CYLUS

DATA SHEET

Secure Every System. Keep Rail in Motion.

Strengthen cybersecurity across rail networks with a platform that empowers cybersecurity and operations teams to collaborate, monitor, and protect signaling, onboard, and trackside systems from a single, unified solution.

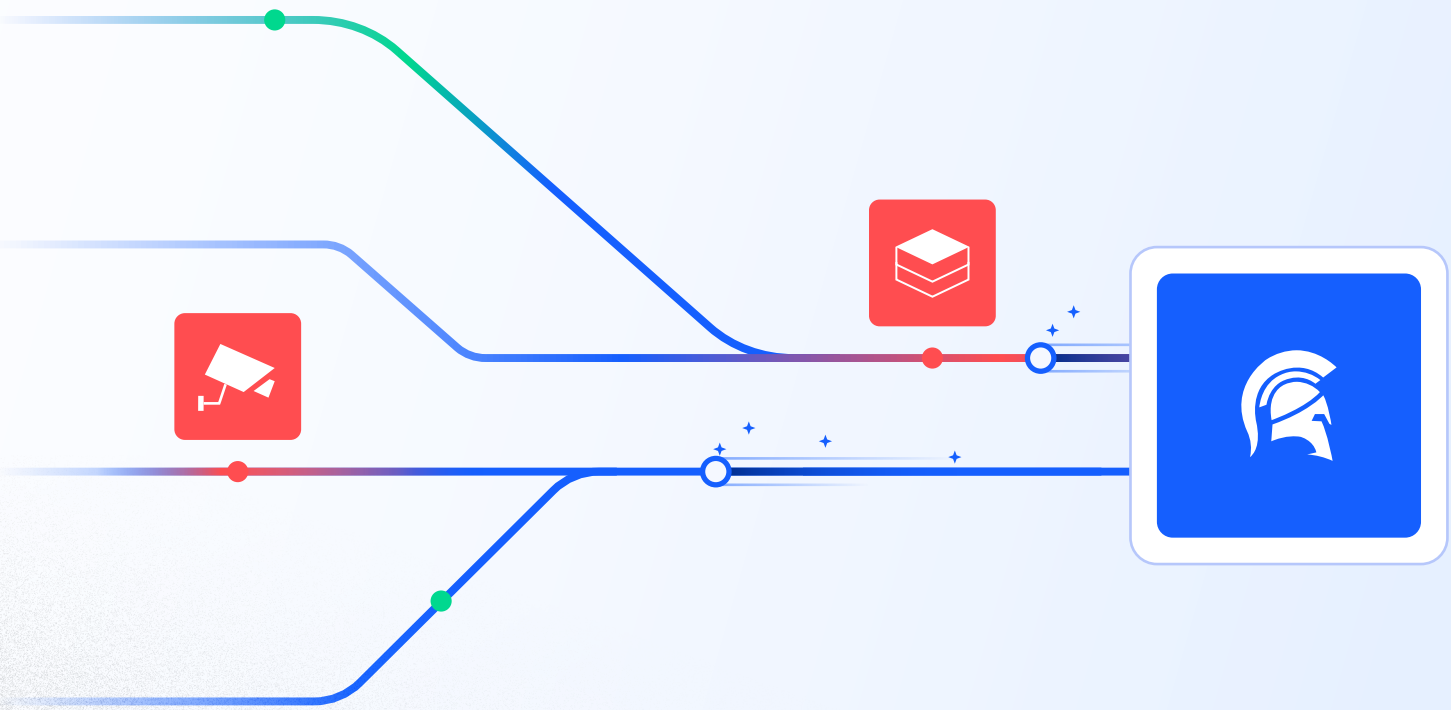


Table of Contents

Asset Discovery and Network Visualization

By correlating data across all operational rail environments, CylusOne provides operators with true visibility into their systems for the first time. It delivers contextual, real-time insights that reveal what's happening both onboard and trackside, enabling faster and more informed decision-making. With this clarity, operators can strengthen threat detection, streamline incident response, and standardize security workflows across diverse environments. Onboard monitoring as a core capability ensures risks are identified and addressed early, helping rail companies manage threats more efficiently while maintaining resilient, uninterrupted operations and compliance.

Automatically Identify and Classify Rail OT Assets

As a part of a unified rail cybersecurity platform, CylusOne automatically identifies and classifies all assets in the operational networks, delivering a precise, real-time, and continuously updated asset inventory. This integrated capability eliminates the need for manual inventory maintenance, enables immediate detection of newly connected devices, and ensures full visibility into asset changes over time.

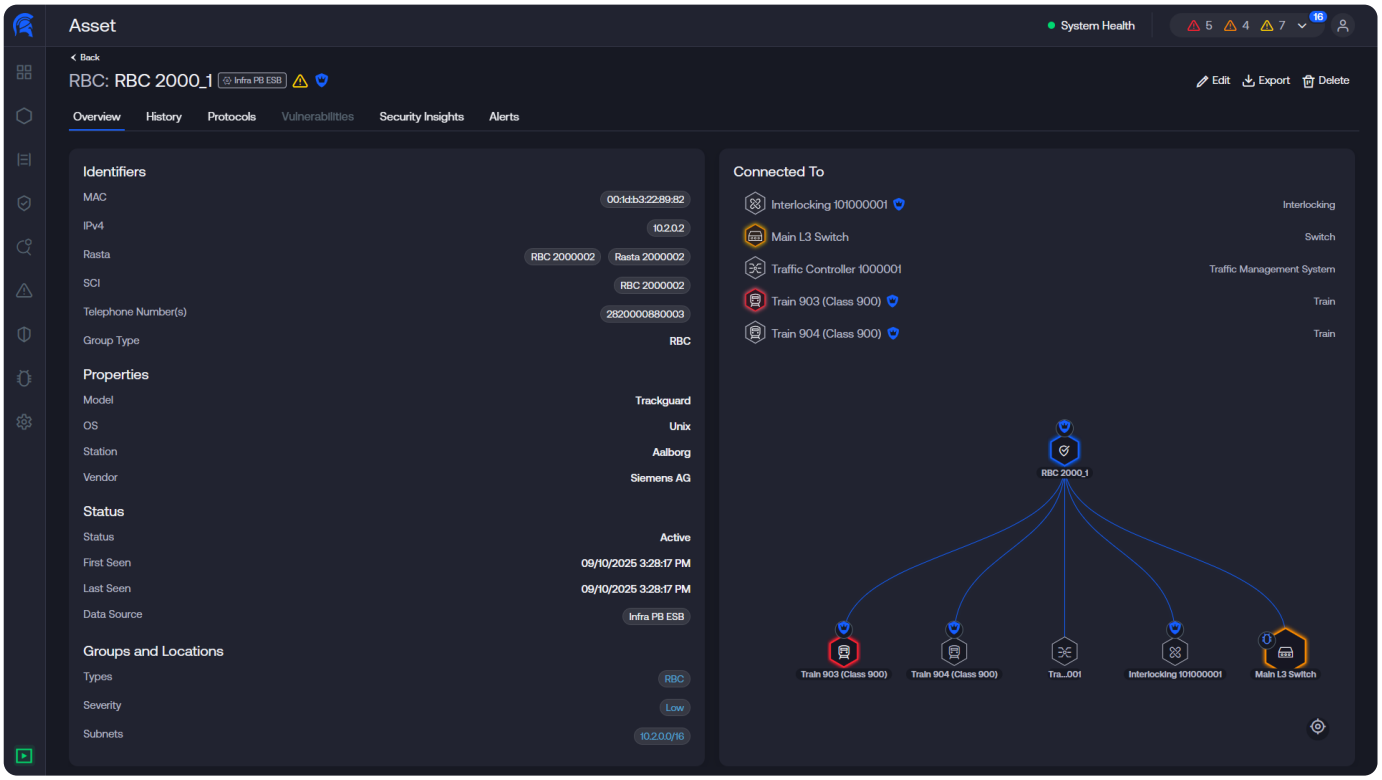
CylusOne classifies assets based on their rail function or the application (e.g., automatic train protection (ATP), camera, HMI, etc.). This contextualized classification is essential not only for operations teams, who rely on it to interpret data within the operational environment and make informed decisions, but also for security teams, who must assess asset importance and system criticality in order to prioritize protection efforts and respond to threats effectively.

CylusOne provides the following properties or attributes, depending on the discovered asset:

Group	Properties
Device ID	Name, Asset ID, MAC, IP, Rail or OT Protocol ID
Metadata	Data Source, First Seen, Last Seen, Asset Owner, Tags
Classification	Type, Subsystem, Safety Level, Criticality, Purdue model level, Zone
System Software	OS Name & Version, Software Name & Version, Firmware Version
Hardware	Model Number, Revision, Vendor, MAC OUI, Serial Number
Network Configuration	Hostname, FQDN, Subnet, VLAN, DNS Server, Domain
Certificates	Issuer, Organization, Validity Period, DNS Names
Location	Geolocation, Train, Consist, Car, Station/Site, Rail Block, Last Read Balise Group
Operational Metric	Status, Speed, Door Status, Driving mode, Industry-specific Process Variables

Individual Asset View

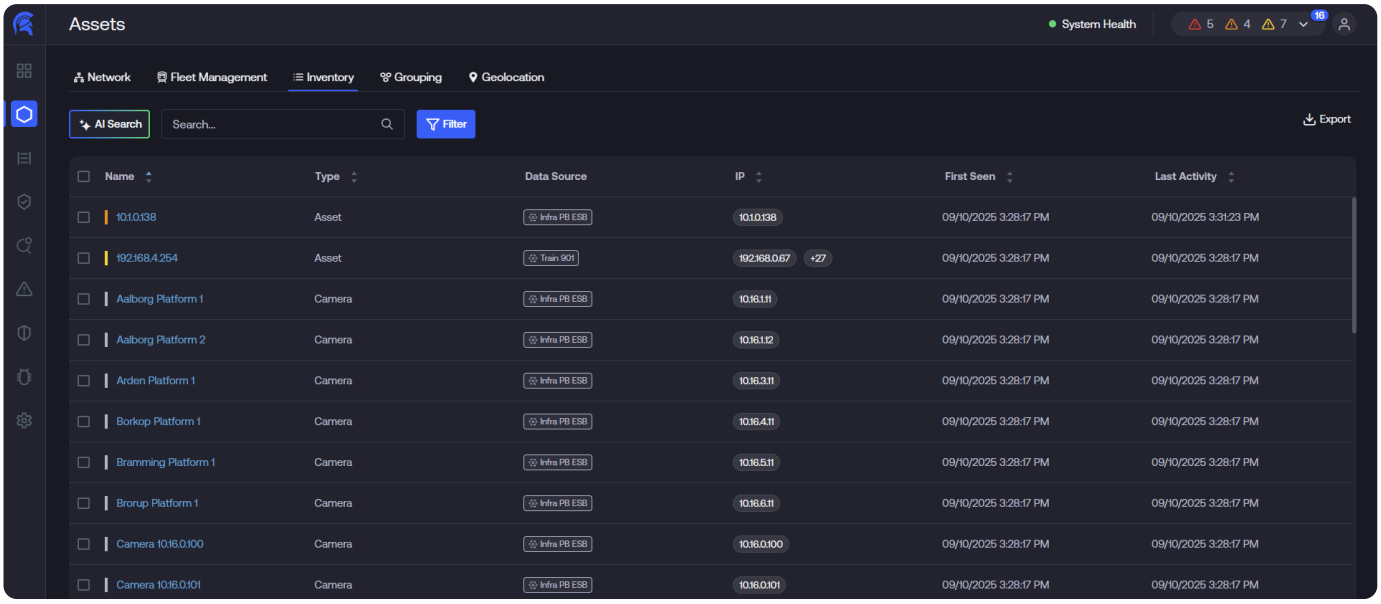
Users can drill down into each asset to gain more information about asset properties and identify its specific connection to other assets. This level of visibility is invaluable for risk analysis and supports effective investigation of potential incidents or anomalies.



CylusOne can detect trains based on both infrastructure communication and onboard network monitoring. By analyzing CBTC, PTC, ERTMS, and other rail train control technologies, cybersecurity specialists gain a deeper understanding of how their mobile assets (i.e., trains) communicate with their fixed wayside assets. This can help to understand which rail assets might be exposed to threats due to an attack on wayside assets and detect operational issues related to train and ground communications.

Assets Inventory View

The Asset Inventory View displays all assets detected by CylusOne in a searchable, filterable table, allowing users to locate specific assets or groups of assets quickly. With AI-powered search, users can simply type a natural language query, such as “interlocking from station X with Linux OS”, and CylusOne will instantly surface the relevant results.

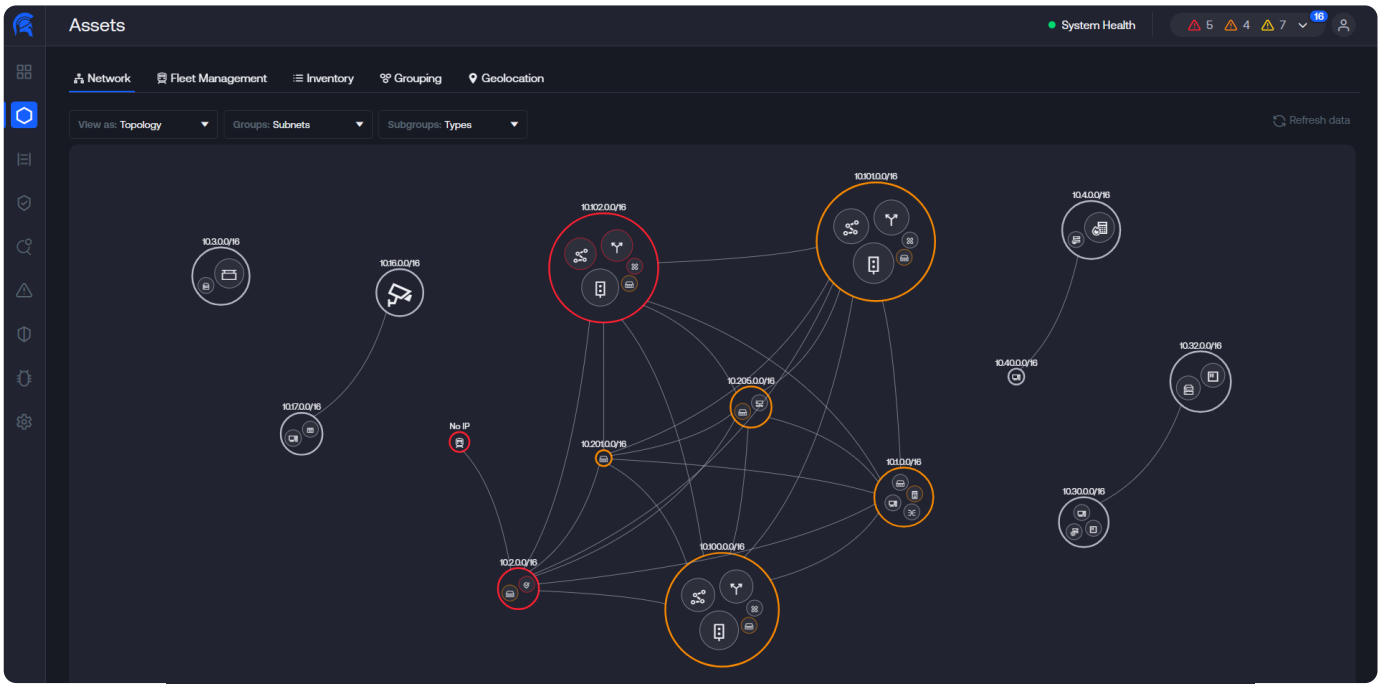


Network Discovery and Topology Mapping with Data Flow Views

CylusOne automatically discovers and provides full visibility to the monitored operational network, including all connectivity and communications. This insight gives instant awareness into the rail network and 'normal' activity patterns. It includes data such as network connections, traffic throughput, and protocols. Below are a few of the typical network views.

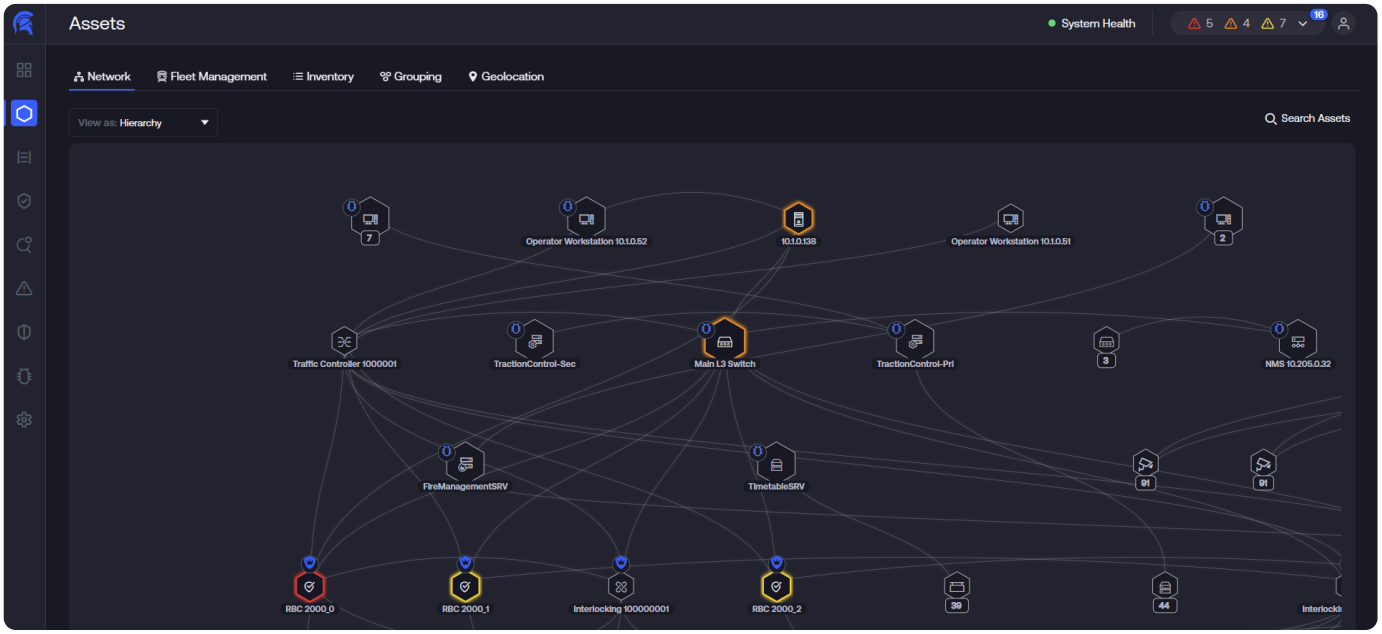
Network View

The Network View provides a connectivity-based view of the network and allows users to identify the critical assets and the network layout quickly



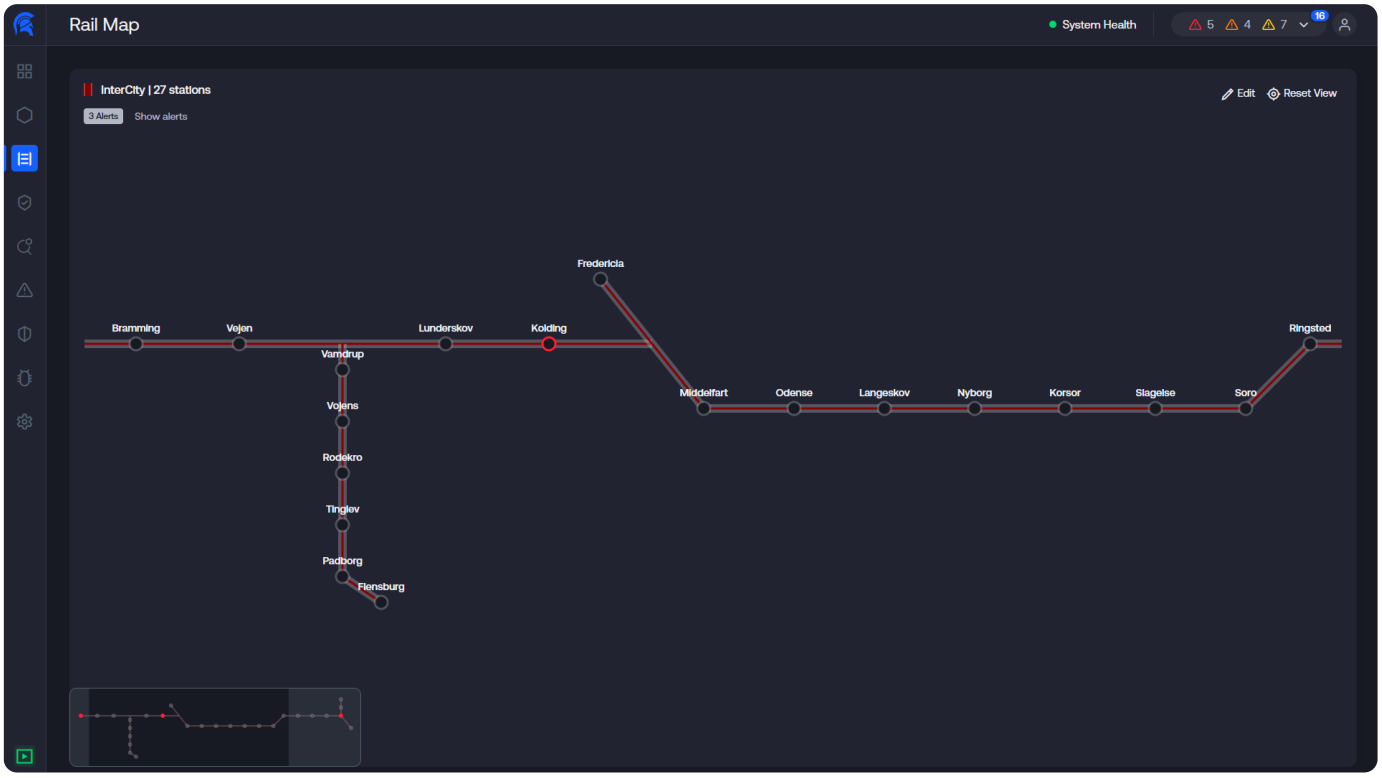
Hierarchical View

The Hierarchical View offers a different visualization of the network, helping users understand the relationship and structure of rail assets. Based on Cylus's adaptation of the Purdue Model for Rail, this view illustrates how different layers interact, enabling users to identify communication flows and detect inconsistencies visually. At the base of the hierarchy are signaling field elements, such as point machines and level crossings, while the top layer features Operations Control Center (OCC) assets, including operator HMIs and management servers for signaling, maintenance, and more.



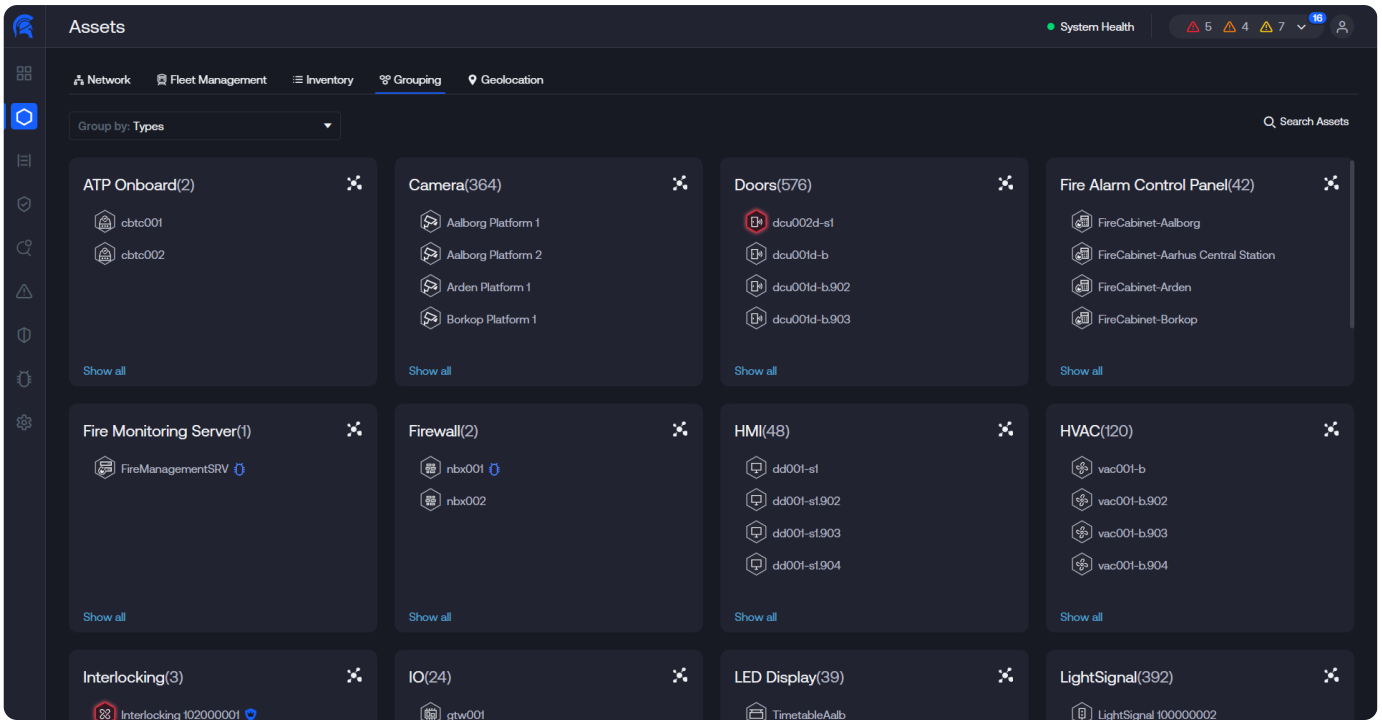
Rail Map View

The Rail Map View offers a comprehensive, map-based visualization of all connected rail assets, mirroring the familiar operational interface used in rail control centers. By delivering this perspective within the cybersecurity platform, it bridges the gap between rail operations and cybersecurity teams. This experience enables both groups to work from the same dynamic view, streamlining communication, accelerating incident response, and enhancing system-wide awareness.



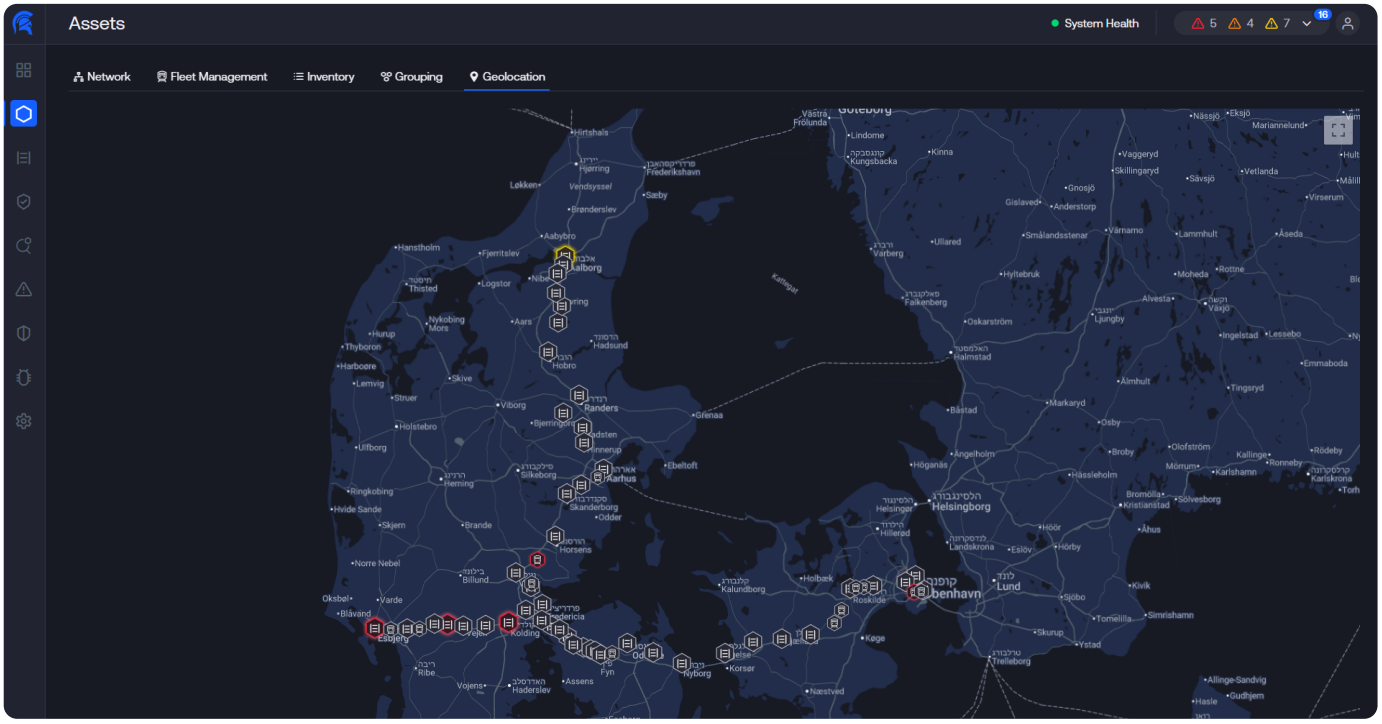
Grouping View

The Grouping View transforms complex rail environments into clear, logical representations, consolidated into a single, intuitive interface. Users can instantly switch between groupings such as asset type, subnet, operating system, or geographic location to surface the specific insights they need. By offering multiple perspectives within one unified view, the Grouping View empowers rail and cybersecurity teams to quickly understand system composition, identify anomalies, and focus investigations with precision.



Geolocation View

The Geolocation View visually maps discovered assets across the rail network, giving teams immediate geographic context within a unified interface. This real-world overlay helps operations centers pinpoint asset locations and dispatch the right personnel to the right place for on-site investigation or mitigation. By correlating cyber alerts with physical locations, the Geolocation View enables faster, more targeted responses, helping teams assess which parts of the rail system may be affected and initiate local mitigation actions before disruptions escalate.

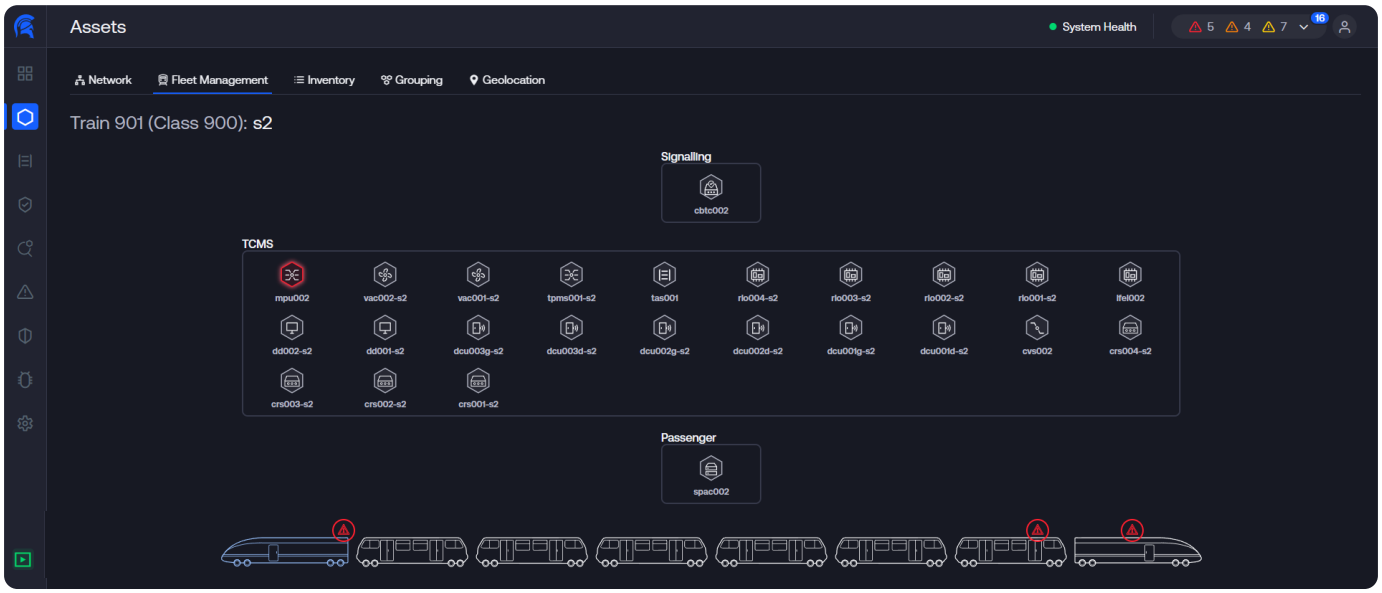


Rolling Stock View: Full-Fleet Visibility and Protection

CylusOne provides dedicated fleet, train, and car-level views for comprehensive cybersecurity monitoring across rolling stock environments. This multi-layered visibility allows operators to:

- View the entire fleet at a glance, with real-time security status across trains.
- Drill down to a specific train, revealing onboard systems, network segments, and active alerts.
- Investigate at the car level, exposing asset-level communications, anomalies, and threat details.

This hierarchical view, unique to CylusOne, enables faster threat detection, localized investigation, and streamlined response, ensuring safety, service availability, and regulatory alignment across the fleet.



Vulnerability and Risk Management

CylusOne continuously identifies vulnerabilities across operational rail networks and provides contextual insights into their potential impact. By prioritizing risks based on real-world operational relevance, operators can address the most critical issues first and maintain resilient, uninterrupted service.

Vulnerability Management - Built for Rail

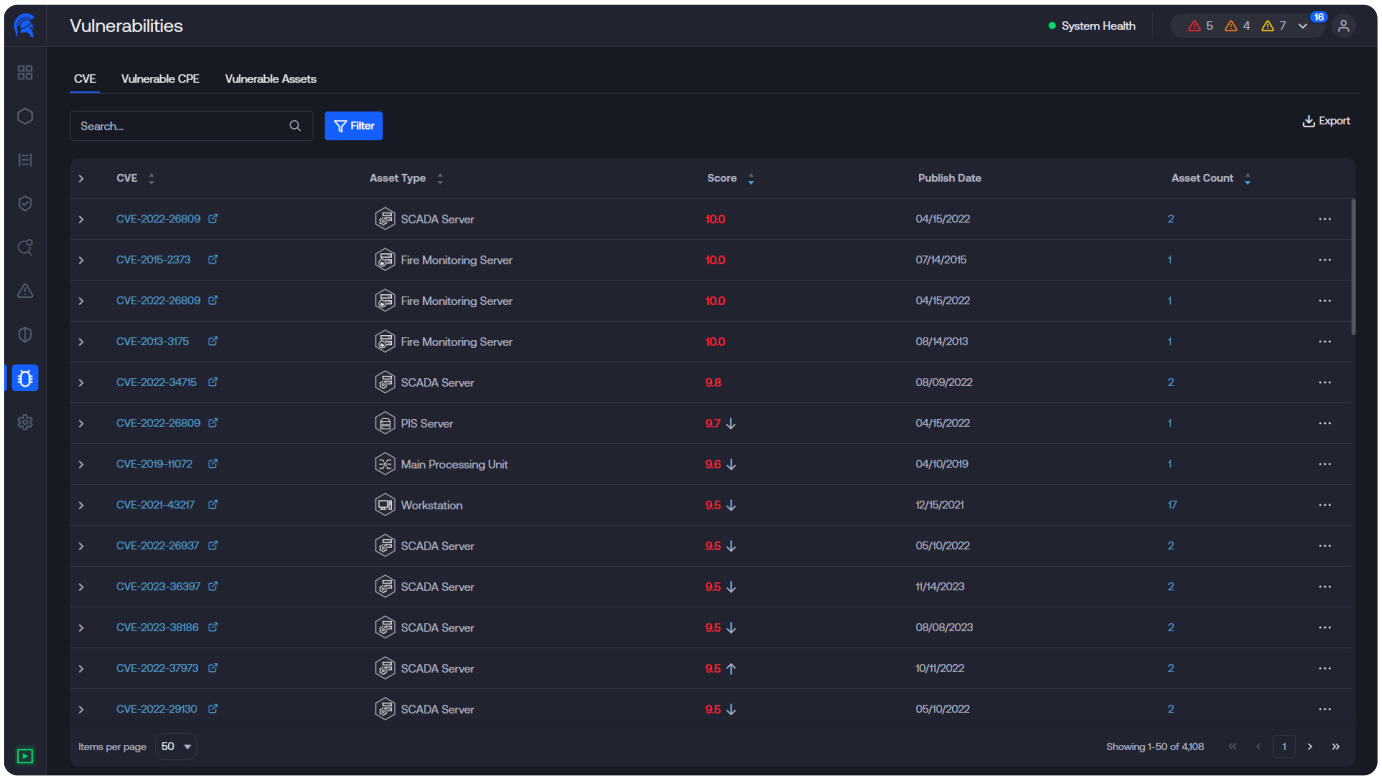
CylusOne's passive vulnerability management is purpose-built for the rail industry, where exploited vulnerabilities can directly impact safety and operations. Leveraging proprietary rail threat intelligence, including security advisories and known vulnerability databases, CylusOne identifies vulnerable assets across the network without disrupting operations. This enables rail operators to quickly detect, evaluate, and prioritize vulnerabilities for effective mitigation.

Customer-Specific Vulnerability Prioritization and Scoring

CylusOne goes beyond traditional severity scoring by prioritizing vulnerabilities based on actual risk to the rail environment. Its scoring considers multiple factors, such as attack vector, complexity, and potential impact on confidentiality, integrity, and availability, alongside deep awareness of operational context, including asset roles and network communications.

With full visibility into the operational rail technology ecosystem, CylusOne delivers highly accurate risk prioritization, enabling operators to focus mitigation efforts on the most critical vulnerabilities. This is especially important in rail environments, where system complexity can make patching difficult or delayed.

CylusOne supports customizable approaches to vulnerability and patch management, helping customers align their security efforts with their operational realities and priorities. By filtering out low-priority noise and highlighting high-impact threats, CylusOne strengthens and complements existing patch management programs.



Vulnerability Response

CylusOne empowers organizations to take control of their vulnerability response lifecycle. The platform supports teams in reducing exposure, monitoring threats, and making informed decisions on how to address each vulnerability:

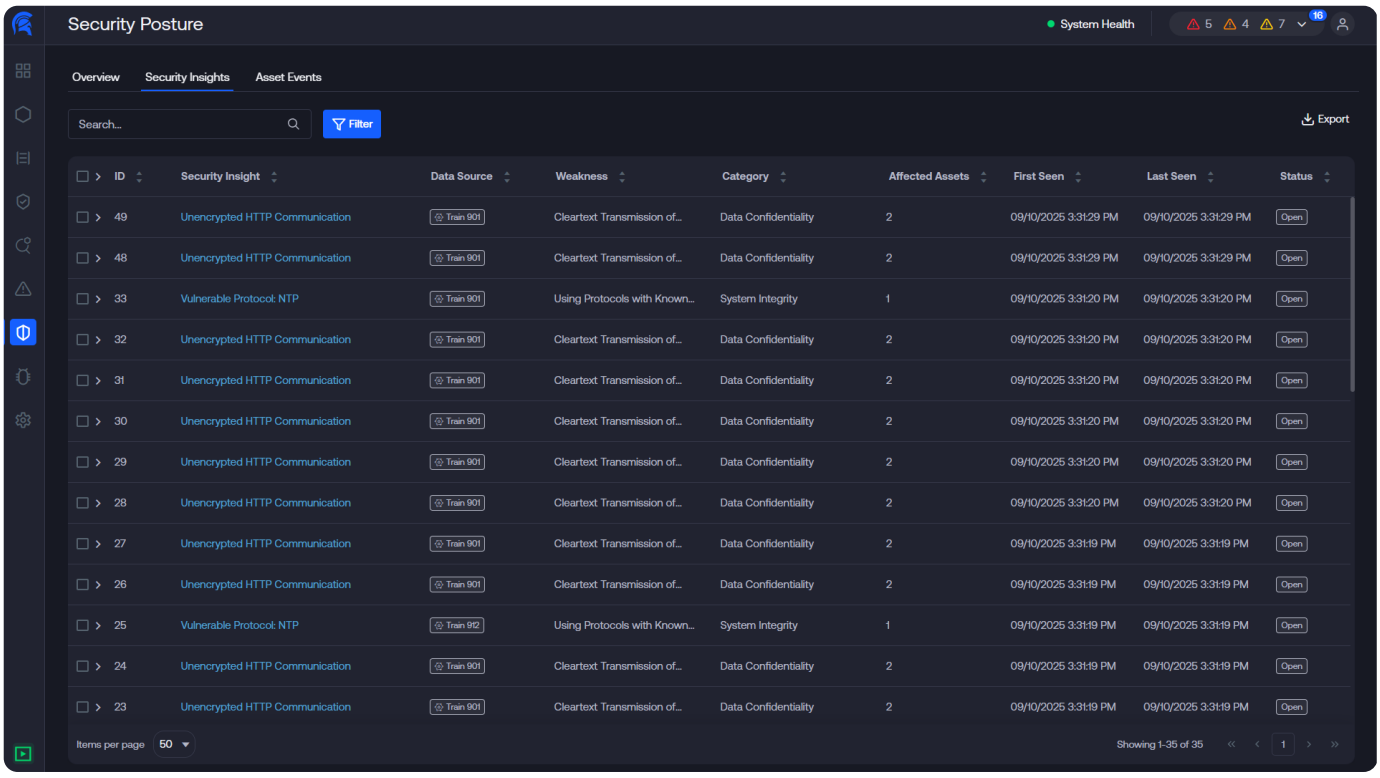
1. Risk Reduction & Monitoring - Continuously tracks vulnerabilities across all operating systems and monitors signs of potential exploitation. This allows security teams to act proactively, reducing the risk of operational disruption or compromise.

2. Risk Acceptance - Recognizes that not every vulnerability can or should be remediated immediately. CylusOne provides a structured approach for organizations to document and manage the residual risk associated with specific vulnerabilities, while maintaining visibility and accountability.

Additionally, CylusOne acts as a compensating control. Its detection rules and segmentation policies are tailored to defend against known exploit techniques, providing protective coverage even when vulnerabilities remain unpatched. As such, CylusOne serves as both a vulnerability detection and remediation solution purpose-built for rail operators.

Cybersecurity Posture Monitoring

CylusOne provides continuous security posture monitoring to assess the cybersecurity health of the rail network and its digital assets. It delivers real-time insights into security gaps across the environment, enabling cybersecurity teams to quickly identify and address areas of risk. These gaps are detected based on both IT and OT best practices, such as the use of outdated or vulnerable protocol versions, direct asset communication with the internet, and clear-text password usage—helping rail operators strengthen their security posture and reduce exposure.

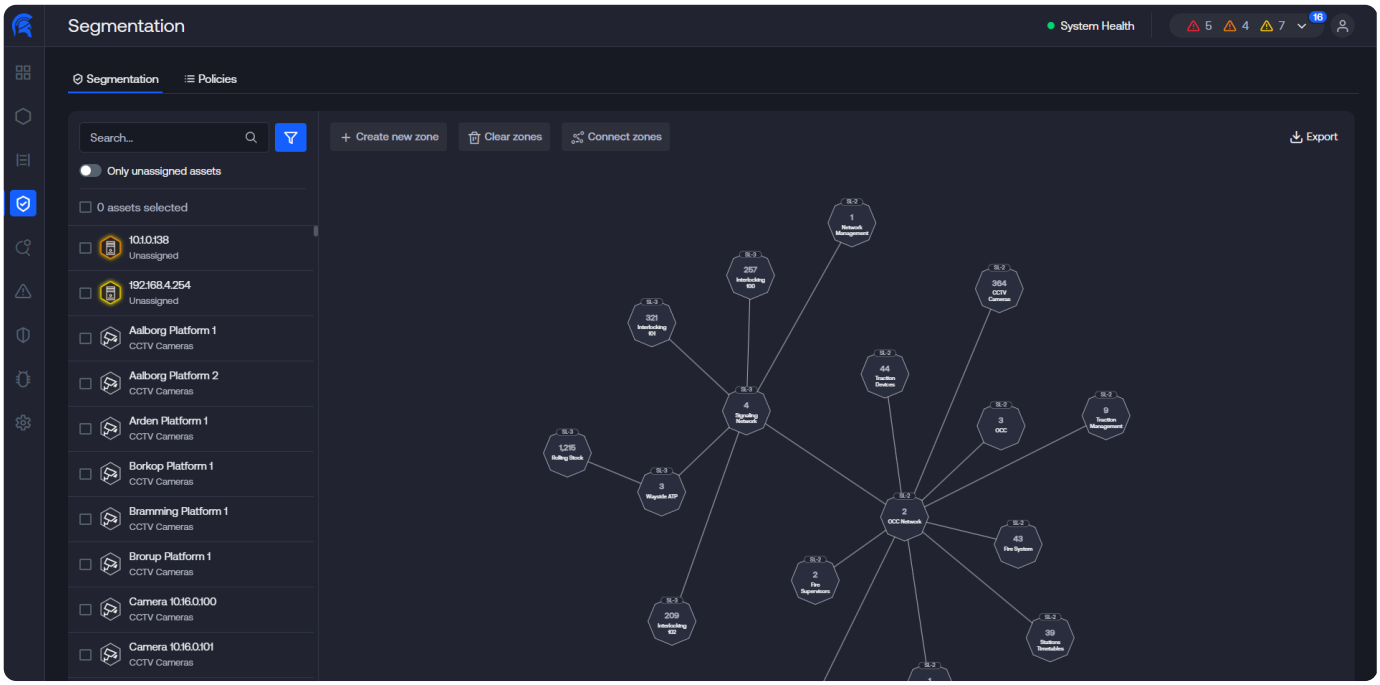


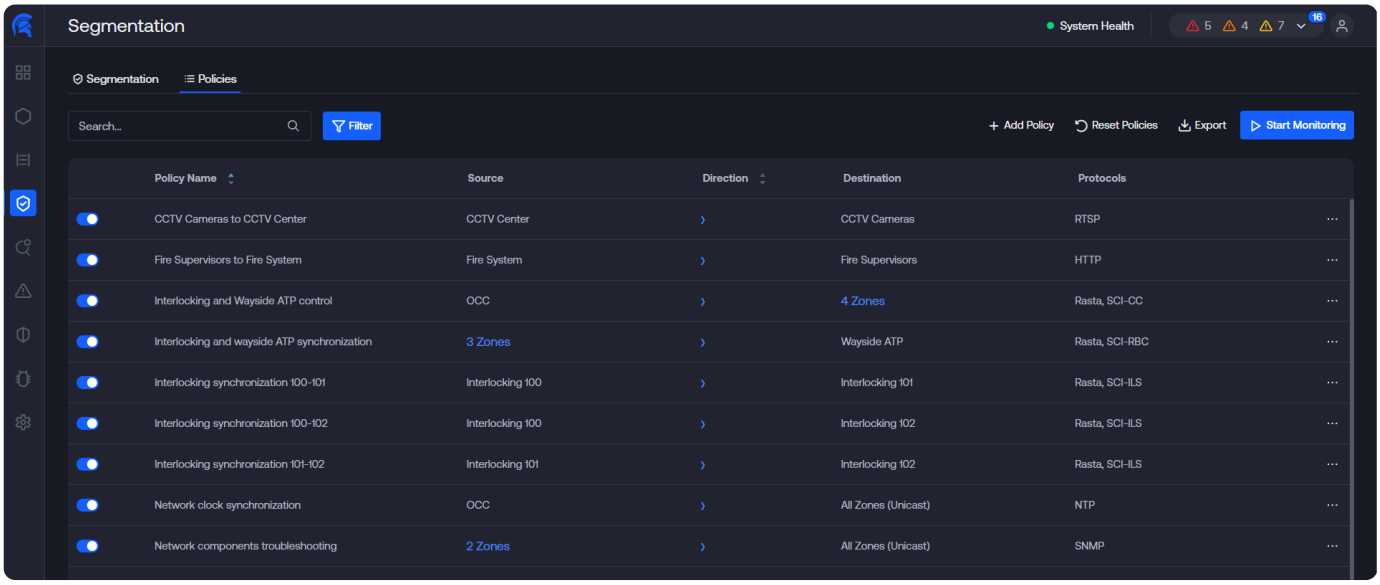
Virtual Network Segmentation and Monitoring

The CylusOne platform can passively and virtually segment the network and divide railway network assets into security zones regardless of the network topology and the characteristics of the protocols in use. The railway zone segmentation is based on the IEC-62443 zones and conduits requirements (ZCRs), which are also embedded into the CENELEC TS-50701 standard.

Once CylusOne maps the rail network and discovers all assets, it recommends a segmentation approach to divide the network into virtual zones based on groupings of similar rail assets and applications (see example in the screenshot below). CylusOne also provides all the recommended segmentation policies to implement these virtual zones (see the second screenshot below). The customer can apply these recommended policies by simply turning them on, or they can edit the policies as they see fit. Additionally, the customer can implement their defined zones, which might come from a prior risk assessment.

Once the segmentation policies are implemented, CylusOne performs automated validation and detects abnormal communications between zones and/or assets, alerting customers to any traffic that violates the defined segmentation policies.





Threat Detection, Investigation, and Response

CylusOne continuously monitors the entire rail operational technology environment, detecting threats to signaling systems, rolling stock, communications networks, control centers, and depot systems to help prevent safety incidents and service disruptions.

Through its integrated platform, CylusOne consolidates security data into a single view, allowing cybersecurity and operations teams to correlate threat indicators, investigate anomalies, and coordinate responses efficiently. This comprehensive approach enhances situational awareness and ensures proactive mitigation of cyber threats across all layers of the railway infrastructure.

Continuous Threat Detection

CylusOne detects a full spectrum of threats to railway systems at their earliest stages using Deep Packet Inspection (DPI) and patented machine learning (ML) algorithms for IT, OT, and railway-specific use. It accurately classifies alerts to enable faster, more efficient responses. CylusOne's anomaly and threat detection capabilities help customers protect fail-safe operational rail technology systems.

Using network-based threat detection, CylusOne provides real-time and continuous detection of known attacks through constant indicators of compromise (IOC) updates via the built-in Cylus threat intelligence feed. CylusOne also detects policy violations and supports the creation of customized threat detection rules defined by the customer.

For every triggered rule, CylusOne automatically supplies an AI-generated description, recommended mitigations, and a clear explanation of the detection logic, turning raw detections into actionable insights without added effort from the operator.

In addition, CylusOne provides anomaly detection based on baseline deviations, configuration changes, and threat modeling, enabling the detection of unknown or previously unseen malicious behaviors.

CylusOne includes rail application threat behavior monitoring, with contextual analytics on all rail technology protocol commands and detection of semantic attacks on rail application logic.

Bundled Rail-Specific Threat Intelligence

The CylusOne platform subscription includes a threat intelligence feed that is provided monthly for on-premise customer deployments or continuously in real-time for SaaS customer deployments. The Cylus Research Team continuously researches new rail environment attack vectors and rail technology protocol vulnerabilities. Customers are given detection rules and mitigations for the latest known threats. This can include threats and vulnerabilities to systems such as ERTMS, CBTC, PTC, and proprietary vendor technologies.

The Cylus threat intelligence includes:

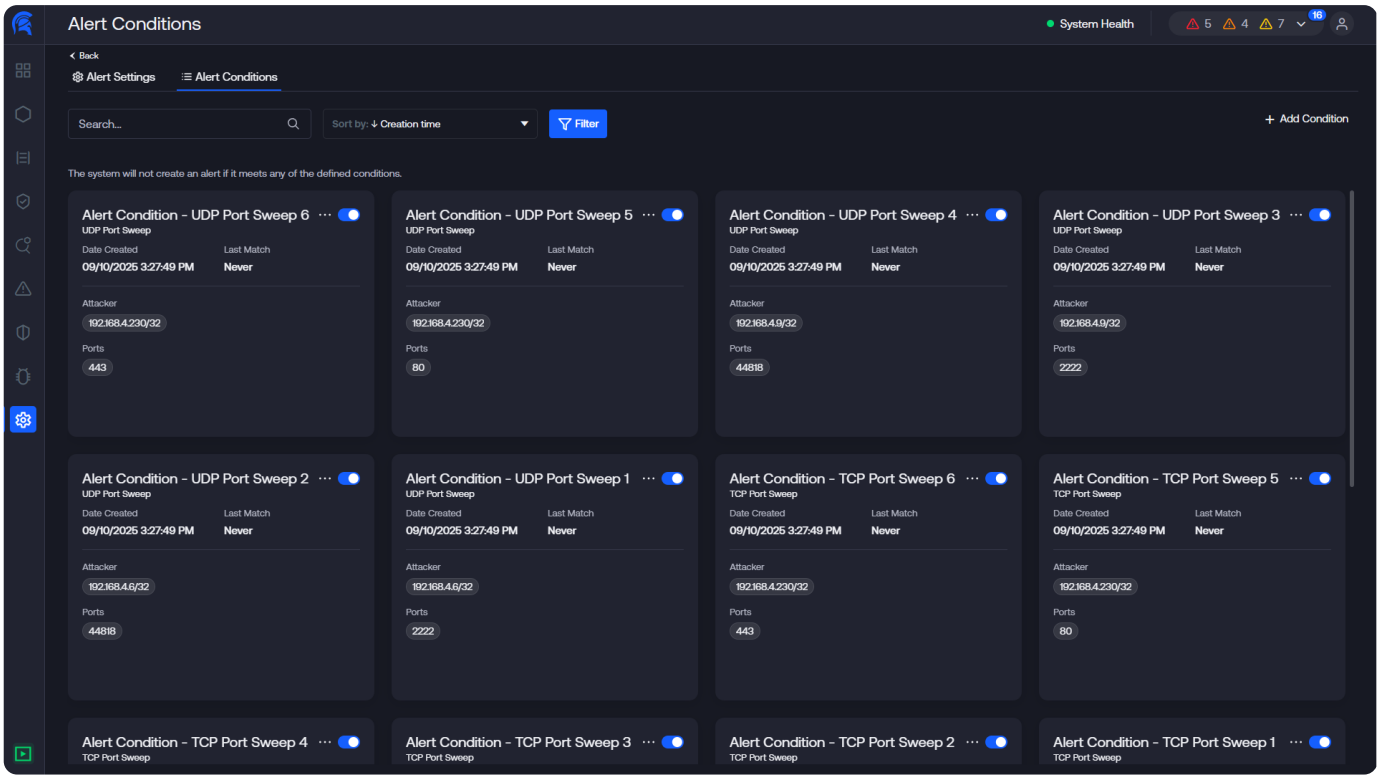
- New and up-to-date vulnerabilities and TTP.
- The latest vulnerability information from NVD and CVE.
- Security advisories from rail technology equipment vendors.
- Security advisories from ICS-CERT.
- Security advisories from rail-specific ISACs, such as ST-ISAC.
- Rules and detections generated by the Cylus Research Team

The feeds are translated to a threat intelligence package that enables the CylusOne platform to identify the latest vulnerabilities and provide detection against the attack vectors that might exploit those vulnerabilities or such that are being used by threat actors targeting rail and CPS environments worldwide.

The Cylus Research Team is constantly evaluating and adding additional threat intelligence sources, including dark web monitoring of rail-specific keywords, such as vendors, protocols, and common software, to provide Cylus' customers with even earlier warnings about possible threat actor intentions and campaigns that might be executed against rail operators worldwide.

Alert Conditions

Alert Conditions help reduce noise and minimize false positives by preventing alerts from triggering on every occurrence. Alerts will be suppressed when they meet the criteria in one of the currently defined conditions. The "Last Match" indicator shows the most recent time an alert that meets the condition criteria was triggered, making it easier to identify which conditions remain relevant and which unresolved misconfigurations continue to generate false positives.



During the alert resolution process, users can automatically create a condition that prevents the same alert from being raised again in the future. This streamlines remediation, reduces repetitive notifications, and ensures that once an issue is addressed, it no longer contributes to unnecessary noise.

Investigating Threats and Alerts with CylusOne

Forensic Network Analysis

CylusOne provides advanced forensic network analysis, enabling users to capture and examine network traffic associated with every security alert. Packet capture (PCAP) files can be downloaded to deliver raw forensic data collected immediately before and after an alert is triggered, offering a complete picture for investigation.

Attack Chain Visibility

CylusOne delivers an attack chain visibility, giving users a clear view of attacker activity across the entire incident lifecycle. This visibility gives insights into the alert type and severity, along with the specific assets targeted at each stage of the attack, making visibility it easier to understand, contain, and respond effectively.

Related Alert Insights

CylusOne's "Find Related Alerts" feature streamlines security investigations:

- Review historical alert instances and their management history.
- Access real-time information on open alerts.
- Identify and respond efficiently when multiple alerts share a common root cause.

MITRE ATT&CK Mapping for Rail

Every CylusOne alert is mapped to the MITRE ICS ATT&CK framework, tailored specifically for the rail industry. This alignment gives operators:

- Immediate context of the incident.
- Insight into the attacker's likely next steps.
- A standardized reference point for response and reporting.

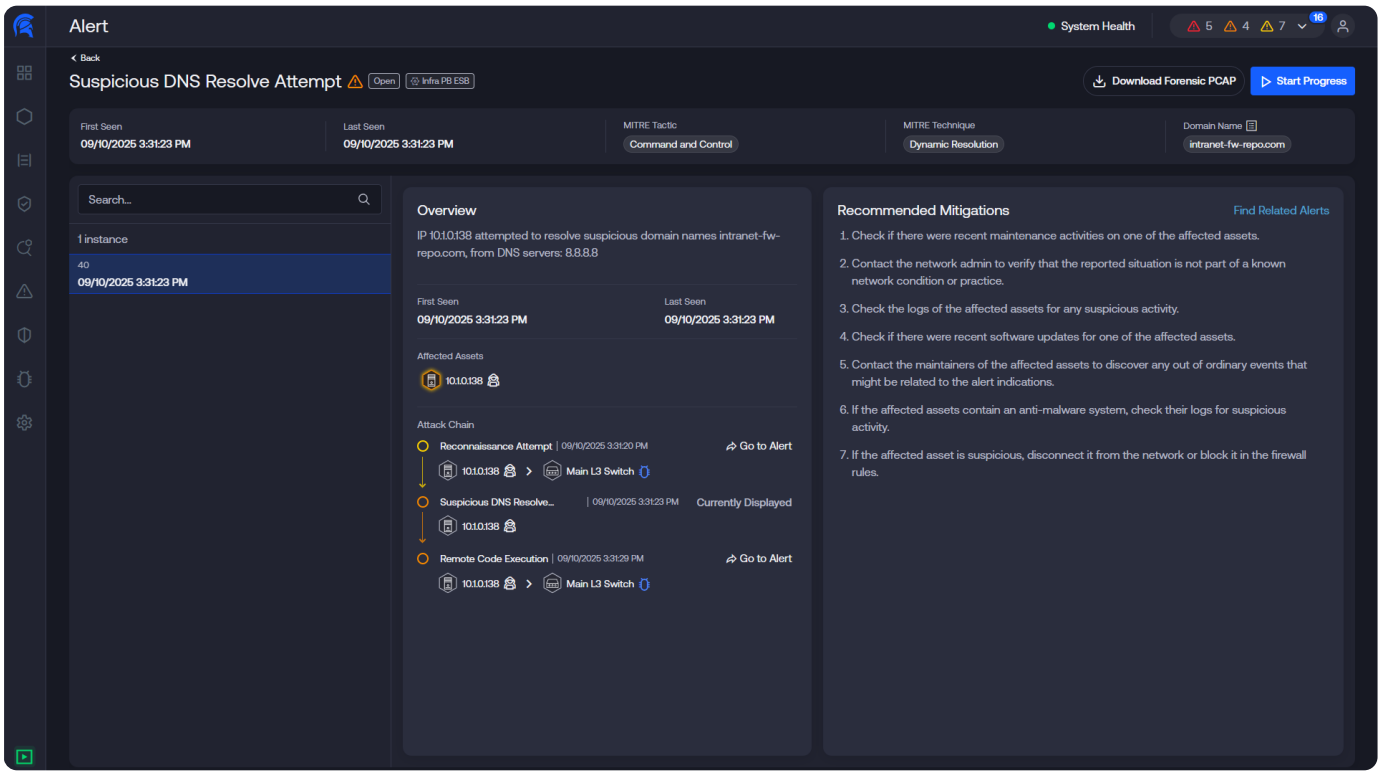
Alert Instances

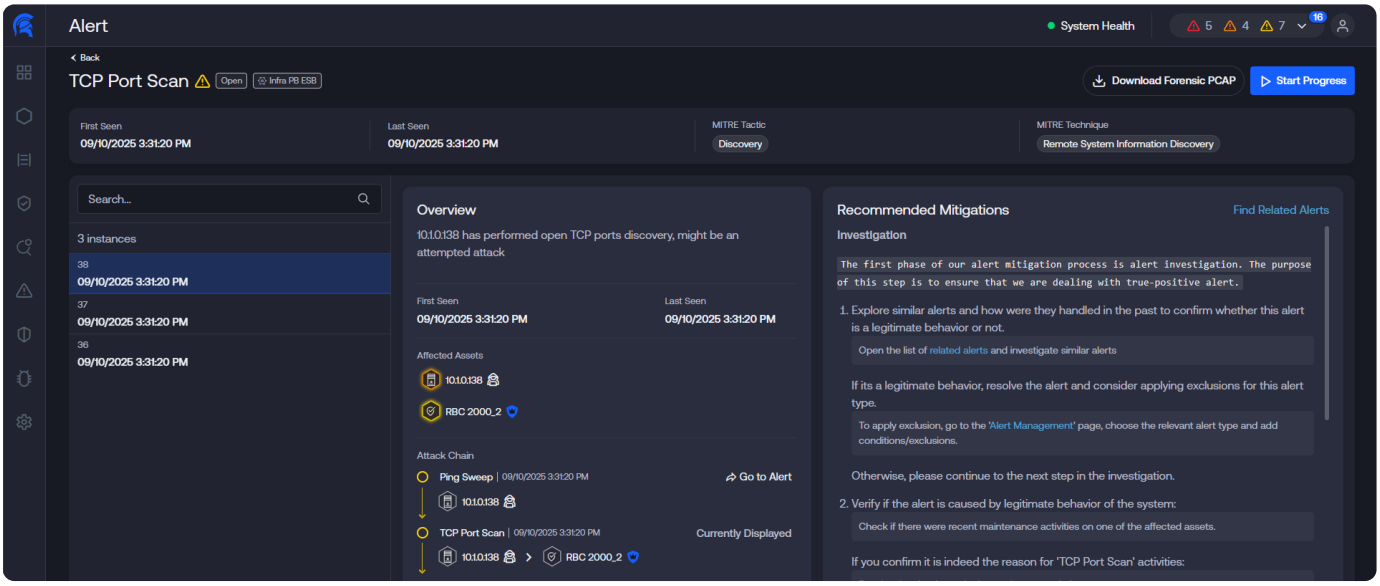
Operators can easily view and track all instances of a specific security alert, ensuring full visibility and a coordinated response across teams.

Rail-Specific Cybersecurity Mitigation Playbooks

Following the detection of any cybersecurity threat, CylusOne provides customers with tools and guidelines to investigate and mitigate the identified threat in the following manner:

- Each alert in CylusOne includes built-in mitigation guidance, which customers can further customize to align with their specific rail environment.
- Root causes of abnormal behavior are linked to each alert to quickly understand the problem.
- The operator can dive into what happened on the network during the alert time. CylusOne provides a comprehensive view of all events and messages, displayed in a user-friendly interface with advanced filtering capabilities based on IP addresses and rail-specific attributes.
- The mitigation instructions in CylusOne are designed in the language of rail operations, enabling both cybersecurity and operations teams to understand and respond to alerts in a coordinated and effective manner.
- Below is an example of a response playbook for an Unauthenticated Emergency Stop of a train, including the recommended mitigation measures and forensics insights.





The CylusOne solution collects data from all operational technology systems across the rail network, from control centers to remote field devices. This provides a complete and accurate view of system status, performance, and security.

Passive Network Integration and Data Collection

CylusOne accesses network traffic through switch SPAN ports, network taps, packet brokers, existing monitoring solutions, or Rail Juridical Recording Units (JRU). It supports both IT, OT, and rail-specific protocols to analyze this traffic, leveraging deep packet inspection to extract valuable insights from communications across all layers of the OSI model. By examining both metadata and DPI data, CylusOne identifies a wide range of operational assets, from workstations and interlockings to field-level components, offering comprehensive visibility across the rail environment.

Polling

Polling is an optional CylusOne capability that augments passive monitoring with tightly controlled, protocol-aware queries across IT, OT, and signaling networks—never touching safety critical logic. When activated, it reaches silent or segmented devices and collects firmware versions, configuration fingerprints, and other lifecycle details that passive sensors can't see.

Because every railway has its own risk tolerance, Polling is off by default and runs only under customer defined scopes, frequencies, and maintenance windows, fully aligned with existing safety and change management procedures. The enriched data streams into CylusOne's single pane of glass, completing asset inventories, mapping vulnerabilities to CVEs and IEC62443 controls, and giving operations teams the clarity they need to secure the entire rail OT environment without disrupting service.

Comprehensive OT Environment Monitoring

Our platform delivers unified visibility across the full operational technology landscape in rail environments, ensuring that every connected asset is accounted for, monitored, and protected in real time.

Monitored Systems Include:

- Signaling Systems – interlockings, track circuits, train detection, and control logic
- Rolling Stock Systems – onboard control, braking, train control management (TCMS), and passenger-facing subsystems
- Control Centers – traction SCADA servers, dispatch consoles, and workstation networks
- Communications Infrastructure – both wired and radio-based communication networks
- Depot & Maintenance Systems – diagnostic networks, automated inspection, and maintenance planning tools
- Station Systems – passenger information displays, CCTV, ticketing gates, and public announcement systems
- Edge & Field Devices – network switches, routers, wayside controllers, and remote terminal units (RTUs)
- Support & Auxiliary Systems – power supply monitoring, HVAC control, lighting systems, and environmental sensors

With a unified view, operators gain complete, end-to-end visibility of all OT assets across the rail network, ensuring no blind spots. This integrated approach enables immediate detection of anomalies, misconfigurations, or unauthorized activity while supporting operational continuity through early warning and proactive incident response.

Reporting and Compliance

CylusOne enables rail operators to keep pace with evolving regulations, aligning security practices with industry standards and ensuring compliance with both today's and tomorrow's requirements.

Prove Compliance to Known Frameworks

CylusOne reports help customers identify and prove their compliance by automatically assessing their security posture and measures against known frameworks

Customers can identify requirements in the standards and regulations that are either met or not met, along with evidence of compliance status. As the monitoring performed by Cylus mainly includes network traffic monitoring and integration to external data standards, the implemented frameworks for compliance are those at the system level or the asset owner level.

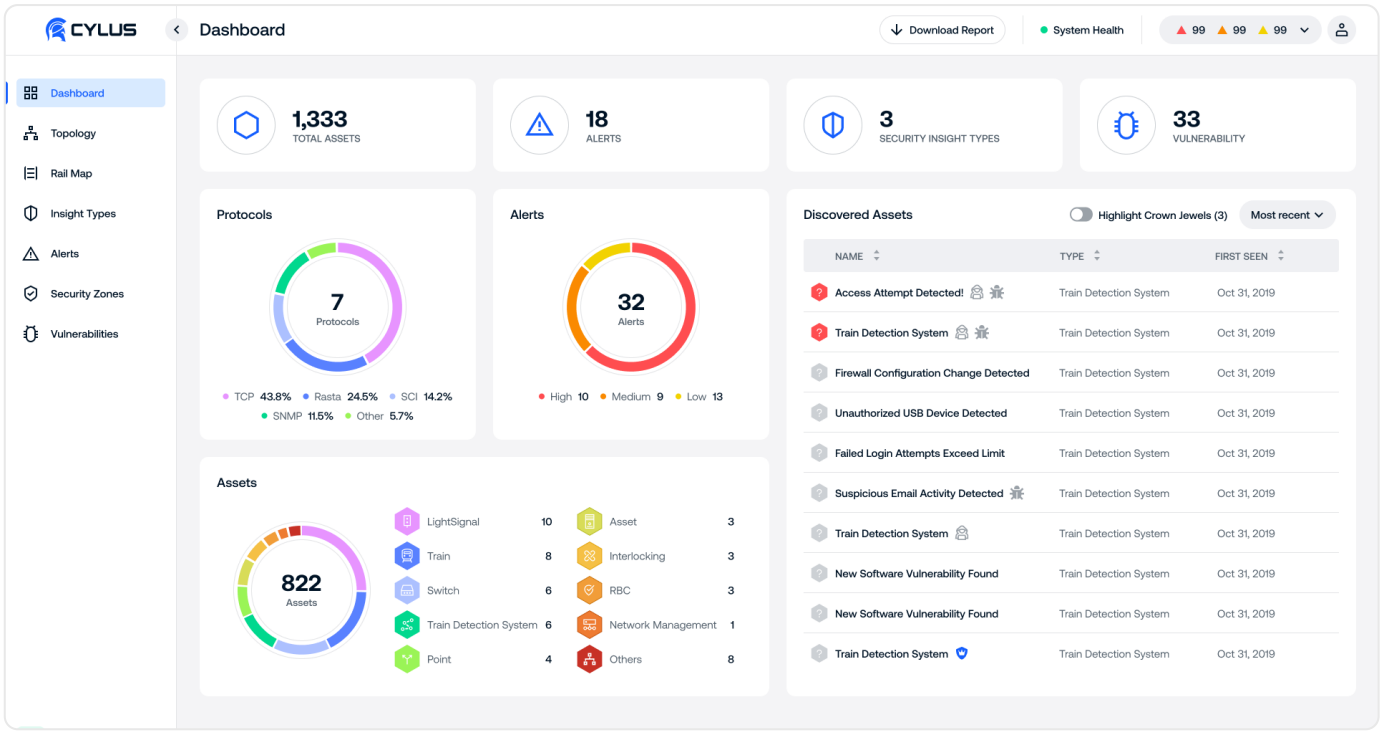
Demonstrate Compliance with Requirements and Security Directives

Additionally, CylusOne helps customers meet certain requirements within global standards, requirements, and security directives, among others.

Dashboard Experience Built for Rail Operations

CylusOne presents rail cybersecurity insights through a dynamic, operator-friendly dashboard designed for continuous operations. The platform adapts to the workflows of cybersecurity and operations teams alike, offering tailored visualizations for asset monitoring, incident response, and network management.

The dashboard supports layout customization, enabling users to focus on what matters most. For enhanced usability across different control room environments, CylusOne includes both light and dark display modes, allowing each user to choose their preferred visual setting without compromising visibility or clarity.



Deployment and Integrations

In 2017, Cylus introduced CylusOne, the first-to-market cybersecurity solution designed specifically for rail operators. Today, as the recognized market leader, we have set the standard for how operators can visualize, monitor, and manage their operational rail cybersecurity.

Deployed Globally in All Rail Type Environments

CylusOne is deployed across North America, Europe, Asia Pacific, and the Middle East, securing both signaling and rolling stock infrastructure. The platform provides a unified view of the entire operational rail technology landscape, supporting a wide range of use cases that extend beyond cybersecurity. From signaling and command-and-control systems to auxiliary, comfort, and public-facing applications, CylusOne offers visibility across rolling stock, trackside networks, train-to-ground communications, operational control centers, maintenance facilities, and station environments, empowering teams to monitor and manage complex rail systems through one streamlined interface.

Integrates Seamlessly into Existing Security and Operations Ecosystems

The CylusOne platform integrates with various existing customer solutions. Examples of the type of integrations and representative vendors/products are listed below.

- SIEM - Microsoft Azure Sentinel, Splunk, and IBM QRadar.
- Firewall / Next-Gen Firewall - Fortinet, Belden, Siemens Ruggedcom.
- Native Probe Integration Running on Network Equipment/FW - Belden, Siemens Ruggedcom, duagon, Digi, Ericsson.
- Service Management / Ticketing - ServiceNow, Jira.
- Identity Providers - Okta, Microsoft Active Directory.
- Rail Maintenance Systems - EVA+ by HaslerRail.
- Location Services - Google Maps, OpenStreetMap.

CylusOne also supports LDAP, discovery services, and SSO solutions, enabling multiple users to securely log in and operate within the system.

Flexible Deployment Architectures

CylusOne is designed for flexible deployment across diverse railway environments. Purpose-built for rail, it protects mainline, urban, and freight operations, including signaling, rolling stock, traffic management, and telecom systems.

Deployment Components

There are two primary components involved in the deployment of CylusOne.

CylusOne Probe

CylusOne Probes are software-based and can use network SPAN (Switched Port Analyzer) ports to non-intrusively monitor networks for rolling stock and signaling deployments. The SPAN port duplicates the communication of the network's critical assets and allows CylusOne to monitor and protect the network. A network TAP and/or network packet broker should be used if the SPAN ports are not available.

Traffic from each monitored network will be sent to one or multiple CylusOne Probes. The Probes will monitor the network and analyze its communication in a non-intrusive manner. Then, the CylusOne Probes will provide the CylusOne Platform with pre-processed information over an encrypted and compressed link, minimizing bandwidth.

Hardware Appliance	Virtual Appliance (VM)	Embedded Probe (Networking Equipment)
Standalone hardware connected to the TAP/SPAN Port	Virtual Machine of CylusOne Probe connected to the Port Mirror/TAP	Container running on existing networking equipment
Recommended Standalone Hardware Requirements: • CPU: based on x86_64/ARM64, 4 Cores • RAM: 8GB • Storage: 16GB SSD • TPM 2.0 • Network Interfaces: per design • OS Support: Ubuntu 22.04 • For Rolling Stock: EN 50155 Certification		**Supported Equipment:** • Belden Eagle40 • Siemens RuggedCom • Cisco IOX Platform • Alstom XPU • Digi TX64 • Ericsson Cradlepoint R1900

CylusOne Platform

The CylusOne platform can be deployed on-premise or as SaaS and is the main component of the solution, receiving data from CylusOne Signaling and Rolling Stock Probes and providing analysis of network communication, threat detection capabilities, live asset inventory, and SIEM (security information and event management) integration. It offers immediate out-of-the-box functionality, including asset visibility, insights into network misconfigurations, and identification of potential security threats.

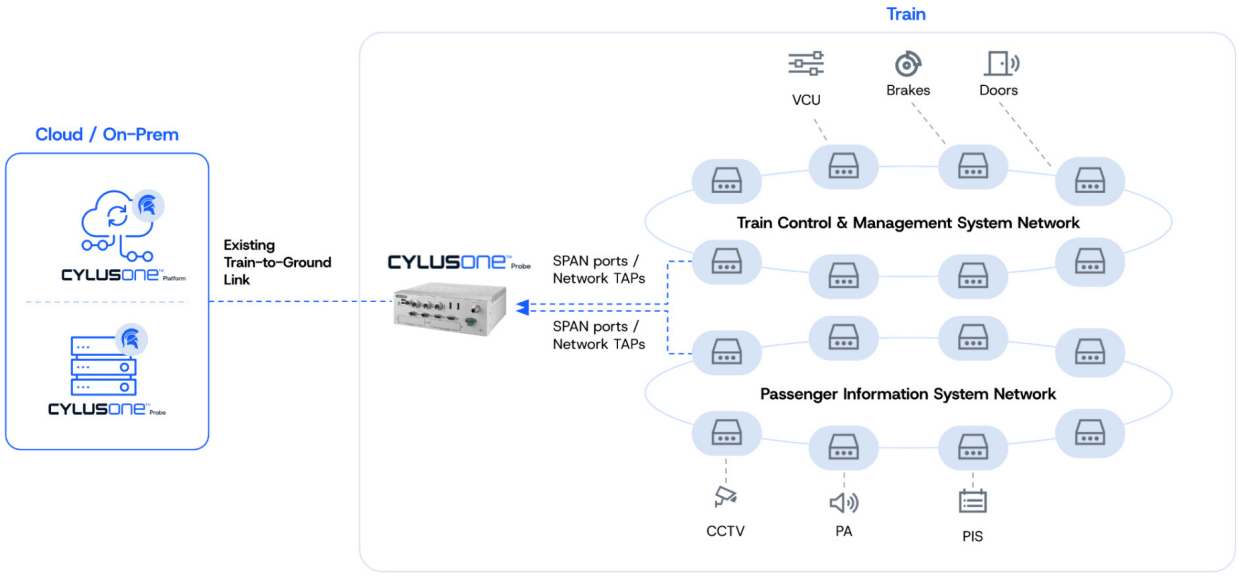
<table>
<tr><th>Cloud / SaaS</th><th colspan="2">On-Premise</th></tr>
<tr><td rowspan="2">Fully Maintained by Cylus
(*) Tenants can be set up in all supported AWS.regions</td><td>Standalone hardware server</td><td>Virtual Machine (ESXi, Proxmox)</td></tr>
<tr><td colspan="2">Minimum Hardware Requirements:
• CPU: based on x86_64, 8 cores with 16 Threads, 2.8GHz
• RAM: 64GB
• Storage: 1TB (RAID 1)
• TPM 2.0
• Network Interfaces: per design
• OS Support: Ubuntu 22.04</td></tr>
</table>

(*) Cylus can support additional hardware on demand.

Deployment in Rolling Stock Environments

CylusOne supports common rolling stock network interfaces, including Ethernet, CAN, MVB, WTB, and serial networks on rolling stock systems. CylusOne Probes are non-intrusive and help maintain the current rolling stock's safety level with zero impact on the rolling stock network. The CylusOne Probe software can run on various HW compliant with EN50155. Additionally, CylusOne data collection is designed to operate under typical train-to-ground (T2G) communications constraints without the loss of any monitored data or alerts.

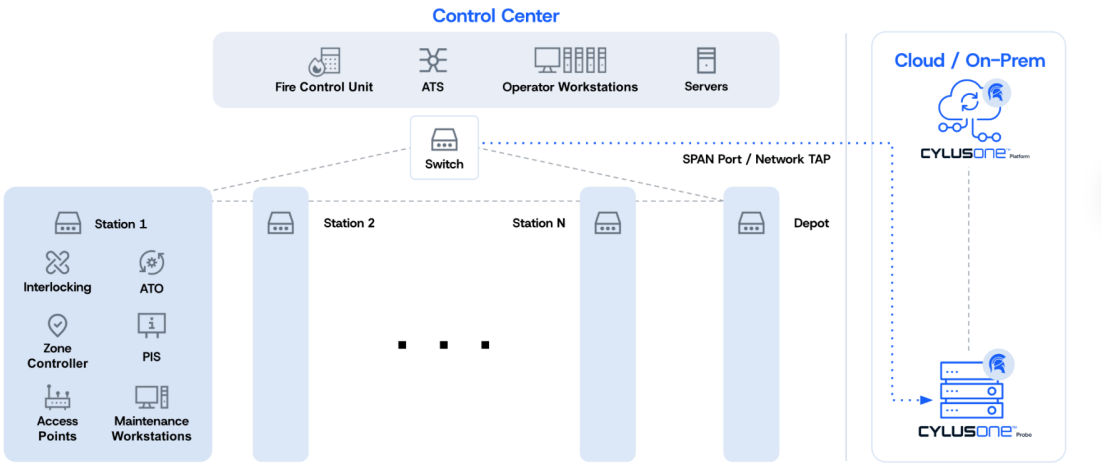
CylusOne Probes efficiently reduce monitored traffic before transmitting data over the train-to-ground communications network to the CylusOne Platform. This helps to minimize T2G bandwidth consumption. Additionally, CylusOne can buffer data locally when there is no T2G connectivity, such as when a train goes through a tunnel or in areas of limited to no communication.



Deployment in Infrastructure Environments

The CylusOne architecture is built to fit any network constraints by providing a scalable architecture to support all operational rail environments. As railway assets are geographically spread across cities and/or countries, CylusOne offers a distributed architecture built from remote CylusOne Probes and a centralized CylusOne Platform, enabling a single cybersecurity control and management view of the entire network.

Below is a typical CylusOne deployment in a rail infrastructure environment.



About Cylus

Cylus provides advanced rail cybersecurity solutions, offering the first dedicated system to protect the entire rail OT and ecosystem. Cylus provides unparalleled visibility and threat detection across infrastructure, rolling stock, control centers, and stations, bringing all components into a unified security solution.

Trusted by rail operators and partners worldwide, Cylus helps ensure compliance with regulatory requirements and industry standards while maintaining safety and uninterrupted operations. Backed by years of rail-specific innovation and global adoption, Cylus empowers organizations to protect their critical systems, detect threats early, and respond effectively, with confidence grounded in proven performance.