BoundaryScore™ Data Rights Q&A

Independent evaluation requires evidence. It does not require surrender of participant control. BoundaryScore™ limits collection to information necessary for the rating and protects participant-specific evidence from disclosure, inference, reconstruction and reverse engineering.

1 What evidence does BoundaryScore™ require?

Only the limited operational evidence needed to calculate, validate, maintain and explain the agreed verification. This may include selected Machine-State Metadata such as system state, command or fallback state, software version, timing and defined event evidence. TraceQ™ supplies an independent record of physical motion, so the rating does not rely solely on participant-reported information.

2 What information is outside scope?

BoundaryScore™ does not require source code, model weights, training datasets, proprietary algorithms or planning logic, internal developer communications, unrestricted network access, or write/control access to the vehicle. The integration is designed to avoid material compute, latency or operational burden.

3 Who owns participant data?

Participant-generated Machine-State Metadata remains participant-owned. Paverly uses it within the agreed BoundaryScore™ framework only to evaluate, reconcile, validate and rate performance and to create protected derived outputs. Each participant retains access to its own observations, metrics, events, trends, version comparisons and reconciled results.

4 Who can access participant-specific data?

Raw Machine-State Metadata, raw event-burst evidence and granular identified operating records are not sold or disclosed to competitors, subscribers, suppliers or unrelated third parties. Identified disclosure occurs only with affirmative participant authorization or when legally required.

5 Can market products reveal a participant?

No. BoundaryScore™ does not release market outputs that permit protected participant data to be identified, inferred, reconstructed or reverse engineered. Aggregation, normalization, obfuscation, suppression, access controls, cybersecurity, policy and contractual restrictions work together to prevent disclosure. If a proposed data slice creates an identification path, it is not released.

6 Why is confidential evidence appropriate?

The model is familiar: physicians maintain medical records, auditors review financial records, and credit systems handle highly sensitive information because access is necessary to perform an evaluation. Access does not make the underlying record public. BoundaryScore™ applies the same separation between evidence access and external disclosure.