亿欧智库

“中国智能电动汽车”

系列报告

“CHINA INTELLIGENCE ELECTRICAL VEHICLE” SERIES REPORT

2021中国智能网联汽车数据安全研究报告

亿欧智库 https://www.iyiou.com/research

亿欧智库

最懂中国智能电动汽车的第三方研究机构

目录

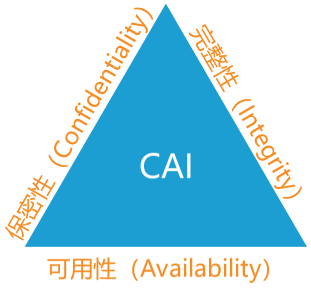
CONTENTS

中国智能网联汽车数据安全背景介绍

数据安全概念开始普及，中国市场规模逐年递增

◆ 广义的数据安全（Data Security），是基于“安全体系以数据为中心”的立场，泛指整个安全体系，侧重于数据分级及敏感数据全生命周期的保护。它以数据的安全收集（或生成）、安全使用、安全传输、安全存储、安全披露、安全转移与跟踪、安全销毁为目标，涵盖整个安全体系。数据安全也包括个人数据安全与法律合规，即隐私保护方面的内容。亿欧智库预计，2025年中国数据安全行业规模将达到181.5亿元。

亿欧智库：数据安全概念解析



数据安全：保障数据全生命周期的安全与处理合规

1、安全性

- 保密性 (Confidentiality)： 保障数据不被未授权的用户访问或泄露
- 可用性(Availability)：保障已授权用户合法访问数据的权利
- 完整性(Integrity)：保障数据不被未授权的篡改

2、处理合规

- 符合各项适用法律法规的要求

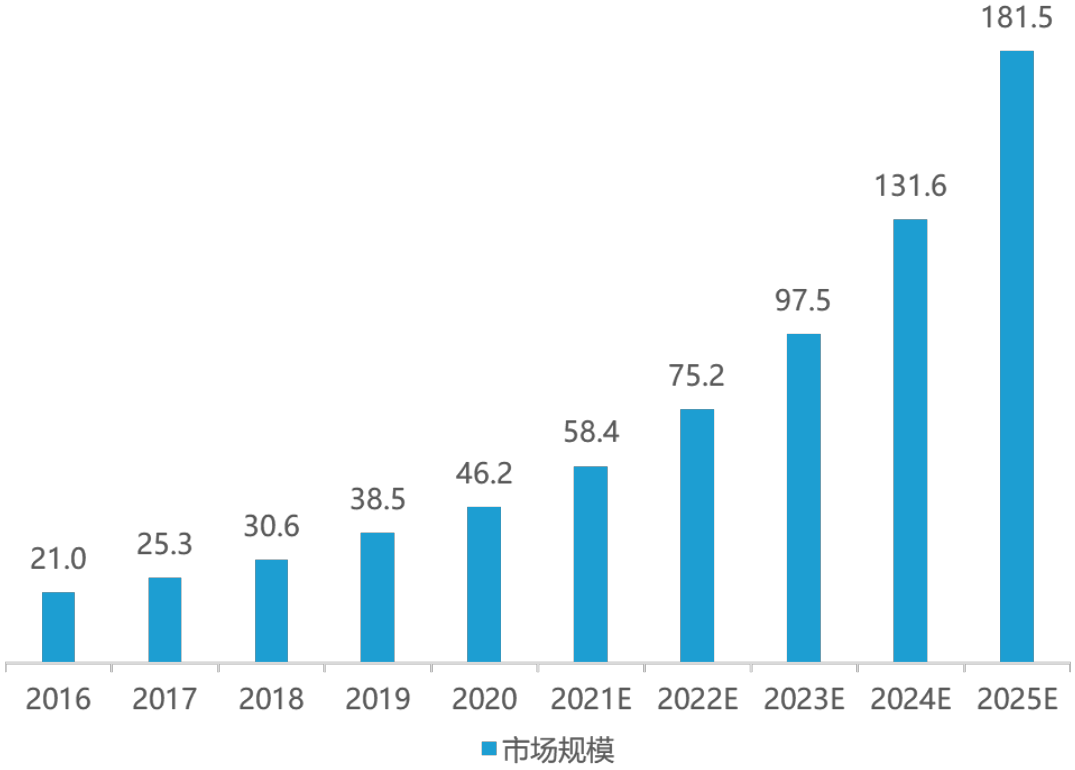
信息安全

网络安全

数据安全

数据安全概念由信息安全及网络安全演变而来.....

亿欧智库：2016-2025年中国数据安全行业市场规模（亿元）



数据来源：亿欧智库

从边界安全到数据保护，中国数据安全防护体系成形

- 庞大产业规模的背后，是从边界安全（身份认证、网络隔离、传输安全）、访问控制（权限控制、审计管理）、数据审计（数据生命周期管理、日志审计）到数据保护（数据加密、数据脱敏、多租户隔离、数据容灾、侵权保护）的一整套中国数据安全防护体系。以完整体系为依托，中国数据安全产业开始跳出传统计算机与手机行业范畴，向“万物互联”的方向渗透。

亿欧智库：中国数据安全防护体系

边界安全

- 授权合法用户访问大数据平台集群

身份认证

关注外部用户或者第三方服务对集群的访问过程中的身份鉴别，用户在访问启用安全认证的集群时，需通过服务所需要的安全认证方式。

网络隔离

大数据平台集群支持通过网络平面隔离的方式保证网络安全。

传输安全

关注数据在传输过程中的安全性，包括采用安全接口设计及高安全的数据传输协议，保证在通过接口访问、处理、传输数据时的安全性，避免数据被非法访问、窃听或旁路嗅探。

访问控制

- 定义可以访问、应用数据的用户

权限控制

包括鉴权、授信管理，即确保用户对平台、接口、操作、资源、数据等都具有相应的访问权限，避免越权访问；分级管理，即根据敏感度对数据进行升级，对不同级别的数据提供差异化的流程、权限、审批要求等管理措施。

审计管理

基于底层提供的审计数据，在权限管理、数据使用、操作行为等多个维度上对大数据平台的运转提供安全审计能力，确保及时发现大数据平台中的隐患点。

数据审计

- 数据溯源、数据使用和销毁路径跟踪

数据生命周期管理

追溯大数据平台中数据的来源，熟知数据使用、销毁情况，通过安全审计监测大数据系统中是否存在非法数据访问。安全审计的目的是捕获系统内的完整活动记录，且不可被更改，遵守“事前可管、事中可控、事后可查”，三大原则。

日志审计

对日志审计记录做集中管理与分析。

数据保护

- 数据加密和脱敏；多租户隔离；数据侵权保护；容灾管理

数据加密

提供数据在传输过程中及静态存储的加密保护，在敏感数据被越权访问时仍然能够得到有效保护。

数据脱敏

提供数据脱敏和个人信息去标识化功能，提供满足国际密码算法的用户数据加密服务。

多租户隔离

实施多租户访问隔离措施，实施数据安全等级划分，支持基于标签的强制访问控制，提供基于ACL的数据访问授权模型，提供全局数据视图和私有数据视图，提供数据视图的访问控制。

数据容灾

为集群内部数据提供实时的异地数据容灾功能。

侵权保护

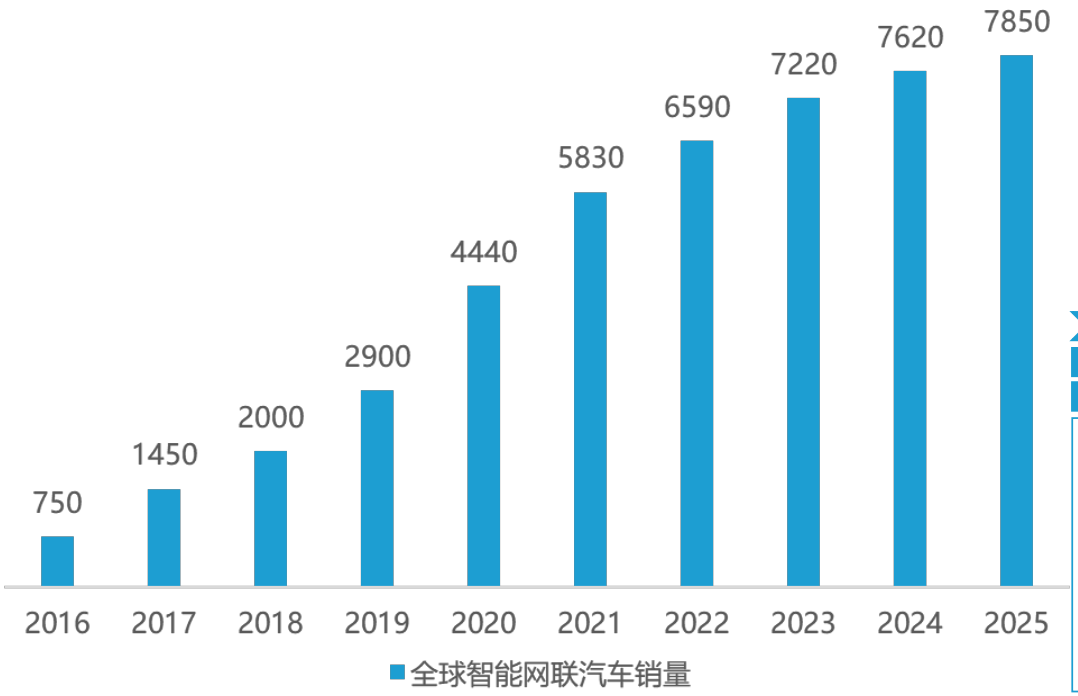
利用区块链类似技术实现数据的溯源确权。

数据来源：亿欧智库

智能网联汽车销量“井喷”，汽车安全概念向数据安全迁移

◆ 智能网联汽车，是指车联网与智能车的有机联合，是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与人、路、后台等智能信息交换共享，实现安全、舒适、节能、高效行驶，并最终可替代人来操作的新一代汽车。随着全球汽车产业新四化进程持续推进，智能网联汽车销量或将节节攀升。亿欧智库预测，2025年全球智能网联汽车销量将达到7850万辆。以往，汽车安全主要指代主动安全、被动安全、功能安全这三大概念。从端到管到云，智能网联重新定义汽车，随着汽车越来越像一台大号的“手机”，汽车安全概念开始向数据安全迁移。

亿欧智库：2016-2025年全球智能网联汽车销量（万辆）



亿欧智库：汽车安全概念动态变化过程

被动安全

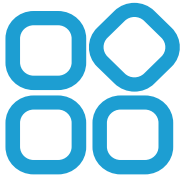
三点式安全带	安全气囊
汽车头枕	吸能式车身

1959年，沃尔沃工程师Nils Bohlin发明三点式安全带，标志着汽车被动安全框架雏形基本出现。经过数十年发展，汽车被动安全部分保证了乘客的物理安全。

主动安全

ABS	EBD/CBC
EBA/BAS/BA	ASR/TCS/TRC
ESC/ESP/DSC	并线辅助
车道偏离预警	车道保持辅助
交通标识识别	主动刹车

自1978年博世推出ABS开始，主动安全成为汽车安全不可或缺的组成部分，并迅速发展。具有主动安全的汽车，其避免事故能力较高。



功能安全

系统功能安全	软件功能安全
硬件功能安全	

功能安全是为了避免因电气/电子系统故障而导致的不合理风险。ISO26262标准通过提供适当的要求和流程，避免或降低因汽车产品中电子电气系统的功能因系统性失效和随机硬件失效造成对人身伤害的风险。

数据安全

传输交换安全	存储安全
计算安全	平台管理安全

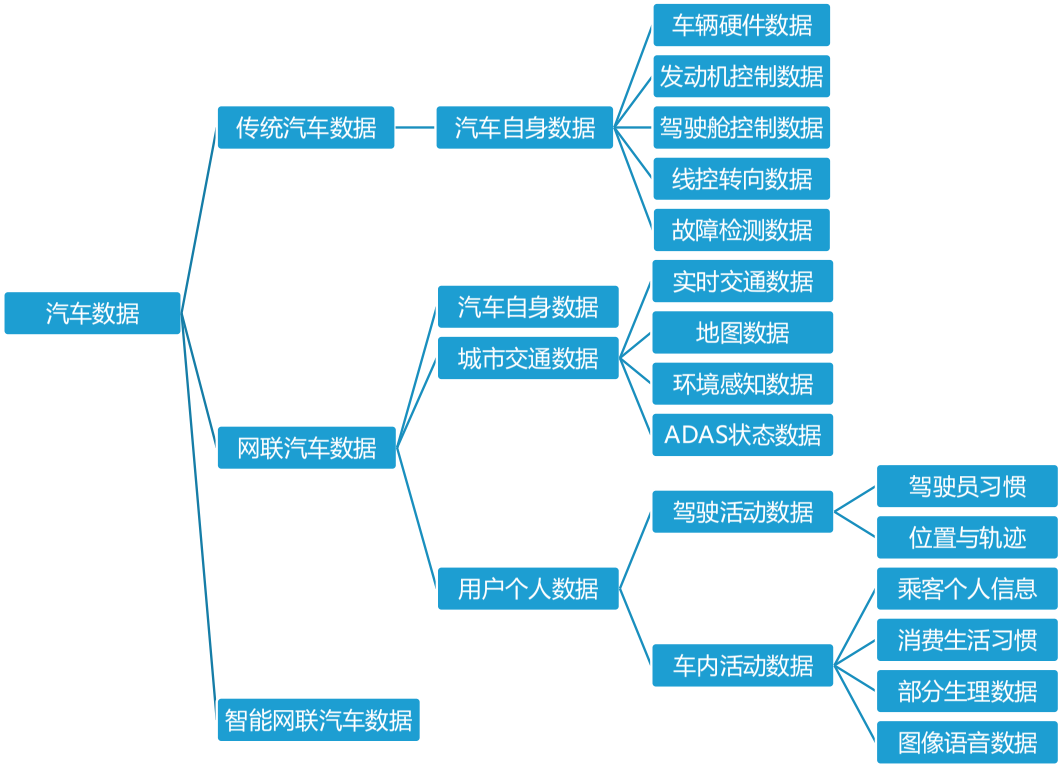
近年来，从端到管到云，智能网联重新定义汽车，将其由单一交通工具向移动智能终端改变，可以说，汽车越来越像一台“大号的手机”。随之而来的是，智能网联汽车也面临数据安全隐患的威胁，这种威胁关乎生死、较手机更严峻。因此，汽车数据安全被摆上桌面。

数据来源：亿欧智库

智能网联汽车数据类别繁复，面临三类数据安全威胁

◆ 从汽车数据类别来看，汽车数据可分为传统汽车数据、网联汽车数据与智能网联汽车数据三大类。目前阶段，智能网联汽车数据与网联汽车数据几乎相同，主要由汽车自身数据、城市交通数据和用户个人数据组成。其中，城市交通数据与用户个人数据的应用价值更大、泄漏后果也更严重。对车企而言，智能网联汽车云管端的安全隐患不胜枚举，并且具备以下三个特点：终端种类多，车载终端安全存在漏洞；网络协议多，通讯数据安全受到威胁；使用场景多，云平台安全保护较弱。

亿欧智库：汽车数据具体类别划分



亿欧智库：中国智能网联汽车云管端安全隐患

终端种类多

车载终端包括Linux系列的IVI、TBOX、中央网关以及车载框架ECU系列，网络协议包括IP网络和车载CAN网络；路侧设备包括Linux系列的收费设备、测速传感设备、智能路灯、充电桩等；移动端包括Android、IOS系列移动智能终端；云端包括Windows、Linux、Unix系列服务器与工作站。

网络协议多

车载远程通讯协议包括蜂窝网、LET-V2X、5G-V2X等远程通讯协议；车载短程通讯协议WIFI、RFID、Bluetooth等近距离通讯协议；以及车载雷达、车内CAN网络等车内通讯协议。

使用场景多

车、路、人、云，不同交互场景。车与车、车与路通信要求网络传输延时低，车与云通讯要求网络具备广连接与高带宽能力。

车载终端安全存在漏洞

TBOX、IVI层加密方式易破解，车内数据传输只采用简单的报文校验，车载终端架构ECU体系不检测数据包。

通讯数据安全受到威胁

在车载终端与外部主体通信过程中，敏感数据明文传输、密钥暴露等现象较为普遍。

云平台安全保护较弱

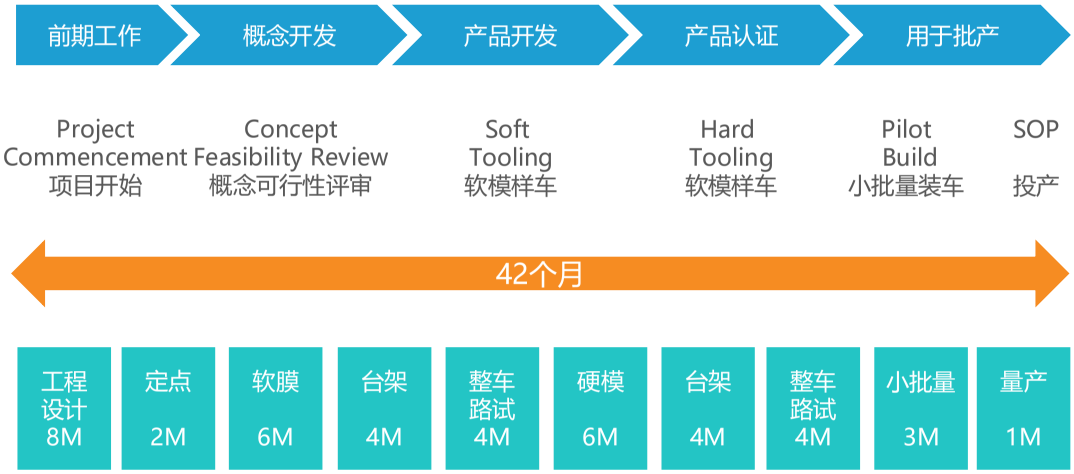
云平台缺乏对外部终端设备接入的身份认证与访问控制能力，以及敏感数据加密存储、数据防泄露等数据安全保护能力。

数据来源：亿欧智库

智能网联汽车云管端安全隐患众多，软件系统迭代频繁

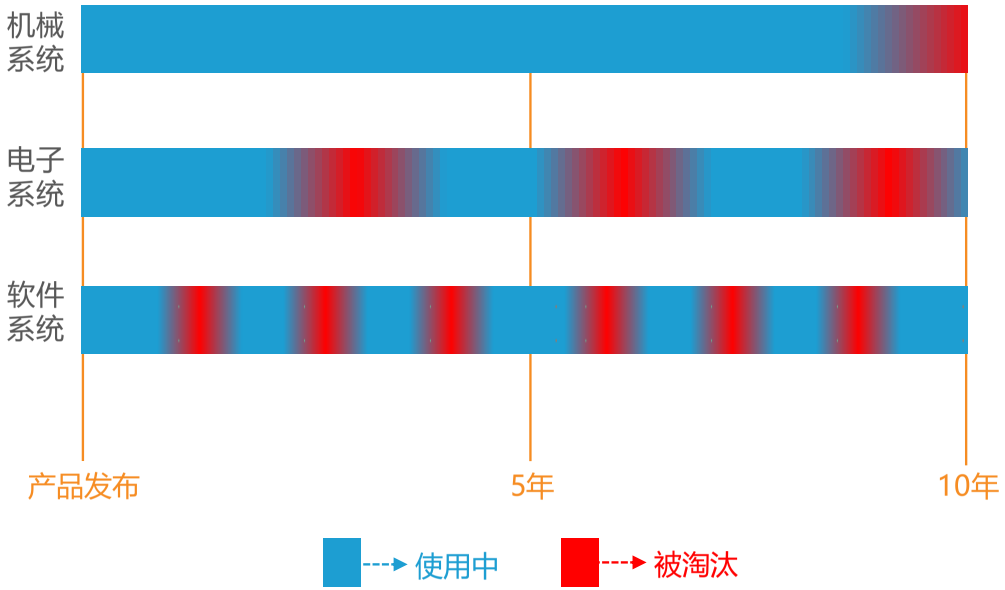
- 以往，从0完成一辆传统汽车的开发需要42个月，考虑到发动机则需要48个月，是一场马拉松式的“拉锯战”。但在“软件定义汽车”时代，汽车软件系统的迭代速度又远超机械系统与电子系统，这对车企的“软实力”提出了巨大要求。如何在保证汽车软件开发速度与功能体验的同时，减少软件系统漏洞、保障汽车数据安全？这已成为车企发展智能网联汽车的一大难点。

亿欧智库：某车型整车开发周期情况



- 上述开发周期仅为整车开发周期，若包括发动机，整个周期需要再延长6个月，周期总长达到48个月

亿欧智库：汽车机械系统、电子系统与软件系统迭代周期对比

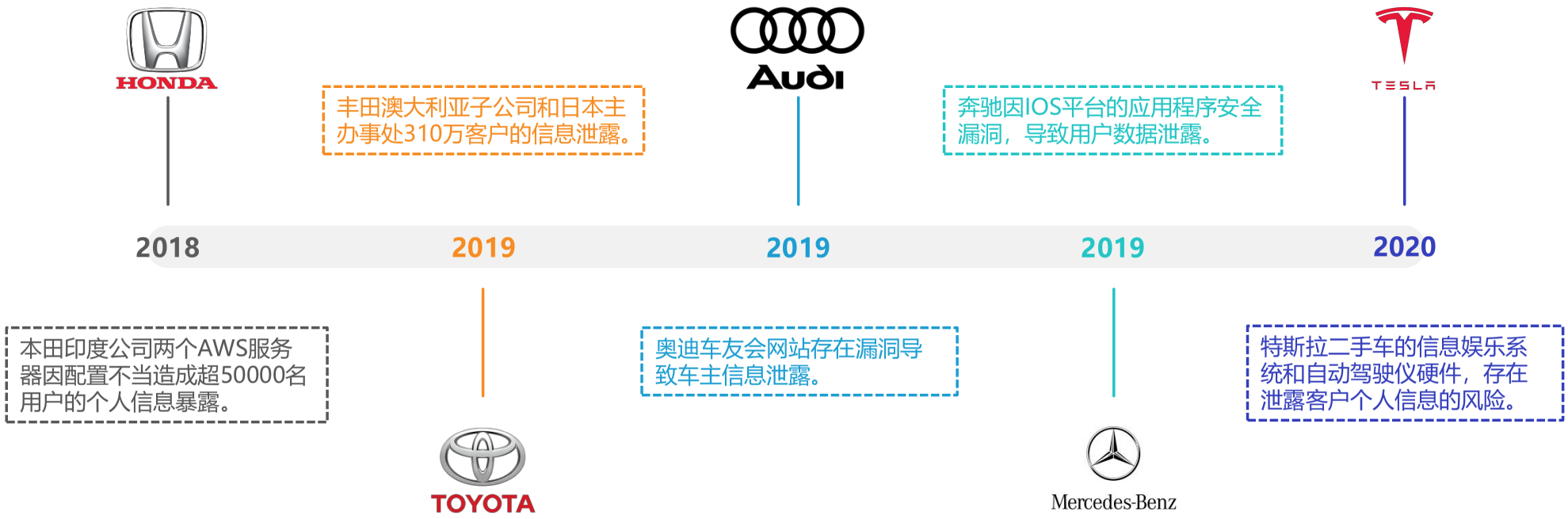


数据来源：亿欧智库

智能网联汽车数据安全事件频发，数据安全保障程度有待提升

- 回顾2018年至今的智能网联汽车数据安全事件可以发现，包括多家全球知名汽车品牌在内，智能网联汽车从端到管到云的安全漏洞问题层出不穷。从本田印度AWS服务器因配置不当导致5000名用户个人信息暴露，再到特斯拉二手车信息娱乐系统和自动驾驶仪硬件存在泄露个人隐私风险，每一次事故的发生既损害了消费者利益、影响了车企品牌形象，也是对智能网联汽车数据安全产业的一次敲打。此外可以看到，围绕汽车数据的安全事件，其所在领域逐渐由云端、管端向车端渗透。

亿欧智库：2018-2020年全球智能网联汽车数据安全事件



数据来源：亿欧智库

中国智能网联汽车数据安全产业基本情况

中国智能网联汽车数据安全产业图谱

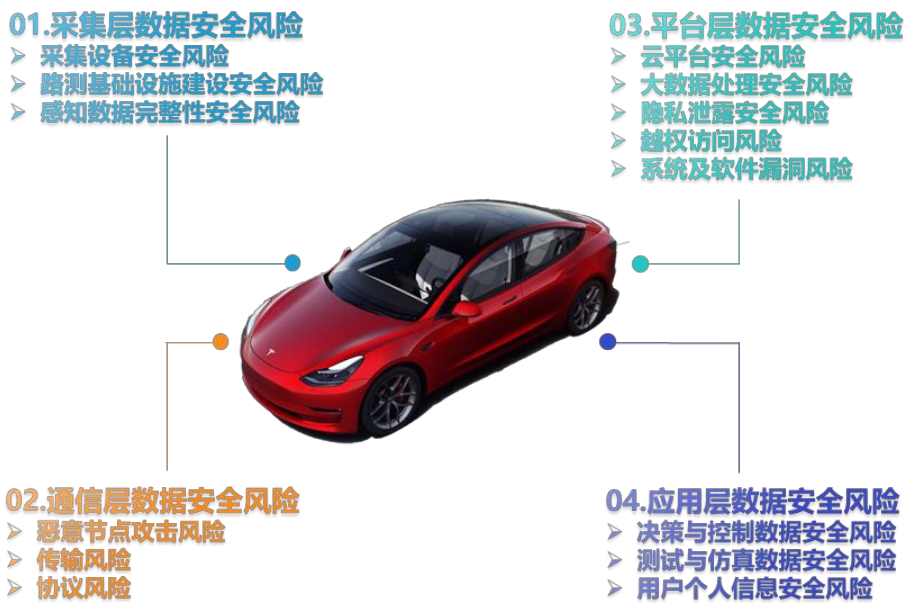
- 中国智能网联汽车数据安全产业可分为监管评估、控制应用和安全服务三大层面。监管评估层面由数据安全监管方和数据安全评估方组成；控制应用层面由数据控制方和数据应用方组成；安全服务层面由数据安全与服务提供方组成，后者主要包括PKI认证体系、车联网安全和应用数据安全。各方携手，共同组成了中国智能网联汽车数据安全产业，为中国用户提供更智能、更安全的智能网联汽车产品。

数据来源：亿欧智库

智能网联汽车面临数据安全风险，用户、企业、政府三方立场与角色不同

- 目前，智能网联汽车主要面临4层数据安全风险，主要涉及采集层、通信层、平台层和应用层。而用户、企业、政府三方对待智能网联汽车的态度也不尽相同。之于用户，智能网联汽车数据安全目前仍是个“陌生词”；对企业来说，建设汽车数据安全的动力主要来自道德、而非法规；随着相关法律法规的持续推出，政府逐渐收紧管控。可以说，用户、企业与政府是中国智能网联汽车数据安全的三个最核心参与者。

亿欧智库：智能网联汽车面临4层数据安全风险



亿欧智库：用户、企业、政府对待智能网联汽车态度

用户

用户对于汽车数据安全的感知度较低，并未意识到汽车数据安全重要性，但其在大数据时代已经近乎“裸体”。因此，用户认知亟待变革。

企业

车企建设智能网联汽车数据安全的驱动力由道德软性驱动转向法规强制驱动。同时，中国智能网联汽车数据安全产业开始蓬勃发展、势不可挡。

政府

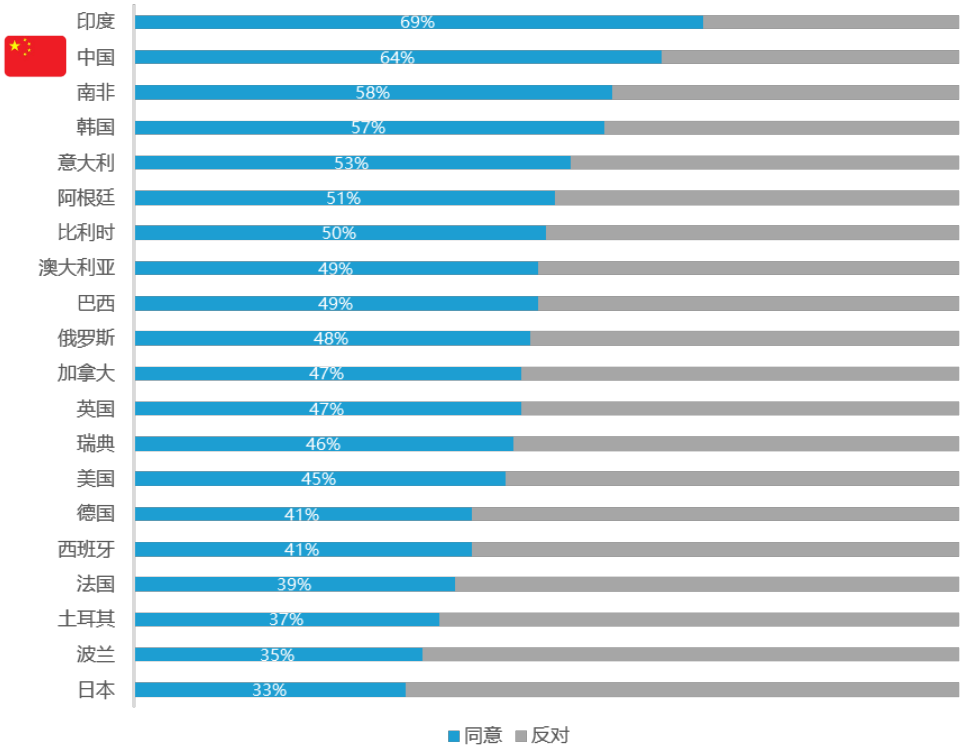
政策对于智能网联汽车数据安全的把控曾经相对宽松，随着相关法律法规的不断推出，中国智能网联汽车数据安全更加有法可依、有规可循。

数据来源：亿欧智库

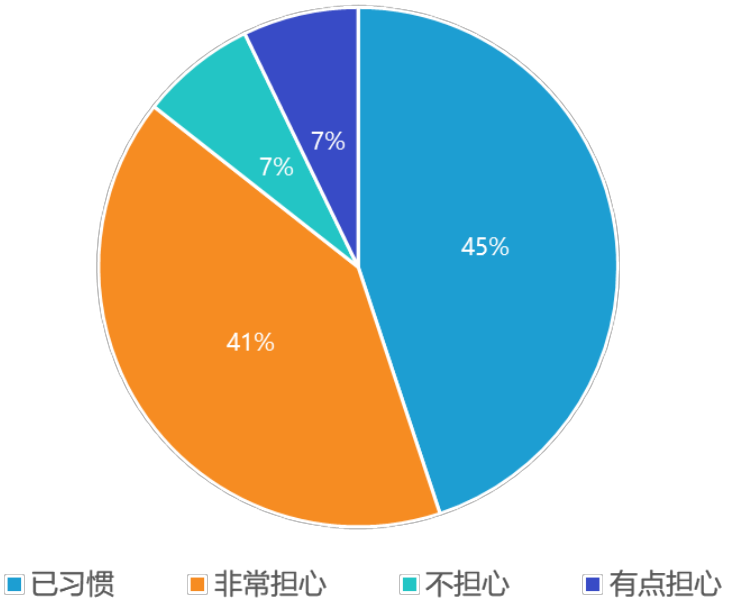
中国用户对个人信息敏感度较低，汽车数据安全防范意识薄弱

- 在“以个人信息换取优质服务”方面，中国用户的同意比例高达64%，这一数字位居世界前列，仅次于印度。可以说，中国用户在数据安全上体现出极强的实用主义特点。之于汽车数据安全，超过半数以上的中国用户持“不担心”、“已习惯”态度，即“无感“态度。中国智能网联汽车用户对于汽车数据的安全意识相对淡薄，这与汽车数据的重要地位不相匹配。

亿欧智库：2021年全球用户对“以个人信息换取优质服务”态度



亿欧智库：2021年中国用户对智能网联汽车数据安全态度



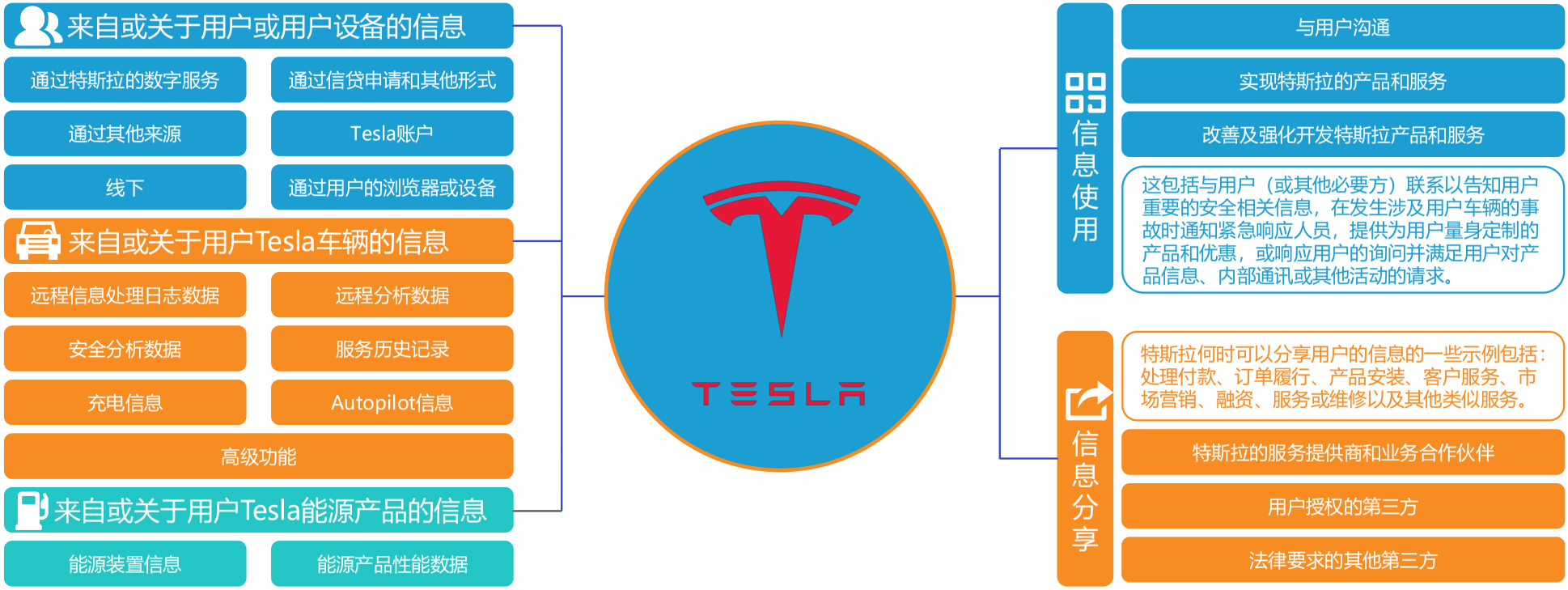
- 超过半数以上的中国用户对智能网联汽车数据安全持“不担心”、“已习惯”态度，即“无感“态度。中国用户数据安全防护意识有待提升。

数据来源：亿欧智库

车企搜集、使用数据于“无形”，用户数据安全意识亟待提升

- 实际上，汽车数据安全与消费者利益息息相关。以特斯拉信息搜集与使用路径为例，特斯拉从用户设备、特斯拉车辆和能源产品三个渠道，搜集特斯拉用户多维度的数据信息，将其用于特斯拉数字服务等路径，并分享给服务提供商、业务合作伙伴、用户授权的地方及法律要求的其他第三方等。诸如特斯拉等智能网联汽车生产企业，搜集用户数据之大，及其商业价值之不菲，超乎普通用户的直观感受。

亿欧智库：特斯拉信息搜集与使用路线图

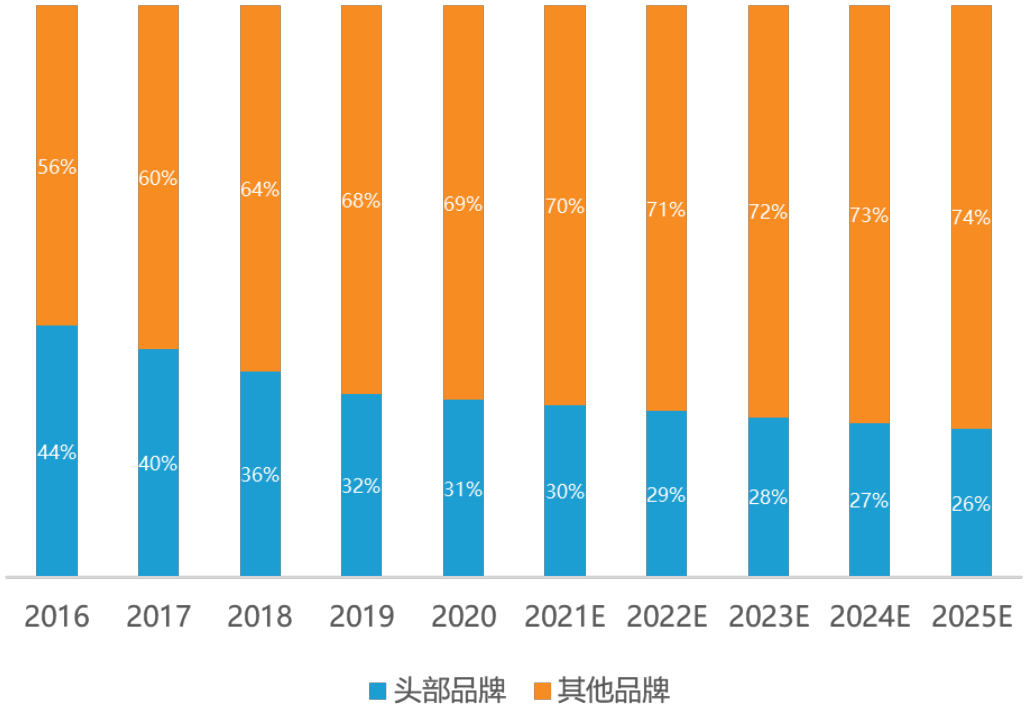


数据来源：亿欧智库

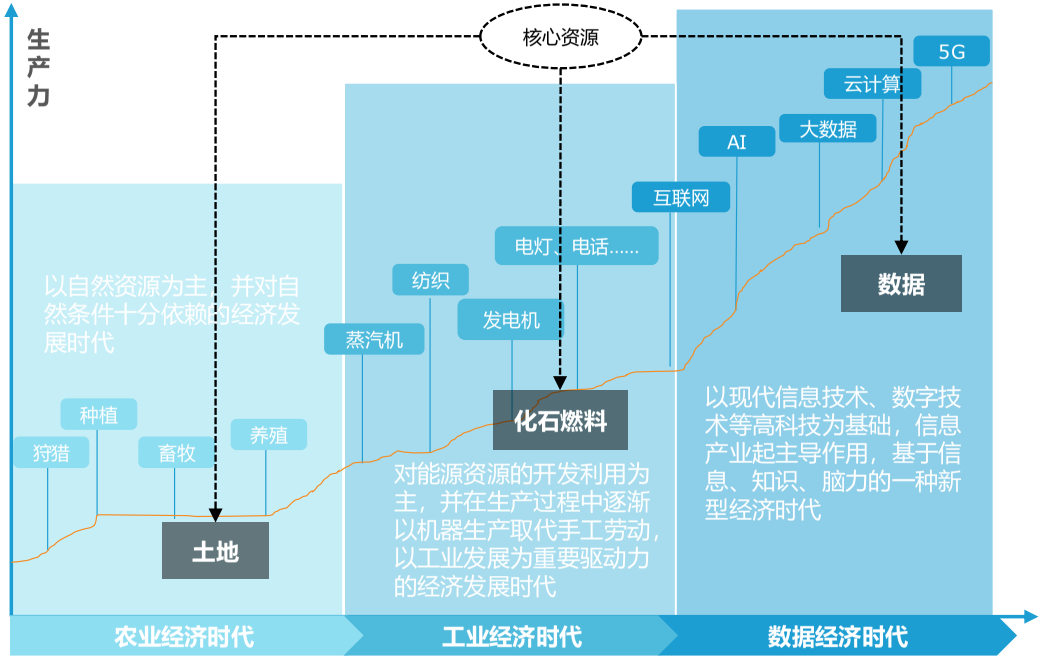
中国乘用车市场竞争加剧，数据是车企在智能网联时代决胜关键

- 对车企而言，中国乘用车市场竞争愈加强烈，预计2025头部品牌市占率将达到74%，留给剩余参与者的市场份额仅为26%。如何在存量市场中争取更大的生存发展机会？数据是解题思路之一。随着人类社会由农业经济时代、工业经济时代向数据经济时代切换，社会核心资源不再是土地或化石燃料，而是数据。之于智能网联汽车，数据是车企下一阶段的决胜关键。

亿欧智库：2016-2025年中国乘用车市场集中度情况



亿欧智库：数据是智能网联汽车决胜关键



数据来源：亿欧智库 注：头部品牌指过去4年销量达市场前15的品牌

法规是智能网联汽车数据安全建设最大驱动力，面临三大制定难点

亿欧智库

- 之于中国车企智能网联汽车数据安全建设，无论是道德驱动、用户驱动还是产品驱动，都不及法规驱动直接有效，后者是汽车数据安全建设的核心驱动力。但是目前来看，中国智能网联汽车数据安全法律法规体系尚不完善，车企处于无法可依、无规可循的状态之中。相关法律法规的制定，也面临着至少三方面挑战：其一，如何平衡安全与发展；其二，如何实现国际溢出效应；其三，如何协同多方共治。

亿欧智库：中国车企智能网联汽车数据安全建设驱动力分析

道德驱动

车企出于道德感自发开展智能网联汽车数据安全建设，但车企意志薄弱、驱动力不强，道德驱动是锦上添花而非主驱动力，属于软性驱动。

产品驱动

车企在设计产品核心功能之余，间接提供了一定的数据安全保障措施，但驱动力不强，属于间接驱动。

用户驱动

车企从服务用户的角度开展智能网联汽车数据安全建设，当用户“人微言浅”时，该驱动力并不牢固，属于软性驱动。

法规驱动

法律法规以强制规定的形式，“逼迫”车企必须进行智能网联汽车数据安全保障，否则将面临严重责任后果。法规驱动是汽车数据安全建设的核心驱动力。

亿欧智库：中国智能网联汽车数据安全法律法规三大制定难点

安全发展难平衡

智联网联汽车领域出现的数据安全问题是全行业面临的共性问题，立法的初衷和规则设计应该具有普遍性，避免产生针对特定产品或事件进行立法的印象。同时，规则制定也需要考虑对产品使用复杂程度或消费者体验可能带来的影响。

国际溢出难接轨

汽车数据化是全球趋势，当前的突出问题不仅在中国存在，其他国家和地区也在积极寻找应对和解决措施。制定数据治理规则需要考虑到国际溢出效应，要能够与国际接轨。

多方共治难协同

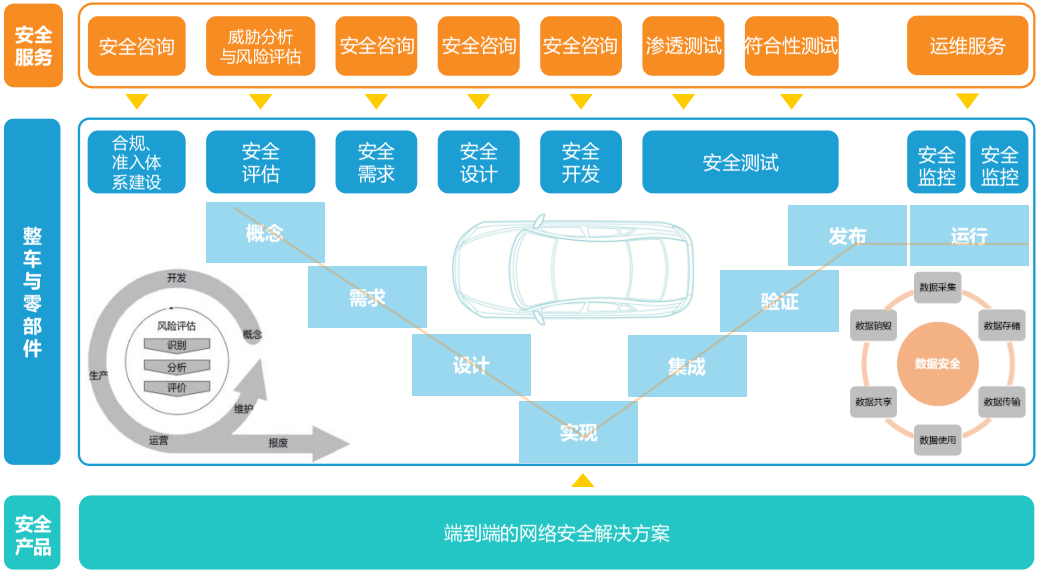
智能网联汽车与互联网息息相关，对于互联网治理的经验和做法可以充分借鉴。除了政府主管部门外，作为利益相关方的汽车制造商、相关行业组织、技术提供商、网约车企业、车主等也应参与到智能网联汽车数据治理中来，共同做出合理和适当的决策。

数据来源：亿欧智库

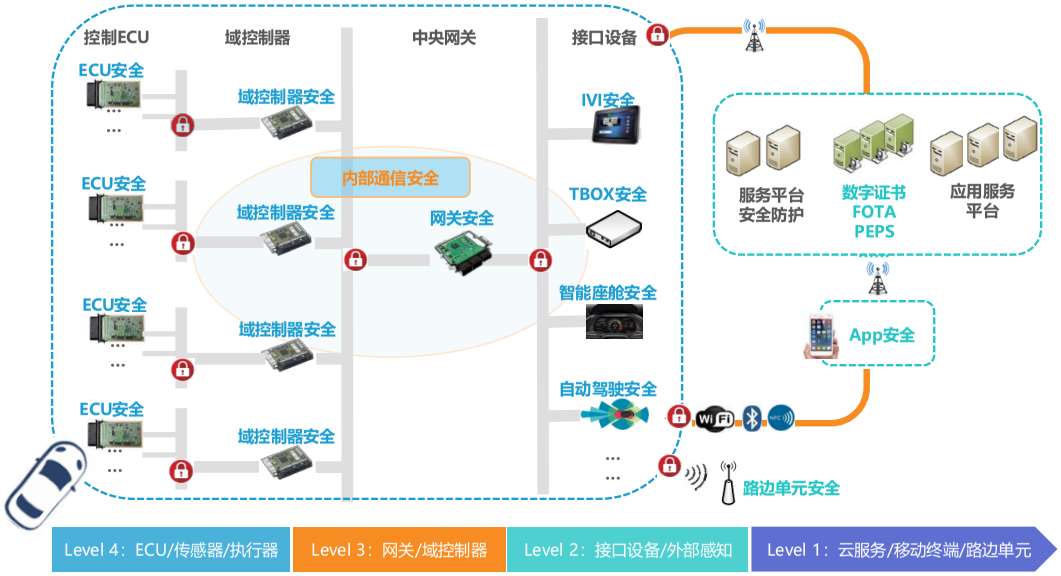
为辰信安：智能汽车网络安全解决方案提供商

- 为辰信安专注于智能汽车网络安全，能为智能汽车建立基于层次的纵深防御体系，提供覆盖智能汽车全生命周期的网络安全解决方案deCORE AUTO。
- deCORE AUTO覆盖智能汽车全要素，包括IVI、TBOX、智能座舱、中央网关、自动驾驶、控制类型ECU等关键零部件，CAN/CANFD、Ethernet等通信协议，以及FOTA、蓝牙钥匙、远程控制等关键业务，拥有支持国际/国内密码算法的密码模块、IDPS、安全通信、可信执行环境等方面的基础产品，并提供网络安全方面的系列化测试工具和汽车靶场，以及渗透测试和咨询等方面的安全服务。
- deCORE AUTO提供完整的数据安全解决方案，覆盖采集、存储、传输、使用、共享、销毁等数据安全全生命周期。相关咨询与产品能够满足国内外数据安全与隐私保护方面的标准、法规与准入要求。

亿欧智库：deCORE AUTO覆盖智能汽车全生命周期



亿欧智库：deCORE AUTO为智能汽车建立基于层次的纵深防御体系

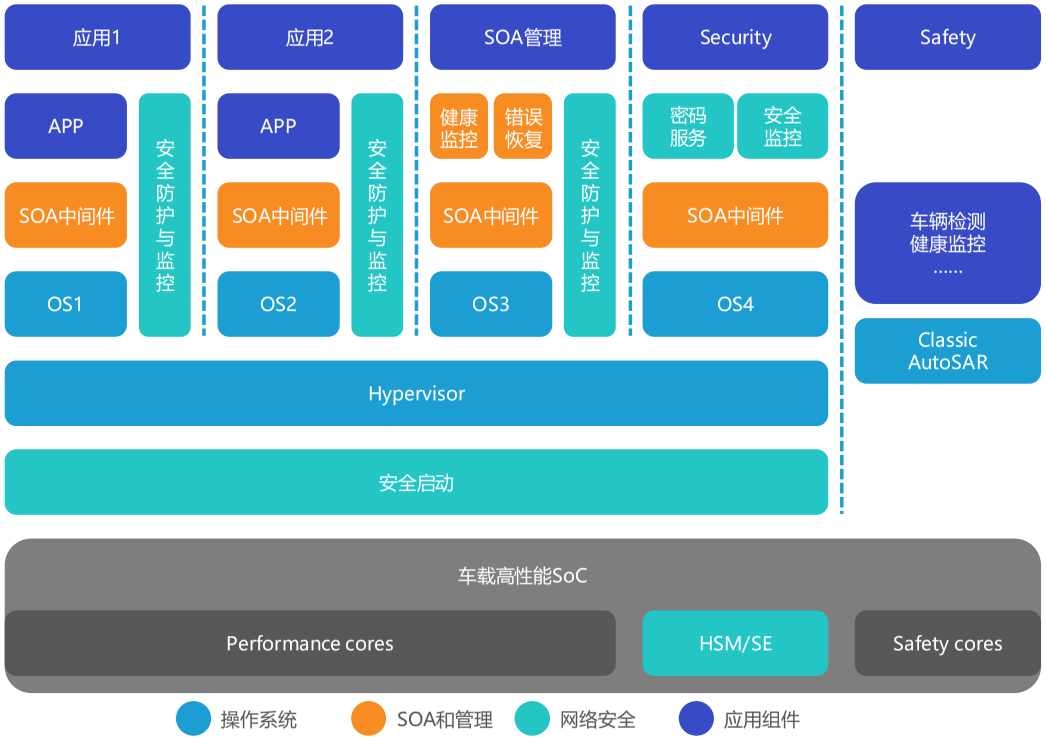


数据来源：亿欧智库

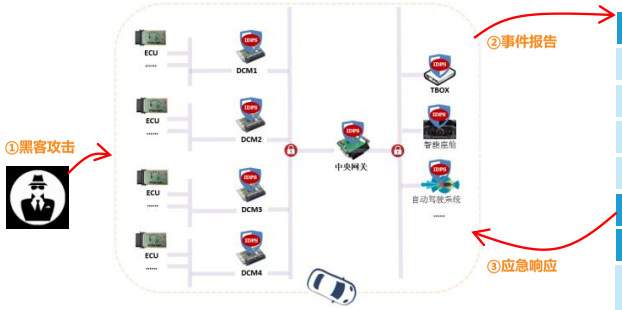
为辰信安：智能汽车网络安全解决方案提供商

- deCORE AUTO相关产品与服务已经提供给主流整车厂、零部件供应商、检测机构，并已经实现了数十万车辆的量产应用。
- 面向零部件的网络安全解决方案能够满足智能座舱、中央网关、域控制器、自动驾驶等下一代零部件的网络安全需要；面向车辆的安全运营中心能基于部署在车辆端的IDPS，以及漏洞管理、威胁情报和应急响应体系的建立，实现车辆运营阶段的全方位安全监控与威胁处置；为客户建立的网络安全实验室能够开展零部件、整车、自动驾驶、V2X、OTA等全要素的渗透测试与合规测试业务。

亿欧智库：为辰信安下一代零部件网络安全解决方案



亿欧智库：为辰信安车辆端IDPS+车辆安全运营中心



车辆端IDPS： deCORE IDPS

分布式部署、具有主从结构特性的，为整车提供满足合规、准入要求的安全监控体系

车辆安全运营中心： deCORE vSOC

亿欧智库：为辰信安安全测试工具/渗透测试+符合性测试

- ✓ 零部件测试工具
- ✓ 整车测试工具
- ✓ 自动驾驶测试工具
- ✓ V2X测试工具
- ✓ OTA测试工具

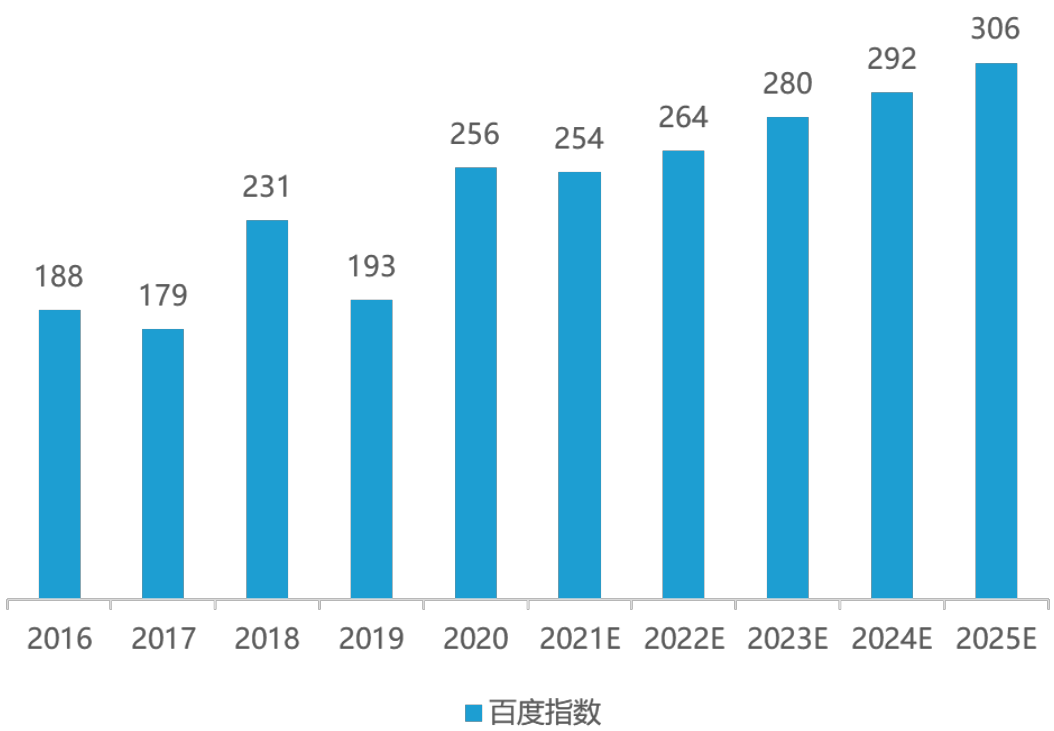
数据来源：亿欧智库

中国智能网联汽车数据安全产业趋势洞察

中国用户“隐私保护”意识逐年提升，数据安全将影响购车决策

- 从过去5年中国用户“隐私保护”意识总体逐步提升的情况来看，未来5年中国用户对于“隐私保护”、包括汽车数据安全的关注程度有望进一步提升。而随着数据安全成为汽车产品力的组成维度，其或将成为消费者购车决策因素的重要组成。用户意识的觉醒，也将倒逼产业与政策的更迭，促使智能网联汽车数据安全产业各方向前推进。

亿欧智库：2016-2025年中国“隐私保护”关键词百度指数情况



亿欧智库：2021年中国用户购车因素TOP10

主被动安全、智能科技、动力尺寸等因素仍然占据中国用户购车主导位，用户数据安全识有待提升。**未来，数据安全或将成为汽车产品力的重要组成部分，成为消费者购车决策因素重要组成。**

数据来源：亿欧智库

数据安全保障体系融入汽车产品全生命周期

- 从产品角度而言，车企将数据安全融入汽车产品全生命周期之中，以安全设计、安全研发、安全测试、安全运营四大手段共同组成数据安全保障体系，进而保障从研发、生产、营销到服务的汽车产品全生命周期数据安全。

亿欧智库：数据安全保障体系融入汽车产品全生命周期

研发			生产	营销	服务	
策划阶段	设计阶段	试制试验阶段			线下	线上
市场调研	概念设计	样机试制	试生产准备阶段	渠道网络	汽车保养	远程OTA
技术调研	方案设计	样机试验	批量试生产阶段	营销策略	汽车维修	用户社群
可行性分析	详细设计	小批试制	预生产阶段	用户画像	汽车保险	积分商城
可行性报告评审	同步工程	形成产品文件	量产阶段	数字营销	充换电	品牌电台

数据安全保障体系

安全设计 | 安全研发 | 安全测试 | 安全运营

数据来源：亿欧智库

汽车数据安全法律法规逐步推出，企业“戴着镣铐起舞”

- 围绕智能网联汽车数据，国家主管部门发布了《智能网联汽车生产企业及产品准入管理指南（试行）》（征求意见稿）、《信息安全技术 网联汽车 采集数据的安全要求》标准草案、《汽车数据安全管理若干规定》（征求意见稿）等相关文件，力图从法律法规层面对智能网联汽车数据安全进行规定、引导与限制，一方面限制车企及相关利益方肆意搜集、滥用智能网联汽车数据，另一方面为企业合理合法搜集、使用汽车数据打开了绿灯。

亿欧智库：国家主管部门关于汽车数据安全法规征求意见一览

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

2021-04-07

《智能网联汽车生产企业及产品准入管理指南（试行）》（征求意见稿）

为加强道路机动车辆生产企业及产品准入管理，推动智能网联汽车产业健康有序发展，根据《中国人民共和国道路交通安全法》《中华人民共和国网络安全法》《道路机动车辆生产企业及产品准入管理办法》等规定，针对申请准入的具备有条件自动驾驶、高度自动驾驶功能的智能网联汽车生产企业及其产品，工业和信息化部装备工业一司制定本指南。

《指南》对智能网联汽车生产企业、智能网联汽车产品本就保护汽车数据安全提出了多条规定与要求，包括企业建立覆盖车辆全生命周期的网络安全防护体系、产品明确驾驶自动化功能及其设计运行条件等。

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China

2021-04-29

《信息安全技术 网联汽车 采集数据的安全要求》标准草案

为落实《网络安全法》相关要求，加快网联汽车标准研制工作，全国信息安全标准化技术委员会组织起草形成了《信息安全技术 网联汽车 采集数据的安全要求》标准草案。

《要求》对数据传输、数据存储、数据跨境这三方面提出了具体要求，并提出“不得基于网联汽车所采集数据及经其处理得到的数据开展与车辆管理、行驶安全无关的数据处理活动”和“国家行政管理部门对汽车处理数据另有要求的，从其要求”这两条基本要求。

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China

2021-05-12

《汽车数据安全管理若干规定》（征求意见稿）

为加强个人信息和重要数据保护，规范汽车数据处理活动，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》。

《规定》要求汽车设计、制造、服务企业或者机构，包括汽车制造商、部件和软件提供者、经销商、维修机构、网约车企业、保险公司等，在中华人民共和国境内设计、生产、销售、运维、管理汽车过程中，收集、分析、存储、传输、查询、利用、删除以及向境外提供个人信息或重要数据，应当遵守相关法律法规和本规定的要求。

数据来源：亿欧智库

车企与用户共治共享汽车数据，功能、技术与组织成为数据安全“三把伞”

- 对车企而言，如何提升用户贡献个人数据的意愿度是一方面。同时，如何对用户数据建立有效可靠的保护体系是另一方面。智己汽车CSOP模式与数据安全保护体系为行业做了一个参考。智己汽车CSOP以股权收益为背书，通过“里程式开采”和“养成式开采”两种方式向用户发放原石，实现了数据共享共赢。此外，智己汽车在功能、技术和组织三个维度发力，以成熟体系保护汽车数据安全。

亿欧智库：智己汽车CSOP模式

01 独创CSOP模式

智己汽车以创始轮投资中的4.9%股权收益作为背书，发行3亿枚“原石”对应上述股权的资产收益，应用包括区块链在内的技术，以数据权益方式回馈用户。

02 原石发放规则

CSOP用户数据权益计划的“原石”投放总量固定为3亿枚，产出规律遵循“四年减半”原则；原石与车主用户账户深度绑定；初期投放量大，采集概率高。

03 原石获取方式

购车用户通过“里程式开采”和“养成式开采”两种方式获取原石，前者基于驾驶产生的“驾驶行为数据”获取“原石”，后者依赖于路径更长的用户APP互动任务。

亿欧智库：智己汽车数据安全保护体系

功能

取消人脸识别，避免搜集人脸等敏感信息。

技术

制订IDPP用户数据隐私及保密计划，以区块链技术、零知识证明、差分隐私等前沿科技保障所有数据透明、可控、不关联。

组织

建立隐私保护委员会，制订用户隐私保护整体策略，监督检查数据安全措施落实工作；建立隐私合规工作小组，落实数据安全和隐私保护。

数据来源：亿欧智库

中国智能网联汽车数据安全榜单

中国智能网联汽车数据安全服务商TOP10榜单评选标准

- 评选方法：亿欧智库对近50家中国智能网联汽车数据安全服务商进行筛选，按公司规模与财务情况、智能网联汽车业务深度、细分赛道行业地位等维度进行定量打分，并对各细分项进行加权处理后综合计算出总分，评选出《中国智能网联汽车数据安全服务商TOP10榜单》。

亿欧智库：中国智能网联汽车数据安全服务商TOP10榜单评选标准说明

公司规模与财务情况

01

结合工商信息、财报信息、公开消息等信源，亿欧智库对候选企业的公司规模与财务情况进行定量评分、定性分析，公司规模与财务情况越良好、该项得分越高。

智能网联汽车业务深度

02

结合产品矩阵、客户清单、技术储备等情况，亿欧智库对候选企业的智能网联汽车业务深度做出评估，智能网联汽车业务深度越深、该项得分越高。

细分赛道行业地位

03

借助产业图谱扫描和行业专家访谈，亿欧智库对候选企业在细分赛道的行业地位进行评估，细分赛道行业地位越高、该项得分越高。

加权综合

数据来源：亿欧智库

中国智能网联汽车数据安全服务商TOP10榜单

- 纵览中国智能网联汽车数据安全产业，亿欧汽车筛选出中国最具服务能力的10家智能网联汽车数据安全服务商，分别为：华为、为辰信安、东软集团、数字认证、启明星辰、博泰车联网、梆梆安全、吉大正元、格尔软件和派拉软件。上榜企业或为汽车行业巨擘，或为细分赛道龙头，或为行业潜力新星，是推动中国智能网联汽车数据安全产业进一步发展的中坚力量。

亿欧智库：中国智能网联汽车数据安全服务商TOP10榜单

注：排名不分先后

团队介绍和版权声明

◆ 团队介绍：

亿欧智库（EqualOcean Intelligence）是亿欧EqualOcean旗下的研究与咨询机构。为全球企业和政府决策者提供行业研究、投资分析和创新咨 询服务。亿欧智库对前沿领域保持着敏锐的洞察，具有独创的方法论和模型，服务能力和质量获得客户的广泛认可。

亿欧智库长期深耕汽车、科技、消费、大健康、产业互联网、金融、传媒、房产新居住等领域，旗下近100名分析师均毕业于名校，绝大多数具有丰富的从业经验；亿欧智库是中国极少数能同时生产中英文深度分析和专业报告的机构，分析师的研究成果和洞察经常被全球顶级媒体采访和引用。

以专业为本，借助亿欧网和亿欧国际网站的传播优势，亿欧智库的研究成果在影响力上往往数倍于同行。同时，亿欧EqualOcean内部拥有一个由数万名科技和产业高端专家构成的资源库，使亿欧智库的研究和咨询有强大支撑，更具洞察性和落地性。

◆报告作者：

王瑞

亿欧EqualOcean 分析师

Email：wangrui@iyiou.com

◆报告审核：

武东

亿欧EqualOcean 研究总监

Email：wudong@iyiou.com

杨永平

亿欧EqualOcean 执行总经理、亿欧汽车总裁

Email：yangyongping@iyiou.com

黄渊普

亿欧EqualOcean 首席执行官、亿欧智库院长

Email：huangyuanpu@iyiou.com

团队介绍和版权声明

◆ 版权声明：

本报告所采用的数据均来自合规渠道，分析逻辑基于智库的专业理解，清晰准确地反映了作者的研究观点。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。本报告的信息来源于已公开的资料，亿欧智库对该等信息的准确性、完整性或可靠性作尽可能的追求但不作任何保证。本报告所载的资料、意见及推测仅反映亿欧智库于发布本报告当日之前的判断，在不同时期，亿欧智库可发出与本报告所载资料、意见及推测不一致的报告。亿欧智库不保证本报告所含信息保持在最新状态。同时，亿欧智库对本报告所含信息可在不发出通知的情形下做出修改，读者可自行关注相应的更新或修改。

◆ 关于亿欧：

亿欧EqualOcean是一家专注科技+产业+投资的信息平台和智库；成立于2014年2月，总部位于北京，在上海、深圳、南京、纽约有分公司。亿欧EqualOcean立足中国、影响全球，用户/客户覆盖超过50个国家或地区。

亿欧EqualOcean旗下的产品和服务包括：信息平台亿欧网（iyiou.com）、亿欧国际站（EqualOcean.com），研究和咨询服务亿欧智库（EqualOcean Intelligence），产业和投融资数据产品亿欧数据（EqualOcean Data）；行业垂直子公司亿欧大健康（EqualOcean Healthcare）和亿欧汽车（EqualOcean Auto）等。

亿欧服务

- 基于自身的研究和咨询能力，同时借助亿欧网和亿欧国际网站的传播优势；亿欧EqualOcean为创业公司、大型企业、政府机构、机构投资者等客户类型提供有针对性的服务。

- 创业公司

亿欧EqualOcean旗下的亿欧网和亿欧国际站是创业创新领域的知名信息平台，是各类VC机构、产业基金、创业者和政府产业部门重点关注的平台。创业公司被亿欧网和亿欧国际站报道后，能获得巨大的品牌曝光，有利于降低融资过程中的解释成本；同时，对于吸引上下游合作伙伴及招募人才有积极作用。对于优质的创业公司，还可以作为案例纳入亿欧智库的相关报告，树立权威的行业地位。

- 大型企业

凭借对科技+产业+投资的深刻理解，亿欧EqualOcean除了为一些大型企业提供品牌服务外，更多地基于自身的研究能力和第三方视角，为大型企业提供行业研究、用户研究、投资分析和创新咨询等服务。同时，亿欧EqualOcean有实时更新的产业数据库和广泛的链接能力，能为大型企业进行产品落地和布局生态提供支持。

亿欧服务

◆ 政府机构

针对政府类客户，亿欧EqualOcean提供四类服务：一是针对政府重点关注的领域提供产业情报，梳理特定产业在国内外的动态和前沿趋势，为相关政府领导提供智库外脑。二是根据政府的要求，组织相关产业的代表性企业和政府机构沟通交流，探讨合作机会；三是针对政府机构和旗下的产业园区，提供有针对性的产业培训，提升行业认知、提高招商和服务域内企业的水平；四是辅助政府机构做产业规划。

◆ 机构投资者

亿欧EqualOcean除了有强大的分析师团队外，另外有一个超过15000名专家的资源库；能为机构投资者提供专家咨询、和标的调研服务，减少投资过程中的信息不对称，做出正确的投资决策。

◆ 欢迎合作需求方联系我们，一起携手进步；电话 010-57293241，邮箱 hezuo@iyiou.com

获取更多报告详情
可扫码关注

亿欧智库

网址：https://www.iyiou.com/research

邮箱：hezuo@iyiou.com

电话：010-57293241

地址：北京市朝阳区霞光里9号中电发展大厦A座10层