

# FLEXIDS

## Zero Trust. Real-Time. AI-Trained Embedded Intrusion Detection

Cyberattacks do not wait at the perimeter — their targets are the embedded devices at the physical edge. From legacy industrial controllers to next-gen AI-driven ECUs and IoT nodes, every embedded device is a target. FLEXIDS is the only embedded IDS designed for this reality, delivering AI-enhanced intrusion detection and microsecond real-time enforcement inside the device itself.

The FLEXIDS cycle operates as a continuous loop of Monitor > Analyze > Detect > Adapt. A lightweight agent first monitors software execution inside the device with minimal overhead. Statistical, probabilistic, and machine learning models then analyze this data to establish a baseline of normal behavior. Any deviation is detected instantly as a potential anomaly, enabling corrective action to be taken in microseconds. FLEXIDS adapts continuously: retraining models in production to reduce false positives toward zero and staying resilient against evolving zero-day threats.

### KEY FEATURES

- **Zero Trust, Built In**  
Validates every execution path against a behavioral trust model, enforcing runtime integrity inside the device.
- **AI-Enhanced Detection**  
Learns normal behavior, flags anomalies instantly, signature-free and zero-day ready. Detection rates 20% higher than SVM, up to 500× fewer false positives.
- **Real-Time Embedded Processing**  
Responds in microseconds with no SOC or cloud dependency. Enables corrective action in mission- and safety-critical environments.
- **Embedded-First, Small Footprint**  
Optimized for MCUs, ECUs, IoT, and FPGAs. Lightweight CPU/memory requirements.
- **Legacy-Ready & Future-Proof**  
Secures installed embedded deployments while preparing for next-gen AI platforms.



### DATA COLLECTION

Lightweight agent runs inside the device — monitoring execution paths, tasks, and threads with minimal CPU and memory overhead.



### ANALYSIS

Statistical, probabilistic, and AI-trained models build baselines of normal behavior. Proven to achieve 20% higher detection rates than SVM and 500x fewer false positives than competing ML.



### ANOMALY DETECTION

Any deviation from trusted execution is flagged in microseconds, enabling corrective action before compromise can spread.



### MODEL REFINEMENT

Adaptive AI retrains in production, driving false positives toward zero and ensuring protection against zero-day and evolving threats.

### TECHNICAL PROOF POINTS

FLEXIDS is not just conceptually different, it is technically proven to deliver superior performance in embedded environments:

- **Detection latency in microseconds:** anomalies are flagged and acted upon before compromise spreads, meeting the demands of mission- and safety-critical systems.
- **Lowest false positive rates:** demonstrated up to **500× fewer false positives** compared to competing ML approaches, reducing noise/analyst fatigue.
- **Highest detection rates:** proven **20% higher** than Support Vector Machines (SVM) and **14% higher** than Density Based Spatial models (DBS) across zero-day and evolving threats.
- **Lightweight deployment:** runs entirely on-device without reliance on SOC, cloud, or backhaul; requires no source code modifications.
- **Compliance alignment:** supports standards and requirements in automotive, aerospace, and industrial domains (e.g., **ISO 26262**, **DO-326A**, **IEC 62443**).

### CORE VALUE TO PARTNERS

#### Semiconductors & IP Providers

Differentiate silicon with embedded runtime security.

#### Industrial & OT

Protect PLCs, SCADA, and long-lifecycle systems without forklift upgrades.

#### Automotive & Aerospace

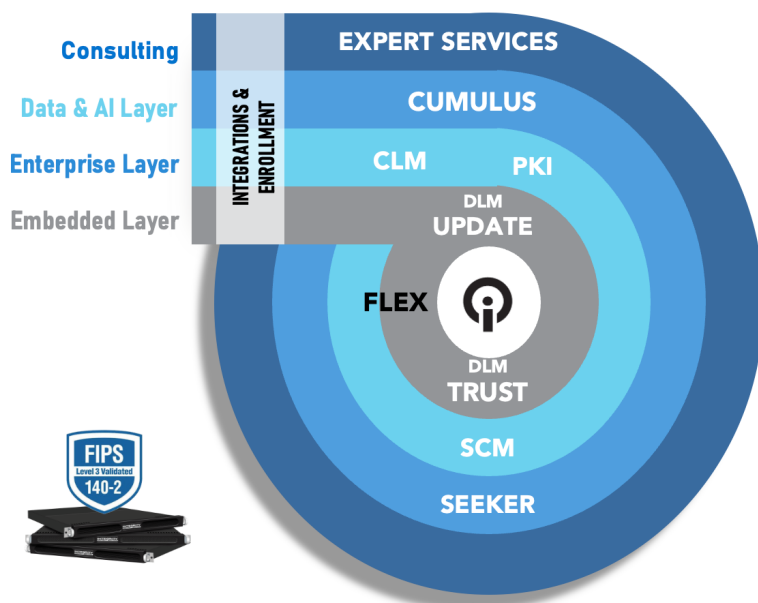
Secure ECUs and flight systems with real-time anomaly detection.

#### AI & Robotics

Guarantee runtime trust for agentic and autonomous platforms.

# About ISS

Introducing Integrity Security Services (ISS): ISS is the embedded security authority and market leader - the only Trust Lifecycle Management (TLM) platform designed to span the full chain of trust, from chip to cloud to AI. Unlike enterprise-only security vendors, ISS begins upstream, where trust is born inside devices and controllers at the physical edge.



## END-TO-END TLM ARCHITECTURE

ISS delivers layered trust across three domains:

- **Embedded Layer**  
Security built into firmware and hardware from the start, enabling cryptographic enforcement, secure updates, and runtime anomaly detection. This is where FLEX resides, and where FLEXIDS delivers embedded intrusion detection.
- **Enterprise Layer**  
Lifecycle management, policy enforcement, certificate handling, and supply chain trust at scale. Includes CLM, PKI, and update services that connect embedded devices to enterprise security.
- **Data & AI Layer**  
Discovery, visibility, and trust intelligence through integrated telemetry, crypto analytics, and insight via Seeker and Cumulus.
- **Consulting & Expert Services**  
Integration, onboarding, architecture design, and mission-critical security validation for partners and customers.

## FLEX AND FLEXIDS IN CONTEXT

As part of the broader FLEX portfolio, FLEXIDS extends ISS' embedded-first philosophy by ensuring devices remain trusted at runtime. It complements secure boot and cryptographic services with real-time intrusion detection inside the device itself. By operating within the ISS TLM platform, FLEXIDS is not a standalone tool, but a connected capability that feeds anomalies into Seeker telemetry and Cumulus governance for lifecycle-wide visibility and compliance.

## VALUE OF ISS & FLEX TO PARTNERS

### Holistic Security

FLEXIDS is anchored in a complete platform that spans embedded, enterprise, and AI.

### Integration & Scale

Partners can start with embedded intrusion detection and expand to full lifecycle trust.

### Expert Support

ISS provides consulting and integration services to accelerate adoption in semiconductor, OEM, and industrial markets.

ISS delivers more than a product: it provides an end-to-end trust lifecycle platform. FLEXIDS is the embedded guardian, amplified through its integration with ISS TLM — securing billions of devices and enabling partners to build trusted systems for the next era of autonomy, connectivity, and safety-critical innovation.