AI EDGE LABS

CYBER SECURITY IN AUTOMOTIVE

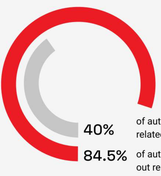
Automotive Under Attack

225% cyber attacks on cars increased in the last three years.

Hackers took control of a Jeep and 1.4 million vehicles had to be recalled to fix the bug that enabled the attack.

The industry can lose up to **$1.1B** for a single attack.

Automotive Cybersecurity Landscape



40% of automotive cybersecurity issues are related to back-end application servers.

84.5% of automotive attacks were carried out remotely.

By 2030, there will be **4x** autonomous robotaxis globally than today.

IoT Devices are Cyber Targets

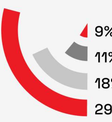
470M IoT devices in vehicles and endpoints with a global revenue of **$389B**.

775M connected cars are projected to be on roads by 2023.

of stakeholders are concerned about cybersecurity vulnerabilities in on-board diagnostic systems

Top Attack Types

Top Attack Vectors



9% Credential harvesting

11% DDoS

18% Server access

29% Malicious insiders

AI Cybersecurity Maturity in Automotive

10% feeling satisfied.

10% of automotive suppliers say cybersecurity ranks high on top management's agenda.

45% consider external partners' security as important.

70% wish for higher cyber maturity in their automotive supply chains.

of OEMs believe a high level of cybersecurity maturity is a significant competitive advantage.

With increasing connectivity, the vulnerability of cars increases too. AI EdgeLabs can be deployed as a smart AI-based Firewall to protect the car from unauthorized access.

AI EdgeLabs is an all-in-one AI-based platform that brings advanced network visibility, early threat detection, automated incident response and remediation vital for the newest technologies in automotive.

PROTECT YOUR EDGE & IOT ENVIRONMENT

AI EDGE LABS