As connected vehicles become the norm, we expect to see more hackers launching targeted cyberattacks, which will impact physical safety, damage your brand and expose you to enormous liabilities. Irdeto's Cloakware technology has been deployed in over 2 billion connected devices, preventing cyberattacks for some of the world's leading companies. Not only does our software secure valuable digital assets, Irdeto has the breadth of knowledge and experience that comes from defeating professional hackers and criminals for almost five decades.

Let us show you how Irdeto's Cloakware for Automotive can protect your brand and save cost in the battle against cybercriminals.

© 2016 Irdeto, All Rights Reserved

When a hacker breaks through, we're the dog behind the door

Cloakware for Automotive

Security Services

Telemetry
Monitoring
Security analysis
Investigations

Secure Environment

Infotainment systems
OTA platforms
Telematics systems
V2X

Software Protection Service

Smart code analysis
Multiple language support
Automated protections
Automated assembly

Keys & Credentials

V2V
Root of Trust
V2I
Communications

Who	What	Why
OEM	Security Operations Center *Telemetry based monitoring*	• Professional security assessments • Cyber incident planning and response • Cyber forensics and law enforcement support
	Keys & Credentials *Manufacturing provisioning service*	• Customization of key packages tailored to HW models • Established relationships with suppliers (System on a Chip (SOC) vendors) • Industry best practices for key management • Factory and in-field key provisioning of ECUs
Tier 1	Secure Environment *Complete module protection*	• Protects against reverse engineering of binaries on the module • Protects against the execution of modified or malicious code on a protected module • Protects the application data on the system, both during storage and in use • Telemetry of security events to Security Operations Center (SOC)
Application Developer	Software Protection *Application "anti-hacking" protection*	• Code obfuscation mitigates against reverse engineering of binaries • White-box cryptography protects keys from being lifted, even while being used • Security tools provide security features and flexibility for software development • Binary protections provide code signing and anti-debug protected for applications