Argus Connected ECU Protection

Argus Connected ECU Protection detects and mitigates a wide range of attacks targeting connected ECUs, reducing the risk of financial loss, extraction of private data, and disruption of vehicle functionality.

MULTI-LAYERED PROTECTION FOR MAXIMUM SECURITY

Connected ECU Protection includes six easy to deploy independent modules that can work individually, or together, to provide comprehensive host-based security.

- **PLATFORM INTEGRITY**: Prevents and blocks unauthorized software from running on the ECU by validating the software at boot and during runtime.
- **SYSLIMITER**: Prevents unauthorized commands and resource access with automotive-grade mandatory access control.
- **ECU FIREWALL**: Prevents attacks from spreading to the in-vehicle network by blocking malicious communications using Deep Packet Inspection.
- **CONTROL FLOW INTEGRITY**: Prevents exploitation of vulnerabilities, by ensuring that the ECU program does not deviate from its expected execution flow.
- **THREAT DETECTION**: Prevents attacks in real time, by identifying and responding to suspicious behavior across the ECU that may indicate an unknown attack.

**KEY BENEFITS**

- Autonomous
- Multi-Layered
- Modular and Scalable
- Automotive-grade

**SECURITY LOGGER**: Collects and securely stores security events from each module, and from other data sources in the ECU, for further analysis by the OEM.
A VULNERABLE TARGET FOR HACKERS

Connected ECUs are at high risk of attack due to their inherent features, for example:

- Many external connectivity interfaces, such as wireless connection, Wi-Fi, Bluetooth and V2X
- Widely-used, high-performance operating systems such as Linux, Android and QNX, with existing databases of vulnerabilities

PROTECTING CONNECTED ECUS

- IVI
- TCU
- ADAS
- and more...

COVERING MULTIPLE ATTACK SCENARIOS

- Initial penetration
- Attack propagation
- Malware installation
- OS anomalies
- Zero-day exploits
- and more...

KEY FEATURES

- Supports Linux, QNX, and Android operating systems
- Offers seamless integration & easy configuration
- Designed for easy reuse across ECUs
- Consumes minimal system resources
- Supports future feature activation

WHY ARGUS

Awarded Production Projects
Multiple SOPs in 2020 with OEMs & Tier 1s

Acknowledged Automotive Vendor
Partnerships with industry leaders

Team of Experts
Automotive & Cyber expertise - offering based on real world hacker expertise

Leading Technology
Outperforms competitors in 3rd party evaluations

Scalable Holistic Offering
Protects connected high-performance ECUs to embedded ECUs throughout their lifespan

WE ARE ARGUS CYBER SECURITY

Argus, the global leader in automotive cyber security, provides comprehensive and proven solution suites to protect connected cars and commercial vehicles against cyber-attacks. With decades of experience in both cyber security and the automotive industry, Argus offers innovative security methods and proven computer networking know-how with a deep understanding of automotive best practices. Customers include car manufacturers, Tier 1 suppliers, fleet operators and aftermarket connectivity providers. Founded in 2013, Argus is headquartered in Tel Aviv, Israel, with offices in Michigan, Silicon Valley, Stuttgart and Tokyo. Learn more at www.argus-sec.com.

Argus is an independent company of Elektrobit, a leading provider of automotive software products and services.

Tel Aviv, Israel - Global HQ and R&D Center
T. +972 77 899 5100
E. contact@argus-sec.com

Stuttgart, Germany - EMEA HQ
T. +49 7021 8668 999
E. emea@argus-sec.com

Detroit, Michigan - North America HQ
T. +1 248 365 8781
E. usoffice@argus-sec.com

Tokyo, Japan - APAC HQ
T. +81 3 3588 0133
E. japan@argus-sec.com

Redwood City, California - West Coast Office
T. +1 650 283 4402
E. westcoast@argus-sec.com

Shanghai, China - China Office
T. +86-21-50431981
E. china@argus-sec.com