2024年中国物联网安全行业概览

解除网络威胁，物联网的智能守护

企业标签：青莲云、梆梆安全

China IoT Security Industry

中国ユビキタスネットワークセキュリティ産業

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
ruowei.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：13080197867（李先生）

深圳市华润置地大厦E座4105室

摘要

物联网安全行业正迎来快速发展期。安全架构需多层次保障，以应对从感知网络层到应用层的各类威胁，确保设备、数据的安全与可靠。中国市场规模持续增长，预计至2027年将达数百亿元，主要得益于物联网普及、安全需求增加和技术进步。产业链上游竞争激烈，传感器制造等技术创新不断；中游云服务厂商、运营商和安全领域厂商等角色多样，商业模式丰富，定制化服务备受青睐；下游物联网安全应用广泛，金融、物流、零售等行业渗透率高，中小城市和新兴领域发展空间广阔。国家政策鼓励与规范并行，推动行业健康发展。设备攻击频发，促使安全技术持续进步，AI、大数据等技术应用显著提升防御能力。未来，行业将注重设计阶段安全，构建多层次防御体系，并利用AI、边缘计算和5G技术提升安全性能。竞争格局激烈，由电信运营商主导，多家企业共同推动技术创新和市场拓展。

- **中国物联网安全市场规模持续增长，预计2027年将达438亿元，复合增速达28.7%**

中国物联网安全市场规模的显著增长主要归因于物联网技术的普及和网络安全事件的频发。2022年市场规模已达124亿元，同比增长33.8%。随着物联网设备与系统数量的激增，对安全保护的需求也同步增加。同时，企业和个人对物联网安全的重视度提升，推动了市场的发展。技术进步，特别是人工智能、大数据、云计算在物联网安全领域的广泛应用，提供了高效解决方案，增强了市场竞争力。

- **物联网安全行业竞争激烈，三大电信运营商主导市场，多家企业凭技术创新和市场拓展共推发展**

物联网安全市场参与者众多，其中中国移动、中国电信、中国联通等三大电信运营商凭借庞大的用户基础和技术积累占据主导。同时，青莲云、奇安信、绿盟科技等第二梯队公司，以及华为、海康威视等第三梯队企业，也通过各自的专业技术和解决方案，在物联网安全领域提供全面保障。例如，绿盟科技专注物联网准入网关研发，安恒信息提供全生命周期安全防护体系，共同推动行业发展。

头豹 LeadLeo www.leadleo.com 400-072-5588

内容目录

研究目标

研究目的

了解物联网安全的技术演变、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物联网安全行业、业务场景以判断行业发展趋势。

研究目标

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

本报告的关键问题

- 中国企业物联网安全行业市场规模情况如何？未来增长情况如何？
- 竞争格局：中国打造物联网安全的企业有哪些？哪些企业更具备发展潜力与优势？
- 发展趋势：中国物联网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

- **感知层：**物联网体系架构中的一个关键组成部分，它位于物联网三层结构中的最底层，具有“感知”环境信息的功能。
- **网络层：**计算机网络体系结构中的一层，主要负责数据包的路由和转发，位于传输层和数据链路层之间。
- **应用层：**计算机网络体系结构中最靠近用户的一层，它直接为用户的应用进程提供服务。应用层协议定义了应用进程间通信和交互的规则，包括交互的内容、交互的方式等。
- **弱口令：**通常指的是那些容易被猜测到或被破解的密码。这些密码通常缺乏足够的复杂性和强度，因此无法提供足够的安全保障。
- **提权：**指提高自己在服务器中的权限的过程。在网络攻击或黑客入侵的场景中，这通常意味着通过利用系统或应用程序的漏洞，使原本具有较低权限的攻击者能够获取更高的权限，从而实现对目标系统的更深度控制。
- **DoS：**全称为Denial-of-Service，并不是指磁盘操作系统（Disk Operating System），而是计算机网络中的一种攻击方式。
- **中间人攻击：**（Man-in-the-Middle Attack，简称MITM攻击）是一种网络安全威胁，它涉及攻击者在两个通信方之间秘密地拦截和转发消息，使双方误以为他们正在直接通信。
- **无线模组：**一种将芯片、存储器、功放器件等集成在一块线路板上的功能模块，它提供标准接口，使各类终端能够借助其实现通信或定位功能。
- **蜂窝物联网芯片：**一种基于运营商网络系统的通信连接芯片，主要用于对无线信号进行调制与解调。
- 它是一种核心芯片，将物理设备（如传感器）与互联网连接起来，使这些设备能够搭载在与智能手机相同的移动网络上进行通信。
- **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。

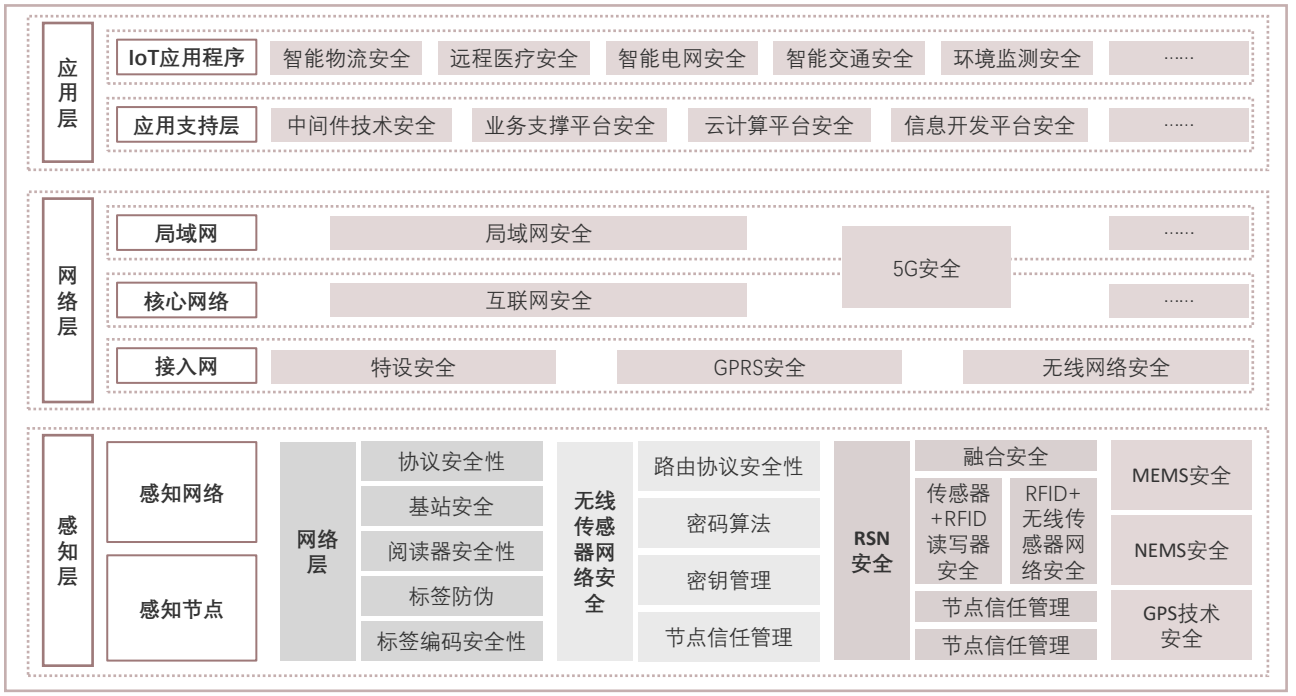
Chapter 1
行业综述

- 定义：物联网安全架构需多层次保障，从感知网络层到应用层均需采取安全措施，确保设备安全、数据传输可靠，并保护用户数据隐私，确保IoT应用的安全性和可靠性
- 安全隐患：物联网安全威胁遍布各架构层与端点，需加强数据加密、身份验证、访问控制等措施，确保数据、网络及设备的安全，抵御物理攻击、数据篡改等风险
- 发展历程：物联网技术从萌芽到成熟，经历了从特定领域应用到全球性安全标准的制定，安全问题日益凸显，国际合作加强，推动物联网行业向更安全、更可靠的方向发展
- 市场规模：中国物联网安全市场规模持续增长，得益于物联网普及、安全需求增加和技术进步。预计随着技术发展和应用场景扩展，物联网安全市场将迎来更广阔发展空间

中国物联网安全行业综述——物联网安全定义

- 物联网安全架构需多层次保障，从感知网络层到应用层均需采取安全措施，确保设备安全、数据传输可靠，并保护用户数据隐私，确保IoT应用的安全性和可靠性

物联网安全架构图



■ **物联网安全架构是一个综合性的系统，涉及多个层次和方面，从感知网络层到IoT应用程序层，每个层次都需要采取相应的安全措施**

在感知网络层，包括传感器、RFID（无线射频识别）等技术，需要确保这些设备的物理安全和数据传输的机密性、完整性和可用性。为此，可以采取一系列安全措施，如加密技术、密钥管理、节点信任管理等。此外，对于RFID技术，还需要特别关注标签防伪和编码安全性。

在网络层，包括局域网、核心网络和接入网等，需要确保数据传输的可靠性和安全性。这涉及到网络安全协议的选择、网络攻击的检测和防御、数据的加密传输等方面。特设安全、GPRS安全、5G安全和无线网络安全等技术可以提供不同层次的安全保障。

在应用支持层，包括中间件技术安全、业务支撑平台安全、云计算平台安全等。这些平台和应用需要确保数据的机密性、完整性和可用性，同时还要防范各种网络攻击和威胁。密码算法、访问控制等技术可以在这一层次提供安全保障。

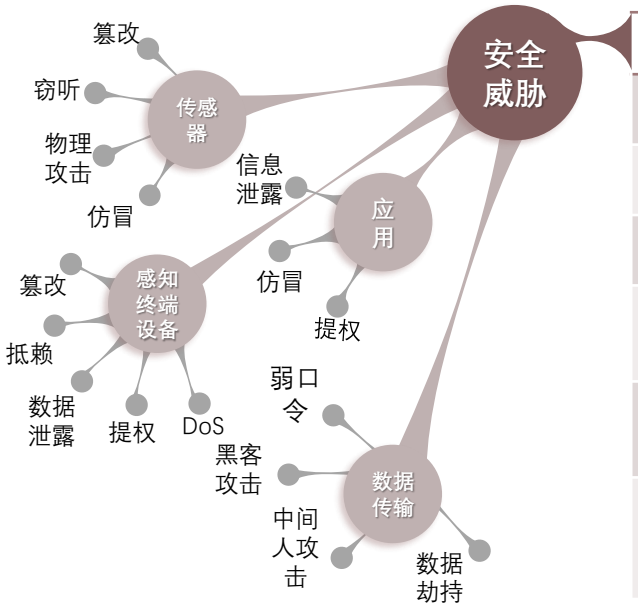
在IoT应用程序层，涵盖了智能物流、远程医疗、智能电网、智能交通和环境监测等领域。在这些领域，物联网安全架构需要确保应用程序的安全性和可靠性，保护用户数据的隐私和安全。例如，在远程医疗中，需要确保医疗数据的机密性和完整性，防止数据泄露和被篡改。

来源：专家访谈、头豹研究院

中国物联网安全行业综述——物联网安全隐患

- 物联网安全威胁遍布各架构层与端点，需加强数据加密、身份验证、访问控制等措施，确保数据、网络及设备的安全，抵御物理攻击、数据篡改等风险

物联网安全威胁地图



安全特性	设备/硬件侧	网络侧	云/服务器侧
机密性	硬件攻击	低计算能力设备的加密	隐私
完整性	缺乏证明，非法升级	低计算能力设备的签名	数据丢失
可用性	物理攻击，无线阻塞	网络不可靠	身份验证缺失
认证	缺乏用户输入，硬件导出密钥	联合身份认证的挑战	缺乏设备识别实施标准
访问控制	物理访问，缺乏本地授权	访问控制的轻量协议	需要用户管理访问控制
不可抵赖性	没有安全的本地存储低计算能力设备	低计算能力设备的签名	没有完整的日志记录

- **物联网安全威胁分布于各架构层与端点，应用层需保护数据机密性、完整性与可用性；感知层需应对物理攻击与数据篡改；云端需防范数据泄露与非法访问；网络层需确保数据传输安全；设备端需强化物理与硬件防护**

从不同物联网架构层来看，在物联网的应用层，安全威胁可能涉及到数据的机密性、完整性和可用性。例如，数据可能被非法访问、篡改或丢失。应用层的安全特性可能包括数据加密、用户身份验证和访问控制等，以确保数据的安全传输和存储。而传感器作为物联网的感知层，其安全威胁主要来自于物理攻击、窃听和数据篡改。由于传感器通常具有较低的计算能力，因此它们可能更容易受到攻击。安全特性可能包括硬件加密、物理防护和固件签名等，以提高传感器的安全性。感知设备层包含了各种用于感知和识别环境信息的设备。主要的威胁可能包括信息的完整性破坏、设备仿冒等。针对这些威胁，需要采取数据加密、设备签名等措施来确保信息的完整性和设备的真实性。

从不同端来看，在云端，物联网安全威胁主要包括数据泄露、非法访问和攻击。由于云端存储了大量敏感数据，因此安全特性需要特别强大，包括数据加密、访问控制、入侵检测和防御等。网络层的安全威胁主要涉及到数据传输的可靠性和安全性。可能的威胁包括网络不可靠、无线阻塞和数据劫持等。为了应对这些威胁，网络层的安全特性可能包括加密传输、身份验证和访问控制等。设备端的安全威胁则可能包括物理攻击、硬件攻击和数据篡改等。由于设备可能直接与用户交互，因此其安全性至关重要。安全特性可能包括硬件加密、物理防护和固件签名等，以确保设备的完整性和安全性。

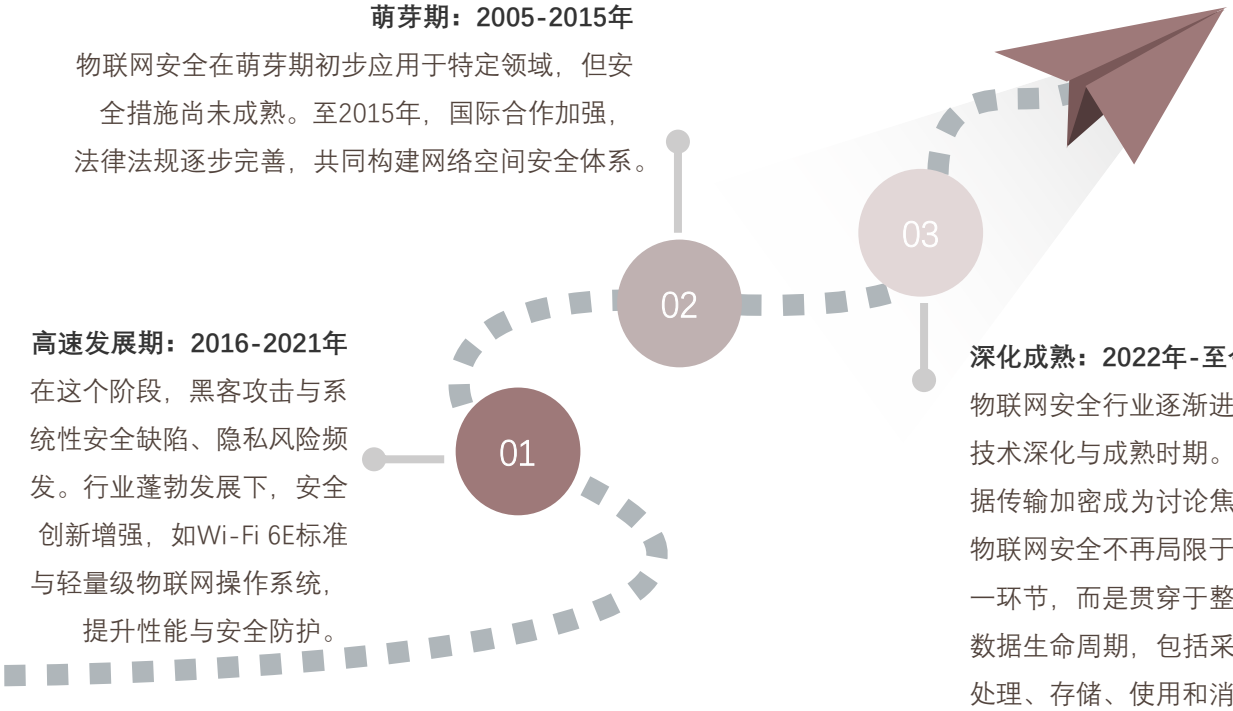
来源：专家访谈、头豹研究院

中国物联网安全行业综述——发展历程

- 物联网技术从萌芽到成熟，经历了从特定领域应用到全球性安全标准的制定，安全问题日益凸显，国际合作加强，推动物联网行业向更安全、更可靠的方向发展

中国物联网安全发展历程，2005年-至今

萌芽期：2005-2015年
物联网安全在萌芽期初步应用于特定领域，但安全措施尚未成熟。至2015年，国际合作加强，法律法规逐步完善，共同构建网络空间安全体系。



高速发展期：2016-2021年
在这个阶段，黑客攻击与系统性安全缺陷、隐私风险频发。行业蓬勃发展下，安全创新增强，如Wi-Fi 6E标准与轻量级物联网操作系统，提升性能与安全防护。

深化成熟：2022年-至今
物联网安全行业逐渐进入技术深化与成熟时期。数据传输加密成为讨论焦点。物联网安全不再局限于单一环节，而是贯穿于整个数据生命周期，包括采集、处理、存储、使用和消费等各个阶段。

- **萌芽阶段：**2005年，国际电信联盟（ITU）在一次国际性峰会上首次明确了物联网概念，这标志着物联网技术的萌芽期开始。在这个阶段，物联网技术开始在一些特定领域得到应用，如工业园区、智能家居等，但安全措施尚未形成体系。2015年，中国在网络安全领域与多个国家开展了合作，并主张“各国加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体”。
- **高速发展期：**在这个阶段，随着物联网设备的普及和应用，物联网安全问题开始受到更多关注，黑客攻击事件频发，物联网设备的系统性安全缺陷和隐私风险成为热点话题。2019年1月份，安全研究人员发现沃尔玛和百思买等大型零售商销售的热门联网或智能家居设备普遍存在严重安全漏洞和隐私问题。2020年，中国物联网行业迎来了蓬勃发展期，Wi-Fi 6E标准公布，推动物联网行业快速发展。
- **深化成熟阶段：**随着物联网设备的普及，行业开始完善安全标准的制。2023年，国际电联（ITU）发布了全球物联网安全标准，旨在提高物联网设备的安全性和可靠性，物联网安全行业逐渐进入技术深化与成熟时期。数据传输加密成为讨论焦点。

来源：专家访谈、头豹研究院

中国物联网安全行业综述——市场规模

- 中国物联网安全市场规模持续增长，得益于物联网普及、安全需求增加和技术进步。预计随着技术发展和应用场景扩展，物联网安全市场将迎来更广阔发展空间

中国物联网安全市场规模，2018-2027年预测

完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

物联网安全市场规模测算逻辑

来源：专家访谈、头豹研究院

- **2022年中国物联网安全市场规模达到124亿元，同比增长33.8%，预计2027年将达到438亿元，2022-2027年期间复合增速为28.7%**

中国物联网安全市场规模的增长，主要得益于以下几个方面的原因。首先，随着物联网技术的不断普及和应用，越来越多的设备和系统接入到网络中，这些设备和系统产生的海量数据需要得到有效的保护和管理，这为物联网安全市场带来了巨大的需求。其次，随着网络安全事件的频发，企业和个人对物联网安全的认识和重视程度不断提高，这进一步推动了物联网安全市场的发展。

此外，技术的进步也为物联网安全市场提供了有力支持。研究人员和企业正在从静态分析、动态模糊测试到同源性分析等多个方面进行深入研究，以发现和修复潜在的安全漏洞。同时，人工智能、大数据、云计算等技术的快速发展为物联网安全提供了更加高效的解决方案。这些技术的应用使得物联网设备的安全监测、威胁预警和应急响应更加高效和准确，进一步提升了物联网安全市场的竞争力。

总的来说，中国物联网安全市场规模的增长是一个必然趋势。随着技术的不断进步和应用场景的不断扩展，物联网安全市场将迎来更加广阔的发展空间。

Chapter 2
产业链分析

- 产业链图谱：中国物联网安全行业的产业链上游为硬件供应商和软件提供商，中游为云服务厂商、运营商、安全领域厂商和硬件厂商，下游则为物联网安全的终端用户
- 上游发展概述：物联网芯片市场竞争激烈，传感器制造集中化且技术创新推动行业发展，无线模组技术多样，应用场景不断拓展，特别是在智慧物流领域展现出高效智能的潜力
- 中游商业模式：物联网安全厂商商业模式多样，定制化服务受市场青睐，年度购买模式因公有云普及而减少，一次性买断模式因缺乏灵活性而占比下降
- 下游行业场景：物联网安全应用在各行业差异显著，一线城市及头部机构应用广泛，中小城市和新兴领域发展空间大，金融、物流、零售行业渗透率较高

中国物联网安全产业链分析——产业链图谱

- 中国物联网安全行业的产业链上游为硬件供应商和软件提供商，中游为云服务厂商、运营商、安全领域厂商和硬件厂商，下游则为物联网安全的终端用户

中国物联网安全行业产业链图谱

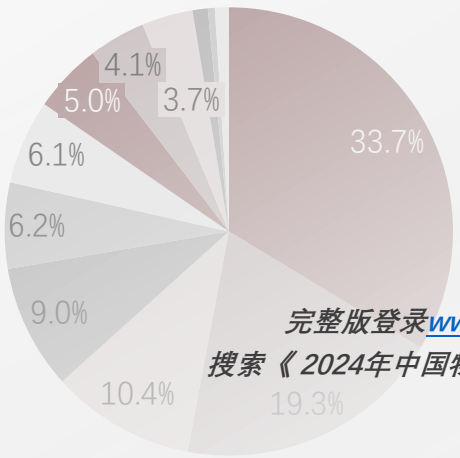
完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

来源：专家访谈、头豹研究院

中国物联网安全产业链上游分析——发展概述

- 物联网芯片市场竞争激烈，传感器制造集中化且技术创新推动行业发展，无线模组技术多样，应用场景不断拓展，特别是在智慧物流领域展现出高效智能的潜力

全球蜂窝物联网芯片出货量市场份额，2022年

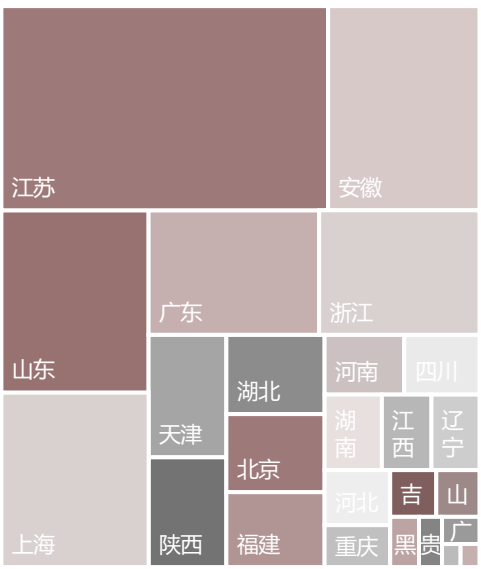


完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

■ 全球蜂窝物联网芯片市场竞争激烈，主要厂商如

全球蜂窝物联网芯片市场的份额分布相对较为
和品牌影响力，在市场上占据了重要的地
其中，高通占据了33.7%的市场份额
还有许多其他厂商也在这个市

传感器制造企业分布情况及技术发展趋势，2023年



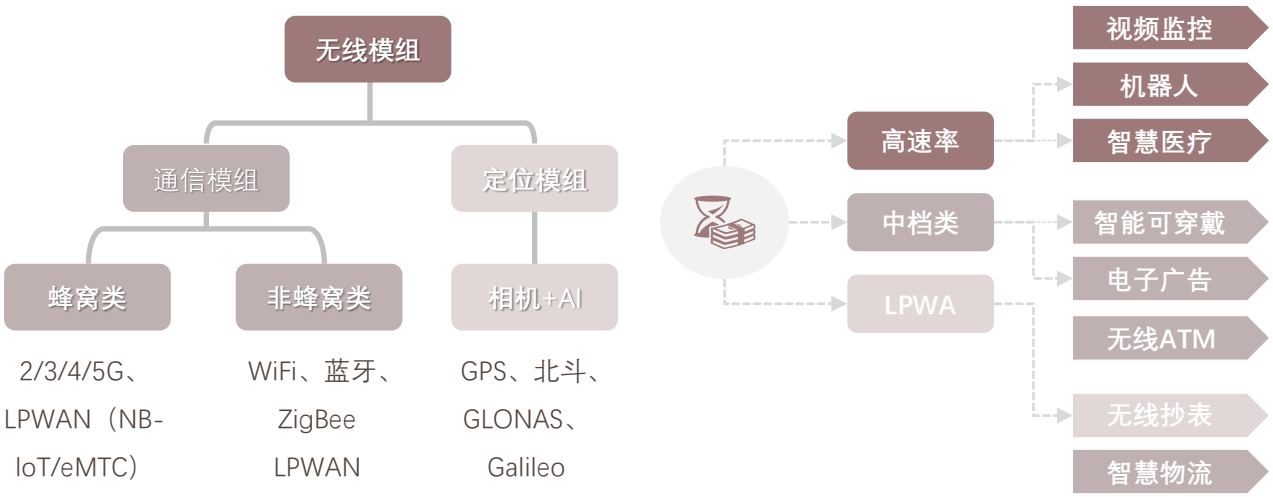
来源：专家访谈、电子工程世界、宝通集团、头豹研究院

（接上页——上游发展概述）

- **传感器制造行业在江苏、安徽等地集中，得益于产业链、政策和人才优势。技术发展正迈向系统化、创新化、微型化、智能化和无源化，推动行业持续进步，提供更先进、可靠的解决方案**

目前，江苏、安徽、广东、浙江、山东等省份是中国传感器制造行业较为集中的地区。通常，这样的行业集中与当地的产业链完善、政策支持、人才储备等因素有关。而从技术发展来看，传感器技术正朝着更加系统化、创新化、微型化、智能化和无源化的方向发展。随着计算机技术和通信技术的不断进步，传感器不再孤立存在，而是融入更大的系统中，实现数据的采集、处理和分析一体化。同时，新原理、新效应和新技术的运用不断推动传感器技术的创新，为企业带来更高性能、更低成本的产品。微型化技术使得传感器尺寸大幅缩小，功能更加集成，而智能化则赋予传感器记忆、存储、思维、判断和自诊等高级功能。此外，无源化传感器的发展使得设备无需外部电源即可工作，极大地拓宽了传感器的应用范围。

无信模组分类及应用场景，2024年



- **无线模组技术多样，广泛应用于多个领域，并随着技术发展不断拓展应用场景，尤其在智慧物流领域结合AI技术，为行业带来更高效智能的解决方案**

无线模组广泛应用于视频监控、机器人、高速率通信和智慧医疗等领域，以满足不同场景下的数据传输需求。而通信模组则进一步细分为定位模组和中档类，定位模组主要服务于位置跟踪和定位服务，而中档类则涵盖了智能可穿戴设备、电子广告等多个领域。在技术方面，蜂窝类技术如2/3/4/5G、WiFi、蓝牙和GPS等，以及非蜂窝类技术如LPWAN（NB-IoT/eMTC）、ZigBee、GLONAS等，共同构成了无信模组的技术基础。特别是LPWAN技术，以其低功耗、广覆盖的特点，在无信模组中占据重要地位。

此外，随着技术的不断发展，无信模组的应用场景也在不断扩大。例如，智慧物流作为新的应用场景，对无信模组的需求也在不断增长。通过相机+AI等技术的结合，无信模组在物流领域的应用将更加广泛，为物流行业带来更高效、智能的解决方案。

来源：专家访谈、电子工程世界、宝通集团、头豹研究院

中国物联网安全产业链中游分析——商业模式

- 物联网安全厂商商业模式多样，定制化服务受市场青睐，年度购买模式因公有云普及而减少，一次性买断模式因缺乏灵活性而占比下降

物联网安全厂商商业模式，2023年

- **物联网安全厂商商业模式多样，包括一次性买断、定制化服务和年度购买，定制化服务受青睐，而公有云服务普及下年度购买模式逐渐减少**

物联网安全厂商的商业模式主要包括一次性买断模式、定制化服务模式和年度购买模式。一次性买断模式占据总销售额的20%，安全厂商将安全组件集成到智能设备中，用户在购买设备时即获得了内置的安全保护。这种模式类似于传统的软件销售，用户一次性支付费用后拥有长期使用权。然而，随着技术的发展和市场需求的变化，这种模式的占比逐渐减少，因为它缺乏灵活性和更新升级的便利性。

其次为定制化服务模式，比例为40%，它针对云环境中的安全需求，由安全厂商提供定制化的安全解决方案。这是当前市场上较为流行的模式，特别是针对大型企业和有一定规模的公司。安全厂商提供基于云的安全解决方案，这些方案可以根据企业的具体需求进行定制。

年度购买模式占比则为40%，通常按照服务内容和服务级别进行收费，这种模式更适合传统的私有云或传统机房部署的用户。企业会购买硬件设备和软件许可，有时还会包括额外的服务支持。但随着公有云服务的普及和成本效益的提升，这种模式正在逐渐减少。

来源：专家访谈、头豹研究院

中国物联网安全产业链中游分析——参与厂商类型

- 物联网安全领域参与者多样，包括电信运营商、安全公司、设备制造商和云服务厂商等，它们共同构建安全生态系统，推动技术创新和标准制定，保障物联网安全发展

物联网安全参与厂商类型，2023年

来源：专家访谈、头豹研究院

中国物联网安全产业链下游分析——行业场景

- 物联网安全应用在各行业差异显著，一线城市及头部机构应用广泛，中小城市和新兴领域发展空间大，金融、物流、零售行业渗透率较高

物联网安全在部分行业的应用，2023年

完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

■ **物联网安全在不同行业的应用情况呈现出多样化的特点，在金融、物流和零售等行业应用渗透率较高**

在金融领域，尽管存在饱和趋势，但并非所有城市银行都已达到100%的应用渗透率，整体渗透率约在90%。金融监管机构对银行业有特定的安全要求，因此监控和审计措施普遍存在于柜台等关键区域。

医疗行业方面，一线城市的社区健康服务中心（社康）由于需求增长，其物联网安全应用正在逐步增加，尤其是在终端设备的自动化和智能化方面。然而，整体渗透率仍处于发展阶段，约在50%左右，主要集中在一线城市和头部机构。

物流行业的快递柜应用已接近饱和，但物流园区的物联网安全应用才刚刚开始，预计渗透率在85%左右，主要集中在快递柜的应用上。零售行业的自动化设备如自动贩卖机与物流行业共享基础设施，其应用渗透率较高，约在85%左右。

政府及政务相关领域的物联网安全应用在一二线城市较为成熟，智慧城市建设中已有较多安全考量。但在二三线及以下城市，由于财政限制和实际需求尚未完全满足，物联网安全的应用渗透率较低，初次购买需求减少，更多的是年度维护或置换需求。在一线城市，渗透率可能超过90%以上，而在三四线城市则相对较低，因此在城市整体的渗透率约为60%。

综上所述，物联网安全在各行业的应用渗透率差异较大，一线城市及头部机构的应用更为广泛和深入，而中小城市和新兴领域仍有较大的发展空间。

来源：专家访谈、电子工程世界、宝通集团、头豹研究院

中国物联网安全产业链下游分析——智能摄像头

- 中国消费级监控摄像头市场销量稳步增长，但物联网安全问题凸显。需加强安全意识和防御体系，采取更新固件、更改密码等措施提高摄像头安全性，政府和行业协会应推动标准化和认证，确保产品安全

中国消费级监控摄像头市场销量，2020-2023年

完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

中国消费级监控摄像头市场销量稳步增长，但物联网安全问题日益严重，智能摄像头存在多种安全漏洞，需加强安全意识并采取相应安全措施，确保产品安全

中国消费级监控摄像头市场销量呈现出稳定的增长趋势。从2020年到2023年，该市场的销量逐年上升。2020年销量为4,039万台，而到了2021年，销量增长至4,590万台，同比增长率达到13.6%。2022年，销量进一步增长至4,820万台，在2023年，销量达到5,343万台，同比增长率升至10.9%。其中，2023年线上市场的消费级摄像头销量为2,663万台，占到全渠道的49.9%。小米位居线上监测市场的首位，销量占比为15.9%。

然而，随着摄像头在各家各户的普及，摄像头行业的物联网安全问题日益凸显，成为全球共同面临的重要挑战。智能摄像头作为物联网产品之一，其安全漏洞多种多样，包括远程弱口令、预置后门、敏感信息泄露等。例如，中国深圳的一家厂商生产的智能摄像头就曝出了远程侵入漏洞，影响了至少17.5万设备。此外，通过Kalay平台发现的漏洞导致数百万物联网设备暴露在外。这些漏洞不仅使摄像头容易被黑客控制，还可能导致隐私泄露和数据窃取。据调查，19.5%的智能摄像机存在常见安全漏洞，其中远程弱口令漏洞占比最高，为91.7%。很多摄像头在出厂时采用默认密码，极易被黑客攻破。此外，有不法分子利用一些智能摄像头存在的安全漏洞，窥视他人家庭隐私生活，录制后在网上公开贩卖

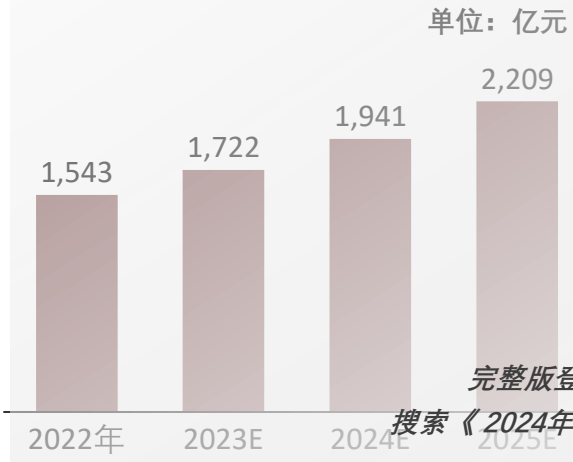
为了应对这一问题，需要多方联防联治，构建立体防御体系，以确保智能摄像头的安全。专家建议加强视频监控系统使用者的安全意识，并联合各方尽快采取相应安全措施。例如，可以通过更新固件、更改默认密码、使用加密传输等方式来提高摄像头的安全性。

来源：专家访谈、洛图科技、上海安防、头豹研究院

中国物联网安全产业链下游分析——智能园区

- 中国智慧园区行业市场规模持续增长，但物联网安全问题凸显。为保障园区安全，需强化安全管理和技术创新，并在园区建设初期将物联网设备和系统集成到基础设施中，实现高效、安全的智慧园区建设

中国智慧园区行业规模，2022-2025年预测



某园区大数据安全管理中心遭受的攻击，2023年

完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

智慧园区合作价格与市场零售价对比，2023年

■ **中国智慧园区行业市场规模稳步增长，但物联网安全问题凸显，需加强安全管理和技术创新来保障园区安全**

从2022年至2025年，中国智慧园区行业的市场规模呈现稳步增长的趋势。具体来看，2022年的市场规模为1,543亿元。受益于技术的不断进步和政策的支持，预计未来几年仍将保持增长态势。预计到2025年，中国智慧园区市场规模预计将达到2,209亿元。

然而，物联网安全问题不容忽视。首先，物联网终端和数据的海量性、多种数据协议和接入方式带来了复杂的安全风险，任何一个层面的缺陷都可能导致严重威胁。其次，DDoS攻击等网络攻击手段对物联网设备和基础设施构成了巨大挑战，需要通过网络流量监测、入侵检测系统和云端防护等手段进行应对。

因此，在园区建设初期，就需将物联网设备和系统集成到建筑和基础设施中，如智能照明、能源管理、安防监控等，这样可以确保设备的最佳布局和系统的无缝对接。通过与设备制造商直接合作，可以获得较低的成本价格。与市场零售价相比，合作伙伴能够以4到5倍的价格优势采购设备，这对于大规模的园区建设来说具有显著的经济效益。

来源：专家访谈、头豹研究院

Chapter 3
行业分析

- 政策分析：近年来，国家出台了一系列物联网安全相关政策，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
- 发展驱动力：物联网设备攻击频发，企业和个人愈发重视安全，推动安全技术发展。静态分析、动态测试等技术结合AI、大数据等，显著提升物联网安全，推动行业进步
- 发展趋势：中国物联网安全行业将重视设计阶段安全、构建多层次防御体系，利用AI提升预警与响应，持续审计与更新，以及利用边缘计算和5G技术提升性能，确保物联网设备的安全性和响应效率
- 竞争格局：物联网安全行业竞争激烈，由电信运营商主导，辅以专业厂商。中国移动等技术领先者凭借技术和用户基础引领行业发展，众多企业共同推动物联网安全领域的技术创新和市场拓展

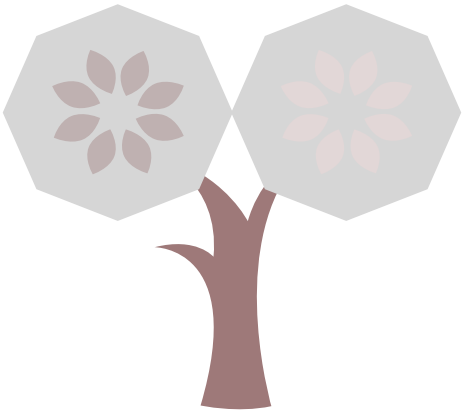
中国物联网安全行业分析——政策分析

- 近年来，国家出台了一系列物联网安全相关政策，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

中国物联网安全相关政策梳理，2021-2023年

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。



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。

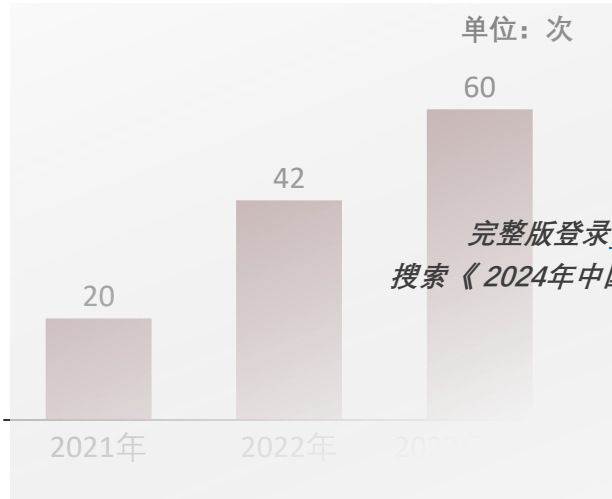
政策名称	颁布日期	颁布主体	主要内容及影响
《数字中国发展报告（2022年）》	2023-05	国家网信办	2022年，网络安全法律法规和标准体系逐步健全、网络安全防护能力大幅提升、网络安全产业规模同比增长13.9%、数据安全管理和个人信息保护有力推进。
《关于调整网络安全专用产品安全管理有关事项的公告》	2023-04	国家网信办、工信部、公安部、财政部、认监委	规定网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。
《电力行业网络安全等级保护管理办法》	2022-11	国家能源局	明确了电力行业网络安全保护等级划分和等级保护工作原则，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

中国物联网安全行业分析——发展驱动力

- 物联网设备攻击频发，企业和个人愈发重视安全，推动安全技术发展。静态分析、动态测试等技术结合AI、大数据等，显著提升物联网安全，推动行业进步

全球物联网设备遭受攻击次数，2021-2023年



全球各洲物联网设备遭受攻击次数，2023年1-2月

完整版登录www.leadleo.com
搜索《2024年中国物联网安全行业概览》

物联网设备攻击频发，企业和个人日益重视其安全性，推动物联网安全技术发展。通过静态分析、动态模糊测试等技术手段，结合人工智能、大数据等先进技术，物联网安全得到显著提升，行业发展因此得到推动

随着物联网设备的广泛普及，近年来针对这些设备的网络攻击数量也呈现出不断攀升的态势。网络犯罪分子敏锐地察觉到物联网设备往往是网络中的薄弱环节，许多设备因缺乏适当的保护和管理而容易成为攻击目标。这些存在漏洞的物联网设备，如摄像头和打印机等无人管理的设备，为攻击者提供了可乘之机。一旦攻击者获取了直接访问权限和隐私信息，他们便能在企业网络内建立起初始立足点，进而在受损的网络中肆意妄为。

在2023年的前两个月，全球范围内每个机构平均每周遭受了近60次物联网设备攻击，这一数字相较于2022年增长了41%，更是两年前攻击数量的三倍多。这种攻击趋势在全球各个区域和行业中都有所体现。欧洲地区目前成为了物联网设备攻击的重灾区，平均每个机构每周要面对近70次此类攻击。亚太地区紧随其后，平均每周遭受64次攻击，而拉丁美洲地区为48次，北美洲地区虽然数量较少，但增幅最大，与2022年相比高达58%，平均每周有37次攻击。即便是非洲地区，每个机构平均每周也面临着34次物联网网络攻击。

随着物联网设备攻击事件的频发，企业和个人对物联网安全的认识和重视程度不断提高，这推动了物联网安全技术的研发和应用。研究人员和企业正在从静态分析、动态模糊测试到同源性分析等多个方面进行深入研究，以发现和修复潜在的安全漏洞。这些技术的进步不仅提高了物联网设备的安全性，也推动了整个行业的发展。而人工智能、大数据、云计算等技术的快速发展为物联网安全提供了有力支持。这些技术的应用使得物联网设备的安全监测、威胁预警和应急响应更加高效和准确。

来源：专家访谈、头豹研究院

中国物联网安全行业分析——发展趋势

- 中国物联网安全行业将重视设计阶段安全、构建多层次防御体系，利用AI提升预警与响应，持续审计与更新，以及利用边缘计算和5G技术提升性能，确保物联网设备的安全性和响应效率

中国物联网安全行业发展趋势，2023年

中国物联网安全行业发展趋势将聚焦于设计安全、多层次防御体系、AI应用提升预警与响应、持续安全审计与更新，以及利用边缘计算和5G技术提升性能，确保物联网设备的安全性、预警准确性和响应效率

首先，物联网安全的设计阶段将受到更多的关注。这意味着在物联网设备的初始设计过程中，安全性将成为关键考量因素，以确保设备从底层芯片到网络传输的各个层面都能得到全面的安全保护。其次，构建一个多层次的物联网安全防御体系变得至关重要。这包括身份验证、加密和更新机制等关键安全要素，以确保设备在面对潜在威胁时具备足够的防御能力。此外，随着人工智能技术的发展，AI在物联网安全领域的应用将越来越广泛。通过分析大量数据，AI能够识别潜在威胁并预测可能的设备行为异常，从而提高安全预警和响应的效率和准确性。再者，定期进行安全审计和更新是确保物联网设备长期安全的关键措施。随着物联网设备的不断增加和复杂性的提升，持续的安全监控和及时的更新修补将是保障设备安全性的必要手段。最后，随着边缘计算和5G技术的发展，物联网设备将能够实现更高效的数据处理和更快的响应时间。这将有助于提升物联网安全系统的性能和效率，使其在应对安全威胁时更加迅速和准确。

综上所述，中国物联网安全行业的发展趋势将更加注重设计阶段的安全性、构建多层次防御体系、利用人工智能技术提升安全预警和响应能力、加强持续的安全审计和更新以及利用边缘计算和5G技术提升安全系统的性能和效率。

来源：专家访谈、头豹研究院

中国物联网安全行业分析——竞争格局

- 物联网安全行业竞争激烈，由电信运营商主导，辅以专业厂商。中国移动等技术领先者凭借技术和用户基础引领行业发展，众多企业共同推动物联网安全领域的技术创新和市场拓展

中国物联网安全安全竞争格局

- **物联网安全行业参与者众多，包括传统的网络安全公司、物联网设备制造商、云服务提供商、电信运营商等，竞争激烈，市场集中于三大电信运营商**

物联网安全行业呈现以下梯队情况：第一梯队公司有中国移动、中国电信、中国联通等；第二梯队公司为青莲云、奇安信、绿盟科技、郴郴安全、安恒信息等；第三梯队有华为、海康威视等。物联网安全行业的竞争格局形成主要得益于多家企业和机构在技术和市场方面的积极布局。中国移动凭借其显著的技术实力和标准制定能力，率先在物联网安全领域提出创新的安全技术需求和安全架构，并通过提供多种安全产品和服务，如“和云盾”设备安全接入解决方案和获得CCRC EAL4+权威认证的OneOS物联网操作系统，展示了其在该领域的领先地位。同时，绿盟科技、安恒信息、青莲云和郴郴安全等企业也通过各自的专业技术和解决方案，为物联网安全提供了全面的保障。如绿盟科技专注于物联网准入网关的研发，通过设备主动探测发现、威胁实时报警等功能，结合机器学习算法和访问关系白名单技术，实现对网络行为的全面管控。安恒信息则以其全生命周期安全防护体系为特点，提出了综合性的物联网安全解决方案，有效应对物联网安全的核心痛点。此外，中国移动、中国联通和中国电信等电信运营商凭借庞大的物联网用户基础和技术积累，也在物联网安全领域展现出显著优势。这些电信运营商构建的广泛网络体系不仅提供了海量的数据资源，也为物联网安全解决方案的研发提供了有力支持。整体而言，物联网安全行业的竞争格局正在逐步形成，多家企业和机构通过技术创新和市场拓展，共同推动该领域的发展。

来源：专家访谈、头豹研究院

头豹 LeadLeo www.leadleo.com 400-072-5588

Chapter 4
典型厂商分析

- 青莲云
- 梆梆安全

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