SENSOR BIOMETRICS

January 2026

SensAbility Snapshot

Real-Time Validation Alerts at the Physical Layer

How SensAbility helps validate device identity and flag signal deviations early

Applications

Predictive maintenance
Device validation and authentication
OT/ICS integrity monitoring
IoT and embedded asset verification
Multi-vendor environment monitoring

Partnership Opportunities

SensAbility is building a partner ecosystem with sensor OEMs, DAS/ICS/OT monitoring vendors, asset management platforms, and system integrators positioned to extend SensAbility into a broader commercial Edge + SaaS offering. Partners can integrate SensAbility into condition monitoring, device validation, and asset integrity workflows to verify hardware identity, identify unauthorized substitutions, and improve confidence across operational environments.

Contact Information

Kirk Byles, CEO | Kirk@rapiertechgroup.com | 303-886-6379

Overview

Most alerts appear only after higher-layer symptoms emerge. By then, the device may already be behaving abnormally, presenting the wrong identity, or introducing risk into the environment.

SensAbility closes that gap by monitoring devices at the physical layer in real time. It compares live signal behavior against a trusted baseline to validate identity and highlight meaningful deviations before they become outages, disruptions, or larger integrity issues.

The Problem

In OT, ICS, IoT, and embedded environments, many tools identify assets through logs, credentials, protocol behavior, or inventory records. Those signals are useful, but they do not prove that the emitting device is actually the trusted device operators expect. A spoofed, substituted, or tampered device can still appear normal at higher layers, delaying detection and expanding blind spots.

The SensAbility Approach

SensAbility uses passive physical-layer fingerprinting to establish a trained baseline for expected device behavior. It then compares live observations against that baseline to validate identity and detect meaningful change in real time. When a device drifts from trusted behavior in a way consistent with spoofing, substitution, tampering, or abnormal operation, the system can raise a focused alert without firmware access, agents, or reliance on device self-reporting.

What It Can Help Detect

- Unauthorized or unknown devices attempting access
- Trusted hardware showing anomalous signal behavior
- Spoofing or substitution attempts
- Early device-level changes that precede higher-layer indicators

Operational Value

By validating devices at the signal layer, SensAbility can help organizations:

- Reduce validation delays when device behavior changes
- Improve response focus with more meaningful alerts
- Increase confidence in trusted device inventories

Deployment Fit

SensAbility fits uptime-critical environments with limited firmware access and mixed fleets of legacy, embedded, and modern equipment. It supports wired or wireless deployment through SaaS, enterprise, OEM, and edge models.