中国工业互联网安全行业现状深度分析与未来投资研究报告（2022-2029年）

报告大纲

观研报告网
www.chinabaogao.com

一、报告简介

观研报告网发布的《中国工业互联网安全行业现状深度分析与未来投资研究报告（2022-2029年）》涵盖行业最新数据，市场热点，政策规划，竞争情报，市场前景预测，投资策略等内容。更辅以大量直观的图表帮助本行业企业准确把握行业发展态势、市场商机动向、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

官网地址：https://www.chinabaogao.com/baogao/202211/618061.html

报告价格：电子版: 8200元　纸介版：8200元　电子和纸介版: 8500

订购电话: 400-007-6266 010-86223221

电子邮箱: sales@chinabaogao.com

联 系 人 : 客服

特别说明：本PDF目录为计算机程序生成，页面图表可能存在缺失；格式美观性可能有欠缺，实际报告排版规则、美观；可联系客服索取更完整的目录大纲。

二、报告目录及图表目录

一、行业基本概述

工业互联网安全是工业互联网的重要保障，又可以称为工业信息安全2.0，主要涉及到设备的安全，控制的安全，网络的安全、标识解析的安全，平台的安全、数据的安全等六大安全问题。其中标识解析的安全，平台的安全，数据的安全，标识的安全是工业互联网安全的新问题。

工业互联网是新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系，为工业乃至产业数字化、网络化、智能化发展提供了实现途径，是第四次工业革命的重要基石。由此可见，工业互联网有数字化、网络化和智能化三个特征，这3个特征支撑着工业资源的优化配置。

资料来源：观研天下整理

工业互联网包含了网络、平台、数据、安全四大体系，既是工业数字化、网络化、智能化转型的基础设施，也是互联网、大数据、人工智能与实体经济深度融合的应用模式，同时也是一种新业态、新产业，将重塑企业形态、供应链和产业链。

工业互联网内涵构成

网络体系是基础

工业互联网网络体系包括网络互联、数据互通和标识解析三部分。网络互联实现要素之间的数据传输，包括企业外网、企业内网。典型技术包括传统的工业总线、工业以太网以及创新的时间敏感网络（TSN）、确定性网络、5G等技术。

平台体系是中枢

工业互联网平台体系包括边缘层、IaaS、PaaS和SaaS四个层级，相当于工业互联网的“操作系统”，有四个主要作用。一是数据汇聚。网络层面采集的多源、异构、海量数据，传输至工业互联网平台，为深度分析和应用提供基础。二是建模分析。提供大数据、人工智能分析的算法模型和物理、化学等各类仿真工具，结合数字孪生、工业智能等技术，对海量数据挖掘分析，实现数据驱动的科学决策和智能应用。三是知识复用。将工业经验知识转化为平台上的模型库、知识库，并通过工业微服务组件方式，方便二次开发和重复调用，加速共性能力沉淀和普及。四是应用创新。面向研发设计、设备管理、企业运营、资源调度等场景，提供各类工业APP、云化软件，帮助企业提质增效。

数据体系是要素

工业互联网数据有三个特性。一是重要性。数据是实现数字化、网络化、智能化的基础，没有数据的采集、流通、汇聚、计算、分析，各类新模式就是无源之水，数字化转型也就成为

无本之木。二是专业性。工业互联网数据的价值在于分析利用，分析利用的途径必须依赖行业知识和工业机理。制造业千行百业、千差万别，每个模型、算法背后都需要长期积累和专业队伍，只有深耕细作才能发挥数据价值。三是复杂性。工业互联网运用的数据来源于“研产供销服”各环节，“人机料法环”各要素，ERP、MES、PLC等各系统，维度和复杂度远超消费互联网，面临采集困难、格式各异、分析复杂等挑战。

安全体系是保障

工业互联网安全体系涉及设备、控制、网络、平台、工业APP 、数据等多方面网络安全问题，其核心任务就是要通过监测预警、应急响应、检测评估、功能测试等手段确保工业互联网健康有序发展。与传统互联网安全相比，工业互联网安全具有三大特点。一是涉及范围广。工业互联网打破了传统工业相对封闭可信的环境，网络攻击可直达生产一线。联网设备的爆发式增长和工业互联网平台的广泛应用，使网络攻击面持续扩大。二是造成影响大。工业互联网涵盖制造业、能源等实体经济领域，一旦发生网络攻击、破坏行为，安全事件影响严重。三是企业防护基础弱。目前我国广大工业企业安全意识、防护能力仍然薄弱，整体安全保障能力有待进一步提升。

资料来源：观研天下整理

二、行业发展现状

工业互联网成为我国经济稳增长的重要支撑

近年来我国工业互联网从无到有，发展逐步壮大，溢出赋能成效显著，逐渐步入创新发展新阶段。目前工业互联网已延伸至40个国民经济大类，且不断向国民经济重点行业广泛拓展，涉及原材料、装备、消费品、电子等制造业各大领域，以及采矿、电力、建筑等实体经济重点产业，实现更大范围、更高水平、更深程度发展，形成了千姿百态的融合应用实践，形成了平台化设计、智能化制造、网络化协同、个性化定制、服务化延伸、数字化管理六大新模式，赋能、赋智、赋值作用不断显现，有力的促进了实体经济提质、增效、降本、绿色、安全发展。

目前工业互联网成为我国经济稳增长的重要支撑。有数据显示，2021年我国我国工业互联网产业增加值规模突破4万亿元，达到4.10万亿元，名义增速达到14.53%，占GDP的比重达到3.58%。其中平台、网络、数据、安全四大直接产业增加值总规模达到1.17万亿元，名义增速为16.07%；渗透产业为2.93万亿元，名义增速为13.94%。

数据来源：中国工业互联网研究院，观研天下整理

数据来源：中国工业互联网研究院，观研天下整理

在工业互联网拉动下，2021年各地区工业互联网发展百花齐放，广东、江苏、浙江、山东、四川、北京、河南、湖北、福建、上海等13省市的工业互联网产业增加值规模破千亿元。另外长三角地区工业互联网产业增加值首次破万亿元，高达10687.51

亿元，其次为珠三角和长江中游地区次之。

数据来源：中国工业互联网研究院，观研天下整理
工业互联网安全问题不断暴露，网络安全漏洞形势依旧严峻
而虽然近年工业互联网不断发展，但在发展的同时，工业互联网安全问题不断暴露。有相关资料显示，2022 年上半年，网络安全漏洞形势依旧严峻，高危漏洞数量不断增长，漏洞利用渐趋隐蔽，融合叠加风险攀升，在野漏洞利用成为重大网络安全热点事件的风险点以及国家级 APT 活动的新手段。数据显示，2022 年上半年新增通用型漏洞信息共计 12466 条，高危漏洞为4639 个，占比 37%；超危漏洞 1927 个，占比 16%； 中危漏洞 5478 个，占比 44%；低危漏洞 422 个，占比 3%。

数据来源：中国信息安全测评中心、中国信息产业商会信息安全产业分会，观研天下整理
具体来看：
在漏洞数量方面，漏洞增长创新高，危害程度较大漏洞仍然是热点，超高危漏洞占比超过50%；微软、谷歌等美企大厂产品漏洞多发，持续成为安全研究焦点；开源软件漏洞频发，软件供应链安全风险凸显。
2022 年上半年新增漏洞影响厂商 TOP10
厂商名称
漏洞数量
所占比例（%）
WordPress（美）
904
7.25
谷歌（美）
622
4.99
微软（美）
487
3.91
甲骨文（美）
259
2.08
Adobe（美）
213
1.71

IBM（美）
206
1.65
Tenda（中）
170
1.36
苹果（美）
169
1.36
思科（美）
168
1.35
三星（韩）
160
1.28
资料来源：中国信息安全测评中心、中国信息产业商会信息安全产业分会，观研天下整理
在漏洞利用方面，2022 年上半年新增在野利用漏洞数量 475 个，其中公开披露 POC\EXP\漏洞细节的漏洞共有 348 个，超过 70%的漏洞 POC\EXP\漏洞细节已经在互联网上流传 7，8，并被某些 APT 组织或者恶意软件团伙频繁使用， 这些漏洞存在较大的现实威胁，需尽快修复。同时新增在野利用漏洞中，Windows、Linux、macOS/iOS、Android 等操作系统相关漏洞共计 90 个，网络设备漏洞共计 82 个，浏览器、办公软件等终端软件相关漏洞共计 92 个，这三类漏洞占所有新增在野利用漏洞近 55%。2022年最受关注十大 Web 漏洞被国内外黑客大量用于对我境内目标的攻击活动，单一漏洞最大利用量超过 8000 万次10。
2022 年上半年最受关注的十大 Web 漏洞
漏洞名称
漏洞编号
利用量
Apache Log4j 远程代码执行漏洞
CNNVD-202112-799
(CVE-2021-44228)
84371231
IBM WebSphere Portal SSRF
-

2879741
Atlassian Crowd 远程代码执行漏洞
CNNVD-201905-1031
(CVE-2019-11580)
1149725
Apache Druid 任意文件读取漏洞
CNNVD-202109-1676
(CVE-2021-36749)
1039259
帆软报表 V8 任意文件读取漏洞
CNVD-2019-41405
1028775
若依管理系统任意文件读取漏洞
CNVD-2021-15555
929449
Apache Flink 目录遍历漏洞
CNNVD-202101-271
(CVE-2020-17519)
845748
泛微 OA 前台任意文件下载漏洞
-
831286
Fortinet FortiOS 路径遍历漏洞
CNNVD-201905-1026
(CVE-2018-13379)
776811
Spring4Shell 远程代码执行漏洞
CNNVD-202203-2514
(CVE-2022-22965)
729057
资料来源：中国信息安全测评中心、中国信息产业商会信息安全产业分会，观研天下整理
在漏洞现实威胁方面，高价值漏洞“寄生”于多类目标，现实危害严重，影响持久。边界设备、操作系统、服务器软件、开源组件、协同办公软件、云原生、移动终端等目标对象漏洞在攻击活动中频繁现身；攻击者通过漏洞攻破网络“大门”、横向移动传播、获取控制权、破坏或窃取数据形

成完整网络攻击组合拳；漏洞修复不完善引发“次生灾害”，
历史漏洞重复利用或修复后再被突破，对漏洞治理提出更高要求。
工业互联网安全是落实总体国家安全观的重要抓手
在上述背景下，工业互联网安全就显的尤为重要。目前工业互联网安全是我国实施制造强国和网络强国战略的重要保障，也是落实总体国家安全观的重要抓手。近年来，随着工业互联网政策的不断出台，以及政府、企事业单位对工业互联网安全需求的增加，我国工业互联网安全市场规模具有较快的增长率。数据显示，2021年我国工业互联网安全产业规模由2017年的72.8亿元增长228亿元，复合年均增长率为33%。预计2022年我国工业互联网安全产业规模将达276.8亿元。

资料来源：观研天下整理（WW）
观研报告网发布的《中国工业互联网安全行业现状深度分析与未来投资研究报告（2022-2029年）》涵盖行业最新数据，市场热点，政策规划，竞争情报，市场前景预测，投资策略等内容。更辅以大量直观的图表帮助本行业企业准确把握行业发展态势、市场商机动向、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

行业报告是业内企业、相关投资公司及政府部门准确把握行业发展趋势，洞悉行业竞争格局，规避经营和投资风险，制定正确竞争和投资战略决策的重要决策依据之一。本报告是全面了解行业以及对本行业进行投资不可或缺的重要工具。观研天下是国内知名的行业信息咨询机构，拥有资深的专家团队，多年来已经为上万家企业单位、咨询机构、金融机构、行业协会、个人投资者等提供了专业的行业分析报告，客户涵盖了华为、中国石油、中国电信、中国建筑、惠普、迪士尼等国内外行业领先企业，并得到了客户的广泛认可。

本研究报告数据主要采用国家统计数据，海关总署，问卷调查数据，商务部采集数据等数据库。其中宏观经济数据主要来自国家统计局，部分行业统计数据主要来自国家统计局及市场调研数据，企业数据主要来自于国家统计局规模企业统计数据库及证券交易所等，价格数据主要来自于各类市场监测数据库。本研究报告采用的行业分析方法包括波特五力模型分析法、SWOT分析法、PEST分析法，对行业进行全面的内外部环境分析，同时通过资深分析师对目前国家经济形势的走势以及市场发展趋势和当前行业热点分析，预测行业未来的发展方向、新兴热点、市场空间、技术趋势以及未来发展战略等。

【目录大纲】

第一章 2018-2022年中国工业互联网安全行业发展概述
第一节工业互联网安全行业发展情况概述
一、工业互联网安全行业相关定义
二、工业互联网安全特点分析
三、工业互联网安全行业基本情况介绍
四、工业互联网安全行业经营模式
1、生产模式
2、采购模式
3、销售/服务模式
五、工业互联网安全行业需求主体分析
第二节中国工业互联网安全行业生命周期分析
一、工业互联网安全行业生命周期理论概述
二、工业互联网安全行业所属的生命周期分析
第三节工业互联网安全行业经济指标分析
一、工业互联网安全行业的赢利性分析
二、工业互联网安全行业的经济周期分析
三、工业互联网安全行业附加值的提升空间分析

第二章 2018-2022年全球工业互联网安全行业市场发展现状分析
第一节全球工业互联网安全行业发展历程回顾
第二节全球工业互联网安全行业市场规模与区域分布情况
第三节亚洲工业互联网安全行业地区市场分析
一、亚洲工业互联网安全行业市场现状分析
二、亚洲工业互联网安全行业市场规模与市场需求分析
三、亚洲工业互联网安全行业市场前景分析
第四节北美工业互联网安全行业地区市场分析
一、北美工业互联网安全行业市场现状分析
二、北美工业互联网安全行业市场规模与市场需求分析
三、北美工业互联网安全行业市场前景分析
第五节欧洲工业互联网安全行业地区市场分析
一、欧洲工业互联网安全行业市场现状分析
二、欧洲工业互联网安全行业市场规模与市场需求分析
三、欧洲工业互联网安全行业市场前景分析
第六节 2022-2029年世界工业互联网安全行业分布走势预测
第七节 2022-2029年全球工业互联网安全行业市场规模预测

第三章 中国工业互联网安全行业产业发展环境分析
第一节我国宏观经济环境分析
第二节我国宏观经济环境对工业互联网安全行业的影响分析
第三节中国工业互联网安全行业政策环境分析
一、行业监管体制现状
二、行业主要政策法规
三、主要行业标准
第四节政策环境对工业互联网安全行业的影响分析
第五节中国工业互联网安全行业产业社会环境分析

第四章 中国工业互联网安全行业运行情况
第一节中国工业互联网安全行业发展状况情况介绍
一、行业发展历程回顾
二、行业创新情况分析
三、行业发展特点分析
第二节中国工业互联网安全行业市场规模分析
一、影响中国工业互联网安全行业市场规模的因素
二、中国工业互联网安全行业市场规模
三、中国工业互联网安全行业市场规模解析
第三节中国工业互联网安全行业供应情况分析
一、中国工业互联网安全行业供应规模
二、中国工业互联网安全行业供应特点
第四节中国工业互联网安全行业需求情况分析
一、中国工业互联网安全行业需求规模
二、中国工业互联网安全行业需求特点
第五节中国工业互联网安全行业供需平衡分析

第五章 中国工业互联网安全行业产业链和细分市场分析
第一节中国工业互联网安全行业产业链综述
一、产业链模型原理介绍
二、产业链运行机制
三、工业互联网安全行业产业链图解
第二节中国工业互联网安全行业产业链环节分析
一、上游产业发展现状

二、上游产业对工业互联网安全行业的影响分析
三、下游产业发展现状
四、下游产业对工业互联网安全行业的影响分析
第三节我国工业互联网安全行业细分市场分析
一、细分市场一
二、细分市场二

第六章 2018-2022年中国工业互联网安全行业市场竞争分析
第一节中国工业互联网安全行业竞争现状分析
一、中国工业互联网安全行业竞争格局分析
二、中国工业互联网安全行业主要品牌分析
第二节中国工业互联网安全行业集中度分析
一、中国工业互联网安全行业市场集中度影响因素分析
二、中国工业互联网安全行业市场集中度分析
第三节中国工业互联网安全行业竞争特征分析
一、企业区域分布特征
二、企业规模分布特征
三、企业所有制分布特征

第七章 2018-2022年中国工业互联网安全行业模型分析
第一节中国工业互联网安全行业竞争结构分析（波特五力模型）
一、波特五力模型原理
二、供应商议价能力
三、购买者议价能力
四、新进入者威胁
五、替代品威胁
六、同业竞争程度
七、波特五力模型分析结论
第二节中国工业互联网安全行业SWOT分析
一、SOWT模型概述
二、行业优势分析
三、行业劣势
四、行业机会
五、行业威胁
六、中国工业互联网安全行业SWOT分析结论

第三节中国工业互联网安全行业竞争环境分析（PEST）
一、PEST模型概述
二、政策因素
三、经济因素
四、社会因素
五、技术因素
六、PEST模型分析结论

第八章 2018-2022年中国工业互联网安全行业需求特点与动态分析
第一节中国工业互联网安全行业市场动态情况
第二节中国工业互联网安全行业消费市场特点分析
一、需求偏好
二、价格偏好
三、品牌偏好
四、其他偏好
第三节工业互联网安全行业成本结构分析
第四节工业互联网安全行业价格影响因素分析
一、供需因素
二、成本因素
三、其他因素
第五节中国工业互联网安全行业价格现状分析
第六节中国工业互联网安全行业平均价格走势预测
一、中国工业互联网安全行业平均价格趋势分析
二、中国工业互联网安全行业平均价格变动的影响因素

第九章 中国工业互联网安全行业所属行业运行数据监测
第一节中国工业互联网安全行业所属行业总体规模分析
一、企业数量结构分析
二、行业资产规模分析
第二节中国工业互联网安全行业所属行业产销与费用分析
一、流动资产
二、销售收入分析
三、负债分析
四、利润规模分析
五、产值分析

第三节中国工业互联网安全行业所属行业财务指标分析
一、行业盈利能力分析
二、行业偿债能力分析
三、行业营运能力分析
四、行业发展能力分析

第十章 2018-2022年中国工业互联网安全行业区域市场现状分析
第一节中国工业互联网安全行业区域市场规模分析
一、影响工业互联网安全行业区域市场分布的因素
二、中国工业互联网安全行业区域市场分布
第二节中国华东地区工业互联网安全行业市场分析
一、华东地区概述
二、华东地区经济环境分析
三、华东地区工业互联网安全行业市场分析
（1）华东地区工业互联网安全行业市场规模
（2）华南地区工业互联网安全行业市场现状
（3）华东地区工业互联网安全行业市场规模预测
第三节华中地区市场分析
一、华中地区概述
二、华中地区经济环境分析
三、华中地区工业互联网安全行业市场分析
（1）华中地区工业互联网安全行业市场规模
（2）华中地区工业互联网安全行业市场现状
（3）华中地区工业互联网安全行业市场规模预测
第四节华南地区市场分析
一、华南地区概述
二、华南地区经济环境分析
三、华南地区工业互联网安全行业市场分析
（1）华南地区工业互联网安全行业市场规模
（2）华南地区工业互联网安全行业市场现状
（3）华南地区工业互联网安全行业市场规模预测
第五节华北地区工业互联网安全行业市场分析
一、华北地区概述
二、华北地区经济环境分析
三、华北地区工业互联网安全行业市场分析

（1）华北地区工业互联网安全行业市场规模
（2）华北地区工业互联网安全行业市场现状
（3）华北地区工业互联网安全行业市场规模预测
第六节东北地区市场分析
一、东北地区概述
二、东北地区经济环境分析
三、东北地区工业互联网安全行业市场分析
（1）东北地区工业互联网安全行业市场规模
（2）东北地区工业互联网安全行业市场现状
（3）东北地区工业互联网安全行业市场规模预测
第七节西南地区市场分析
一、西南地区概述
二、西南地区经济环境分析
三、西南地区工业互联网安全行业市场分析
（1）西南地区工业互联网安全行业市场规模
（2）西南地区工业互联网安全行业市场现状
（3）西南地区工业互联网安全行业市场规模预测
第八节西北地区市场分析
一、西北地区概述
二、西北地区经济环境分析
三、西北地区工业互联网安全行业市场分析
（1）西北地区工业互联网安全行业市场规模
（2）西北地区工业互联网安全行业市场现状
（3）西北地区工业互联网安全行业市场规模预测
第九节 2022-2029年中国工业互联网安全行业市场规模区域分布预测

第十一章 工业互联网安全行业企业分析（随数据更新有调整）
第一节企业
一、企业概况
二、主营产品
三、运营情况
1、主要经济指标情况
2、企业盈利能力分析
3、企业偿债能力分析
4、企业运营能力分析

5、企业成长能力分析
四、公司优势分析
第二节企业
一、企业概况
二、主营产品
三、运营情况
四、公司优劣势分析
第三节 企业
一、企业概况
二、主营产品
三、运营情况
四、公司优势分析
第四节 企业
一、企业概况
二、主营产品
三、运营情况
四、公司优势分析
第五节 企业
一、企业概况
二、主营产品
三、运营情况
四、公司优势分析
``` ```

第十二章 2022-2029年中国工业互联网安全行业发展前景分析与预测
第一节中国工业互联网安全行业未来发展前景分析
一、工业互联网安全行业国内投资环境分析
二、中国工业互联网安全行业市场机会分析
三、中国工业互联网安全行业投资增速预测
第二节中国工业互联网安全行业未来发展趋势预测
第三节中国工业互联网安全行业规模发展预测
一、中国工业互联网安全行业市场规模预测
二、中国工业互联网安全行业市场规模增速预测
三、中国工业互联网安全行业产值规模预测
四、中国工业互联网安全行业产值增速预测
```

五、中国工业互联网安全行业供需情况预测
第四节中国工业互联网安全行业盈利走势预测

第十三章 2022-2029年中国工业互联网安全行业进入壁垒与投资风险分析
第一节中国工业互联网安全行业进入壁垒分析
一、工业互联网安全行业资金壁垒分析
二、工业互联网安全行业技术壁垒分析
三、工业互联网安全行业人才壁垒分析
四、工业互联网安全行业品牌壁垒分析
五、工业互联网安全行业其他壁垒分析
第二节工业互联网安全行业风险分析
一、工业互联网安全行业宏观环境风险
二、工业互联网安全行业技术风险
三、工业互联网安全行业竞争风险
四、工业互联网安全行业其他风险
第三节中国工业互联网安全行业存在的问题
第四节中国工业互联网安全行业解决问题的策略分析

第十四章 2022-2029年中国工业互联网安全行业研究结论及投资建议
第一节观研天下中国工业互联网安全行业研究综述
一、行业投资价值
二、行业风险评估
第二节中国工业互联网安全行业进入策略分析
一、目标客户群体
二、细分市场选择
三、区域市场的选择
第三节 工业互联网安全行业营销策略分析
一、工业互联网安全行业产品策略
二、工业互联网安全行业定价策略
三、工业互联网安全行业渠道策略
四、工业互联网安全行业促销策略
第四节观研天下分析师投资建议
图表详见报告正文·····

详细请访问：https://www.chinabaogao.com/baogao/202211/618061.html