SENSOR BIOMETRICS

January 2026

SensAbility Snapshot

Device Validation and Unauthorized Hardware Detection

How SensAbility helps identify rogue, spoofed, or unauthorized devices at the physical layer

Applications

Predictive maintenance
Device validation and authentication
OT/ICS integrity monitoring
Multi-vendor asset verification
Unauthorized hardware detection

Partnership Opportunities

SensAbility is building a partner ecosystem with sensor OEMs, DAS/ICS/OT monitoring vendors, asset management platforms, and system integrators with the resources to develop SensAbility into a broad commercial Edge + SaaS product line. Partners can integrate SensAbility into existing condition monitoring, device validation, and asset integrity offerings to verify hardware identity, detect unauthorized substitutions, and improve confidence across complex multi-vendor environments.

Contact Information

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

Overview

Unauthorized or substituted hardware can blend into normal operations by reusing valid credentials, expected protocols, or familiar network behavior. That leaves a gap for devices that look legitimate in software but are not the device you expected to see.

SensAbility addresses that gap by monitoring devices at the physical layer. It compares live signal behavior against a trusted baseline to validate device identity and flag rogue, spoofed, cloned, or unauthorized replacement hardware in real time.

The Problem

In OT, ICS, IoT, and embedded environments, many tools identify assets by metadata, credentials, or network behavior. But unauthorized devices can imitate those indicators or inherit them through component swaps and physical access. When that happens, higher-layer monitoring may still show a healthy endpoint even though the emitting device is untrusted.

The SensAbility Approach

SensAbility uses passive physical-layer fingerprinting to establish a baseline for expected device behavior. It then compares new observations against that baseline to validate identity and detect meaningful change. This allows teams to catch unauthorized devices and suspicious deviations without firmware access, agents, or reliance on device self-reporting.

What It Can Help Detect

- Rogue devices introduced through physical access
- Spoofed or cloned hardware imitating trusted endpoints
- Unauthorized hardware replacements
- Signal-level deviations from known-good baselines

Operational Value

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

- Reduce blind spots in multi-vendor environments
- Respond faster to unauthorized hardware changes
- Improve confidence in connected devices

Deployment Fit

SensAbility is suited for environments where firmware access is limited, uptime is critical, or fleets include a mix of legacy, embedded, and modern equipment. The platform is positioned for wired or wireless deployments and can support SaaS, enterprise, OEM, and edge delivery models depending on the operating environment.