Cervello

Cybersecurity intelligence for modern rail networks

vossloh
enabling green mobility

Problem description

Rail networks face cyber threats in a connected world

Digital transformation in rail has created interconnected systems across IT, OT, IoT, signaling, and rolling stock. While improving efficiency, it also brings cybersecurity risks that generic tools can't address.

Limited visibility, misconfigurations, and unpatched vulnerabilities expose assets – like signaling and onboard systems – to threats such as spoofing, DoS, and protocol manipulation, risking safety and service. With rising standards like TS50701 and IEC 62443, operators need purpose-built solutions offering real-time, contextual insights and proactive defense.

Cervello delivers this – turning cyber risks into actionable intelligence.

Solution description

Rail-specific, passive network defense powered by AI

Cervello delivers an all-in-one platform for cybersecurity visibility, threat detection, and risk mitigation across complex rail environments. It passively collects and analyzes network traffic across IT, IoT, OT, signaling, and rolling stock infrastructure – without disrupting operations.

The system maps all assets and detects vulnerabilities, misconfigurations, and active threats using patented rail-specific algorithms. Collected data is securely transmitted to the Cervello Brain platform, which applies AI and contextual rail intelligence to provide real-time alerts, risk scores, and actionable recommendations.

Each insight is tied to operational impact – allowing asset managers to prioritize based on service, safety, or regulatory risk. Automated compliance monitoring ensures alignment with TS50701, IEC 62443, TSA Directives, and more. Cervello empowers railway operators to shift from reactive defense to proactive, resilient cyber-physical protection.

How it works

Main Features

- Unified visibility across IT, OT, IoT, and signaling networks
- Patented threat detection for rail-specific environments
- Passive traffic monitoring – no service disruption
- Asset mapping with operational and contextual insight
- Automated risk scoring linked to real-world impact
- Regulatory compliance tracking and reporting

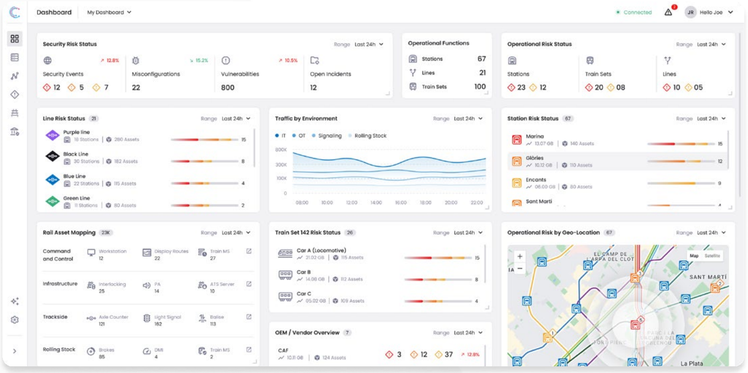
Hardware and implementation

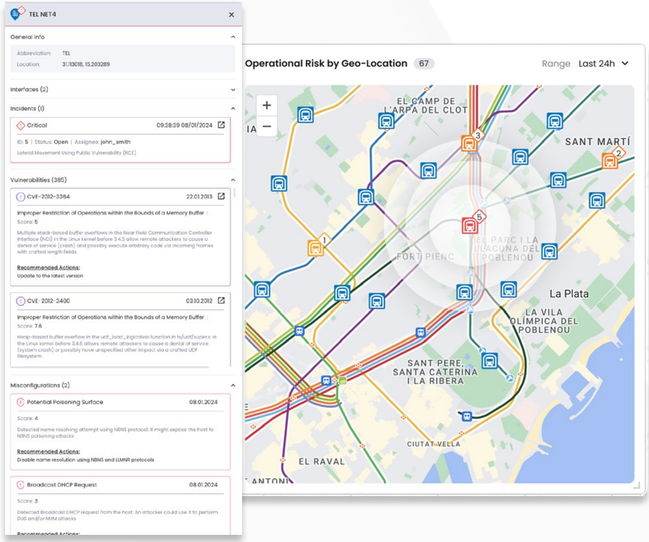
The Cervello platform is powered by lightweight, non-intrusive software collectors (Cervello-XE), which passively monitor traffic across all layers of the rail network: rolling stock, signaling, power systems, telecom, and more.

These collectors require no changes to existing infrastructure and can be deployed across trains, stations, and control centers. Data is sent via secure channels to the Cervello Brain – available as a virtual/on-premise server – where AI modules and a proprietary rail vulnerability database process and evaluate findings.

The system continuously updates its knowledge base, leveraging global rail cybersecurity research to stay ahead of emerging threats. The management console integrates with existing SOC/NOC workflows and provides intuitive dashboards for real-time visualization, incident response, and policy management.

This architecture ensures complete cyber protection while maintaining operational continuity and safety.

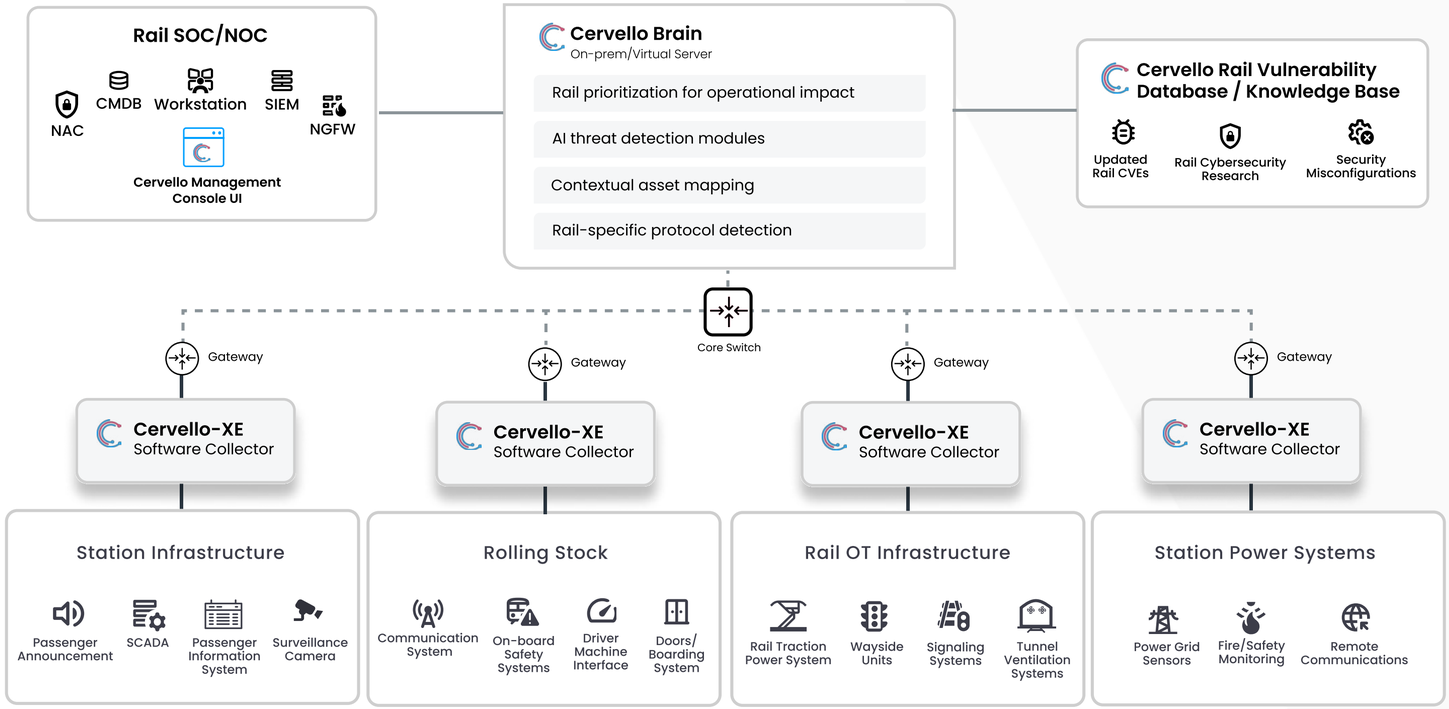




Cervello

Cybersecurity intelligence for modern rail networks

Deployment architecture



Sensor Type	Software-based passive collectors (Cervello-XE)
Coverage	Rolling Stock, Signaling, OT/ICS, IT, IoT, Telecom
Deployment	Non-intrusive, no downtime or configuration changes
Data Frequency	Real-time traffic monitoring
Data Processing	Cervello Brain with AI + rail threat models
Alerting	Contextual alerts linked to operational impact
Compliance	TS50701, IEC 62443, TSA Directives, NIS2
Visualization	Real-time dashboards, asset maps, risk scores
Integration	Connects to SIEM, CMDB, NAC, NGFW, and more