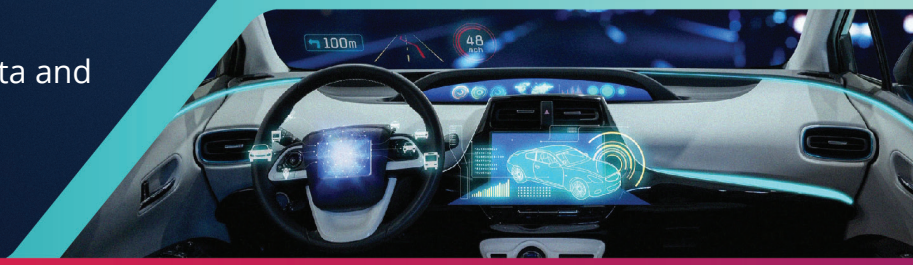
Smart Cockpit Protection

VicOne

Safeguarding Every Aspect of the Smart Cockpit: From Personal Data and Privacy to Outside Connections



Software-enabled services represent your next opportunity for generating revenue, so protecting your customers' personally identifiable information (PII) and data privacy is crucial to earning their trust. With the increasing use of in-vehicle infotainment (IVI) systems in smart cockpits, attackers could abuse leaked PII to compromise your customers' smart cockpits and even breach their home networks. This could enable attackers to eavesdrop on your customers' intimate conversations in the car or at home, or even steal their identities or vehicles. Don't let the vehicle become the weakest link in safeguarding your customers' personal data, privacy, IVI systems, and outside connections.

Key Benefits

Protect Your Customers From Identity Theft

Our solutions enable OEMs to offer a smart cockpit security app that customers can download directly from the OEMs' app stores or that comes preinstalled in the IVI systems. This not only helps protect customers' personal data, but also allows OEMs to monetize their cybersecurity efforts.

Maintain Positive Brand Image

Giving customers the option to purchase smart cockpit protection builds trust and increases customer loyalty. This is a smart move as OEMs can give customers the solutions to protect their personal data and privacy.

Create New Revenue Streams

OEMs can offer more innovative services to customers by building on a foundation of security. Additionally, OEMs can create new revenue streams by monetizing cybersecurity.

Extend Attack Surface Visibility

Attack surface visibility can be extended from the system level to the application level to support OEMs for future threat detection and response.

Key Features

IVI Privacy and Identity Protection
Our solutions can detect and block malicious apps that can access personal data excessively or unnecessarily, preventing the leakage of personal data.

Car Companion App Protection
By integrating our security SDK into car companion apps, OEMs can ensure that the apps run in a secure mobile environment, preventing the leakage of personal data.

IVI App Vulnerability Detection
IVI apps might have design flaws or zero-day vulnerabilities that mcalicious actors could exploit. Our solutions can detect and identify vulnerable apps, enabling car owners ro easily block them to prevent PII leakage.

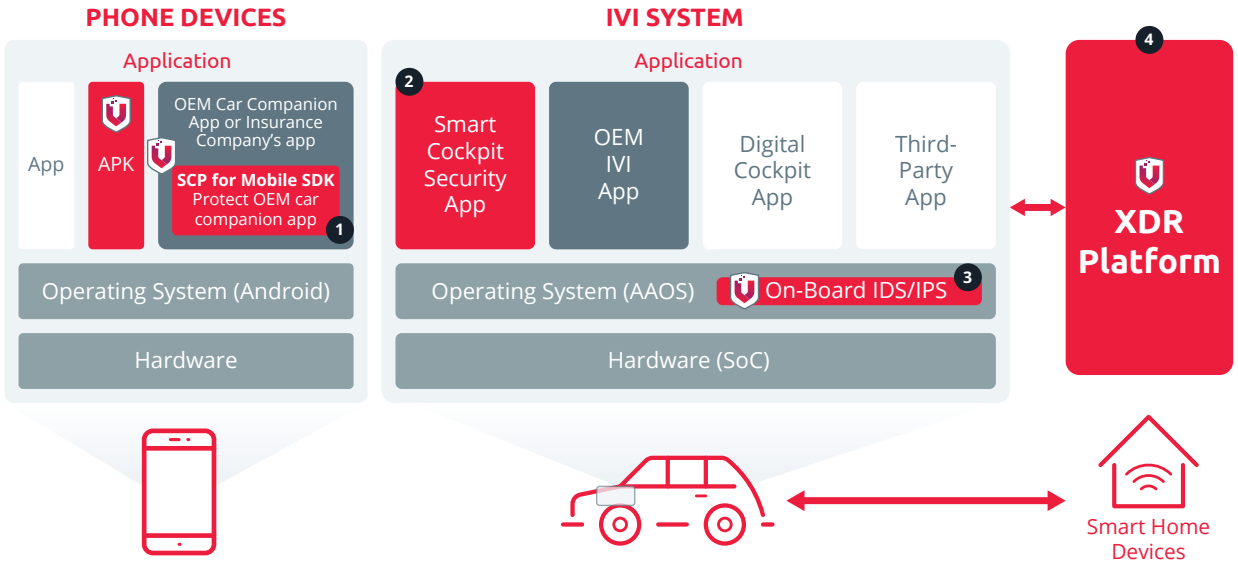
Malicious URL Detection
Our solutions perform regular scans for browser vulnerabilities and alert car owners when they attempt to connect to suspicious websites, preventing attackers from accessing their personal data.

IVI App Performance Check
Our solutions continously monitor IVI app performance, including power consumption and storage usage, to detect any abnormality.

IVI Privacy and Identity Protection
Our solutions monitor the internet and the dark web to safeguard your customers' personal information, including credit card details, social security numbers, and more. They trigger alerts as soon as the find PII has been leaked.

Securing the Smart Cockpit From the System Level to the Application Level

1. **Smart Cockpit Mobile SDK** Protect OEM car companion app
2. **Smart Cockpit Security App** Secure personal data, privacy, and outside connections in IVI system
3. **xCarbon** Secure on-board ECUs with IDS/IPS
4. **xNexus** Detect and respond to threats with XDR platform for VSOCs



VicOne
Driving Automotive Cybersecurity Forward

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