**随着云计算的普及和应用的增加，云安全问题日益突出，相关的云安全工具和技术如云防火墙、云上身份管控和云上终端安全检测等应运而生。
- 高速发展阶段：**2021年之后，数据隐私泄露事件频发，涉及面广，影响力大。如在2021年，共有近2.2亿人受到数据安全事件的影响。2022年，中国云安全行业规模达到171亿元，头部云厂商基于自身在云计算领域的技术积累，可真正实现安全防护服务的云化。

来源：全栈云技术架构、专家访谈、头豹研究院

中国云安全行业综述——市场规模

- 2022年中国云安全市场规模达171亿元，预计2027年将达到979亿元。企业需求、技术应用将促使市场不断释放潜力，云原生、人工智能、物联网等技术将推动更多细分安全场景需求

中国云安全市场规模，2018-2027年预测



- 2022年中国云安全市场规模达到171亿元，同比增长41.72%，预计2027年将达到979亿元，2022-2027年期间复合增速为42%

云安全市场迅速增长受多重因素推动。首先，在政策方面，中国数据安全法规不断完善，为市场提供引导和规范。其次，企业对云安全的需求进入高峰期。随着云服务模式的广泛应用，各个领域的安全实践推动了市场需求的急速增长。2022年，中国企业工业设备上云率提升至17.7%，较2021年提升了2.2个百分点，企业业务上云普及率为41.4%，较2021年增长了3个百分点。

随着云原生的成熟和安全架构升级的趋势下，以及客户安全意识上升，中国云安全的市场需求将会持续释放，预计2027年将达到979亿元，2022-2027年期间复合增速为42%。此外，混合多云、云原生、人工智能、物联网等新技术的广泛应用，将导致更多细分的安全场景和需求，同样助推云安全市场发展。

来源：专家访谈、奇安信公告、头豹研究院

Chapter 2

产业链分析

- 上游分析：云安全产业链上游可分为硬件和软件供应商。目前，中国云安全产业链上游的发展要点主要包括制定行业标准、技术发展和构建生态等
- 细分市场分析：公有云服务中小企业，成本低且便捷，应用比例达60%。相较之，大型企业等对数据安全要求高，更倾向私有云或混合云
- 商业模式：云安全厂商主要采用订阅、授权和定制等商业模式
- 行业场景：互联网、工业云和金融行业成攻击焦点。金融主要用私有云，电信主要用公有云，航空航天以本地私有云为主，互联网主要用公有云
- 业务场景：云安全在身份与访问控制、基础架构防护、监控与检测和合规审计等场景中的应用渗透率较高，均超50%

中国云安全产业链分析——产业链图谱

- 中国云安全行业的产业链上游为硬件供应商和软件提供商，中游为互联网厂商、传统IT厂商、运营商和安全领域厂商，下游则为云安全的终端用户

中国云安全行业产业链图谱

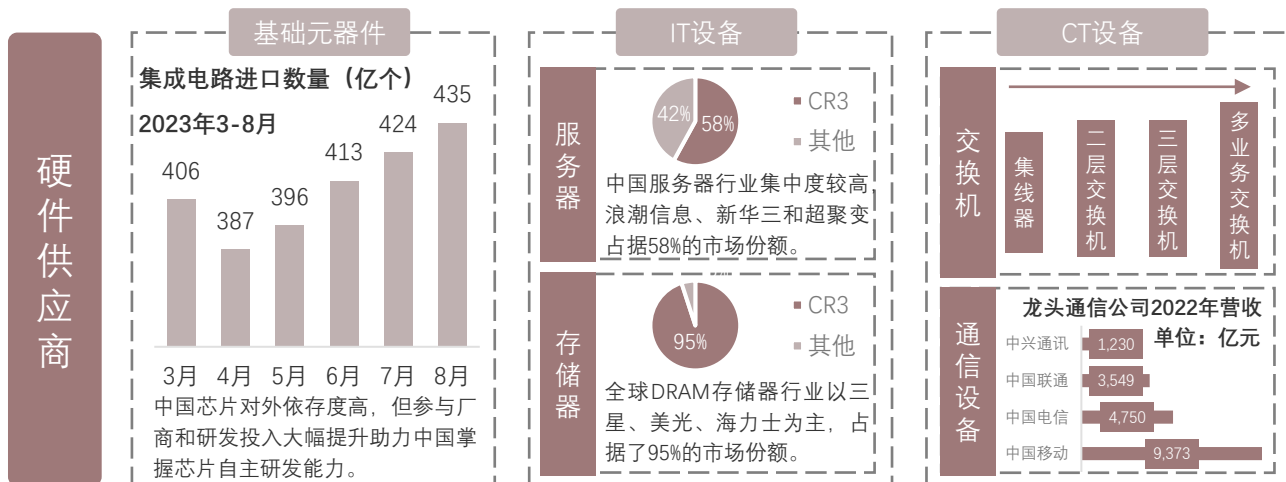


来源：专家访谈、头豹研究院

中国云安全产业链上游分析——发展概述

- 云安全产业链上游可分为硬件和软件供应商，其中硬件供应商可细分为基础元器件、IT设备和CT设备，软件供应商可分为IT系统和IT应用等

中国云安全产业链上游-硬件供应商发展情况



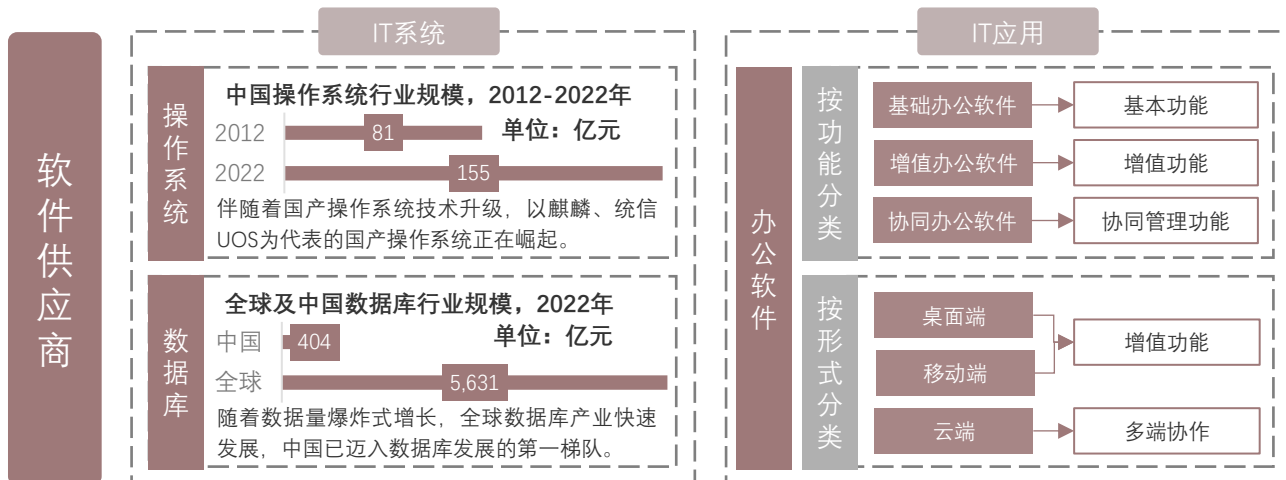
云安全产业链上游硬件供应商包括基础元器件、IT设备和CT设备等设备和零件供应商

基础元器件：芯片主要由集成电路、光电器件、分立器件、传感器等部分组成，其中集成电路占了器件80%以上的份额。2023年第一季度，中国进口集成电路1,082亿件，同比下降22.9%。尽管目前芯片对外依存度还处于高位，但景嘉微、海光信息和龙芯中科等厂商生产技术的提升将助力中国掌握芯片自主研发能力。

IT设备：在信创市场高速发展的背景下，国产服务器厂商近年来增速迅猛，行业集中度较高，竞争格局稳固，浪潮信息、新华三和超聚变占据58%的市场份额。尤其是浪潮信息，已逐渐缩小和戴尔、惠普的差距。

CT设备：交换机是一种用于电、光信号转发的网络设备，最常见的交换机是以太网交换机。目前中国交换机头部企业为华为、新华三、锐捷网络等，而数据中心的快速发展或是交换机行业增长主要驱动力。

中国云安全产业链上游-软件供应商发展情况



来源：专家访谈、电子工程世界、宝通集团、头豹研究院

（接上页——上游发展概述）

- 云安全产业链上游软件供应商包括IT系统、IT应用等，其中IT系统可细分为操作系统、数据库和中间件等，IT应用可分为服务软件和办公软件等

操作系统：目前，Windows、macOS在中国桌面操作系统行业中占据主导地位，Linux则占据中国服务器操作系统市场领先地位。2022年中国操作系统市场规模达到155.1亿元，2012-2022年的复合增长率达6.7%。国产操作系统在生态数量和用户使用体验上均得到极大提升，麒麟软件生态数量率先突破200万款。

数据库：随着数字化转型深入推进和数据量的爆炸式增长，中国已经迈入全球数据库发展的第一梯队。2022年全球数据库市场规模为833亿美元，中国数据库市场规模为59.7亿美元，占全球的7.2%。目前，中国数据库产品数量呈现以关系型为主，非关系型数据库为辅的局面。截至目前，中国拥有关系型数据库156个，非关系型数据库82个，占比分别为65.5%和34.5%。

IT应用：办公软件按功能可分为基础办公软件、增值办公软件及协同办公软件。2022年中国办公软件市场规模达401.55亿元，较2021年增长12.18%。其中，协同办公软件市场规模达到217.28亿元。

中国云安全产业链上游的发展要点



- 中国云安全产业链上游的发展要点主要包括制定行业标准、技术发展和构建生态等

首先，制定行业标准有助于推动技术创新，建立行业共识和加强整体安全防护。上游厂商参与标准制定，不仅提升自身实力，还为整个行业的发展提供了指导和引领。标准制定有助于明确行业规范，提高产品互操作性，促进市场发展。其次，目前中国芯片产业在多个方面仍面临着诸多挑战，比如供应链的不稳定性、设备技术的不足、工艺流程的优化需求，以及在电子设计自动化工具方面的技术短板等，解决这些问题将对中国芯片产业的全面发展起到关键作用。再者，构建生态有助于全面保障安全需求、促进技术创新以及推动行业标准化。生态系统的建设可以覆盖整个云安全产业链，从基础设施到服务层，以及与之相关的技术和标准，能够使企业更好地适应市场需求，形成合作伙伴关系，实现资源的共享，提高行业的技术创新水平。

中国云安全产业链中游分析——细分市场

- 公有云服务中小企业，成本低且便捷，应用比例达60%。相较之，大型企业等对数据安全要求高，更倾向私有云或混合云，构建灵活本地和云上防护

中国云安全细分市场占比（按部署模式划分）



完整版登录www.leadleo.com

中国工业企业数量, 2022年

搜索《2024年中国云安全行业概览：打破“云威胁”阴霾，筑牢安全“生命线”》

426,948 单位：家

中国大、中、小和微型工业企业数量

指标名称	数量
小型工业企业	426,948
中型工业企业	36,949
大型工业企业	8,112

- 公有云主要服务中小企业，成本低、便捷。相较于中小企业，大型企业等对数据安全要求高，倾向采用私有云或混合云，构建更灵活的本地和云上防护体系

公有云主要服务中小企业，由于其成本较低、便捷性强，中小企业占据了公有云市场的主体，约占50%以上。对于这些中小企业，数据安全法对数据管控的要求相对较低，且它们的服务和数据对经济的直接影响有限。而中小企业是中国企业的重要组成部分。以工业为例，2022年，中国小型企业共有426,948家企业，而大型企业仅有8,112家。因此，尽管应用公有云的中小企业体量不大，但数量上占据优势，因此，公有云应用比例达到60%。相比之下，大型企业、金融机构、政府和央企等重要行业客户更倾向于采用私有云或混合云的方式。这是因为这些行业对数据安全的要求较高，且受到数据安全法等法规的约束。大型企业可能存在大量重要数据，不愿将其放到公有云上，而更倾向于建设自己的私有云或采用混合云模式，在本地和云上进行防护。

来源：专家访谈、头豹研究院

中国云安全产业链中游分析——商业模式

- 云安全厂商主要采用订阅、授权和定制等商业模式。订阅模式主导市场，灵活适用于中小企业，授权许可提供更灵活选择，定制化服务大型企业，满足个性化需求

中国云安全厂商的商业及收费模式



■ 云安全厂商的商业模式主要包括定制、授权和订阅等

云安全厂商采用定制、授权和订阅等多种商业模式以满足不同客户需求。其中，订阅模式是主流，通过以月或年为单位的订阅方式提供安全能力和组件，以更低的价格满足中小企业需求，约占市场的60%。此外，授权许可模式提供安全产品的使用授权，允许客户按需一次性购买特定组件的使用权。另一种模式是定制化模式，主要服务私有云客户，云安全厂商根据其业务需求，为其提供只适用于其业务的云安全解决方案，适用于对成本相对不敏感的大型企业。

这三种商业模式各有特点。订阅模式灵活且经济，适用于广大中小企业，占主导地位。授权许可模式提供更灵活的选择，允许客户根据需要购买特定的授权许可，适用于有特殊需求的企业。定制化模式适用于那些对安全组件有明确需求且对成本不敏感的大型企业，提供全套定制化的解决方案。在实际项目中，商业模式的选择受到客户属性、预算、项目需求等多方面因素的影响。一些客户更愿意采用灵活的订阅模式，以更小的成本获取所需的安全服务。而一些大型企业可能更愿意通过授权许可或定制的方式获取适用性更强和更全面的解决方案，尽管成本相对较高。

总体而言，云安全厂商通过多样化的商业模式，灵活满足了不同客户的需求，促使云安全市场的健康发展。未来，订阅模式有望继续占据主导地位，但其他模式也将根据市场需求得到合理应用，实现互补共生的发展格局。

来源：专家访谈、头豹研究院

中国云安全产业链下游分析——行业场景

- 互联网、工业云和金融行业成攻击焦点。金融主要用私有云，电信主要用公有云，航空航天以本地私有云为主，互联网主要用公有云

云上各行业受攻击占比，2023年上半年

中国云安全行业场景中公有云、私有云、混合云应用



- 互联网、工业云和金融行业是攻击焦点，攻击次数分别为53.97%、8.17%和7.1%

截至2023年上半年，从不同行业的拦截数据来看，遭受攻击的次数呈现明显差异。互联网（包括通用工具、技术服务和通用SaaS）、金融和工业云成为受攻击次数最多的前三个行业。互联网行业因庞大用户群和云计算技术支持服务，成为攻击者的首要目标，占据上半年云上总攻击次数的53.97%。工业云，作为制造业数字化转型的支撑，面临高攻击风险，攻击者试图窃取商业机密或干扰生产过程，占总攻击次数的8.17%。金融行业因涉及敏感数据和资金交易，一直是黑客攻击的焦点。与其他行业相比，金融行业在云上的攻击不仅频繁，而且手段更加高级和隐蔽，上半年被攻击次数占总次数的7.1%。

- 金融偏向私有云混合云保障数据安全，电信主用公有云处理公开数据，航空航天专注本地私有云涉密数据，互联网强调公有云满足云服务需求

首先，金融行业对数据安全性要求极高，特别是涉及个人账户和敏感信息。因此，金融行业在云安全方面主要采用私有云和混合云模式，占比超过80%，以确保核心业务数据的安全。其次，电信行业拥有庞大的用户数据，但其中大部分数据为公开数据，因此，电信行业更多地采用公有云，占比达到70%。再者，在航空航天行业中，涉及到的数据通常是涉密的，因此该行业主要采用本地私有云，占比接近100%，较少使用公有云。此外，互联网行业是云服务的重要用户，连接各大网络群体，因此主要采用公有云，占比高达90%。

来源：专家访谈、头豹研究院

Chapter 3

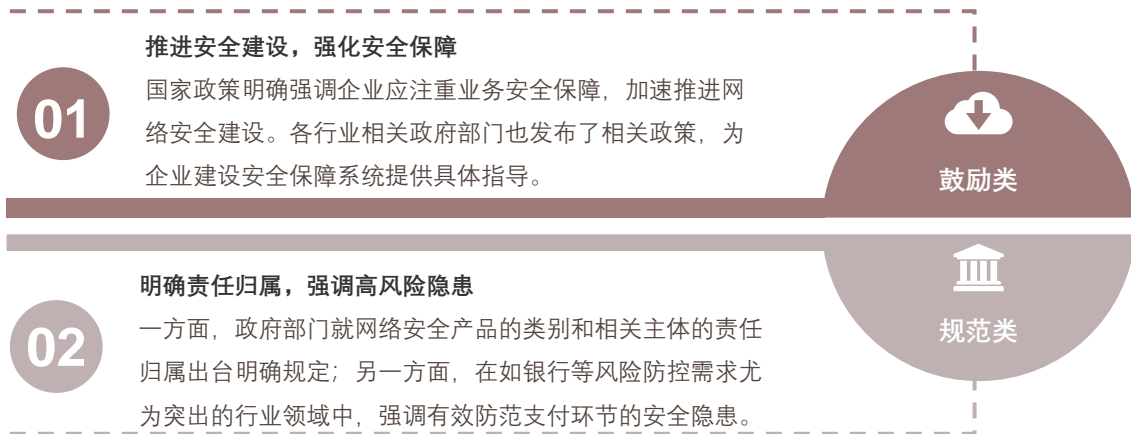
行业分析

- **政策分析：**近年来，国家出台了一系列网络安全相关政策，可分为鼓励类和规范类两种政策
- **制约因素：**云安全行业面临的短期挑战包括技术创新、性能云扩展性、可扩展性和合规性，长期挑战包括人才培养和其他外部因素。目前中国云安全在一些方面与国际存在差距，迎头赶超或需3-5年
- **发展趋势：**云安全行业的发展趋势包括技术升级、零信任和云原生等的发展，向C端拓展以及符合合规需求
- **竞争格局：**云安全竞争激烈，腾讯云、奇安信、天融信等领先，行业竞争呈多元格局

中国云安全行业分析——政策分析

- 近年来，国家出台了一系列网络安全相关政策，可分为鼓励类和规范类两种政策。其中，鼓励类政策内容主要为推进安全建设，强化安全保障；规范类政策内容主要为明确责任归属，强调高风险隐患

中国云安全相关政策梳理，2021-2023年



01

推进安全建设，强化安全保障

国家政策明确强调企业应注重业务安全保障，加速推进网络安全建设。各行业相关政府部门也发布了相关政策，为企业建设安全保障系统提供具体指导。

02

明确责任归属，强调高风险隐患

一方面，政府部门就网络安全产品的类别和相关主体的责任归属出台明确规定；另一方面，在如银行等风险防控需求尤为突出的行业领域中，强调有效防范支付环节的安全隐患。

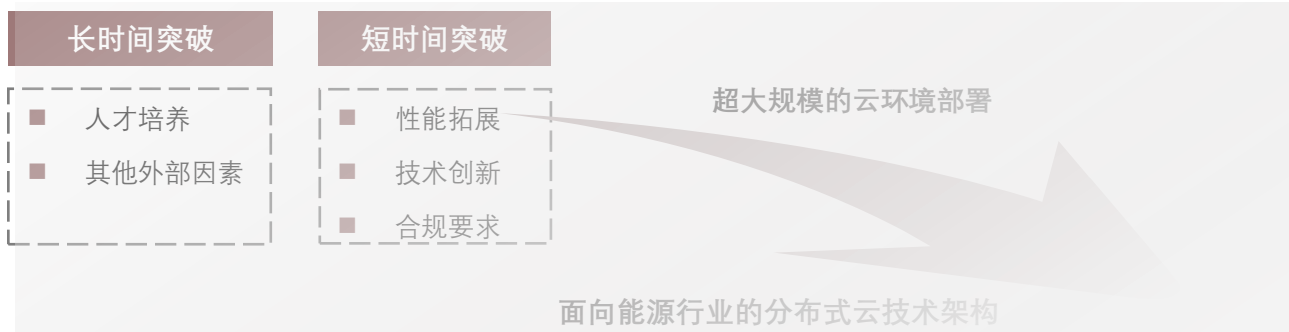
政策名称	颁布日期	颁布主体	主要内容及影响
《数字中国发展报告（2022年）》	2023-05	国家网信办	2022年，网络安全法律法规和标准体系逐步健全、网络安全防护能力大幅提升、网络安全产业规模同比增长13.9%、数据安全管理和个人信息保护有力推进。
《关于调整网络安全专用产品安全管理有关事项的公告》	2023-04	国家网信办、工信部、公安部、财政部、认监委	规定网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。
《电力行业网络安全等级保护管理办法》	2022-11	国家能源局	明确了电力行业网络安全保护等级划分和等级保护工作原则，规定了国家能源局及其派出机构、电力企业及网络安全等级保护测评机构在电力行业网络安全等级保护定级、审核、建设、测评、检查及密码管理等方面的有关要求以及法律责任。
《人民法院在线运行规则》	2022-02	最高人民法院	鼓励法院建设安全保障系统，强调应当为各类信息基础设施、应用系统和数据资源提供主机安全、身份认证、访问控制、分类分级、密码加密、防火墙、安全审计和安全管理等安全服务。
《车联网网络安全和数据安全标准体系建设指南》	2022-02	工信部	提出到2023年底，初步构建起车联网网络安全和数据安全标准体系。重点研究基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等标准。
《关于加强支付受理终端及相关业务管理的通知》	2021-10	中国人民银行	为有效提升支付受理终端及相关业务风险管理水平，有力斩断跨境赌博等犯罪“资金链”，保障社会公众利益。
《关于进一步压实网站平台信息内容管理主体责任的意见》	2021-09	国家互联网信息办公室	对信息内容呈现结果负责，严防违法信息生产传播，自觉防范和抵制传播不良信息，确保信息内容安全。

来源：政府官网、头豹研究院

中国云安全行业分析——制约因素

- 云安全行业面临的短期挑战包括技术创新、性能云扩展性、可扩展性和合规性，长期挑战包括人才培养和其他外部因素。目前中国云安全在一些方面与国际存在差距，迎头赶超或需3-5年

中国云安全行业制约因素



中国云安全与国外的技术差距



- 云安全行业短期可突破技术创新、性能云扩展性和合规要求等问题，但国内仍与国际存在差距，需3~5年迎头赶超

云安全行业短时间内可能会突破的障碍主要包括技术创新、性能云扩展性和可扩展性、以及满足合规要求。技术创新涉及算法、智能化机器学习等在安全领域的应用，有望在短期内取得重大突破。性能云扩展性和可扩展性是在超大规模云环境下进行安全防护建设所需解决的难题，技术手段可能有望在短期内应对这一挑战。此外，合规性方面，通过按照法律法规的要求进行建设，也是相对容易在短期内取得突破的方向。其中，解决云安全超大规模部署的方法可采取分布式集中管理的混合模式。这意味着在超大规模环境中，部署将结合集群和分布式架构，通过联动多个分布式节点实现云安全的管理。

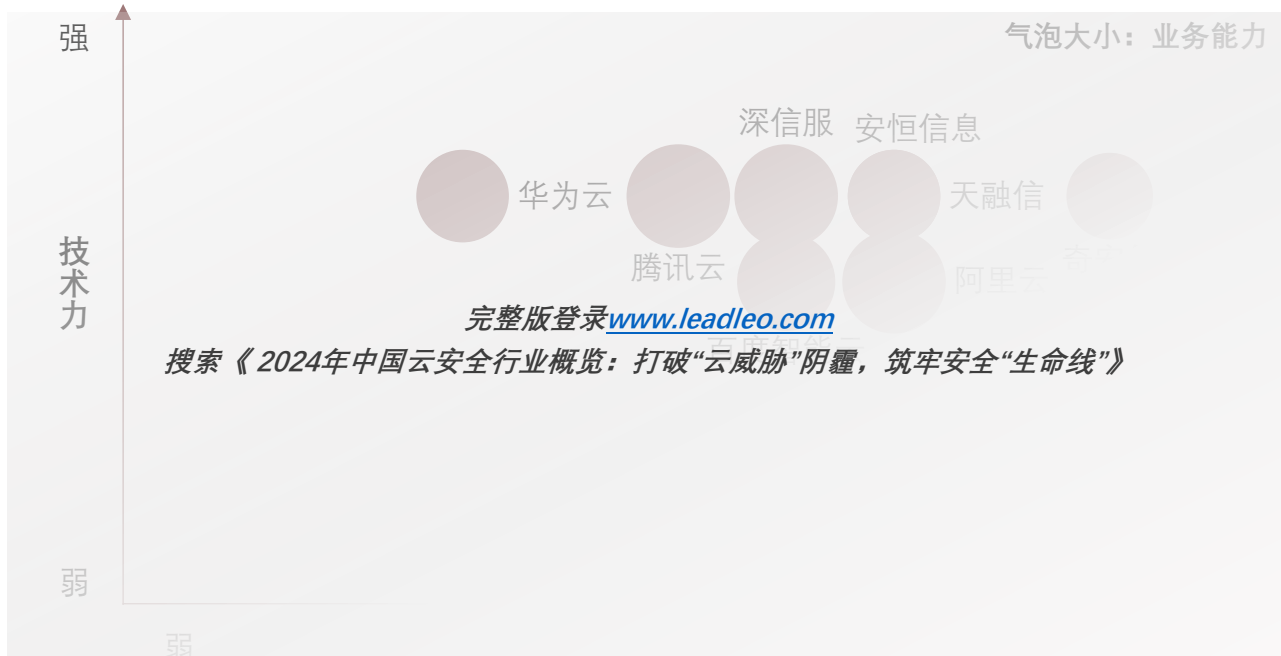
目前，国内云安全行业在一些关键方面与国际水平仍存在一定差距。这差距主要体现在自研算法、产品专利、以及底层技术的应用上。虽然国内的云安全产品已经部分实现国产化，但底层的算法、专利和芯片等关键技术多数仍依赖于国外。因此，中国的云安全行业仍需要3~5年的时间才能追赶上国际技术水平。

来源：专家访谈、头豹研究院

中国云安全行业分析——竞争格局

- 云安全竞争激烈，腾讯云、奇安信、天融信等领先，行业竞争呈多元格局，愈发多厂商加入、产品升级、产品创新与差异化运营成竞争格局变动的关键

中国云安全竞争格局



■ 云安全竞争格局多元化，腾讯云、奇安信和天融信等企业领跑

云安全竞争格局呈现多元化的特点，其参与方包括云服务提供商、IT运维厂商和安全厂商，行业市场集中度较低，市场竞争激烈。具体竞争格局如下：第一梯队为腾讯云、奇安信、天融信等企业，在信息安全领域深耕多年，拥有多种云安全产品及服务，研发能力强。第二梯队为阿里云、百度智能云等企业，综合实力强，但安全领域的竞争力弱于第一梯队。第三梯队为绿盟科技、启明星辰等企业，技术研发能力、安全领域实力和综合竞争力均较弱。

■ 随着愈发多云安全厂商加入、产品和服务不断升级以及厂商的运营策略愈发多样化，云安全行业竞争将加剧

首先，随着云计算的普及，保障云上数据和应用的安全成为企业迈向数字化未来的关键挑战，愈发多的云安全服务厂商开始不断加大投入布局该赛道。此外，云安全厂商积极推出适用不同云计算环境的云安全服务和产品，助安全生态构建，推动产业发展壮大。2023年12月16日，腾讯云安全发布“全域安全”解决方案，通过打造CNAPP+SIEM的安全一体化平台，结合AI安全助手的应用，进一步助力企业实现智能的统一安全运营。再者，为应对竞争激烈，各大云安全厂商采取差异化的精细运营策略，不断开拓新产品或市场，以丰富中国网络安全产品线，争夺更多市场份额。2023年9月，思科宣布以280亿美金收购Splunk，以提高其威胁检测和响应到威胁预测和预防能力。而仅在2023年，思科就收购了威胁检测平台Armorblox、身份管理公司Oort以及两家云安全公司Valtix和Lightspin。

来源：专家访谈、头豹研究院

Chapter 4

典型厂商分析

- 奇安信
- 绿盟科技
- 深信服

方法论

- ◆ 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。
- ◆ 研究院依托中国活跃的经济环境，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- ◆ 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- ◆ 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- ◆ 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- ◆ 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- ◆ 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- ◆ 本报告所涉及的观点或信息仅供参考，不构成任何投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。本报告所指的公司或投资标的的价值、价格及投资收入可升可跌。
- ◆ 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本文所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本文所载资料、意见及推测不一致的报告和文章。头豹不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。

业务合作

会员账号

可阅读全部原创报告和百万数据，提供PC及移动端，方便触达平台内容

定制报告/词条

行企研究多模态搜索引擎及数据库，募投可研、尽调、IRPR等研究咨询

定制白皮书

对产业及细分行业进行现状梳理和趋势洞察，输出全局观深度研究报告

招股书引用

研究覆盖国民经济19+核心产业，内容可授权引用至上市文件、年报

市场地位确认

对客户竞争优势进行评估和证明，助力企业价值提升及品牌影响力传播

云实习课程

依托完善行业研究体系，帮助学生掌握行业研究能力，丰富简历履历



业务热线

袁先生：15999806788

李先生：13080197867