WAYSIDE WATCHER

Detection without doubt. Records that verify themselves.

The back-office platform for railroad wayside and on-asset devices — one consistent surface across brake-test, hot-bearing, grade crossing, battery-and-charger, wheel impact, and acoustic bearing systems. Runs on premise or in the cloud, with tamper-evident records auditors and customers can verify on their own.

WHY NOW

The rules changed. The records didn't. Until now.

Three forces converge to make this the right moment for a railroad back office whose operational records are provable rather than merely well-presented. Regulatory direction is set. The technology is mature. The legal substrate exists. What's been missing is purpose-built software for the industry that actually produces records to that standard.

2024

NTSB's final East Palestine report set the agenda.

Cross-railroad data sharing and operational-record quality are now policy questions. The FRA's Safety Advisory 2023-01 and its supplements through July 2024 made the trajectory unmistakable.

Rule 902

Federal Rules of Evidence already accommodate records like these.

The 2017 amendments — subsections 902(13) and 902(14) — made digital records and forensic copies self-authenticating when accompanied by a qualified certification. Admissible without a live witness on the stand. The legal substrate exists; the industry has just not had operational software that produces records to that standard natively.

170 °F

The AAR's new hot-bearing stop-and-inspect threshold — above ambient.

Lowered post-East Palestine. Class I railroads also tightened detector spacing on key routes from about forty miles to about fifteen. More detectors, more events, more records to defend.

Railroads run on operational records. Those records have historically been accepted because the industry has nothing better — not because anyone can independently prove they are authentic.

— THE THESIS BEHIND WAYSIDE WATCHER

THE PLATFORM

One back office. Every wayside device. Every record, verifiable.

Wayside Watcher is a back-office platform for the devices the railroad industry uses to inspect rolling stock and wayside equipment. It runs on premise inside your data center, in your own cloud tenant, or as a managed service from Outlier — with the same features in every option. It does the conventional things a modern back office should do: ingest inspection reports, surface alarms, manage calibration, route notifications, generate compliance documentation, produce data feeds.

It adds one property the incumbents do not have: every operational record it produces is tamper-evident and independently verifiable. The brake-test report, the calibration certificate, the firmware deployment event, the operator certification, the wayside detector inspection — each is an audit-ready artifact under the same framework, with a verification link anyone can open without an account.

DEVICE COVERAGE

One platform, six device categories on the same surface.

ASCTD
FOUNDING DEVICE

Automated Single Car Test Device. Pivotal Rail Products' next-generation brake-test platform — the device Wayside Watcher was built around.

HBD
LIVE TODAY

Hot Box Detectors. Real historical inspection corpus loaded; alarms filterable by AAR-standard categories (Absolute, Differential, Carside).

Grade Crossings
LIVE TODAY

Highway-rail grade crossing equipment. Predictor health, gate, light, bell, and event-recorder data with the audit-ready records FRA inspectors expect under 49 CFR 234.

Battery & Charger
LIVE TODAY

The standby power systems behind every wayside bungalow. Bank state-of-charge, charger health, and aging characteristics — on the same fleet pattern.

WILD
ROADMAP

Wheel Impact Load Detectors. Committed on the same architecture, the same surfaces, the same record format.

ABD
ROADMAP

Acoustic Bearing Detectors. Committed on the same architecture, with the same one-dispatcher-trained-on-one-UI promise.

BUILT FOR THE PEOPLE WHO RUN IT

Different teams, same platform, same surface.

The platform's value lands differently for each team that touches it. Operations lives in the fleet grid and the alarms queue. Maintenance lives in calibration and reliability. Engineering lives in playback and provenance. Compliance lives in the audit log and the verification portal. One platform, four jobs done well.

OPERATIONS & PROGRAM MANAGERS

The normal morning is easier. The bad morning is manageable.

Fleet visibility in one consistent pattern across device classes. Alarm lifecycle with documented ownership and reason capture. An investigations queue that pulls the failed report, the playback, the related health trend, and the calibration record into one place — automatically. Customer and auditor requests turn from "pull, format, sign, send" into "here's the link."

FROM EVIDENCE COURIER → EVIDENCE CUSTODIAN.

MAINTENANCE & RELIABILITY

The M-1003 audit cycle becomes a query, not a paper hunt.

Calibration management is first-class: fleet dashboard, drift per channel, due-date status, technician identity bound to every certificate. Health analytics surface drift, retries, watchdog clusters, and atypical pressure events with the rule, the threshold, and the value that crossed all visible — no opaque scoring. Recommendations come with evidence; maintenance decides what work happens.

PREDICTIVE MAINTENANCE, WITH THE EVIDENCE TO BACK IT.

ENGINEERING

Failed tests are replayable. Cohort questions are queryable.

Every certified report carries firmware version, configuration version, requirements baseline, and calibration package. Test sequence playback at 10 Hz across four pressure channels lets engineering replay any moment of any test. When a firmware version turns out to have an issue, the affected report population is a single filter — not detective work.

FIELD DEFECTS, SCOPED IN SECONDS.

COMPLIANCE & QUALITY

Audit-ready by construction — for AAR, FRA, and customers.

Direct contribution to M-1003 elements E07 (document control), E08 (measuring and testing equipment), E14 (identification and traceability), E15 (process control), E17 (quality records), E18 (nonconformance), E21 (internal audits), and E24 (design control). FRA line of sight via 49 CFR 232.305 / AAR S-4027. Every record carries a tamper-evident audit trail.

RECORDS THAT HOLD UP — IN COURT, IN AUDIT, IN THE PRESS.

RUN IT YOUR WAY

Three deployments. One feature set.

Wayside Watcher runs where your security, data-residency, and procurement posture say it should — with the same capabilities in every option. Pick the boundary that fits your organization; the platform doesn't change underneath.

OPTION A

On-Premises

Runs inside your data center on your hardware, behind your firewall. You own and control the data. Internet egress is required for verification, telemetry, and updates — the platform is not designed to run air-gapped.

- Your servers, your network boundary
- Egress controlled by your firewall policy
- Same UI, same APIs, same record format
- Supported on a defined hardware spec

OPTION B

Customer Cloud

Deployed inside your AWS, Azure, or GCP tenant. Your network, your IAM, your data residency — Outlier supports the platform that runs there.

- Your cloud account, your VPC
- Egress to verification & update endpoints
- Customer-managed encryption keys
- Supported under a documented run-book

OPTION C

Outlier SaaS

Fully managed by Outlier. Often the right fit for short lines and smaller operators who want detection and verifiable records without standing up infrastructure.

- Multi-tenant or dedicated single-tenant
- SSO via SAML/OIDC into your IdP
- Outlier owns ops & patching
- Standard data-processing terms

Integration posture — built so your IT team recognizes it.

IDENTITY
SAML 2.0 and OIDC into your existing IdP. Role-based access mapped to your groups.

APIS
Documented REST endpoints; event webhooks; streaming feeds where high volume warrants.

OBSERVABILITY
Structured logs, metrics, traces. Exportable to your SIEM and observability stack.

FRAMEWORKS
Designed against NIST CSF 2.0, NIST SP 800-82 Rev 3, IEC 62443-2-1 (2024).

NEXT STEP

Open the demo. Verify a record without taking our word for it.

A working demo build runs at www.waysidewatcher.com with a ten-device ASCTD fleet, eighty-plus operational reports, the hot-bearing

TALK TO US

Outlier Engineering Group LLC

info@outliereg.com
www.waysidewatcher.com
Founding device partner: Pivotal Rail Products

TRY THE DEMO

www.waysidewatcher.com

A working v0.5 build with realistic seeded data — not a production-hardened system. The public verification page works without an account.

PILOT FIT

Right for you if…

You operate ASCTD or wayside detectors, your back office is a patchwork, and you've been asked — or expect to be asked — to defend specific records.