RazorSecure

SECURITY GATEWAY

Enforcing the segregation and separation of rail critical systems, reducing cyber attack surface.

Modern trains rely on a complex network of digital subsystems with routine interaction between critical operational technology, on-board IT and IoT systems, and wayside infrastructure. With increasing interconnectivity there is a corresponding growth in cyber attack surface, making network protection through security zoning and segregation a necessity as part of a robust cyber security programme.

The RazorSecure Security Gateway (SGW) is designed to easily deploy and manage sophisticated network segregation and separation across a diverse range of on board architectures. Created for both new and existing rolling stock, it uses a Layer 7 firewall with rail protocol support, providing a turnkey solution for the protection and monitoring of on-board networks.

SGW segregates critical on board networks and enforces separation between security zones, reducing cyber attack surface and protecting potentially vulnerable systems. By performing application level traffic inspection and permitting only approved traffic, the SGW protects the train's operational systems, ensuring vehicle safety, availability, and resilience to cyber threats.

SGW alerts operators to any unauthorised traffic detected, and when deployed with RazorSecure's Delta Intrusion Detection System, wider network activity is also monitored to reliably detect threats, anomalies, and changes in network configuration throughout the train.

BENEFITS

PROTECT THE INTEGRITY OF ON-BOARD SYSTEMS

Security Gateway reduces cyber attack surface and eliminates vulnerabilities by ensuring access through conduits is controlled, and separation between security zones is enforced. By passing only approved traffic, and verifying conformance to rail protocols with the expected payload, SGW protects the trains critical operational systems.

DETECT NETWORK THREATS

Security Gateway alerts operators to any unauthorised traffic it detects. When deployed with RazorSecure's Delta Intrusion Detection System, wider network activity is also monitored to reliably detect threats, anomalies and changes in network configuration throughout the train.

CYBER COMPLIANCE FOR NEW & LEGACY FLEETS

Security Gateway is easily integrated with on board networks without modifying existing routing. It can be deployed virtually or as an appliance, supporting compliance with IEC62443 and TS50701 for all types of rolling stock.

EVOLVING CYBER PROTECTION

Security Gateway meets the developing cyber security needs of today's trains by providing a secure on board platform capable of supporting a range of applications, including log aggregation, secure network services, access control, and authentication.

KEY CAPABILITIES

NETWORK VISIBILITY & MONITORING

The Security Gateway is an ideal vantage point for visibility of unauthorised and anomalous traffic attempting to cross between security zones. When deployed with Delta Network IDS, this capability can be extended to a much wider range of traffic, identifying threats and reducing the time, effort, and cost of mitigating and responding to cyber incidents.

FIREWALLS & PROTOCOL FILTERING

The Security Gateway provides firewall capabilities to filter and inspect traffic, including DPI with rail protocol support, delivering a comprehensive array of routing and firewall features configurable to most on-board networking scenarios. Traffic passing through the SGW is analysed to ensure only specific protocols are permitted with the correct payload.

INTEGRITY CHECKING

The SGW Host Operating System ensures Virtual Machines are easily reset to an initial state, limiting scope for any software vulnerability to spread. RazorSecure's Delta Intrusion Detection System is deployed for host protection and filesystems are read only except where required for operation (e.g. logging).

CENTRAL LOG AGGREGATION

An integrated central syslog server provides a single point for the collection, filtering and wayside transport of all logs from the Security Gateway and those collected from other on board systems. Logs can be sent to multiple locations including external SOC/SIEM systems according to configurable criteria such as security level.

DEPLOYABLE AS HARDWARE OR SOFTWARE

Security Gateway can be supplied on EN50155 approved hardware with a range of options and form factors. Alternatively, it can be deployed as a fully virtual solution onto customer hardware. Wayside services can be deployed to customer on-premises infrastructure or hosted by RazorSecure.

PROTECTION FOR THE LIFE OF THE ASSET

Systems within rail may be in operation for a long period of time. The SGW technology has been tested and demonstrated in live deployments, and is consistently effective over a long period of time in a rail environment, even in cases of limited connectivity.

ROBUST CONFIGURATION MANAGEMENT

SGW configuration is centrally versioned, controlled and applied using an actively enforced configuration-as-code strategy that prevents deviation or accidental mis-misconfiguration. Configuration and updates can be deployed over-the-air selectively to individual trains, test groups or to entire fleets. A robust AB partitioning strategy ensures safe roll back is always possible.

SECURE, RESILIENT & EXTENSIBLE

Security Gateway is built on a software stack designed for security and reliability. At its heart is the Host Operating System which features secure boot and disk encryption with a configurable selection of unchangeable Virtual Machines, to meet cyber protection requirements for the life of the train.

RAZORSECURE APPROACH

We recognise that each train fleet is different and requires a holistic approach due to differences in system and network architecture. By understanding your cyber risks, we can advise on security best practices and appropriate risk mitigations. We will then work with you to design, integrate, homologate and deploy the RazorSecure solutions as appropriate. Our flexible approach is customised to manage the unique challenges and requirements of each customer. We will work closely with you to find a solution for any challenge you may have. The first step towards improved cyber security is simply to begin a conversation with us, and our team will be happy to guide you through the process.