



Automotive Cyber **Security**

ARGUS
CYBER SECURITY



ARGUS WORKS WITH THE AUTOMOTIVE INDUSTRY TO ENABLE CONNECTIVITY WITH SECURITY AND PRIVACY

The more advanced cars and commercial vehicles become, the more vulnerable they are to cyber-attacks. With hundreds of millions of connected vehicles expected on the roads by 2020, the safety and security of our roadways and the private and successful use of connectivity rests on automotive cyber security.

Argus Cyber Security addresses the challenges posed by vehicle connectivity with the most comprehensive portfolio in the industry, delivering multi-layered, end-to-end protection against cyber-attacks that is future-proof and ready-to-embed today.

Founded in 2013, Argus is the world's largest, independent automotive cyber security company working with the major OEMs and Tier 1 suppliers. Argus solutions are built from the ground up for the automotive industry by a team of experts with decades of experience in both cyber security and automotive.

Argus stays on the cutting-edge and keeps its customers ahead of the threats through an ongoing commitment to automotive cyber security research, already having garnered over 30,000 research hours and dozens of granted and pending automotive patents.

With the industry's most comprehensive portfolio of solutions and services, Argus is well positioned to meet the dynamic cyber security challenges posed by increased connectivity:



KEEP PASSENGERS SAFE

With 100 million lines of code, modern vehicles are susceptible to cyber-attacks, which can result in physical damage to people and property.



PREVENT CYBER-RECALLS

In the face of a threat, without actionable information and tools, automakers will be subject to widespread, costly cyber-recalls and brand damage.



PROTECT CUSTOMER PRIVACY & PROPERTY

Connected vehicles generate valuable and sensitive data about individuals and fleets including driving habits, location routines, contacts and more.

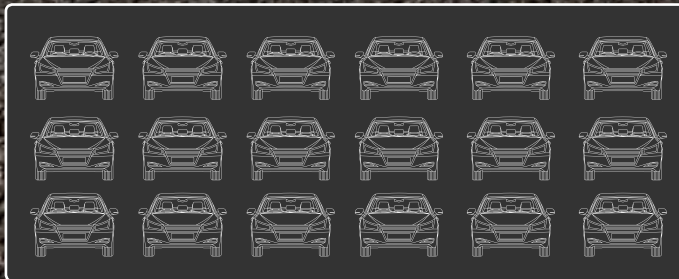


"Drivers shouldn't have to choose between being connected and being protected."

Edward J. Markey, US Senator

ATTACKS CAN ENTER CONNECTED VEHICLES IN MULTIPLE WAYS:

- | | |
|--------------------------|-------------------------------------|
| Wi-Fi | Cellular (3G, 4G) |
| OBD-II dongles | Infotainment\ Telematics |
| USB/CD interfaces | V2X |
| Smart phone applications | Service and dealership equipment |
| Bluetooth | Compromised supply-chain components |



MOST COMPREHENSIVE, MODULAR PROTECTION IN THE INDUSTRY



ARGUS CONNECTIVITY PROTECTION SUITE

Defends the infotainment or telematics units by preventing malware installation, detecting operating system (OS) anomalies, isolating suspicious applications and stopping attacks from spreading to the in-vehicle network. Argus Connectivity Protection also secures the communication channels with the outside world and operates cross platform (Linux/QNX/Android & more) to protect the car's most vulnerable attack surfaces.



ARGUS IN-VEHICLE NETWORK PROTECTION SUITE

Provides in-vehicle network-wide security by detecting attacks and changes in standard in-vehicle network behavior. Deployed centrally, Argus In-Vehicle Network Protection examines all network communication and stops attacks from advancing in the network. Supporting a wide array of network protocols—CAN and CAN-FD, FlexRay, Ethernet (with SOME/IP, DoIP etc.) and more—this suite is well positioned to defend current and future vehicle architectures.



ARGUS AFTERMARKET PROTECTION SUITE

Delivers telematics technology providers, connectivity service providers, fleet managers, insurance companies, dealerships and dongle manufacturers solutions that protect vehicles from attacks exploiting their technologies and services. Argus Aftermarket Protection provides in-vehicle network protection and dongle protection to retrofit connected cars and commercial vehicles on the road.



ARGUS ECU PROTECTION SUITE

Reinforces select electronic control units (ECUs), such as brakes, advanced driver assistance system (ADAS), door control units or any other units deemed critical, from attacks originating inside or outside of the ECU. Located on the ECU, this suite detects and prevents incoming attacks as well as neutralizes malware resulting from supply chain attacks or other attack vectors. Non-intrusive and with a small footprint, Argus ECU Protection supports virtually any ECU.



ARGUS LIFESPAN PROTECTION SUITE

Future-proofs the fleet with an additional layer of protection. Operating from the cloud or integrated in a security operations center (SOC), this suite provides OEMs and fleet managers situational awareness of fleet cyber health on an intuitive dashboard. Argus Lifespan Protection also generates insights on new attacks and trends from big data analytics of OEM and fleet data, and provides the tools to take preemptive action.



Argus Lifespan Protection Dashboard



TRUSTED ADVISOR TO THE WORLD'S LEADING AUTOMAKERS

Led by a team of cyber security and automotive experts, Argus has collected a wealth of unique expertise based on 30,000 hours of research in automotive cyber security. We share this knowledge with our customers through a wide range of services:

- ✓ THREAT ANALYSIS
- ✓ RISK ASSESSMENT
- ✓ VULNERABILITY ANALYSIS
- ✓ CODE REVIEW
- ✓ PENETRATION TESTING
- ✓ INCIDENT RESPONSE
- ✓ CYBER THREAT INTELLIGENCE
- ✓ REQUIREMENTS DEFINITION AND VALIDATION
- ✓ TRAINING
- ✓ CYBER SECURITY MANAGEMENT SYSTEM

ARGUS – Delivering projects to the world's largest OEMs and Tier 1 suppliers

✓ **Most Comprehensive Solutions in the Industry**

Multi-layered, end-to-end protection provides optimal security.

✓ **Technologically Superior**

Mature, modular solutions based on unparalleled innovation with multiple pending and granted patents.

✓ **Automotive and Cyber Excellence**

Solutions built from the ground up for the automotive industry by a team with decades of experience in both cyber security and automotive.

✓ **Futureproof, Ready-to-Embed**

In-vehicle solutions work stand-alone to protect against today's threats or work integrated in a cloud solution to generate insights on new attacks and to provide the tools to take preemptive action.

"The surface area of potential attacks is set to increase significantly and the transport industry needs to get to grips with this immediately."

Andrew Everett, Chief Strategy Officer, Transport Systems Catapult, UK.

ARGUS OFFICES WORLDWIDE

Global HQ and R&D Center

24 Raoul Wallenberg St.

Tel-Aviv 6971920, Israel

T. +972 (0) 77 8995100

E. contact@argus-sec.com

EMEA HQ

European Metropolitan Region, Stuttgart Plotchinger Strasse 58

73230 Kirchheim unter Teck, Germany

T. +49 7021 8668 999

E. emea@argus-sec.com

North America HQ

Suite 350, 41000 Woodward Ave,

Bloomfield Hills, MI 48304

T. +1 248 385 8781

E. usoffice@argus-sec.com

West Coast Office

541 Jefferson Ave, Suite 100

Redwood City, CA 94063

T. +1 650 283 4402

E. westcoast@argus-sec.com

APAC HQ

S601 ARK Kills Executive Tower, 1-14-5 Akasaka, Minato-Ku,

Tokyo, Japan 107-0052

T. +81 3 3588 0133

E. japan@argus-sec.com

WE ARE ARGUS CYBER SECURITY

Argus Cyber Security™ is the world's largest, independent automotive cyber security company whose customers include the major private and commercial OEMs, Tier 1 suppliers, aftermarket connectivity providers and fleet managers. Led by a team of cyber security experts and auto industry veterans, Argus solutions are built on decades of experience in both cyber security and the automotive industry. Committed to helping customers stay ahead of threats, Argus' award winning research team steadfastly keeps up-to-date with current and future cyber threats to continually ensure that Argus' solutions remain on the cutting edge. Founded in 2013, Argus is headquartered in Tel Aviv, Israel, with offices in Detroit, Silicon Valley, Stuttgart and Tokyo.

Visit Argus:

www.argus-sec.com