RAYMON

Raymon Industrial Security Platform

Technical Solution Brief

Version 1.0 · August 2026 · Customer publication

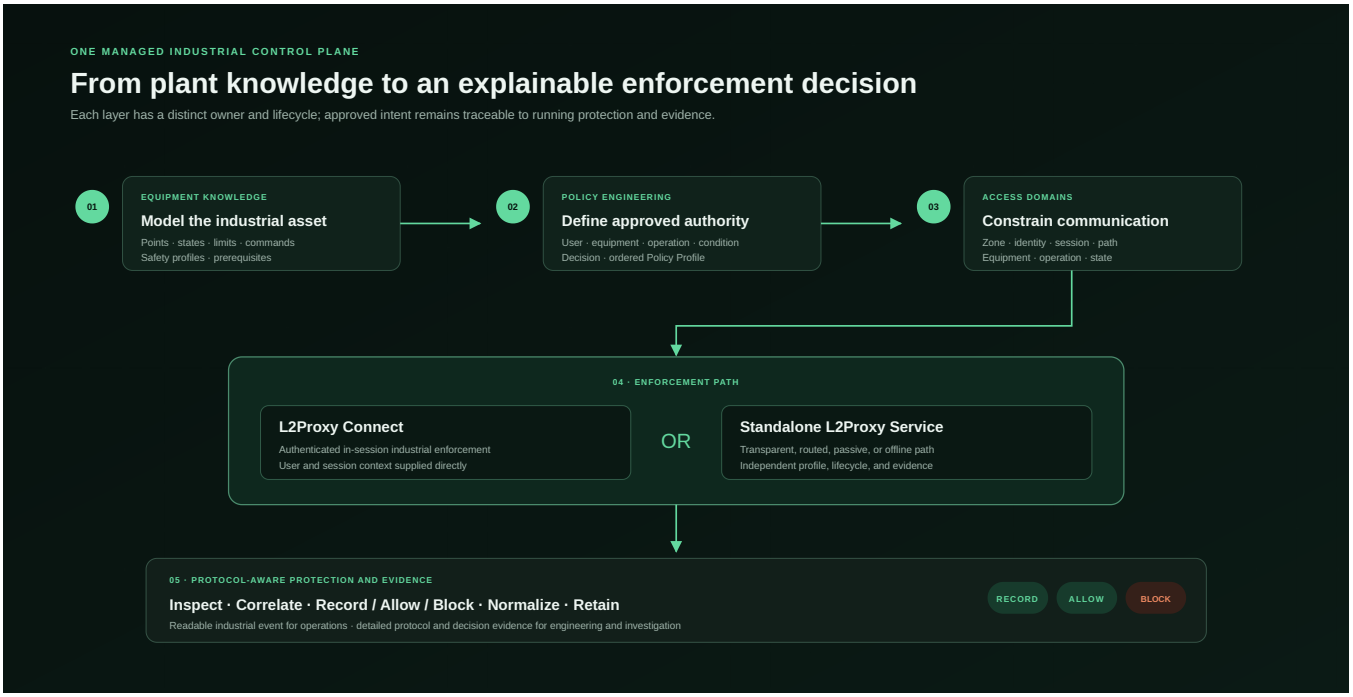
Raymon Industrial Security Platform

Technical Solution Brief

Raymon is an industrial access, inspection, policy, enforcement, and evidence platform for OT and ICS environments. It evaluates industrial protocol meaning together with equipment knowledge, approved policy, process state, and—when **Raymon Connect** is used— the authenticated user and live session.

> **Technical outcome:** determine who introduced an industrial operation, which equipment and process context it affects, whether it is permitted, why Raymon recorded, allowed, or blocked it, and which evidence supports that decision.

Managed platform architecture



The platform separates equipment knowledge, policy intent, access domains, enforcement, and evidence while preserving traceability between them.

Separation of operational responsibilities

Managed layer	Question answered	Raymon capability
Equipment knowledge	Which assets, points, states, limits, and commands exist?	Equipment and Protection Management
Policy intent	Who may do what, to which equipment, under which conditions?	Industrial Policy Management
Identity-aware access	Which user and live session introduced the operation?	**Raymon Connect**
Segmentation	Which domains, equipment, and operations may communicate?	Industrial Segmentation and Microsegmentation
Service operation	Where and how will the approved protection run?	Standalone Service Management
Enforcement	Is the operation permitted and consistent with process state?	Rule Engine and Stateful Protection
Evidence	What happened, why was the decision made, and what does it mean?	Normalization, Event Archive, and Event Explorer

Separating these layers prevents an equipment-library change from silently activating production policy and prevents an approved policy revision from becoming an unreviewed service change.

Inspection and policy model

From protocol frame to explainable decision

```
Traffic + optional session identity
                  ↓
          L2Proxy Dissector
                  ↓
  Protocol fields and semantic helpers
                  ↓
     Ordered stateless/stateful policy
                  ↓
          Record / Allow / Block
                  ↓
Rule event + metadata + state event + normalized industrial event
```

The L2Proxy Dissector decodes industrial traffic into addressable fields. Protocol-aware helpers provide stable predicates and canonical values for policy engineering. Rules are compiled when loaded, evaluated in order, and can add selected scalar metadata to logged matches. Customer-specific identities, equipment mappings, points, timing, permitted values, sequences, and final decisions remain in managed policy rather than being hard-coded into the protocol implementation.

Policy lifecycle

```
Equipment and point definition
            ↓
Rule: one precise industrial test
            ↓
Access Policy: identity + scope + operation + condition + decision
            ↓
Policy Profile: ordered, complete approved policy set
            ↓
Raymon Connect or Service Profile
            ↓
Running enforcement path + retained evidence
```

The engineering workbench supports parser-derived fields, contextual autocomplete, semantic-helper help, operator and value suggestions, reusable templates, lint feedback, and Rule Engine expression compilation. This allows policy authors to confirm what the deployed parser exposes and validate an expression before activation.

Stateless and stateful protection

Stateless policy evaluates one observed operation. Stateful policy can correlate events across messages and time, including:

- authorization followed by command;

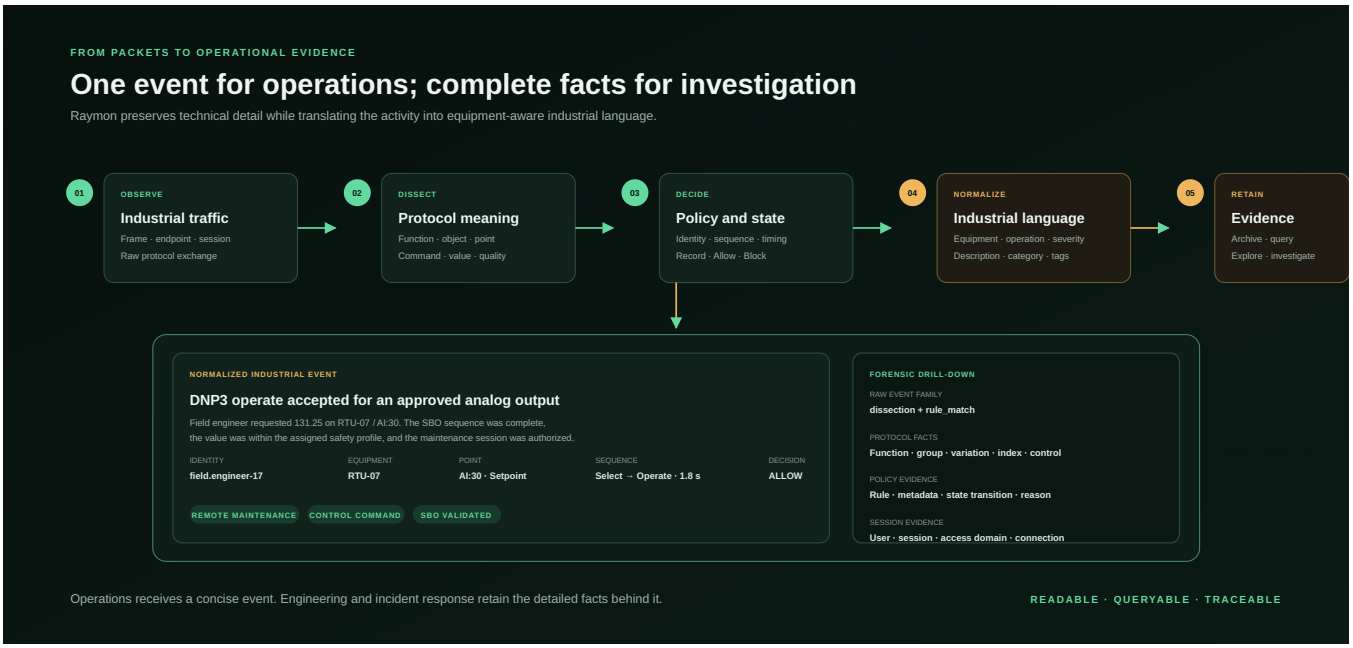
- Select-Before-Operate consistency and expiry;
- command followed by response or process feedback;
- maintenance authorization and identity binding;
- restart, recovery, configuration, and health verification;
- alarm lifecycle, chattering, burst, and replay behavior;
- bounded counters, atomic transitions, and packet-independent timeout events.

Current state is bounded, local to one engine instance, held in memory, and deliberately not restored after restart. Persistent distributed state and atomic multi-key transactions are not current runtime features.

Decision and evidence model

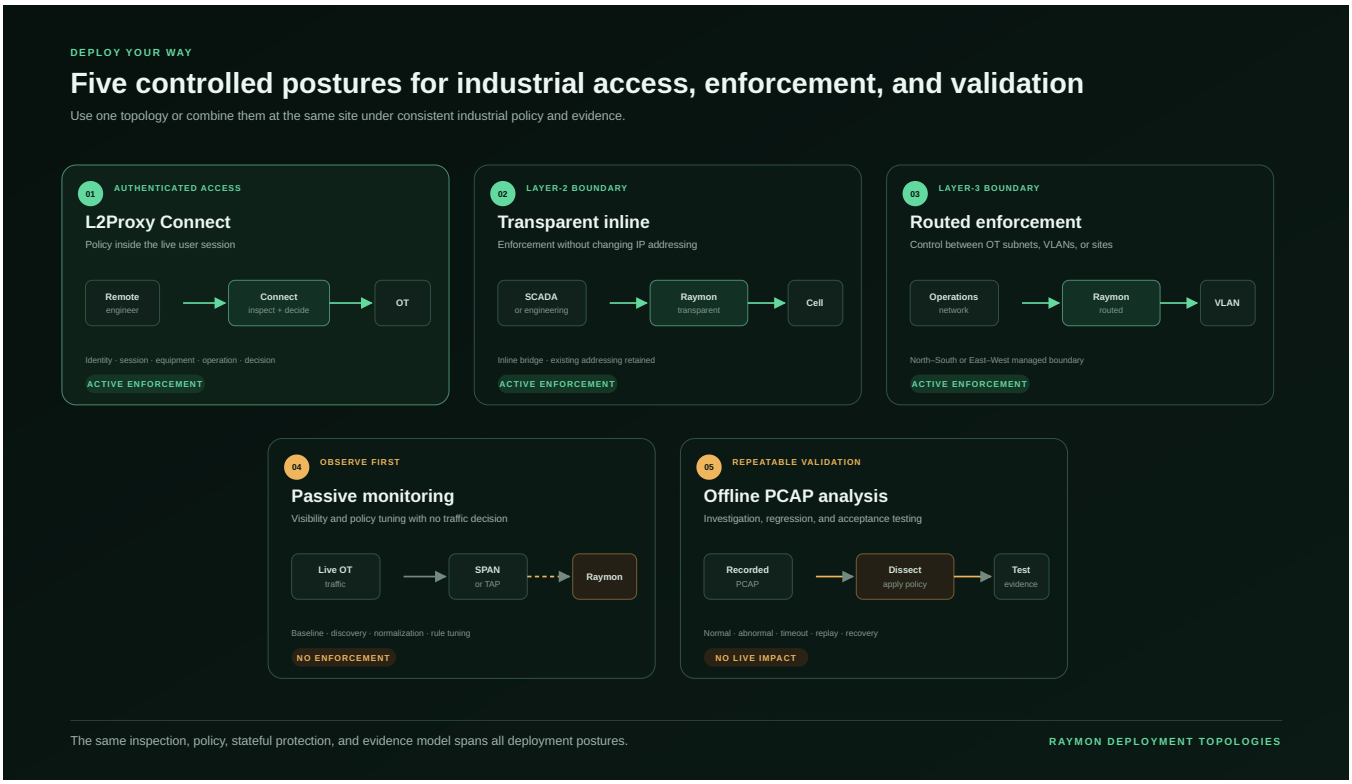
Customer term	Engine action	Result
Record	`log`	Retain the match and selected operational metadata
Allow	`accept`	Permit an operation satisfying policy
Block	`drop`	Stop an operation violating approved inline policy

Evidence can include rule identity, frame, endpoints, protocol layers, verdict, selected metadata, state transition, timeout, and—where **Raymon Connect** supplies it—authenticated user, session, access domain, and connection context.



A concise normalized event serves operations while the raw protocol, policy, state, and session evidence remains available for engineering and investigation.

Deployment and operational workflow



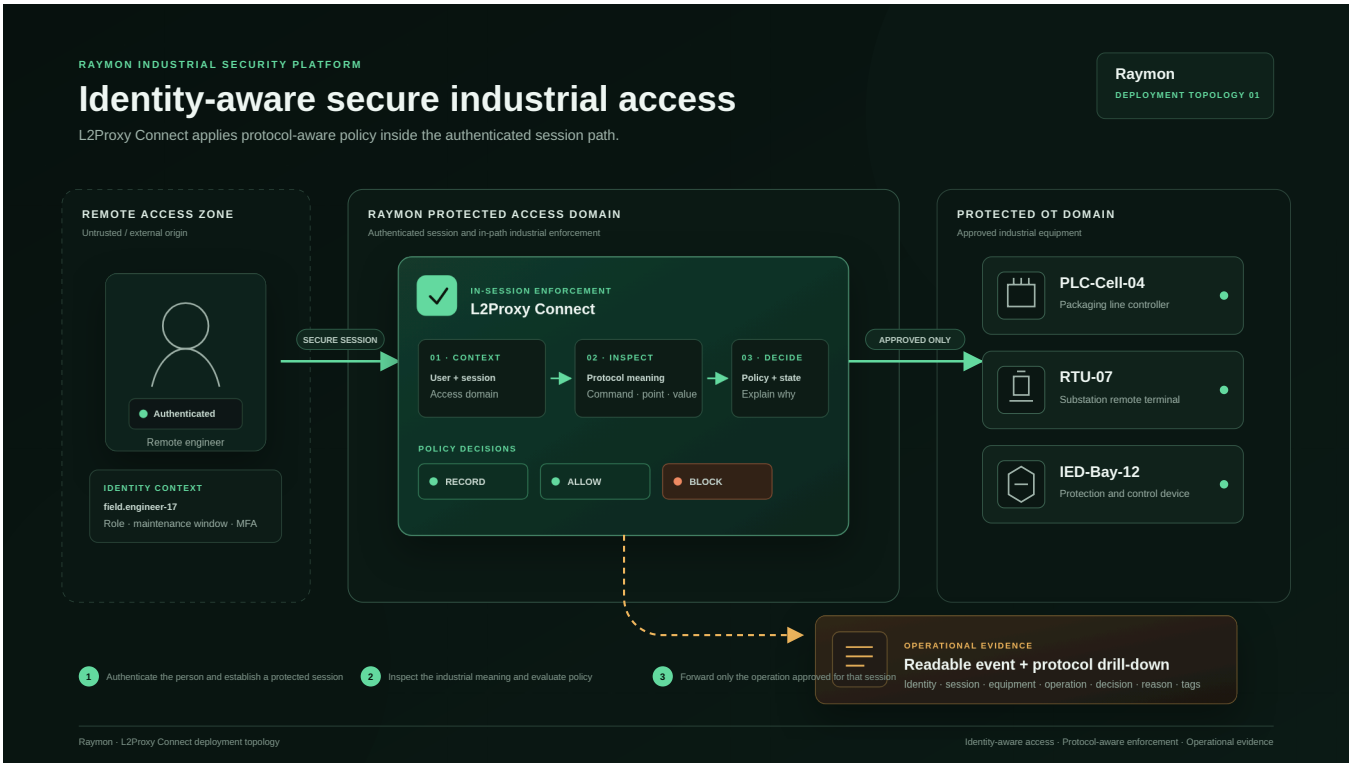
Connect, transparent, routed, passive, and offline postures share the same inspection, policy, stateful protection, and evidence model.

Two enforcement paths

```
                                  ┌→ Raymon Connect
                                  │  Authenticated in-session enforcement
Rule → Access Policy → Policy Profile ┤
                                  │
                                  └→ Service Profile
                                     Independent Raymon Protect instance
```

Raymon Connect

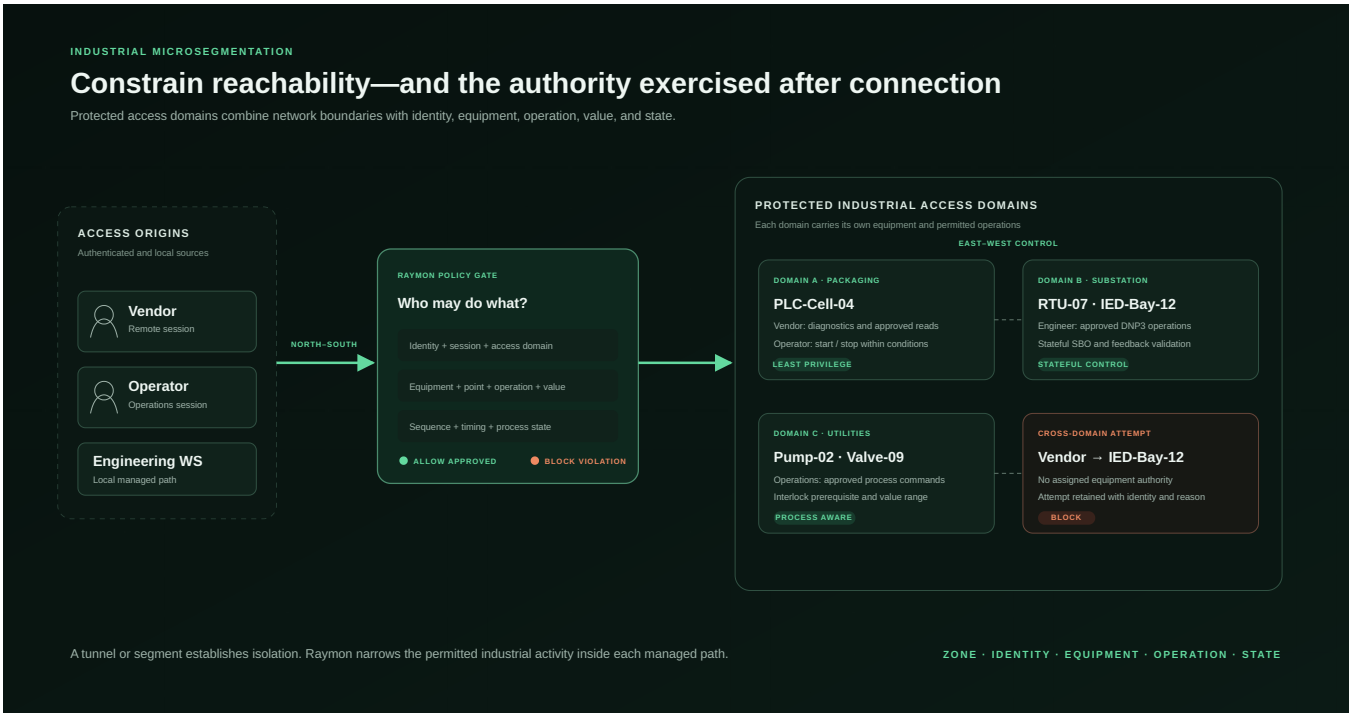
Connect evaluates traffic in the protected virtual access forwarding path. The Rule Engine receives the authenticated user, live session, access domain, and session type with the industrial frame. A separate bridge, routed inspection detour, or address-to-user reconstruction is not required for this path.



Raymon Connect *evaluates industrial activity within the authenticated session path and retains the identity, equipment, operation, decision, and reason as linked evidence.*

Raymon Protect

A Service Profile runs an independent **Raymon Protect** instance for a transparent or routed industrial boundary, isolated access path, passive observation point, or offline validation workflow. Each instance can have its own operating profile, Policy Profile, inspection mode, evidence, service state, and lifecycle.



Standalone boundaries and Connect access domains can jointly constrain North–South and East–West activity at both network and industrial-operation levels.

Deployment selection

Mode	Traffic impact	Primary industrial purpose
Raymon Connect	Active	User- and session-aware enforcement inside authenticated access
Transparent inline	Active	Enforcement without changing the existing addressing plan
Routed inline	Active	Protection at an established OT subnet, VLAN, or site boundary
Passive observation	None	Visibility, baselining, and policy tuning
Offline PCAP analysis	None	Investigation, regression, demonstration, and acceptance testing

Evidence architecture

Raymon preserves multiple evidence levels for different plant responsibilities:

1. decoded protocol facts from industrial traffic;
2. rule decisions and customer-selected metadata;
3. state transitions, counters, and timeout events;
4. normalized descriptions, equipment context, severity, category, and tags;
5. raw event archive and indexed normalized event records;
6. browser-based exploration and detailed frame drill-down.

This separates high-volume parser records from indexed operational events while keeping forensic detail reachable. Retention duration, database partitioning, compaction, backup, access control, integrity protection, and regulatory retention remain deployment choices.

Recommended commissioning sequence

```
Observe → Normalize → Model → Validate → Enforce → Audit
```

- Capture representative bidirectional startup, recovery, maintenance, failover, retry, timeout, and emergency behavior.
- Establish equipment and point mappings and confirm unknown-device discovery.
- Run candidate enforcement as Record policy or against PCAPs.
- Test normal, abnormal, missing-state, replay, duplicate, and out-of-order paths.
- Approve fail-open/fail-closed behavior, rollback, bypass, ownership, and evidence.
- Enable narrowly scoped blocking after operational acceptance.

Capability and qualification matrix

Platform capabilities

Capability	Current position	Qualification note
Ordered conditions with Record / Allow / Block	Production	Expressions compile at load; engine behavior is automated-test covered
Dynamic metadata on logged rule matches	Production	Expressions compile once and evaluate only on logged matches
Bounded state, atomic counters, replay-resistant transitions	Production	Capacity, TTL, concurrency, and race behavior are tested
Packet-independent timeout scheduler	Supported	Optional and disabled by default; service lifecycle must close it correctly
Equipment, point, safety-profile, and protection management	Production	Managed lifecycle includes create, review, search, update, delete, bulk operations, and export
Access Policy and Policy Profile composition	Production	Policies are ordered, revised, and saved as the complete enforcement profile
Raymon Connect in-session enforcement	Production	Provides user, session, access-domain, and connection context to policy and evidence
Multiple independent service instances	Production	Each service has independent profile, policy, lifecycle, and status management
Guided rule-authoring workbench	Supported	Qualify its generated field catalog against the shipped parser version
Event archive and Event Explorer	Supported	Raw dissection and rule decisions can be retained and explored
DNP3 semantic helpers and stateful policy portfolio	Production	Includes tested control, feedback, recovery, authorization, alarm, and rate use cases
DNP3 industrial event normalization	Supported	Qualify descriptions, mappings, and vendor traffic with customer PCAPs
Modbus field and transaction-aware policy	Supported	Existing transaction example; portfolio expansion is not currently active
S7comm field-level policy	Preview	Stateful helper package is not currently offered
Other dissected protocols	Preview / qualify	Parser presence does not imply semantic or stateful production readiness

Protocol capability has four distinct levels

```
1. Dissection
        ↓
2. Stateless field policy
        ↓
3. Semantic helpers and canonical values
        ↓
4. Tested stateful industrial use cases
```

Raymon does not treat “protocol supported” as a single yes/no claim. Production scope must be stated at the maturity level demonstrated for the relevant protocol, vendor implementation, topology, and traffic profile.

Explicit product boundaries

Raymon provides network-level industrial inspection and policy. It does **not** replace:

- safety instrumented systems, relay protection, PLC interlocks, or certified safety functions;
- operator authority, switching procedures, or engineering management of change;
- endpoint authentication, antivirus, backup, restore, or patch management;
- a web application firewall, TLS interception platform, historian, or full SIEM;
- deterministic QoS or bandwidth shaping.

Stateful conclusions depend on observable traffic. Packet loss, asymmetric paths, local panel or HMI activity, alternate routes, encrypted payloads, unsupported variations, and capture beginning mid-sequence can affect the available context.

Evaluation gate

Production acceptance should use representative customer traffic and explicitly verify:

- supported protocol functions, object variations, segmentation, and reassembly behavior;
- normal startup, recovery, failover, maintenance, and emergency procedures;
- identity, equipment, point, command, value, timing, sequence, and feedback assumptions;
- false-positive and false-negative behavior in Record mode;
- state loss, timeout, replay, duplicate, out-of-order, and engine-restart behavior;
- service capacity, storage sizing, rollback, bypass, and operational ownership.

Complete product catalog: Raymon Industrial Security Platform

Qualification guidance: Deployment and Assurance

> **Raymon Industrial Security Platform**
> Industrial access, protocol-aware protection, and explainable operational evidence.