RAYMON

Raymon Industrial Security Platform

Product Brochure

Version 1.0 · August 2026 · Customer publication

Raymon Industrial Security Platform

Control industrial operations—not just network connections.

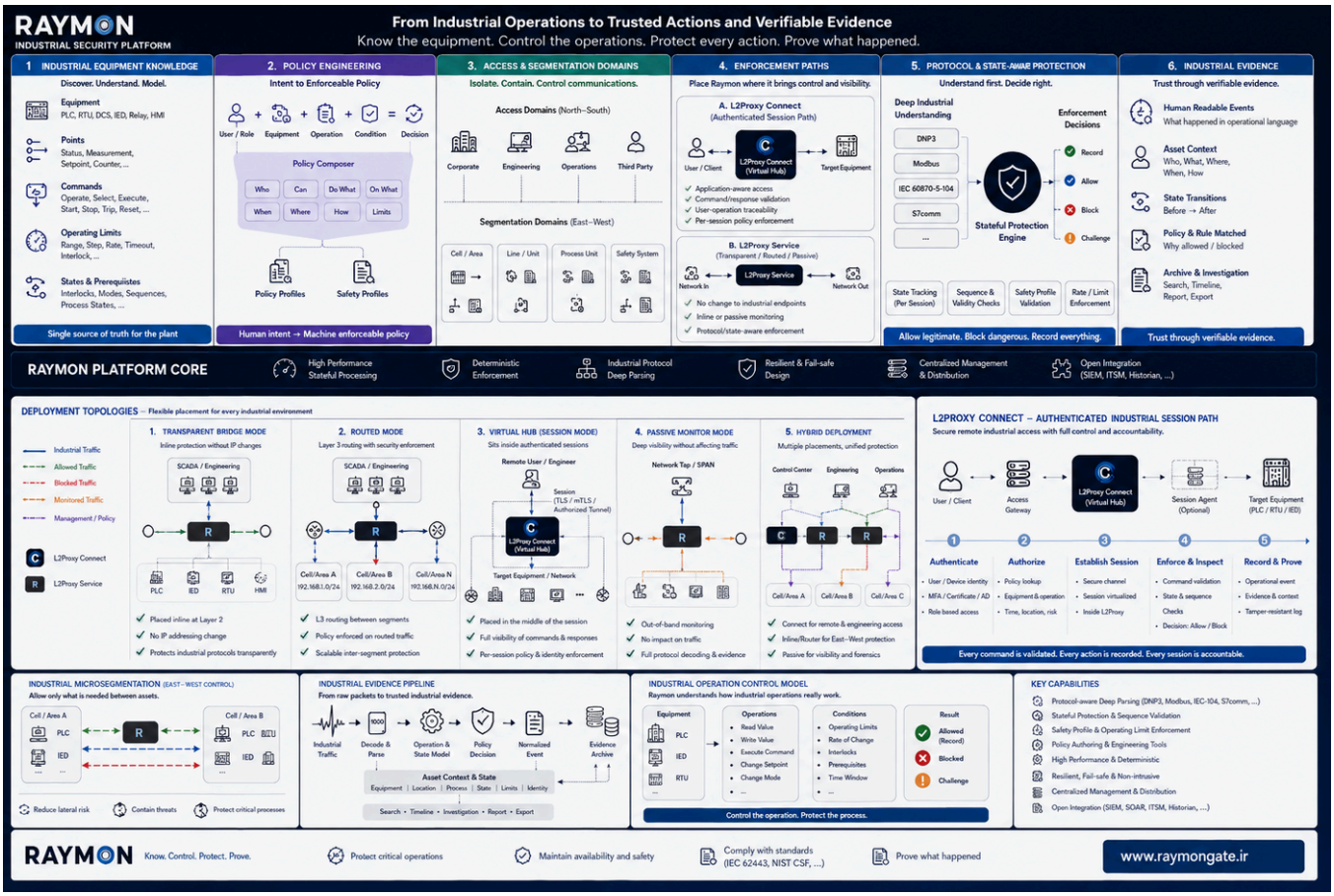


Figure — Product brochure overview of the Raymon Industrial Security Platform.

Raymon connects authenticated users and sessions to the equipment, commands, values, and operational sequences they use—then records, allows, or blocks each activity with evidence that operations, engineering, and OT security teams can understand.

Identity-aware access · Protocol-aware enforcement · Industrial microsegmentation · Stateful protection · Operational evidence

```
Authenticated user → Live session → Industrial equipment → Operation → Record / Allow / Block
```

Extend network security into industrial operations

Raymon complements network-level controls with the context required in operational technology: the acting identity, active session, affected equipment, industrial function, target point, requested value, sequence,

timing, and policy decision.

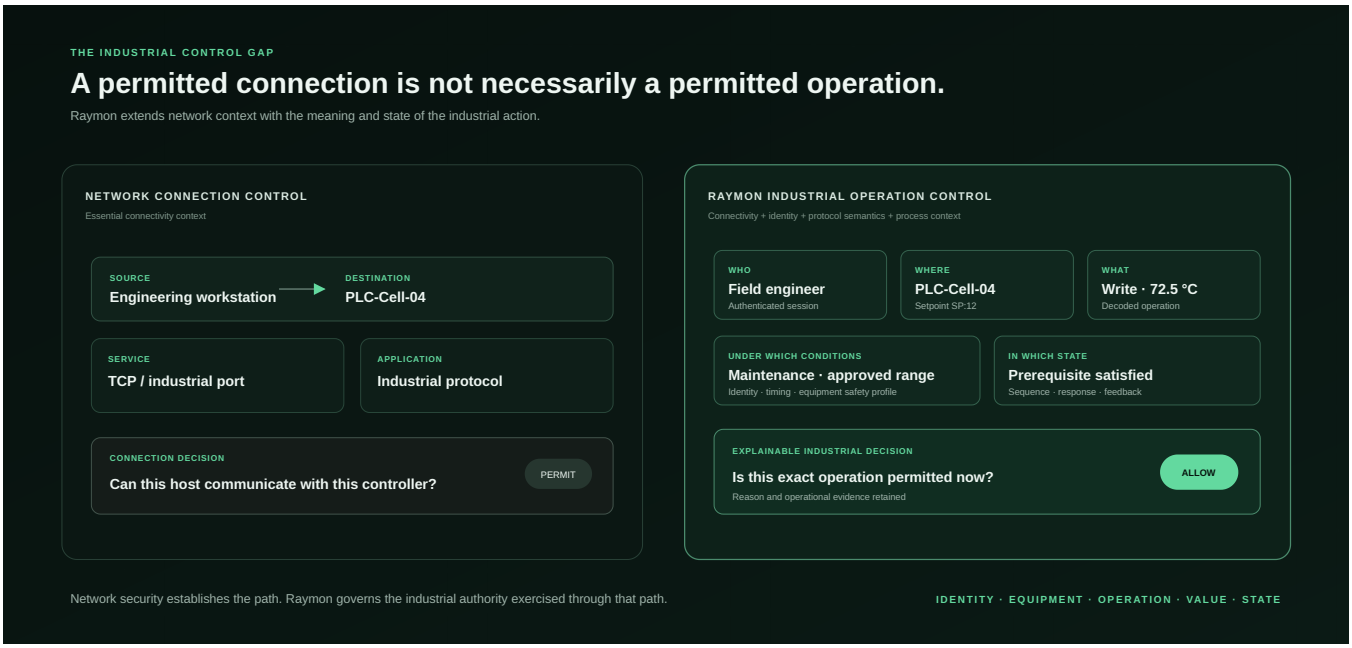
Secure industrial access	Industrial enforcement	Microsegmentation	Detection and evidence
Associate users and sessions with plant activity	Evaluate decoded functions, objects, points, values, and commands	Limit activity by domain, identity, equipment, operation, and state	Explain what happened, why it mattered, and what Raymon decided

Explore the platform: Raymon Industrial Security Platform

Traditional controls see a connection. Raymon sees the industrial operation.

A valid route, address, port, or application does not establish that every operation carried over that connection is appropriate. Industrial environments need to answer a more consequential question:

> **Is this authenticated user permitted to perform this exact operation on this equipment, with this value, at this stage of the process?**



Raymon extends network-level context into the identity, equipment, command, value, sequence, and state of the industrial operation.

From connectivity context to operational context

Conventional network context	Raymon industrial context
Source and destination	Authenticated user and live session
Address, port, and application	Equipment, protocol, function, and point
Connection permitted or denied	Operation recorded, allowed, or blocked
Individual packet or flow	Command sequence, timing, prerequisite, and feedback
Technical network log	Human-readable industrial event and traceable evidence

A practical control example

An engineering workstation is permitted to reach a PLC. That connectivity decision is only the beginning:

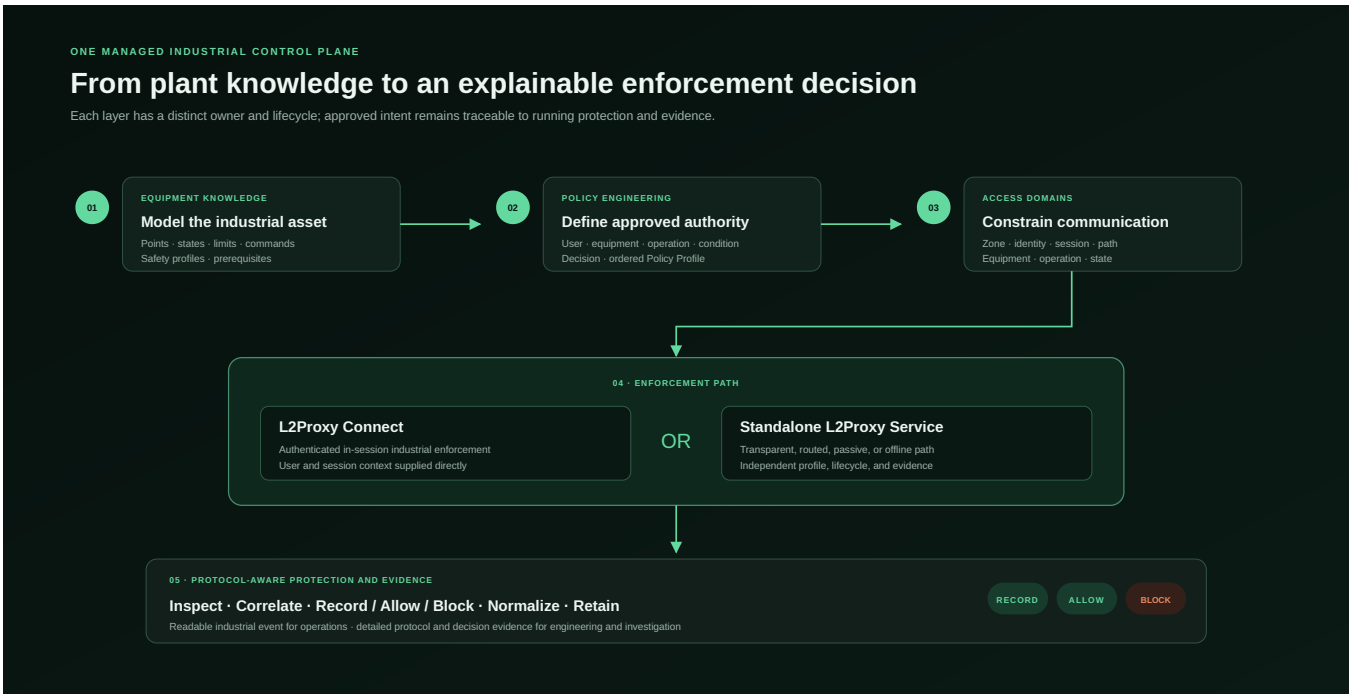
```
Read operating status                          RECORD / ALLOW
Change an approved setpoint within its range ALLOW
Start or stop by an approved operator        ALLOW
Write outside the assigned safety profile    BLOCK
Issue an operation in the wrong sequence     BLOCK
Attempt access to unrelated equipment        BLOCK
```

Raymon can evaluate policy using the industrial meaning carried in the traffic—not only the existence of a session. Where L2Proxy Connect is used, the decision can also include the authenticated user, access domain, and live session without reconstructing identity from an IP address.

Begin with visibility; move to enforcement when ready

The same policy intent can be exercised through passive observation and recorded traffic before blocking is approved. This supports commissioning, baselining, policy tuning, customer acceptance, and controlled OT management of change.

One platform. Six connected industrial capabilities.



Managed equipment knowledge and approved policy remain traceable through the selected enforcement path to the resulting operational evidence.

1. Identity-aware industrial access

Associate authenticated engineers, operators, vendors, and sessions with the industrial activity they introduce. Apply access authority to the user, session, protected access domain, equipment, and operation—not merely to a source address.

2. Protocol-aware enforcement

The L2Proxy Dissector exposes industrial protocol meaning to ordered, testable policy. Raymon can distinguish monitoring from control activity and evaluate decoded functions, objects, points, values, endpoints, and commands.

3. Industrial segmentation and microsegmentation

Create protected access domains and constrain North–South and East–West communication. Reachability can be narrowed further by authenticated identity, session, equipment, operation, value, and process context.

4. Equipment-centric policy engineering

Manage equipment definitions, operational points, normal states, limits, permitted commands, prerequisites, and baseline safety profiles. Compose reviewed policies into complete Policy Profiles for controlled activation.

5. Stateful process protection

Correlate authorization, command, response, feedback, timeout, replay, and prerequisites across multiple messages. Stateful policies can identify a missing selection, expired authorization, mismatched control,

incomplete recovery, or absent process confirmation.

6. Operational evidence

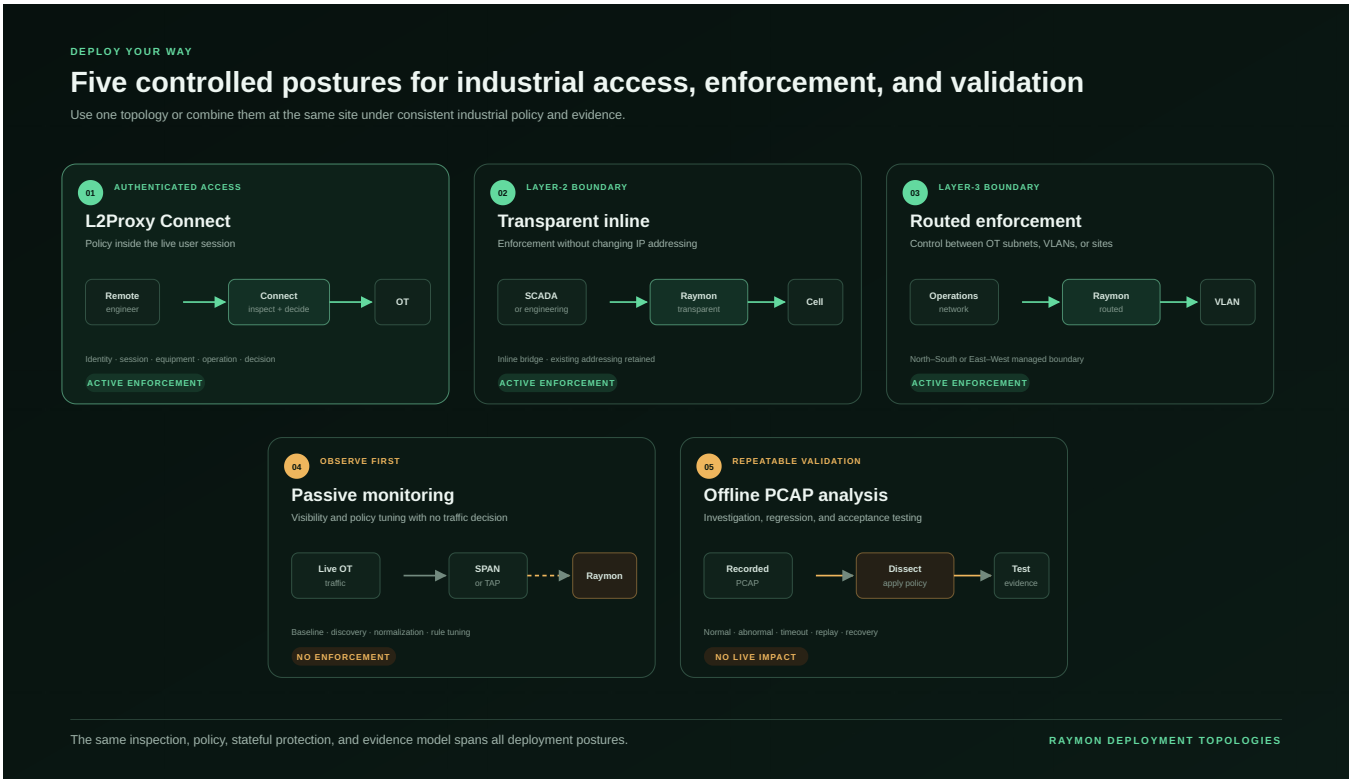
Convert repetitive protocol records into asset-aware events with readable descriptions, category, severity, tags, identity, session context, policy decision, and drill-down evidence. Operations sees the industrial meaning; investigators retain the protocol facts.

Guided engineering—not a blank rule editor

Raymon provides managed equipment knowledge, reusable templates, contextual autocomplete, field and helper guidance, inline validation, and rule compilation. This shortens the path from an industrial requirement to a reviewable and testable policy.

Deploy where industrial control is required

Raymon provides two complementary enforcement models. A site can use either model or combine them while retaining the same inspection, policy, stateful protection, and evidence approach.



Five controlled postures support authenticated access, inline boundaries, passive observation, and repeatable offline validation.

L2Proxy Connect

Apply industrial policy inside an authenticated access session. Raymon receives the established user and session context, evaluates traffic in the protected forwarding path, and links each decision to the person, session, access domain, equipment, and operation.

Best fit: secure remote industrial work, vendor access, per-user authority, and session-level investigation.

Standalone L2Proxy Service

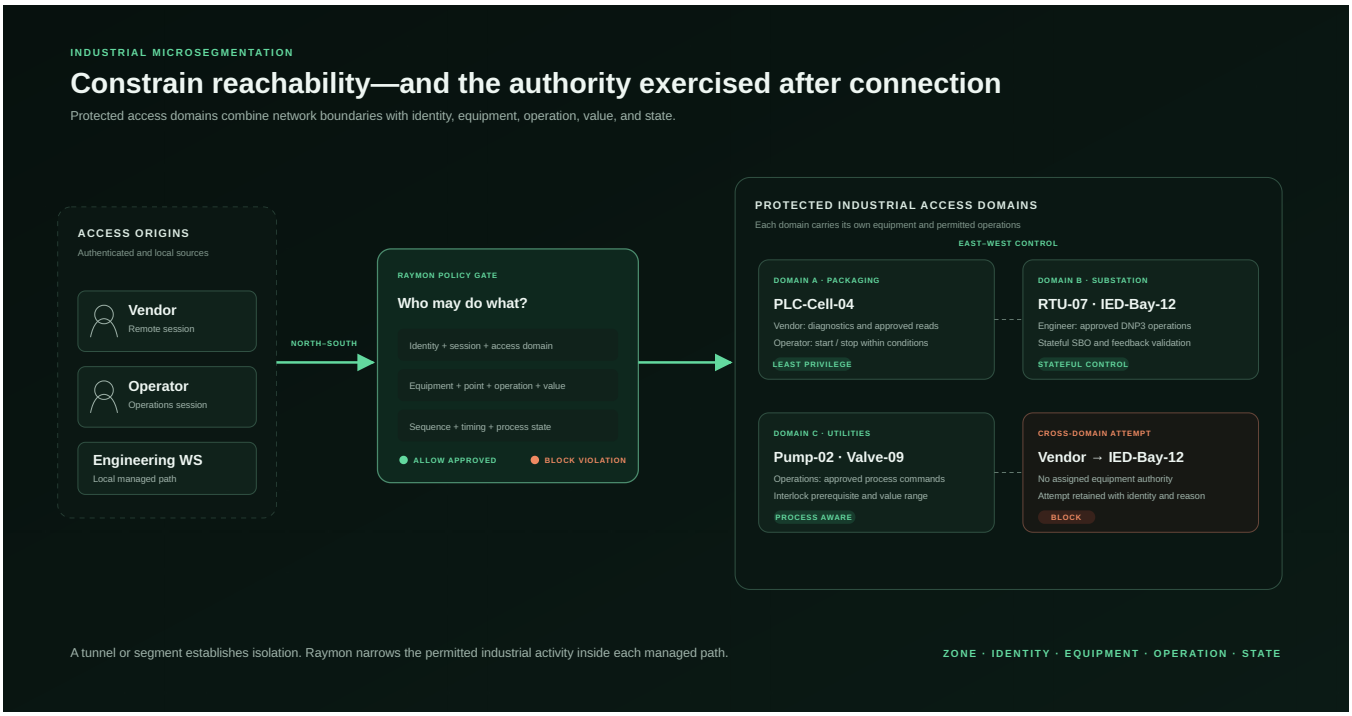
Operate independent protection services with their own Service Profile and approved Policy Profile at industrial boundaries or observation paths.

Best fit: transparent cell boundaries, routed OT zones, isolated user paths, passive observation, and offline traffic analysis.

Supported operating postures

Posture	Industrial purpose
In-session enforcement	Tie authenticated user and session context directly to the operation
Transparent inline	Add enforcement without changing the existing IP addressing plan
Routed inline	Protect established OT subnet, VLAN, site, or supervisory boundaries
Passive observation	Establish normal behavior and tune policy without blocking production traffic
Offline analysis	Investigate captures, validate rules, and perform repeatable acceptance testing

Industrial use cases with operational outcomes



A managed segment defines reachability. Raymon further limits the industrial authority exercised inside that path by identity, equipment, operation, value, and state.

Secure remote industrial work

Situation: A vendor requires diagnostics on assigned equipment during an approved maintenance period.

Raymon control: Authenticate the user, place the session in a protected access domain, permit approved reads and diagnostics, evaluate consequential commands, and retain the session-linked activity.

Outcome: The vendor reaches only the required equipment and operations. Out-of-scope writes, controls, values, or targets can be recorded or blocked with a clear reason.

Grid and substation control protection

Situation: An engineer operates an RTU or IED using DNP3.

Raymon control: Evaluate function, object, point, control fingerprint, identity, timing, and operational state. Validate Select-Before-Operate, command-to-status feedback, maintenance authorization, restart recovery, and other multi-message sequences.

Outcome: Expected control proceeds; a direct, expired, mismatched, replayed, or unconfirmed operation produces an explainable decision and evidence trail.

Industrial microsegmentation

Situation: An engineering workstation needs access to one production cell but not to adjacent cells or unrelated controllers.

Raymon control: Restrict the permitted path by protected domain, identity, session, equipment, protocol operation, and—where policy requires it—value or state.

Outcome: Segmentation limits both reachability and industrial authority, reducing the consequence of credential misuse, configuration error, and unintended lateral movement.

Commissioning, baselining, and investigation

Situation: Operations needs evidence before approving inline enforcement.

Raymon control: Run policy in Record mode, passively inspect representative traffic, or replay PCAPs. Review decoded operations, unknown assets and points, normalized events, rule decisions, timeouts, and state transitions.

Outcome: Engineering can establish expected behavior, test normal and abnormal paths, measure policy quality, and enter the change window with reviewable evidence.

Why Raymon

Industrial least privilege that reaches the operation

Network security foundation	Raymon industrial extension
IP address and port	Equipment, function, point, command, and value
Network identity	Authenticated user + live session + industrial asset
Connection control	Industrial operation control
Generic protocol visibility	Decoded industrial semantics
Individual rules	Stateless and stateful process protection
Technical network events	Normalized operational evidence with protocol drill-down
Manual rule construction	Equipment library, templates, autocomplete, help, and validation

A controlled adoption path

```
OBSERVE → NORMALIZE → MODEL → VALIDATE → ENFORCE → AUDIT
```

1. **Observe** representative industrial communication without affecting production.
2. **Normalize** protocol detail into equipment, operation, severity, and event context.
3. **Model** approved identities, equipment, operations, values, sequences, and timing.
4. **Validate** normal, abnormal, timeout, replay, startup, and recovery behavior.
5. **Enforce** narrowly scoped policies after operational approval.
6. **Audit** retained session, protocol, policy, state, and decision evidence.

The product boundary is explicit

Raymon is an independent network-level industrial inspection and decision platform. It does not replace PLC interlocks, relay protection, safety instrumented functions, engineering procedures, endpoint controls, or operator authority. Production policy requires representative traffic, customer-approved tests, management of change, and a defined rollback or bypass procedure.

See Raymon in your industrial workflow

Evaluate the platform by starting with one protected workflow, its users, equipment, expected operations, and acceptance evidence.

Product catalog: Raymon Industrial Security Platform

Recommended next reads:

- Industrial solution portfolio
- Secure industrial access

- Industrial policy engineering
- Protection and operational evidence
- Deployment and assurance

> **Raymon Industrial Security Platform**
> Know who is controlling each industrial asset—and control what they can do.