AEGIS
SECURE VIRTUALIZATION
AT THE HYPERVISOR LAYER

PERSEUS

Be Simple, Be Secure

WHAT IT IS

Secure Type-1 (bare-metal) automotive hypervisor

Foundational system software for SDV platforms

WHAT IT DOES

Enforces system-level isolation and control below the OS layer

Contains faults and malicious activity between software domains

Protects safety-critical workloads from non-critical software

WHY IT MATTERS

Security enforcement where OS-level controls do not scale

Bounded, deterministic system behavior under fault or attack

A secure foundation for SDV development environments

www.cyberperseus.com

The Need for Scalable, Secure Virtualization

SDV platforms consolidate mixed-criticality functions (infotainment, connectivity, ADAS, and control workloads), as well as connectivity and updateable software onto shared hardware.

These complex software interactions increase attack surface and exposure to faults, denial-of-service conditions, and malicious interference originating in non-critical domains.
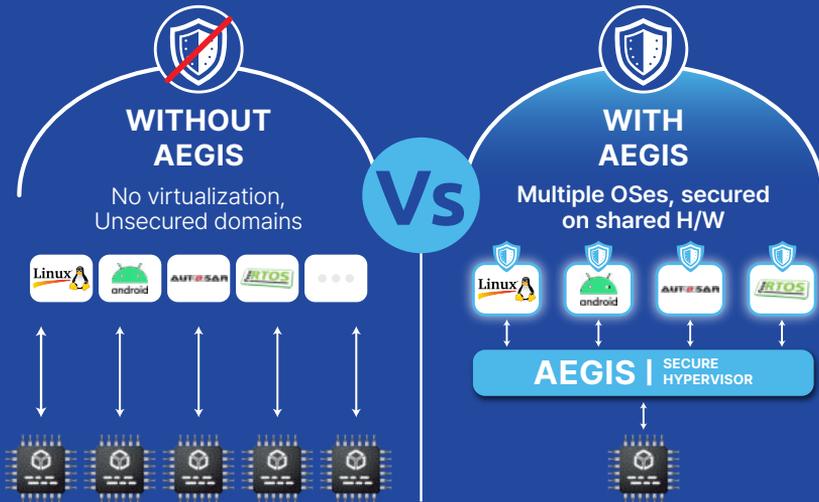
TRADITIONAL APPROACHES NO LONGER SCALE:

OS-level security cannot fully contain compromised OSes or prevent cross-domain interference.

TrustZone-only approaches protect isolated functions but do not scale to full multi-OS, mixed-criticality platforms.

To guarantee safety AND performance, cybersecurity must be enforced at the **hypervisor layer,** where isolation, resource access, and execution behavior are defined and managed.

WITHOUT AEGIS
No virtualization, Unsecured domains

Linux · android · AUTOSAR · RTOS · ●●●

Vs

WITH AEGIS
Multiple OSes, secured on shared H/W

Linux · android · AUTOSAR · RTOS
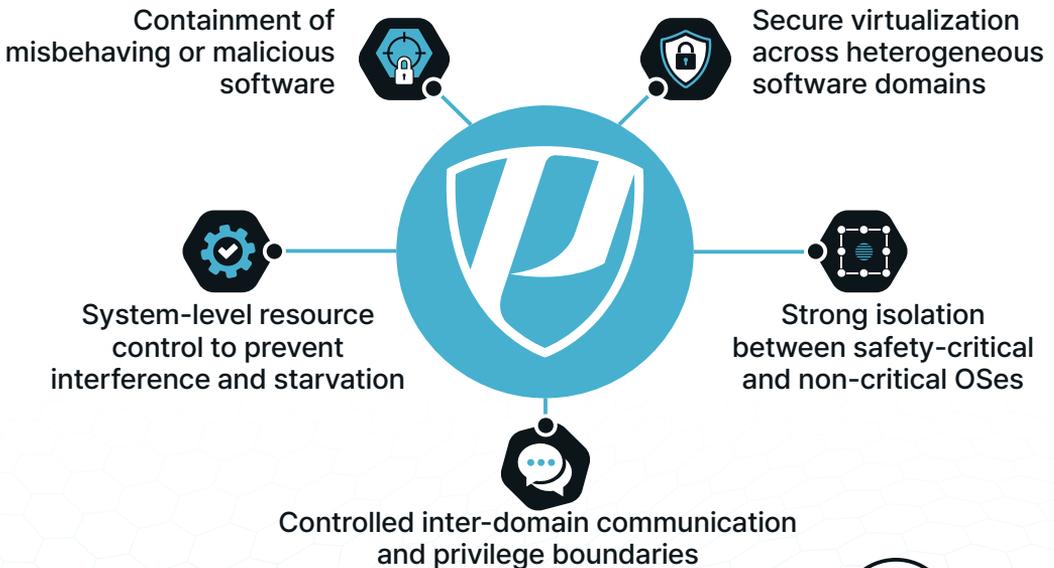
AEGIS | SECURE HYPERVISOR

AEGIS: Secure Hypervisor for SDV Platforms

Designed for **security-first enforcement** at the system layer, AEGIS applies secure virtualization to protect critical workloads from faults and attacks originating elsewhere in the system.

AEGIS establishes strong execution boundaries between software domains and controls access to compute, memory, and I/O resources, to enable containment of compromised software and denial-of-service conditions that cannot be reliably mitigated at higher layers.

SECURITY-FIRST HYPERVISOR DESIGN

Containment of misbehaving or malicious software

Secure virtualization across heterogeneous software domains

System-level resource control to prevent interference and starvation

Strong isolation between safety-critical and non-critical OSes

Controlled inter-domain communication and privilege boundaries

DETERMINISTIC BEHAVIOR UNDER ATTACK

AEGIS preserves bounded, deterministic behavior for critical workloads even when non-critical software is compromised, limiting fault propagation and guaranteeing performance.

Applicable Across SDV Programs

- Connected vehicle cybersecurity and safety-critical control systems
- Safe coexistence of infotainment, connectivity and other functions
- Vehicle gateways & OTA-enabled platforms

PERSEUS

Be Simple, Be Secure

THE PERSEUS
SYSTEM SOFTWARE SUITE

AEGIS
Secure hypervisor

PEGASUS
Automotive hypervisor (ISO 26262 ASIL-D, CPU & MCU)

TACHYON
Linux Fast Boot (under 1.5 sec)

AEGIS-let
TrustZone-based secure kernel for ECUs

GAIA
Secure boot loader for MCU and multi-OS systems

Designed for long-lifecycle SDV programs and built for production, not R&D, AEGIS supports integration with leading Arm-based automotive semiconductor platforms from major Tier-1 ecosystems.

BEYOND AUTOMOTIVE

AEGIS is applicable to other software-defined, safety-critical systems, including logistics & transport, industrial infrastructure, defense & government, edge computing & AI, and high-reliability professional systems.

Talk to us about your system architecture

www.cyberperseus.com

sales@cyberperseus.com