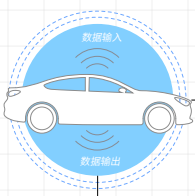
数据故事

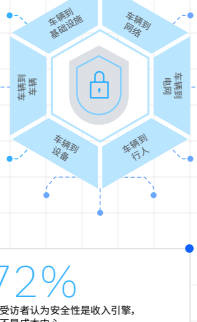
为智能网联汽车保驾护航

设计未来出行方式



软件定义汽车的时代已经来临。预计到2027年，道路上的智能网联汽车将达到3.67亿辆，汽车端点的数量将显著增加。这样一来，汽车内外将有数亿个新的攻击面暴露在网络威胁之中。生成式 AI 的日益普及则进一步加剧了威胁形势。

从自动驾驶汽车到电动垂直起降车辆，各种先进的出行技术也将增加连接的复杂性。然而，在应对智能联网汽车安全与隐私问题时，大多数汽车原始设备制造商(OEM)和汽车供应商都专注于满足当前的标准和法规，而并未通过充分的规划来保护未来的系统免受网络攻击。



汽车行业高管认识到智能网联汽车安全有助于提高产品和品牌价值。[1]

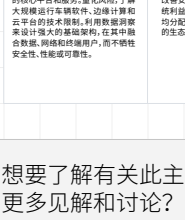
72%

的受访者认为安全性是收入引擎，而不是成本中心。

86%

的受访者认为安全性、保障和信任是其组织从竞争中脱颖而出的品牌特性。

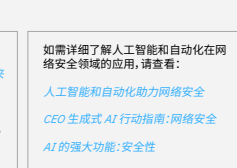
消费者将选择具有卓越安全性和隐私性的品牌



随着智能网联汽车行业日益注重网络安全，确保驾驶员、乘客和其他道路使用者的安全性和隐私性，这显然也将成为消费者选择品牌时最重要的考虑因素。根据调研，53%的消费者会因为品牌提供的卓越安全性和隐私保护而选择该品牌的共享出行和自动驾驶服务。[2]

安全性和连接性是释放更大价值的关键

对于未来的出行解决方案，数据安全和隐私是消费者在选择汽车品牌时优先考虑的主要因素。安全性和连接性等核心服务对于实现高价值的附加服务（如自动驾驶和远程诊断）至关重要。



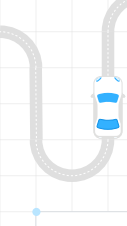
立即采取行动

1.
在整个产品生命周期中嵌入安全性和隐私性，强调安全是每个人的责任，包括利益相关者、合作伙伴甚至客户，从而增强安全性。

2.
采用双模思维，在专注于满足当前监管要求的同时，制定更广泛的安全设计策略来保护未来的出行解决方案。

3.
保护所有物理和数字供应链，为互联、自动驾驶、共享、电动(CASE)生态系统制定规划，使用通用标准、工具和合作伙伴的专业知识来提高效率。

汽车行业 CEO 将安全性和隐私性视为首要挑战

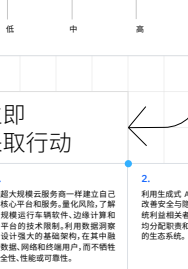


汽车行业 CEO 将安全性和隐私性视为一项主要挑战，其重要性仅排在可持续性之后。随着数据泄露的负面影响日益严重，企业高管认识到车辆的网络安全和隐私问题会损害业务收入和品牌声誉，面对边缘连接、无线软件更新和电信连接覆盖的复杂性，企业需要通过坚定的领导力、团队合作和设计思维来满足不同利益相关者的需求。

宏大愿景与实际行动之间严重脱节

大多数汽车组织都制定了安全战略，但只有不到一半的汽车组织将其落实到行动中。[4]

安全性和隐私性往往都是事后才考虑的因素，并没有从一开始就融入产品开发和生产中。具体的障碍包括缺乏工具、资源、专业知识和组织协同。例如，63%的受访汽车业高管表示缺乏资源，56%的受访高管表示缺乏通用工具，51%的受访高管认为业务部门之间缺乏整合，47%的受访高管认为缺乏共同治理构成了障碍。[5]



前方有路障？

随着智能网联汽车引入越来越多的连接功能，汽车的受攻击面迅速扩大。在考虑网络安全风险时，汽车行业高管意识到声誉受损的影响很大，但可能低估了未来出行威胁的可能性。为了降低风险，智能网联汽车的安全功能应在设计时就嵌入并默认启用。[6]

立即采取行动

1.
像超大规模云服务商一样建立自己的核心平台和服务。量化风险，了解大规模运行车辆软件、边缘计算和云平台的技术限制，利用数据洞察来设计强大的基础架构，在其中融合数据、网络和终端用户，而不牺牲安全性、性能或可靠性。

2.
利用生成式 AI 和自动化的潜力来改善安全与隐私流程，利用生态系统利益相关者的集体智慧，确保平均分配职责和激励，打造更具弹性的生态系统。

3.
在制定商业认证时考虑未来因素。预见智能网联软件定义汽车的安全漏洞，考虑安全性和隐私性如何让您的品牌脱颖而出，并将其价值融入基础架构。

想要了解有关此主题的更多见解和讨论？

请参阅：

保障隐私，迎接互联汽车的光明未来

加速车辆信息安全

立即订阅研究驱动的洞察信息简报，助您做出更明智的业务决策。

如需详细了解人工智能和自动化在网络安全领域的应用，请查看：

人工智能和自动化助力网络安全

CEO 生成式 AI 行动指南：网络安全

AI 的强大功能：安全性

DRQO0E0Z-ZHCN-00