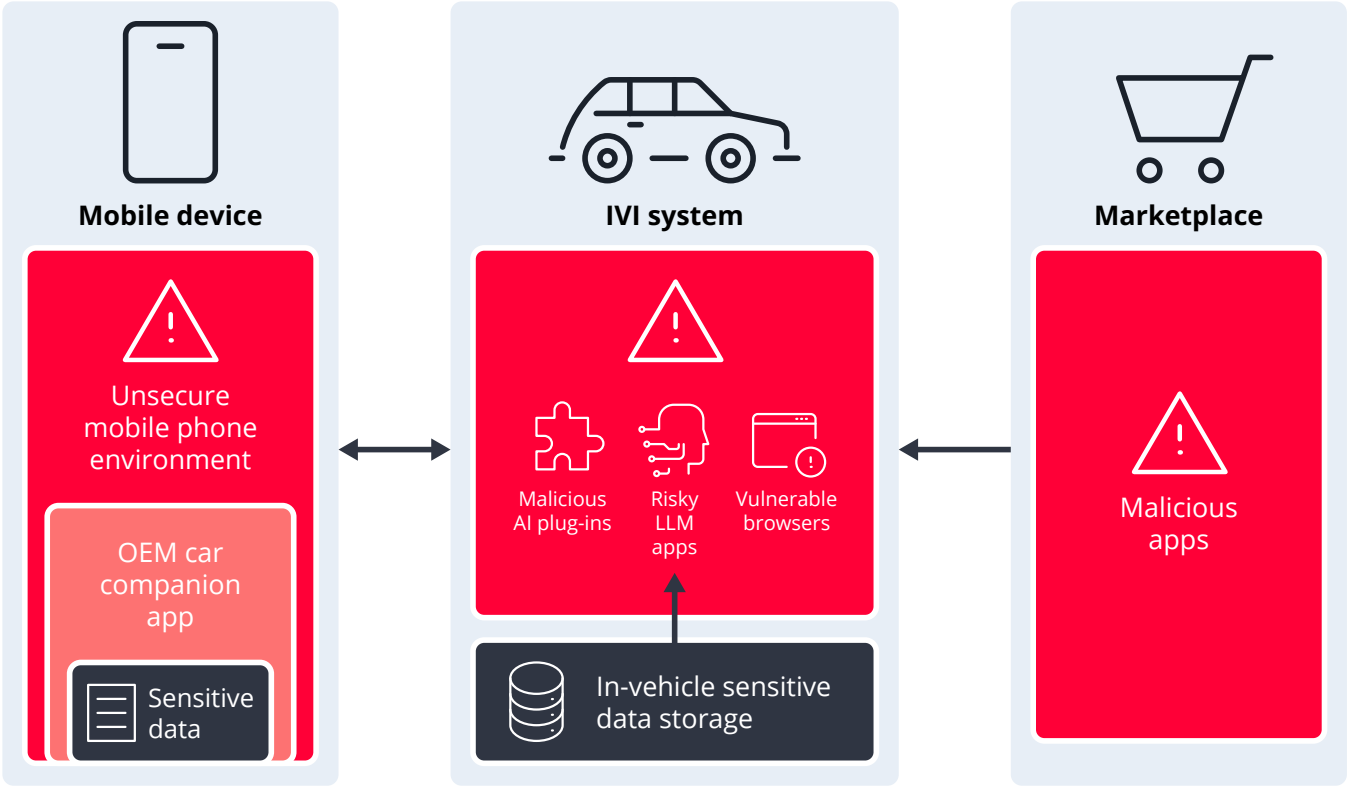
Smart Cockpit Protection

Securely Innovate AI-Powered Cockpits by Avoiding Sensitive Data Leaks and Addressing Security Risks

AI-Powered Cockpit Risks: Battling Sensitive Data Leaks

In the first half of 2023 alone, the automotive industry lost over US$9.5 billion to data leaks and personally identifiable information (PII) exposure.* As the landscape of software-defined vehicles evolves, safeguarding user data becomes paramount. Our experience highlights several potential risks that could lead to sensitive data leaks, including malicious AI plug-ins, risky LLM apps, vulnerable browsers, and other unsafe software. These threats underscore the critical need for robust security measures to protect user-sensitive data in the AI-powered cockpit era.

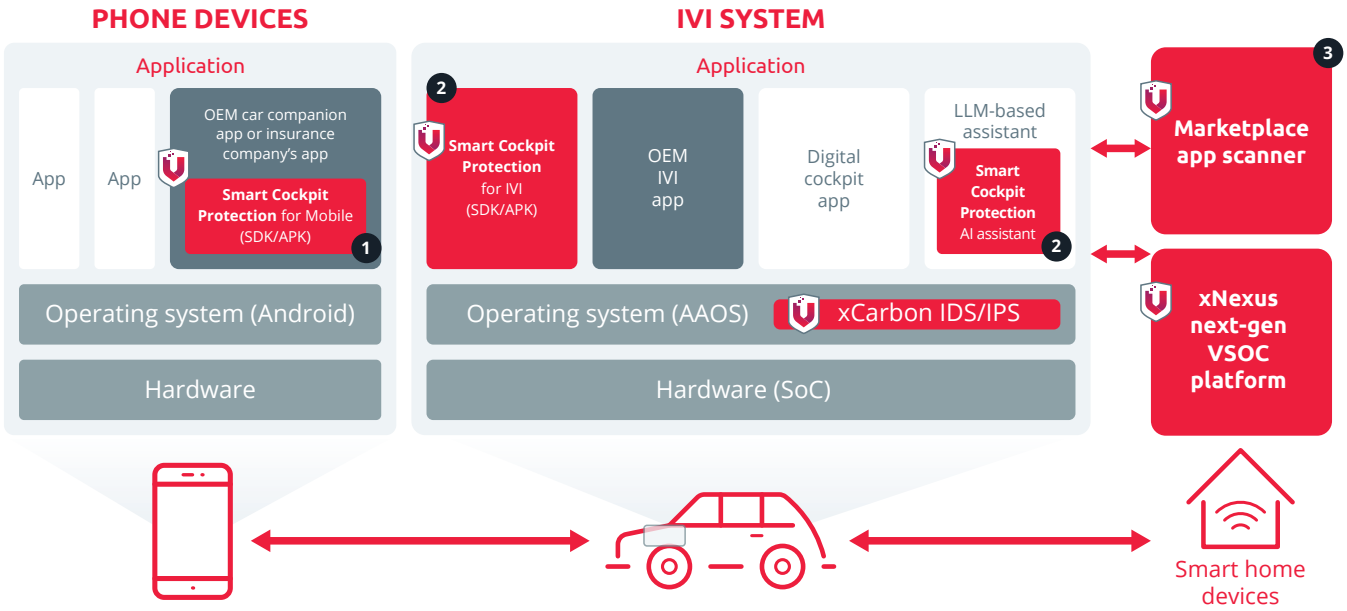


Source: VicOne Automotive Cyberthreat Landscape Report 2023

Be Empowered to Innovate Confidently in the AI Cockpit Era

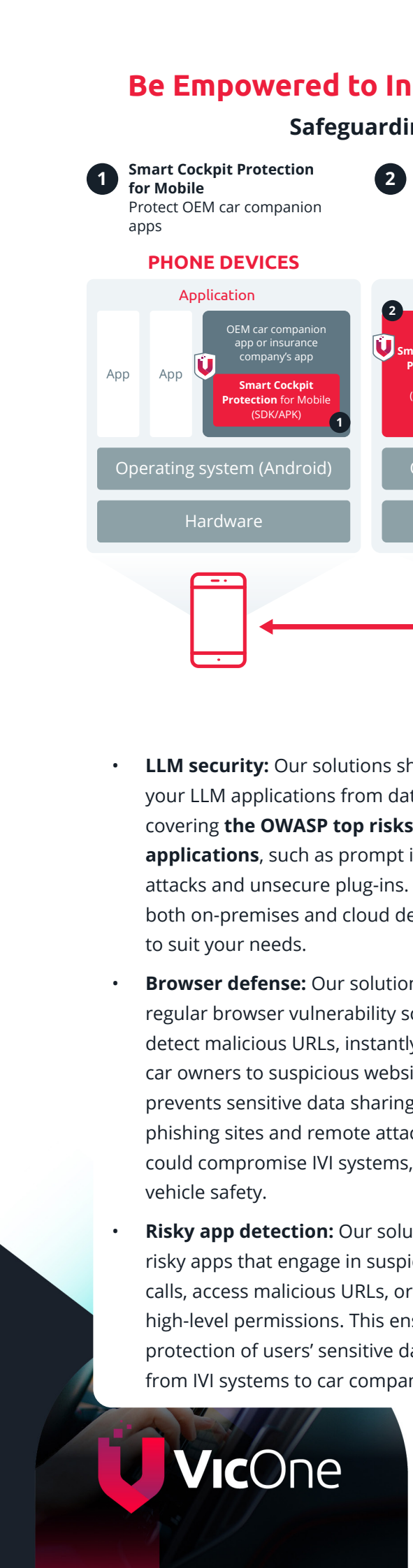
Safeguarding Every Aspect of the Smart Cockpit

1. **Smart Cockpit Protection for Mobile**
   Protect OEM car companion apps
2. **Smart Cockpit Protection for IVI**
   Shield IVI systems and LLM applications against data leaks and security risks
3. **Smart Cockpit Protection for Marketplace**
   Secure marketplaces to avoid malicious apps



Feature Highlights

- **LLM security:** Our solutions shield your LLM applications from data leaks, covering **the OWASP top risks for LLM applications**, such as prompt injection attacks and unsecure plug-ins. We support both on-premises and cloud deployments to suit your needs.
- **Browser defense:** Our solutions conduct regular browser vulnerability scans and detect malicious URLs, instantly alerting car owners to suspicious websites. This prevents sensitive data sharing with phishing sites and remote attacks that could compromise IVI systems, ensuring vehicle safety.
- **Risky app detection:** Our solutions detect risky apps that engage in suspicious API calls, access malicious URLs, or request high-level permissions. This ensures robust protection of users' sensitive data and PII — from IVI systems to car companion apps.
- **24/7 data monitoring:** Our solutions keep an eye on the dark web and other parts of the internet for leaks of customers' PII and automotive data like VINs. Upon detecting a leakage, we alert customers immediately, enabling swift response.
- **Rogue and unsecure Wi-Fi detection:** Our solutions detect unsafe Wi-Fi connections, identifying potential man-in-the-middle attacks and credential leakage risks.
- **Marketplace app scanning:** Our solutions scan for malware, viruses, APK weaknesses, APK vulnerabilities, and malicious AI plug-ins. This ensures that apps are safe before reaching app stores.
- **Automotive mobile app protection:** Integrating our SDK into automotive and insurance apps ensures a secure mobile environment, preventing personal data leaks.



VicOne

Smart Cockpit Protection

Learn more about VicOne by visiting VicOne.com or scanning this QR code: