goldilock

USE CASE 02

Rail sector

Proactively safeguarding rail operations, passenger safety, and national security across the modern rail ecosystem from cyber threat, at the physical connection layer with Goldilock FireBreak™.

Rail networks are fundamental to public mobility, economic prosperity, and national infrastructure, yet they face persistent and evolving cyber threats.

These adversaries range from nation-state actors seeking strategic disruption to financially motivated cybercriminal groups, all constantly probing and exploiting vulnerabilities within legacy Operational Technology (OT) systems that control critical infrastructure such as signalling and traffic management. The increasingly interconnected landscape of converged IT-OT environments, which manage passenger information and logistics, further expands the attack surface. Compounding these risks is the dangerously inadequate network segmentation across disparate operational areas. The potential consequences of successful attacks are severe: widespread train delays and cancellations causing commuter chaos and economic losses; manipulation of signalling systems leading to safety incidents; disruption of freight transport impacting supply chains; and the undermining of public confidence in the reliability and security of rail travel—a domino effect that impacts every aspect of our connected society.

Goldilock's FireBreak Physical Connection Controller offers a groundbreaking, hardware-enforced cyber defence that goes beyond conventional software protections. By physically isolating vital operational technology (OT) such as signalling and control systems, essential IT networks managing operations and passenger data, and critical backups from all network connectivity, FireBreak completely eliminates remote attack pathways. By physically disconnecting these crucial assets from all networks and segments during periods of inactivity or heightened vulnerability, they become undetectable and unreachable by cyber threats, establishing an impenetrable security boundary. FireBreak's network-invisible control channel creates a hardware-enforced isolation barrier that software alone cannot replicate.

The outcome? A physically disconnected environment forms an unassailable security domain, bolstering tamper-proof logging for incident analysis and ensuring adherence to stringent security regulations within the rail sector, providing unparalleled assurance for today's digitally reliant railway operations.

Engineered to satisfy the stringent requirements of Critical National Infrastructure (CNI) resilience frameworks and rail-specific regulatory standards, Goldilock FireBreak delivers unyielding cyber-physical protection that aligns with Zero Trust security principles. Whether safeguarding remote trackside signalling equipment, central traffic control systems, or sensitive passenger data repositories, FireBreak empowers rail operators to maintain uninterrupted service, preserve passenger trust, and effectively defend against the continuously intensifying cyber threat landscape.

Why rail's digital transformation demands a security revolution

The rail sector's accelerating digital transformation, driven by IoT-enabled asset tracking and predictive maintenance, remote infrastructure monitoring, SCADA/ICS systems for signalling and control, and interconnected third-party platforms for logistics and passenger information, has dramatically expanded the cyberattack surface. This rapid expansion typically outpaces traditional security measures, exposing critical vulnerabilities. Given that public safety, economic stability, and national connectivity depend heavily on secure and reliable rail operations, protecting this vital infrastructure requires a proactive and resilient security approach that goes far beyond simply reacting to an ever-growing list of threats.

As a critical part of any nation's infrastructure, the rail sector requires advanced cybersecurity solutions. Goldilock delivers a transformative approach that goes beyond traditional digital defenses by physically isolating key operational and IT systems. This hardware-enforced protection eliminates remote attack paths and secures legacy equipment without costly upgrades , By integrating physical disconnection into cybersecurity strategies, rail operators can achieve unprecedented protection, ensuring operational continuity, regulatory compliance, and the preservation of public trust in an increasingly connected and digitized rail environment.

Critical threats facing the rail sector

- **Ransomware targeting operational systems:** Attackers increasingly encrypt or manipulate dispatching systems and onboard controls, ransomware's has the proven ability to paralyze rolling stock operations through third-party vendor compromises.
- **State-sponsored infrastructure sabotage:** Nation-state actors now prioritise disrupting critical rail systems. Specific targets include SCADA/ICS networks to cause derailments or network-wide paralysis.
- **Insider threats and unauthorised access:** Employees or contractors with elevated access rights can unintentionally introduce malware or, worse, deliberately cause harm. The potential for malicious or compromised employees to exploit their credentials is a significant risk.
- **IT/OT convergence risks:** Insufficient segmentation between passenger-facing IT systems (like Wi-Fi) and safety-critical OT systems creates opportunities for lateral movement by attackers. These risks are exacerbated with the integration of IoT-enabled predictive maintenance tools.
- **Exploitation of legacy system weaknesses:** The prevalence of aging signalling equipment and unsupported software across rail networks presents exploitable "bridgeable air gaps" when these systems are integrated with modern cloud platforms.
- **Emerging threat of AI-driven attack automation:** Generative AI is now being used to create more sophisticated and targeted phishing campaigns against rail employees and to automate the vulnerability scanning of ticketing platforms.
- **Challenges in meeting regulatory compliance:** Despite updates to regulations like NIS2 and IEC 62443, many rail operators still lack robust real-time threat monitoring and resolution capabilities.

The FireBreak advantage: Hardware-enforced security to mission-critical rail systems

Goldilock's FireBreak delivers a groundbreaking hardware-enforced security solution that physically disconnects critical rail assets—such as signalling systems, control units, and backup servers—from all networks during inactive or high-risk periods. This physical disconnection eliminates remote attack pathways, rendering vital operational technology invisible and unreachable to cyber threats. Unlike software-based defenses vulnerable to misconfiguration or insider threats, FireBreak acts as a hardware "circuit breaker," preventing lateral movement from compromised IT systems into sensitive OT environments. Its secure, non-IP control channel ensures operators retain command even during network outages or cyber incidents, protecting legacy infrastructure without costly upgrades.

FireBreak also supports compliance with rigorous regulatory frameworks like NIS2 and IEC 62443 by providing tamper-proof logging and auditable air-gapping capabilities. By physically isolating signalling interlocks during maintenance, air-gapping backup data repositories, and enforcing strict third-party access controls, FireBreak mitigates risks from ransomware, supply chain compromises, and state sponsored attacks. This proactive physical isolation approach transforms rail cybersecurity, safeguarding both modern and legacy systems while ensuring continuous, safe rail operations in an increasingly digital landscape.

Key features and strategic benefits for the rail sector

Physically isolated OT segments

Benefit: Eliminates Remote Attacks on Critical Operations: Isolates critical OT systems including; signalling control, interlocking systems, and traction power control from all networks during idle periods or periods of heightened risk, completely eliminating remote attack vectors that could lead to service disruption or safety incidents.

Example: A signalling control server, responsible for safe train movements on a specific line, only establishes a physical network connection for scheduled software updates or when an authorised technician requires direct, time-bound access for diagnostics or maintenance. Outside these specific windows, the physical network link is entirely severed, rendering it unreachable to cyber threats.

Air-gapped backups for rapid recovery

Benefit: Ensures Swift Operational Restoration—Stores critical system configuration files, operational data (e.g., train schedules, network status), and backup images on a physically unreachable device – safe from ransomware and remote corruption. This protected, physically isolated storage minimises downtime and prevents catastrophic data loss, enabling rapid recovery after a cyber incident.

Example: In the event of a cyber incident such as a ransomware attack that compromises primary traffic management servers, operators can quickly restore the system to its pre-attack operational state using a clean and uncorrupted backup residing on a FireBreak protected device, minimising disruption to passenger and freight services.

Role-based physical access control

Benefit: Access to designated OT systems (e.g., trackside equipment controllers, station management systems) is strictly controlled at the physical network connection level, granted only to authorised personnel (engineers, technicians, vendors) during pre-approved and limited time windows. Hardware level verification (e.g., physical keys, secure tokens) can be required before a physical connection is established, and all connection/disconnection events are logged immutably for audit trails.

Example: A third-party maintenance contractor needing to service a points machine controller at a remote trackside location is granted physical network access via FireBreak for a pre-defined maintenance window. Their connection may require a secure token, and a detailed log of the access period, including the user and time, is recorded and cannot be altered.

Reduced attack surface for OT environments

Benefit: Minimises Vulnerable Entry Points — By physically disconnecting critical OT systems when not actively in use, FireBreak significantly reduces the overall attack surface of the operational environment, minimising the number of potential entry points that cybercriminals can exploit.

Example: By ensuring that trackside signalling controllers are physically disconnected from the network except during brief, authorised maintenance windows, FireBreak drastically reduces the number of ways an attacker could potentially attempt to gain access to these critical safety systems.

Time-bound physical connectivity windows

Benefit: Minimises Attack Opportunities: Network connectivity to critical OT assets is only enabled for pre-defined, limited durations necessary for specific tasks (maintenance, updates, authorised access). This significantly reduces the window of opportunity for cyberattacks by ensuring these systems are offline and unreachable for the vast majority of the time.

Example: Software updates for a train's onboard control system are scheduled for a specific two-hour maintenance window while the train is in a secure depot. Outside this window, the physical network interface to the control system is disconnected by FireBreak preventing any unauthorized remote access attempts.

Compliance with stringent rail security regulations

Benefit: Meeting and Exceeding Regulatory Requirements—FireBreak s physical isolation capabilities can help rail operators meet and even exceed the increasingly stringent cybersecurity regulations and standards specific to the transportation sector, such as those related to Critical National Infrastructure (CNI) protection and operational technology security (e.g., potential future updates to NIS2 or rail specific standards).

Example: When demonstrating compliance with regulations requiring robust protection of critical signalling infrastructure, rail operators can point to the hardware-enforced physical isolation provided by FireBreak as a significant measure exceeding typical software-based security controls.

Why rail operators choose Goldilock FireBreak

Enhanced safety and reliability

By physically preventing unauthorized access to critical train control and signalling systems, FireBreak directly contributes to enhanced railway safety and operational reliability. Eliminating the risk of remote cyberattacks on these systems minimizes the potential for accidents, delays, and disruptions to passenger and freight services.

Future-proof security for existing infrastructure

Seamlessly integrates with essential OT systems like SCADA, ICS, DCS, and even legacy rail equipment (e.g., older signalling units, train control systems), providing advanced security without the costly and disruptive need for immediate modernization. Protect your current investment in vital rail infrastructure, rather than requiring wholesale replacement.

Long term cost savings

While the initial investment in FireBreak delivers a substantial security advantage, its true value lies in the compelling Return on Investment (ROI) it generates. By proactively preventing potentially catastrophic and costly cyber incidents, FireBreak minimises operational downtime, significantly reduces the ongoing expenses associated with constant and complex software security patching on legacy OT systems, and can even lead to lower insurance premiums due to a demonstrably enhanced security posture.

Preservation of operational continuity

By preventing cyberattacks from disrupting essential rail functions like train scheduling, dispatching, and infrastructure control, FireBreak directly contributes to the preservation of operational continuity. This minimises service disruptions for passengers and freight, safeguarding the economic benefits of a reliable rail network

Improved incident response and recovery

In the event of a broader cyber incident affecting less critical IT systems, FireBreak ensures that the core operational technology remains physically isolated and uncompromised. This facilitates a more focused and efficient incident response, allowing operators to restore affected services without the risk of further cascading damage to critical rail operations.

Battle-tested in demanding environments

Proven and trusted in high-stakes sectors like defence, energy, and finance, where system failure carries catastrophic consequences. This robust and reliable technology offers the dependability rail operators need when the safety and efficiency of their networks are paramount.

Peace of mind

Knowing your most critical rail infrastructure is physically isolated and unreachable when not in use provides unparalleled peace of mind in the face of ever-increasing and evolving cyber threats targeting transportation networks. Ensure the safety and reliability of your rail services with the ultimate physical layer of protection.

Conclusion

As cyber threats targeting the rail sector grow increasingly sophisticated, traditional software defenses are no longer sufficient. Goldilock FireBreak combines physical disconnection with operational flexibility to protect critical rail infrastructure from service disruptions, sabotage, and data manipulation, while ensuring compliance with stringent regulations like NIS2 and rail-specific standards. Recognized by NATO and trusted in high-risk industries, FireBreak provides provable, auditable security—offering rail operators the physical assurance required to safeguard public safety and maintain efficient operations.

By physically isolating vital systems such as signalling and control units during vulnerable periods, FireBreak eliminates digital attack surfaces entirely. Its tamper-proof logs and deterministic access controls support regulatory mandates and enable rapid breach containment, legacy system protection, and Zero Trust enforcement for third-party access. With features like dual power redundancy, non-IP control channels, and seamless integration, FireBreak delivers resilient, proactive cybersecurity without disrupting rail operations—transforming how the sector defends against evolving threats. Unlike software -based solutions, FireBreak provides provable, auditable security —a necessity for utilities managing modern rail infrastructures and eco-systems.