CYLUS
Cybersecurity on Track

Solution Brief

CylusOne for Asset Discovery and Inventory

The magnitude of railway networks and the fact that they consist of endless assets, which are spread over large physical spaces, makes it extremely challenging to monitor and protect. The variety of systems and vendors, the growth in using commercial off-the-shelf vs. proprietary systems, and the increasing connectivity, create a wider attack surface and more entry point for attackers.

The complexity and **diversity** of the railway systems and the **lack of comprehensive visibility**, make accurate and timely detection of malicious activities more challenging. Asset discovery and inventory management provide the visibility and management efficiency required for protecting railway companies, enabling them to **meet compliance and build overall cybersecurity resilience.**

Solution Highlights

1. Automated discovery of all assets
2. Full visibility with live asset monitoring
3. Context-aware of rail application logic
4. Smart partitioning into Zones & Conduits
5. Advanced security analytics and reporting
6. Passive, non-intrusive flexible deployment
7. Complying with IEC 62334, TC 50701 & NIS-D

Your Benefits

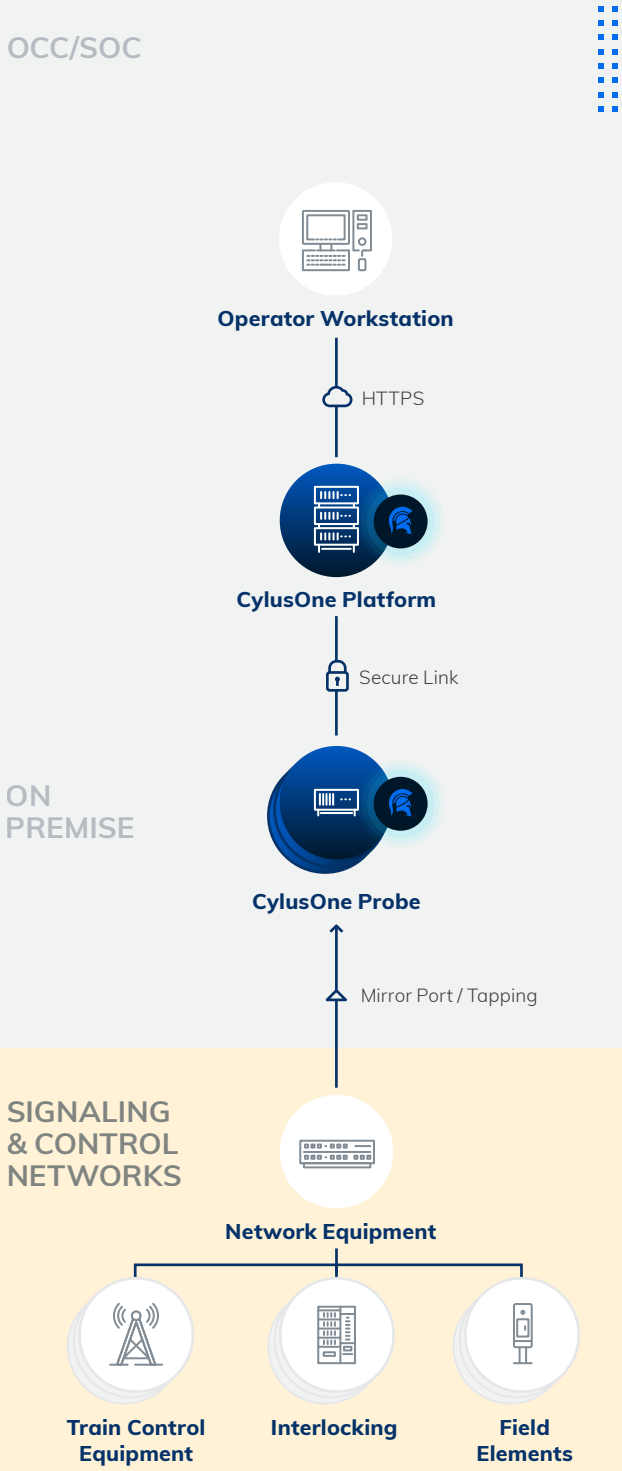
- Address cybersecurity and compliance needs with a single, efficient, and automated security suite
- Ensure maximum safety, availability and cyber resilience, with early detection of threats and operational incidents
- Save your analysts' time with instant reports, and faster incident resolution

Step 1

Flexible Deployment that Fits Your Network

The CylusOne solution can be deployed in various railway environments and has been developed specifically to protect mainline, urban, and freight rail operational (OT) environments, including signaling, rolling stock, traffic management, and telecom systems.

- No Impact on Safety - Fully passive, non-intrusive and does not add latency to safety-critical systems
- Straightforward Deployment - Without requiring prior information on the network
- Integrates with both modern and legacy systems - Supporting a wide-range of rail protocols and applications



Supported Systems

Signaling
ETCS, CBTC, PTC, Interlocking

Rolling Stock (on-board)
TCMS, Passenger Comfort Networks, Onboard Signaling

Auxiliary & Comfort
CCTV, PIS , Ticketing, PA, etc

Traffic Management
TMS, ATS

Telecom
GSM-R, GPRS, WiFi, FRMCS, Radio Technologies

* Quick creation of new protocol support

Safe and Seamless Deployment

CylusOne collects data without impacting safety, its installation is agonistic to the wayside and onboard structure, without the need of modifying the existing installation architecture. We provide a variety of methods to connect to your network so you can choose what suits best for you

The data can be collected in one of the following ways:

1. SPAN or Mirroring port - Connect CylusOne Probe directly to a preconfigured SPAN or mirroring port.
2. CylusOne Safe & Secure passive tapping- Connecting the CylusOne Probe as safe tapping solution.
3. Integrated as lightweight software agent within existing gateway or network devices
4. Integrating with existing 3rd party listening device or data extraction solutions

You can only protect what you can see.

Visibility is key for creating an accurate asset inventory and keeping it updated. This is a particularly challenging and time-consuming task for rail operators.

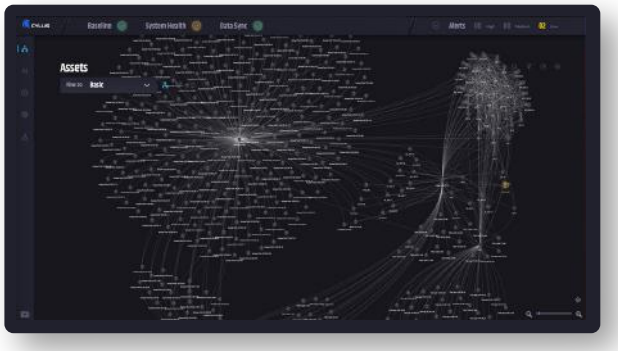
Rail systems consist of a large number of devices from different vendors, and generations-long technologies, all spread over large geographic locations, yet they all have to be accurately documented, managed, and monitored, even if they are being changed or replaced or first introduced in the network.

Step 2

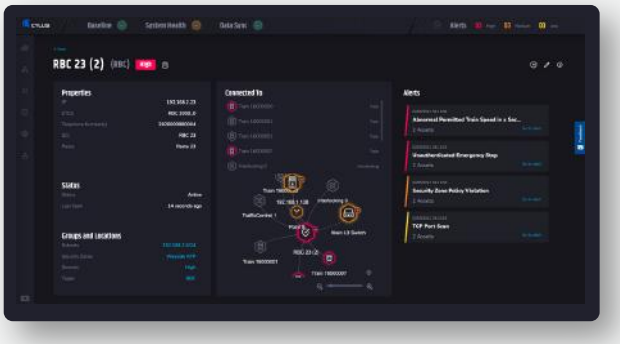
Gain Full Visibility Over Your Assets

Automatic Asset Discovery

CylusOne automatically discovers all assets and **blind-spots**, and enriches them with their respective function, configuration and other fingerprints within the rail systems. In addition, CylusOne monitors and analyzes network flows, device access and authentication attempts to these assets, and estimates the risk of operational malfunctions or failure. The visibility provided by the asset discovery process is critical for cyber resilience, operational monitoring, successful patch management processes and complying with standards requirements.



Automatic real-time discovery of all assets, including non IP and “hidden” field devices according to IEC-62443-3-2 (ZCR1) and TS-50701



Out-of-the-Box Entity Enrichment

Rail-Focused entity enrichment of device OS, configurations, security level, function (e.g: interlocking, point machine, etc.) network & zones, rail application, physical properties and application level identifiers

Live connection mapping

Analyzing all traffic flows including your proprietary rail technologies and protocols. Powered by patented machine learning algorithm the “Live” connection mapping helps create a network baseline that enables anomaly behavior analysis

Your network contains thousands of assets

Managing the rail asset inventory requires significant of effort and resources and is at best carried out periodically. Managing newly discovered devices, unassigned devices, and devices that were not approved is critical. Not knowing the device risk level, access policies, behavioral processes and rules, can have a critical impact on the availability, safety and security.

Step 3

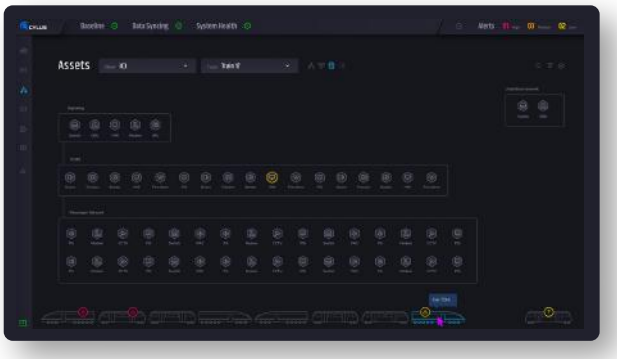
Effectively Manage your Inventory

CylusOne analyzes all assets and traffic flows including your proprietary rail technologies and protocols and facilitates management of your assets and systems' configurations. It then automatically maps in real-time, all the existing zones, conduits, components, and communications over the signaling, on-board, interlocking, passenger information systems, CCTVs and more.

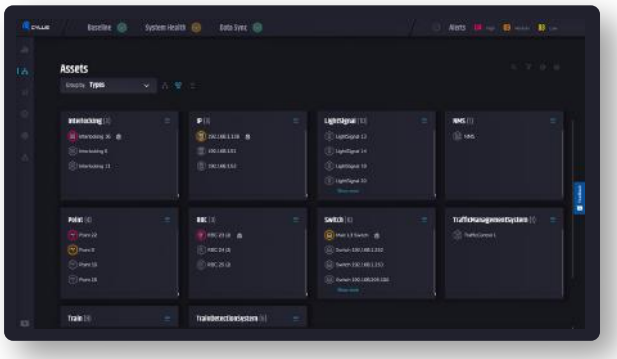
The live inventory monitoring provides your analysts an accurate view of the risks to the networks at any given moment, enabling them to react fast. In addition, the always up-to-date asset inventory ensures timely detection of risk and facilitates compliance (IEC 62443, TS 50701, RISSB AS-7770).

Visualization of Assets

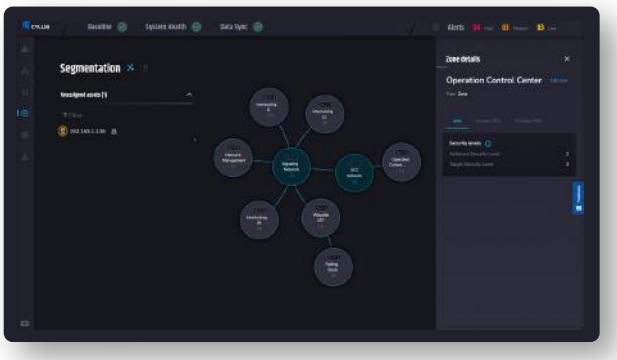
Based on the Cylus innovative Rail-Purdue model, to help you focus on what's important



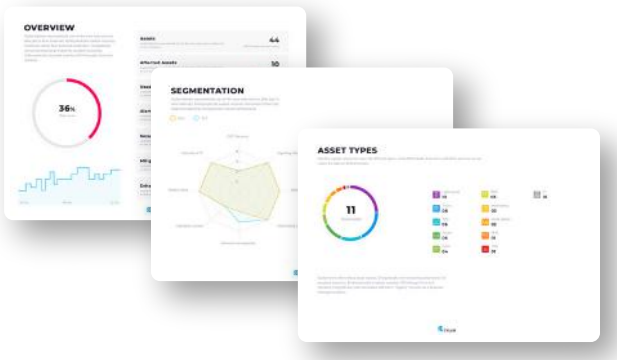
Continuous inventory monitoring of all assets and their functions



Advanced views, grouping and filtering capabilities such as SIL level, Vendor, Severity etc



Automatic virtual segmentation into Zones and Conduits according to IEC-62443-3-2 (ZCR3)

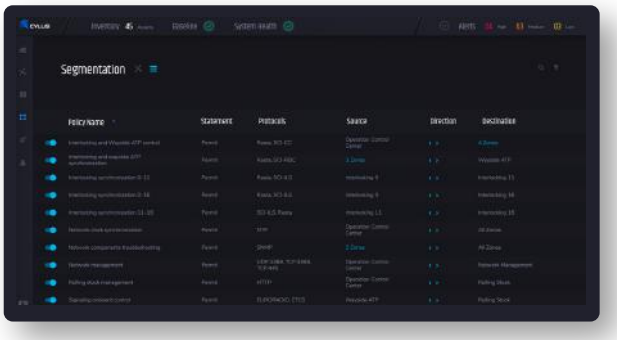


Export of views using built-in or customizable reports for different stakeholders and needs

Advanced Security Analytics

CylusOne conducts continuous risk and vulnerability assessments and maps out the different zones and conduits in your networks. This enables us to identify the associated risk and their impact on your operational environment by matching the corresponding security levels, existing vulnerabilities and the gaps between existing and adequate risk levels. CylusOne then provides vulnerability mitigation recommendations and actions required to reduce the risk to its target level.

- Indication of newly discovered, unmanaged and malicious assets
- Notification on known CVEs as well as vulnerabilities from the Cylus rail-specific proprietary database
- Alerts on security deficiencies including misconfigurations, unauthorized access etc.



- Strict policy definition on proprietary protocols (not just IP & Port, but specific application messages)
- NAC and Zero-Trust compensating controls for complex rail networks topologies and equipments
- Detection of policy violation, baseline deviation and configuration changes

Facilitate Collaboration and Compliance

Bridging the gap between cybersecurity and rail operations

- Live interactive track layout and geolocation map
- Import documentations to compare and detect violations with existing installed base
- API for seamless integration with existing OCC & SOC components, such as: SIEM, FWs, Ticketing, Audit and more.

Reach us at Info@cylus.com or visit our website www.cylus.com

About Cylus

Cylus is a global leader in rail cybersecurity. We address the full spectrum of cybersecurity needs of rail signaling and rolling stock systems, ensuring safety, service availability and facilitating compliance, for mainline and urban railway companies. Cylus rail cybersecurity solutions are trusted by top-tier railway companies globally and promotes cybersecurity of the rail ecosystem as a whole