SEPIO

See what you've been missing

Visibility. Security. Trust. Control.

In the railway industry, securing operational infrastructure, signaling systems, and onboard technologies is paramount. Sepio's hardware security solution provides unparalleled visibility and control over a diverse array of connected devices, delivering substantial value by addressing the unique cybersecurity challenges faced in rail networks.

Comprehensive Visibility

Gain full visibility over all devices across railway networks, including onboard train systems, signaling infrastructure, and station operations. Sepio ensures that only authorized devices connect, providing a clear and complete asset inventory for enhanced security and operational control.

Granular Controls

Set specific USB and network controls based on security policies and operational needs. Whether managing onboard systems, station equipment, or control center infrastructure, enforce granular controls tailored to specific locations, VLANs, user groups, or device models.

Enhanced Protection

Prevent cyber threats caused by rogue hardware and unauthorized devices. Sepio's solution provides a robust defense layer, detecting and mitigating risks that other security solutions miss, ensuring uninterrupted railway operations.

Regulatory Compliance

Easily meet industry-specific regulatory requirements, such as railway safety and cybersecurity standards. Ensure compliance with regulations governing critical infrastructure, passenger safety, and operational resilience.

Operational Efficiency

Improve resource planning and budgeting for hardware across railway systems. Reduce hardware sprawl, enhance network security, and optimize efficiency by maintaining a streamlined and well-protected infrastructure.

// Key Challenges

- **Secured Railway Operations:** Protecting signaling systems, control centers, and onboard train technologies from unauthorized access. Ensuring only authorized devices connect to railway networks, mitigating the risks of cyberattacks and service disruptions.
- **Secured Rail Infrastructure:** Safeguarding station management systems, ticketing kiosks, and operational hardware. Preventing unauthorized devices from accessing railway network systems and critical infrastructure.
- **Secured Corporate & Passenger Services:** Securing railway corporate offices, operational command centers, and station hardware, including workstations, ticketing machines, and IoT devices. Protecting sensitive operational data, passenger information, and communication channels from internal threats and hardware-based cyber risks.

Learn more at: **sepiocyber.com**

SEPIO