

Raymon Industrial Security Platform

Industrial Product Catalog

August 2026

INDUSTRIAL OPERATIONS • POLICY • ENFORCEMENT • EVIDENCE

CONTENTS

Raymon Industrial Security Platform

1. The industrial security problem
2. A common industrial model across the platform
3. L2Proxy Connect — industrial control inside the authenticated session path
4. Industrial segmentation and microsegmentation
5. Equipment-centric protection
6. Policy engineering lifecycle
7. From approved policy to runtime enforcement
8. Stateful industrial protection
9. DNP3 Select-Before-Operate protection
10. Industrial evidence — from protocol traffic to operational meaning
11. Deployment topologies and product placement
12. Commissioning, qualification, and controlled adoption
13. Operating model by responsibility
14. Protocol-aware protection portfolio
15. Product boundaries
16. Why Raymon

Raymon Industrial Security Platform

Appendix A — Master Diagram Placement Index

Appendix B — Figure Publication Checklist

Raymon Industrial Security Platform

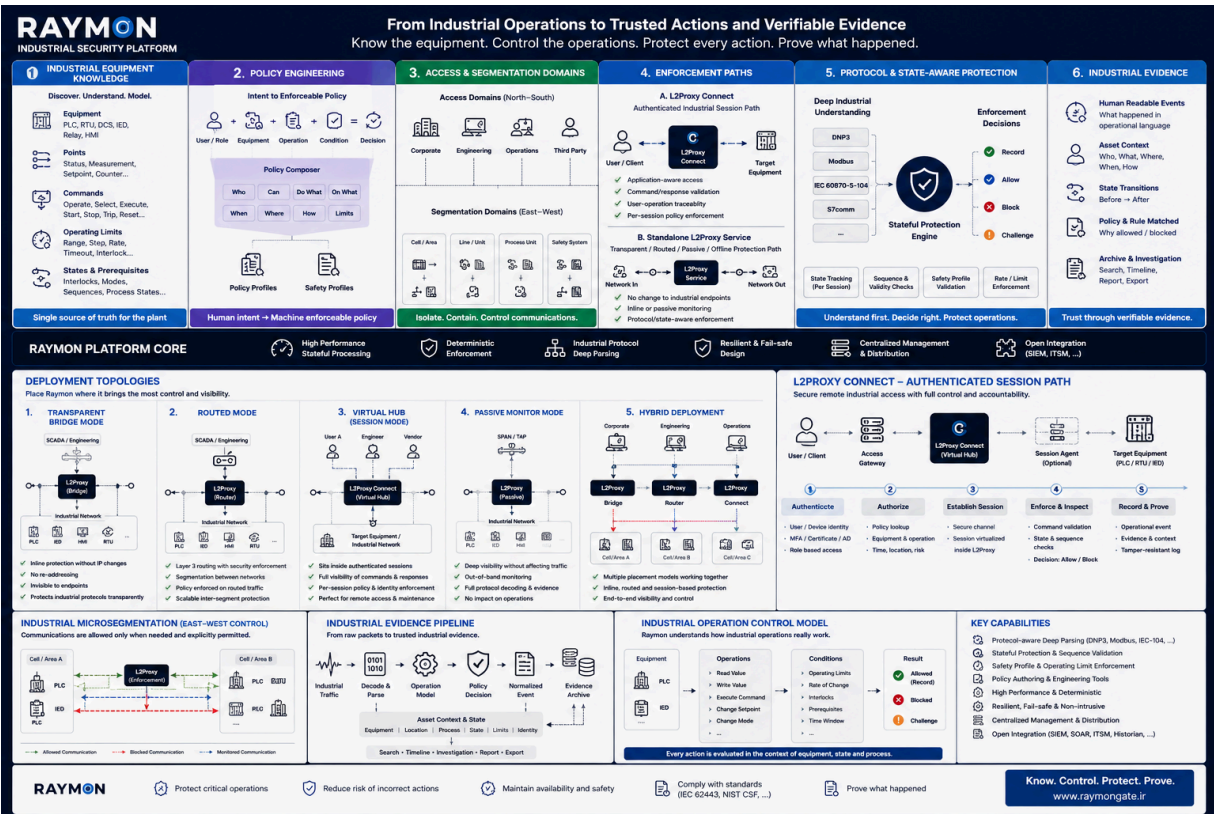
Control industrial operations — not only network connections.

Industrial access becomes meaningful only when the permitted **operation** is understood. A valid route, authenticated session, IP address, TCP port, or protocol connection does not by itself prove that a requested command is appropriate for the equipment, the process state, the user, or the current operating condition.

Raymon extends industrial network security into the operational layer. It combines identity and session context, equipment knowledge, protocol-aware inspection, policy engineering, stateful protection, industrial segmentation, runtime enforcement, and human-readable evidence in one OT-oriented model.

Raymon answers five operational questions for every consequential activity:
Who introduced it? What equipment does it affect? Which operation is being requested? Is it permitted in the current context? What evidence remains after the decision?

Identity-aware access · Equipment-aware policy · Protocol-aware enforcement · Stateful protection · Industrial evidence



Raymon platform architecture connecting industrial operations, policy, enforcement, monitoring, and retained evidence

Figure 1 — Raymon Platform Architecture. Raymon connects industrial equipment knowledge and approved policy to the selected enforcement path, protocol- and state-aware protection, and retained operational evidence.

1. The industrial security problem

Network permission is not operational permission

Traditional network controls are essential for segmentation and connectivity governance, but the industrial consequence of a connection is determined by what travels inside it. The same permitted path may carry harmless monitoring, an engineering change, a control command, a setpoint modification, or a sequence that is only safe when prerequisites are satisfied.

A control system may therefore need to distinguish between activities such as:

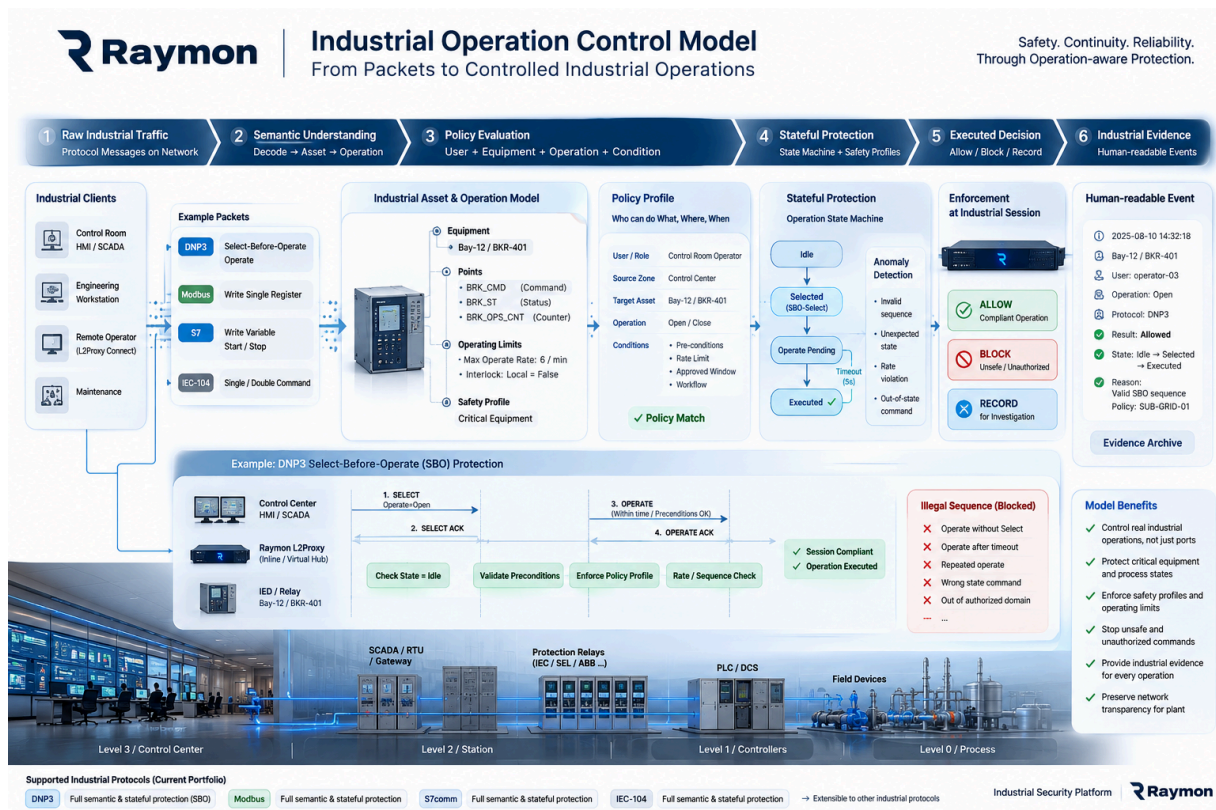
Industrial activity	Typical policy intent
Read process status	Record or Allow
Read diagnostics from assigned equipment	Allow
Write an approved setpoint inside an operating range	Allow
Issue an authorized start/stop operation	Allow
Write outside the approved range	Block
Control unrelated equipment	Block
Execute a command in the wrong sequence	Block
Repeat an expired or consumed authorization	Block
Observe commissioning traffic	Record

Raymon evaluates the **industrial meaning** of the activity rather than treating every packet inside an approved connection as equivalent.

From connection context to operation context

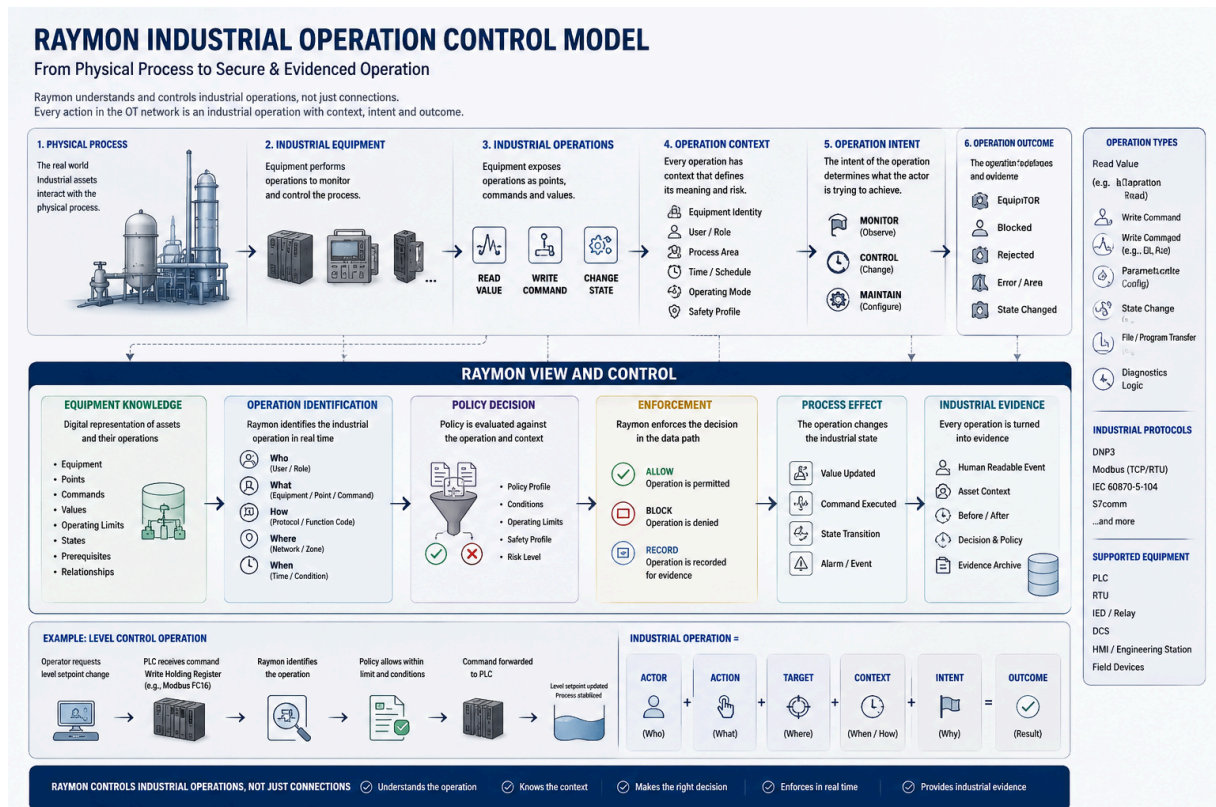
Raymon can combine:

- authenticated user and live session, where session-aware access is used;
- source and destination communication context;
- equipment identity and operational point;
- industrial protocol, function, object, command, and value;
- process state and known prerequisites;
- timing, sequence, replay, and feedback conditions;
- approved policy and protection profile;
- the final Record / Allow / Block decision;
- the evidence required to explain that decision later.



Industrial operation control model from network packets to controlled industrial operations

Figure 2A — From packets to controlled industrial operations. Raymon evaluates identity, equipment, protocol semantics, operating context, and policy before producing an explainable decision.

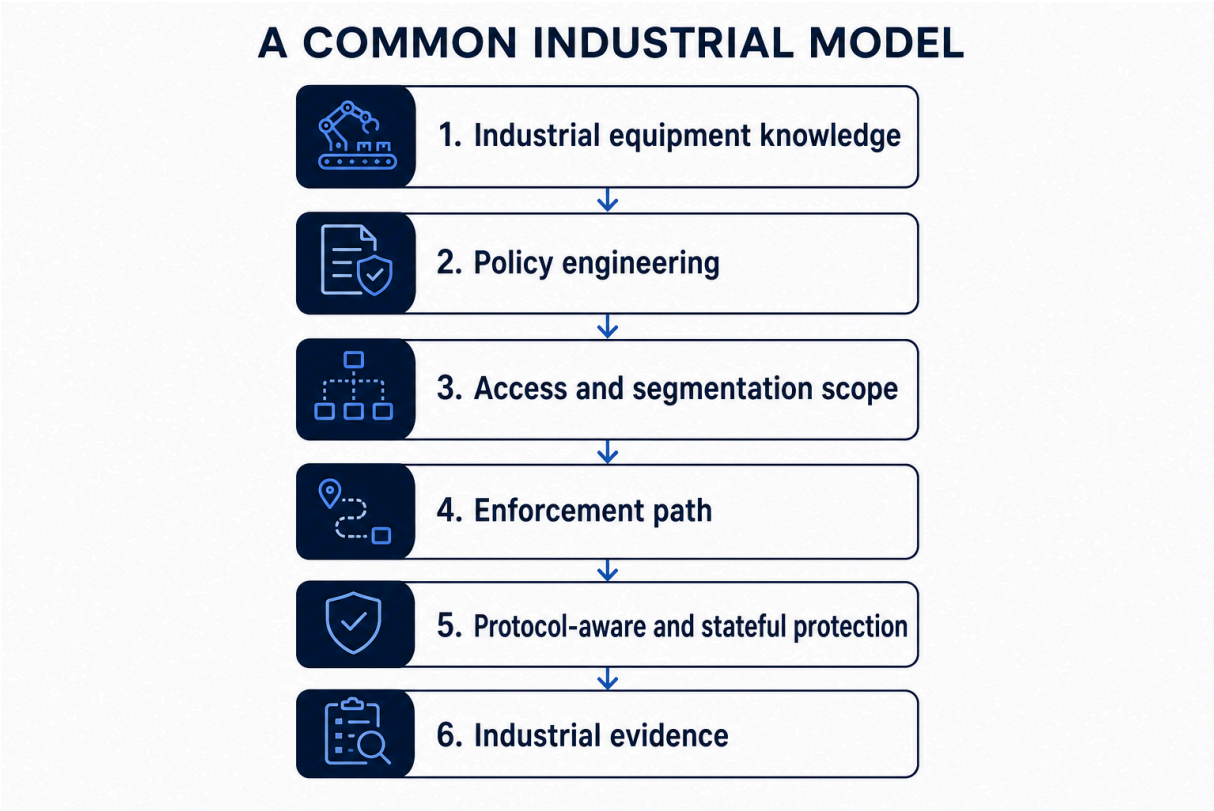


Industrial operation control model from the physical process to secure and evidenced operation

Figure 2B — From physical process to secure and evidenced operation. The same control model connects plant behavior, operational intent, enforcement, and retained evidence.

2. A common industrial model across the platform

Raymon is designed around one consistent chain:



Common industrial model across the Raymon platform

Common industrial model — from equipment knowledge and policy engineering to protocol-aware enforcement and industrial evidence.

This model is intentionally reusable. The same equipment definition, approved operating range, command rule, sequence requirement, or protection profile can be reviewed by engineering and then carried into the enforcement path selected for the site.

The result is a platform that can link **engineering intent** to **runtime behavior** and then to **evidence**.

Core platform capabilities

Capability	Industrial purpose
Equipment knowledge	Model equipment, points, operating ranges, commands, and baseline protections
Policy engineering	Convert industrial requirements into reviewable policies and profiles
Identity-aware access	Associate authenticated users and sessions with industrial activity

Capability	Industrial purpose
Industrial segmentation	Limit reachability and authority by domain, identity, equipment, operation, and state
Protocol-aware inspection	Decode industrial operations beyond generic port/application awareness
Stateful protection	Correlate multi-message sequences, timeouts, prerequisites, feedback, and replay
Runtime enforcement	Record, Allow, or Block according to approved policy
Industrial evidence	Retain readable operational events together with technical drill-down evidence
Qualification workflow	Validate policy and behavior before narrow production enforcement

3. L2Proxy Connect — industrial control inside the authenticated session path

Secure remote access should not end at authentication. Once a person is authenticated, the next question is what industrial authority that session receives.

L2Proxy Connect applies Raymon's industrial inspection and policy model inside the managed authenticated session path. The enforcement engine operates in the session forwarding environment and receives the established identity/session context together with the industrial traffic.

This makes it possible to relate a decision directly to:

- authenticated user;
- live session;
- access domain;
- source and destination;
- equipment;
- industrial operation;
- requested value or control code;
- sequence or state;
- matched policy and decision.

The architecture does not require the customer to reconstruct identity later from an IP address. Identity is available at the point where the industrial operation is evaluated.

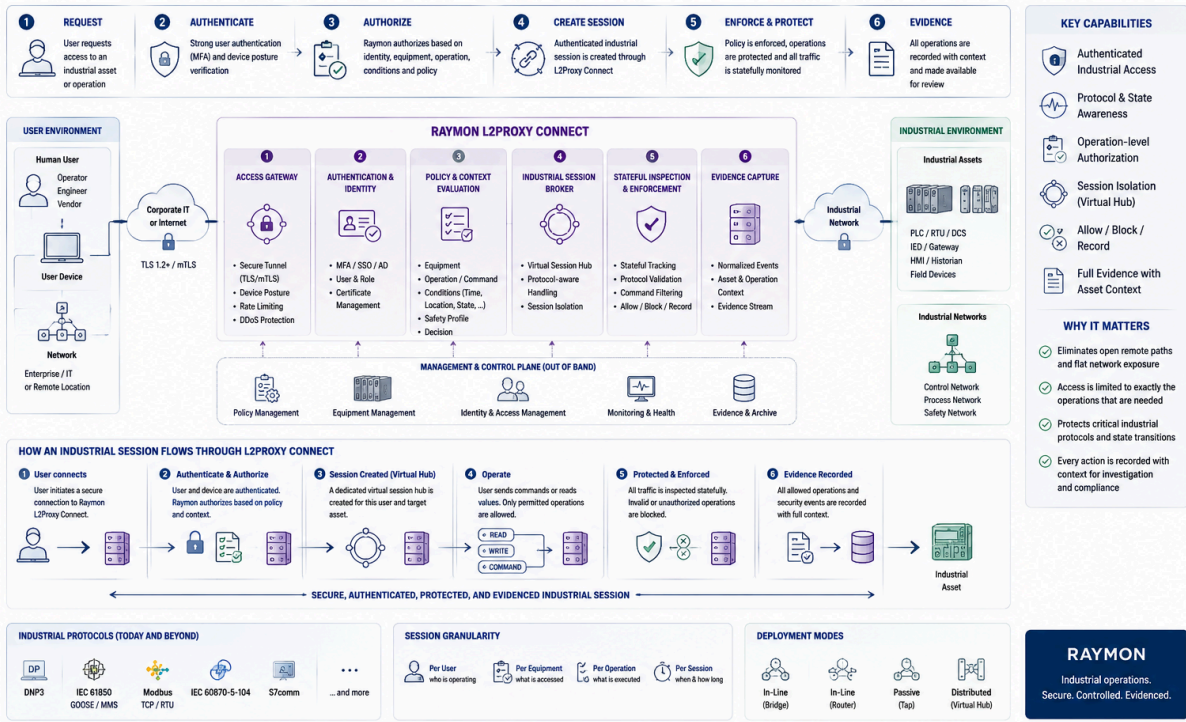
Typical applications

- vendor maintenance with restricted equipment scope;
- remote engineering with operation-level authority;
- per-user or per-session industrial policy;
- temporary work windows and controlled maintenance activities;
- session-linked investigation and evidence;
- differentiated authority for monitoring, control, configuration, and maintenance.

RAYMON L2PROXY CONNECT – AUTHENTICATED INDUSTRIAL SESSION PATH

Secure, Controlled and Evidenced Access to Industrial Operations

RAYMON | INDUSTRIAL SECURITY



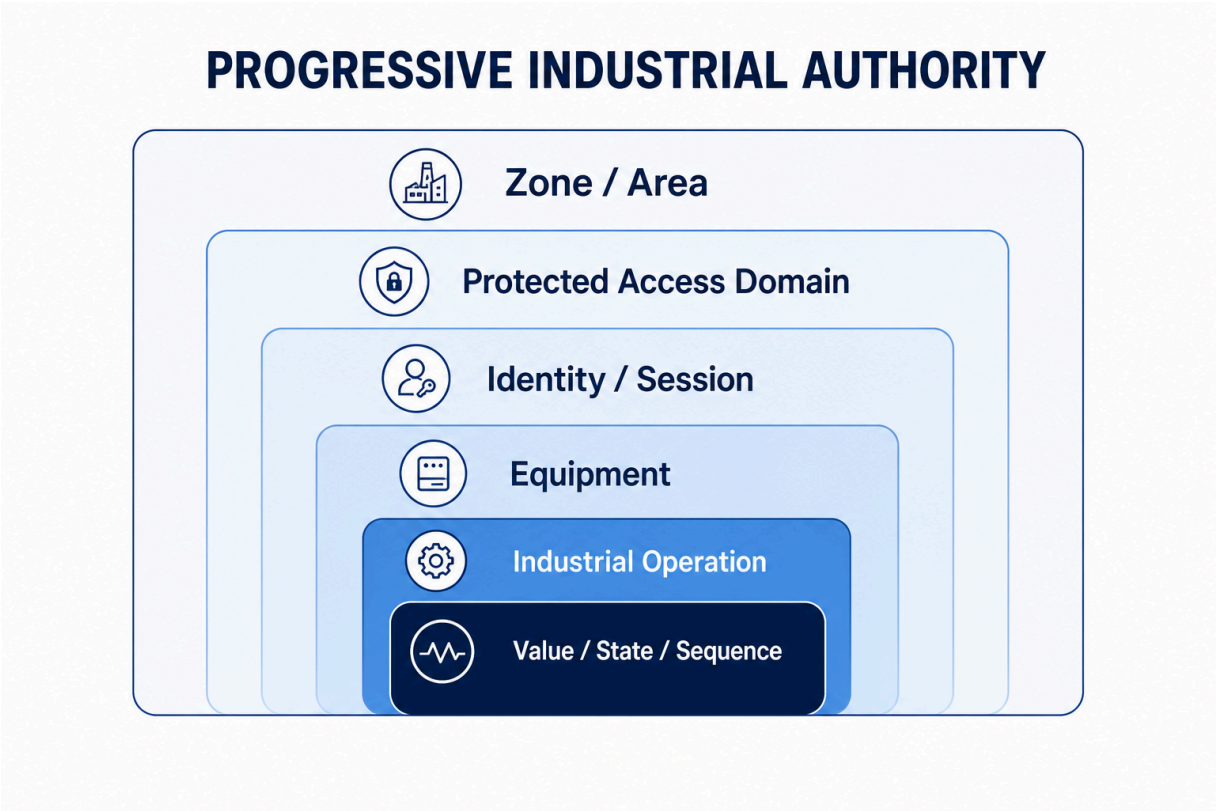
L2Proxy Connect authenticated industrial session path from users through policy enforcement to industrial equipment

Figure 3 — L2Proxy Connect Session Path. L2Proxy Connect evaluates industrial activity inside the authenticated session path and links each decision to the user, session, equipment, operation, and evidence.

4. Industrial segmentation and microsegmentation

Industrial segmentation is most effective when it limits not only **where** a connection can go, but also **what authority** can be exercised after that connection is established.

Raymon can combine conventional network boundaries with industrial context to create progressively narrower policy scopes:



Progressive industrial authority from zone to value, state, and sequence

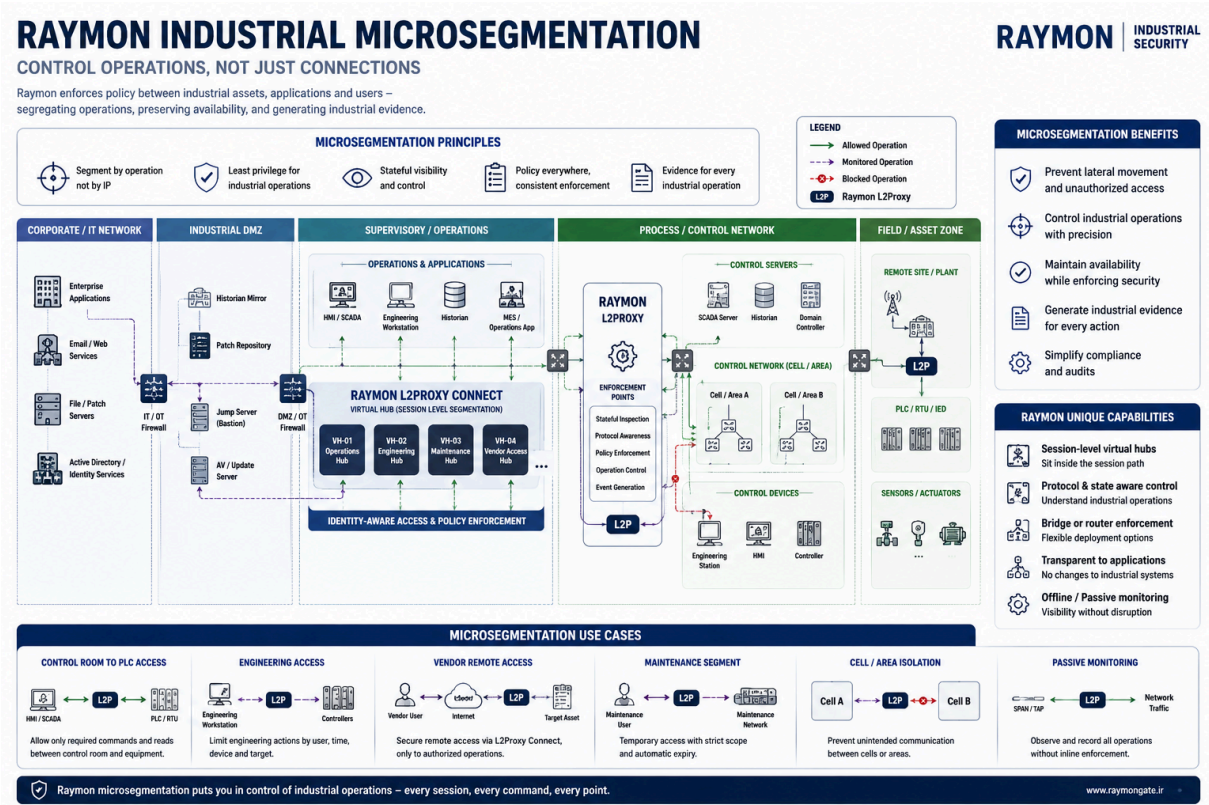
Progressive industrial authority — narrowing access from zone and protected domain to identity, equipment, operation, value, state, and sequence.

This supports both North–South and East–West control while preserving the operational structure of the plant.

Industrial segmentation dimensions

Dimension	Example
Network boundary	Engineering zone → Control zone
Access domain	Vendor maintenance domain
Identity	Approved engineer / operator / service account
Equipment	PLC-01, RTU-South, Relay-04

Dimension	Example
Operation	Read, control, configuration, file operation
Point / object	Breaker command point, analog setpoint
Value	Approved range only
State	Maintenance mode, selected state, recovery state
Time / sequence	Valid SBO window, command-before-feedback sequence



Industrial microsegmentation across identity, equipment, operations, values, and process state

Figure 4 — Industrial Microsegmentation. Raymon narrows industrial authority from network and access domains down to identity, equipment, operation, value, and process state.

5. Equipment-centric protection

Start with the equipment — then refine for the process

Industrial protection should not begin with a blank firewall rule. Raymon organizes protection around the managed equipment and the operational points that matter to the plant.

A reusable equipment model can contain:

- equipment type and identity;
- operational points;
- expected states;
- permitted commands;
- analog or setpoint ranges;
- criticality and operational role;
- baseline protection profiles;
- prerequisites and interlocks;
- process-specific derived rules.

Initial Protection Profiles

A base equipment definition provides an engineering starting point. Initial protection profiles can express common controls such as:

- permitted binary states;
- allowable analog ranges;
- approved control codes;
- setpoint boundaries;
- expected alarms;
- command prerequisites;
- sequence requirements such as Select-Before-Operate.

These are **baselines**, not universal plant truth.

Process-derived protection

The protection model becomes more precise when site and process knowledge is applied. Engineering can derive additional controls from:

- the actual process function of the equipment;
- upstream and downstream dependencies;
- operating mode;
- maintenance state;
- process permissives and interlocks;
- operator role;
- approved timing windows;
- command/feedback relationships;
- local site procedures.

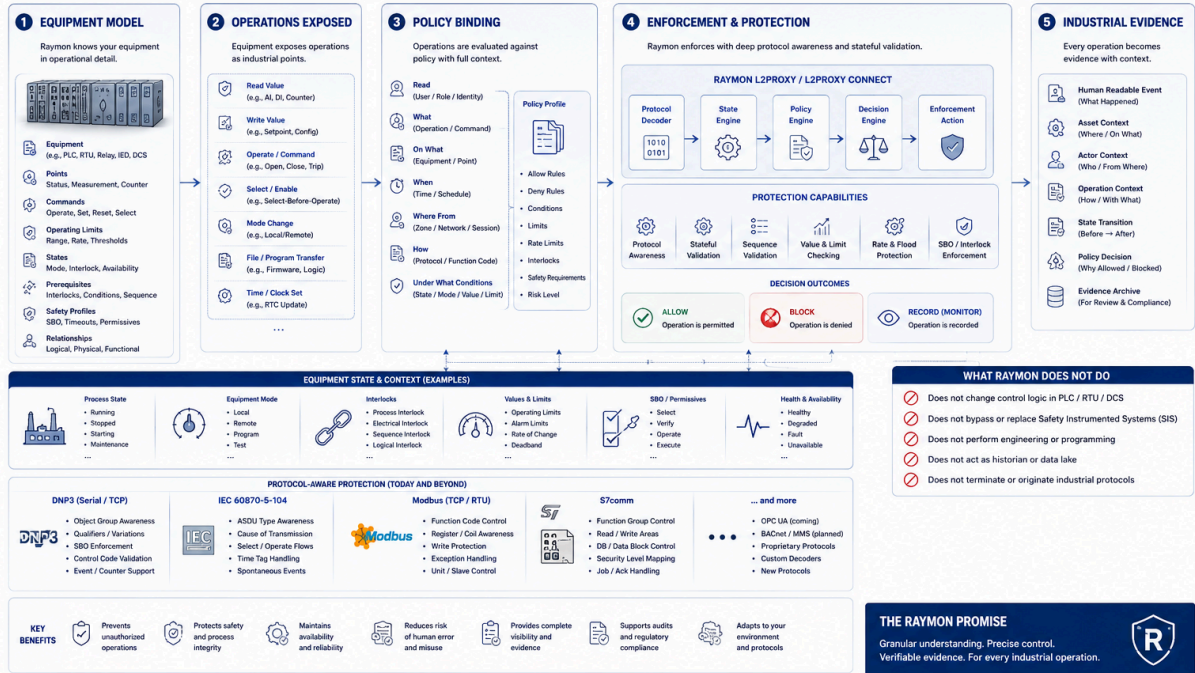
This creates a progression from reusable industrial knowledge to plant-specific protection without forcing every project to start from zero.

RAYMON EQUIPMENT PROTECTION MODEL

Understand Equipment. Control Operations. Protect What Matters.

Raymon builds a precise operational model of industrial equipment and enforces policy on every operation with protocol and state awareness.

RAYMON
INDUSTRIAL SECURITY



Raymon equipment protection model covering equipment knowledge, operational context, policy, enforcement, and evidence

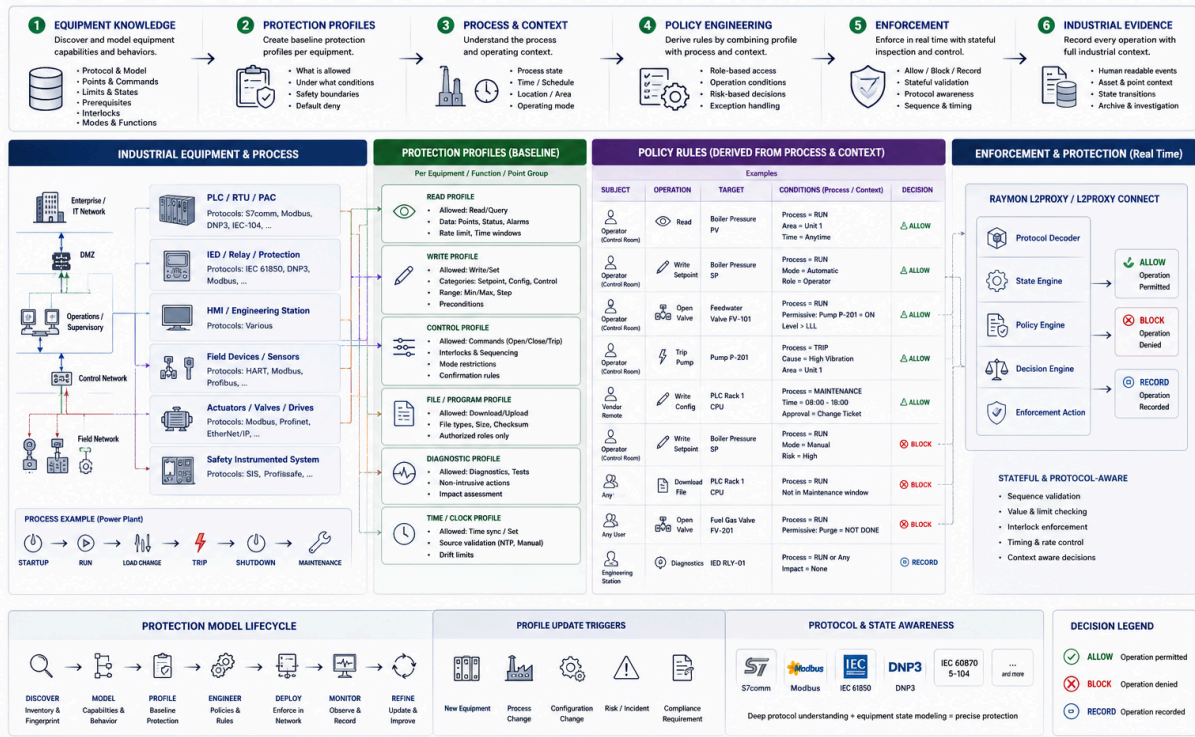
Figure 5A — Equipment Protection Model. Raymon organizes equipment knowledge, operational context, protection policy, enforcement, and evidence into one reusable industrial model.

RAYMON EQUIPMENT PROTECTION MODEL

From equipment knowledge to protection profiles and enforceable rules based on industrial process and context.

Understand Equipment. Control Operations. Protect What Matters.

RAYMON
INDUSTRIAL SECURITY



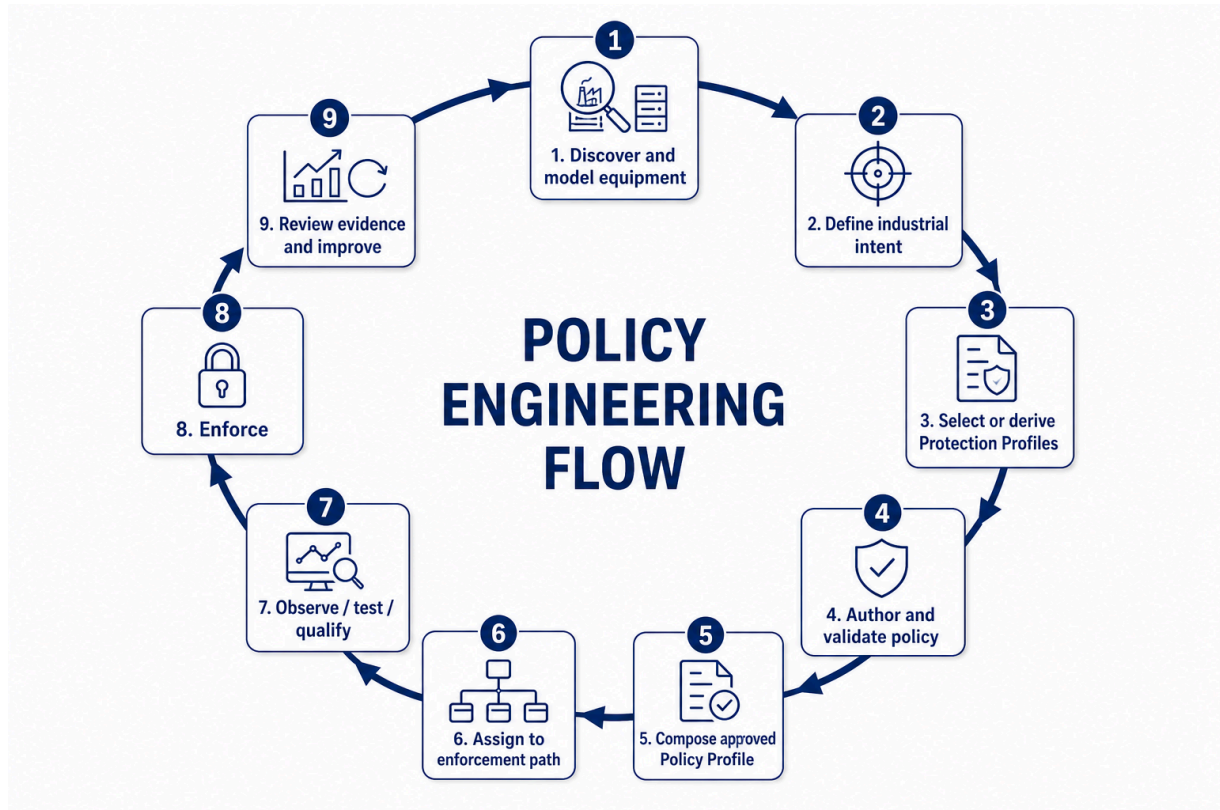
Detailed equipment protection model deriving plant-specific rules from baseline profiles and operational knowledge

Figure 5B — Derived Equipment Protection. Raymon begins with reusable equipment and baseline Protection Profiles, then derives site- and process-specific rules, prerequisites, and interlocks from actual operating requirements.

6. Policy engineering lifecycle

Raymon treats policy as an engineering lifecycle rather than a one-time configuration file.

A practical lifecycle is:



Policy engineering flow from equipment discovery to evidence-driven improvement

Policy engineering flow — a controlled lifecycle from equipment discovery and industrial intent to qualification, enforcement, and improvement.

Engineering inputs

Policy can be built from customer-approved dimensions such as:

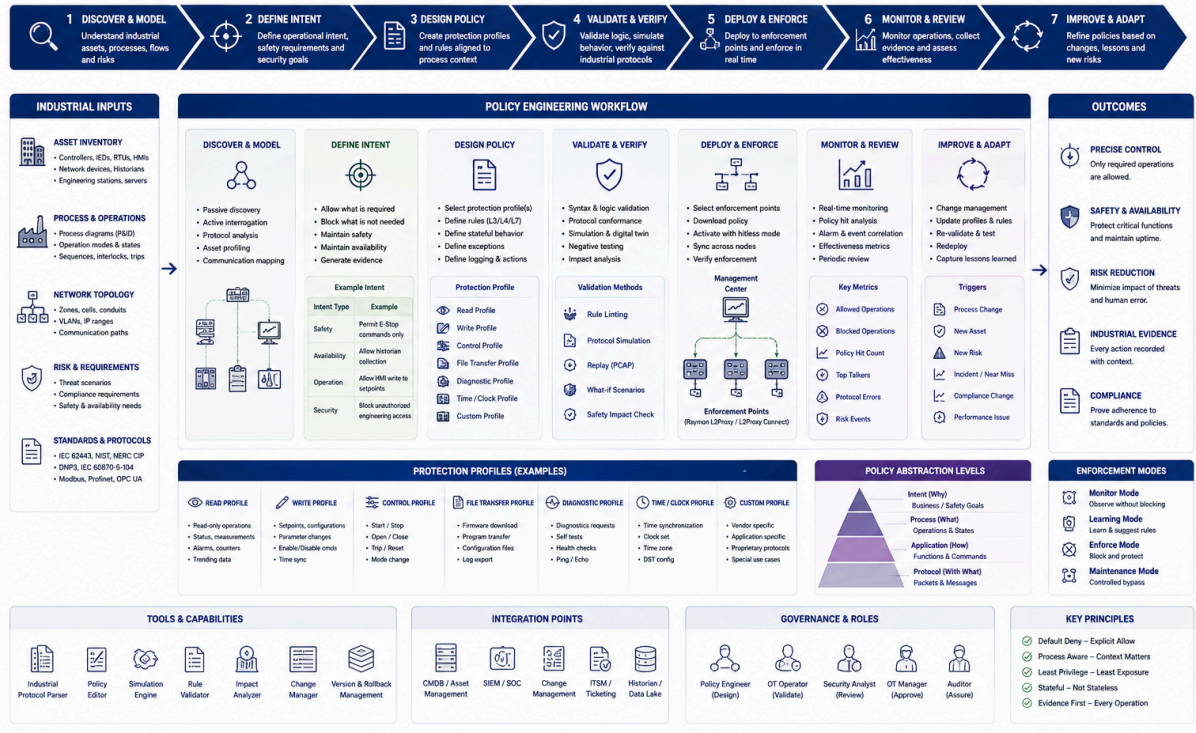
- who may perform the activity;
- source/access domain;
- destination equipment;
- industrial protocol and operation;
- point or object;
- allowed value/range;
- process state;
- prerequisite or prior event;
- timing and sequence;
- final decision and event behavior.

Guided authoring, reusable equipment knowledge, templates, field/helper catalogs, inline validation, and compilation reduce the distance between an OT requirement and a testable policy.

RAYMON POLICY ENGINEERING LIFECYCLE

From Industrial Intent to Enforced Control with Evidence and Continuous Improvement

RAYMON
INDUSTRIAL SECURITY



Raymon policy engineering lifecycle from equipment discovery and intent through validation, enforcement, and improvement

Figure 6 — Policy Engineering Lifecycle. Raymon carries policy from equipment discovery and engineering intent through validation, activation, qualification, evidence, and controlled improvement.

7. From approved policy to runtime enforcement

Industrial policy becomes valuable when the approved engineering intent can be traced to the exact runtime decision.

Raymon separates the stages deliberately:



Trace from equipment and point knowledge to runtime decision and evidence

Policy-to-enforcement trace — preserving accountability from engineering knowledge and approved profiles to runtime decisions and evidence.

This separation helps prevent two dangerous forms of ambiguity:

1. an equipment-library change silently becoming a production enforcement change;
2. an approved policy revision becoming active without a controlled assignment and lifecycle step.

Traceability questions

A reviewer should be able to determine:

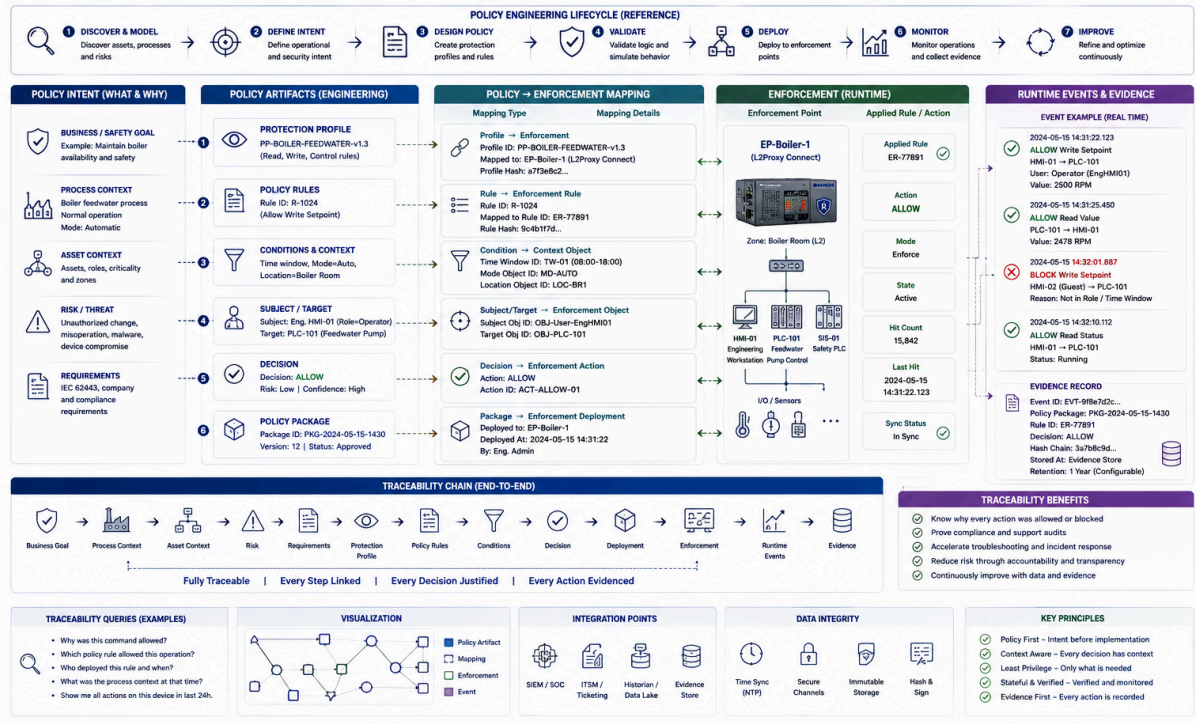
- which engineering requirement produced the rule;
- which Policy Profile contained it;
- which enforcement path received the profile;
- which rule matched at runtime;
- what decision was taken;
- which user/session/equipment/operation was involved;
- what state or prerequisite affected the decision;
- what evidence was retained.

RAYMON POLICY → ENFORCEMENT TRACEABILITY

Every Policy. Every Decision. Every Enforcement. Fully Traceable.

From engineering intent to real-time enforcement and industrial evidence.

RAYMON
INDUSTRIAL SECURITY



End-to-end traceability from industrial policy engineering to runtime enforcement and evidence

Figure 7 — Policy-to-Enforcement Traceability. Approved industrial intent remains traceable from equipment and policy definition to the active enforcement point, runtime decision, and retained evidence.

8. Stateful industrial protection

Industrial safety and control logic often spans multiple messages

A single packet may be syntactically valid and still be inappropriate in the current operational context. Raymon's stateful protection model can correlate events across messages and time.

Examples include:

- authorization followed by a command;
- Select followed by Operate within an approved window;
- command followed by expected response or process feedback;
- maintenance authorization followed by a restricted control;
- configuration change followed by restart and health verification;
- active/standby master state;
- safety trip → acknowledge → clear → reset lifecycle;
- bounded event counters and burst thresholds;
- replay-resistant state consumption;
- timeout and expiry conditions;
- missing prerequisites or invalid transitions.

What stateful protection evaluates

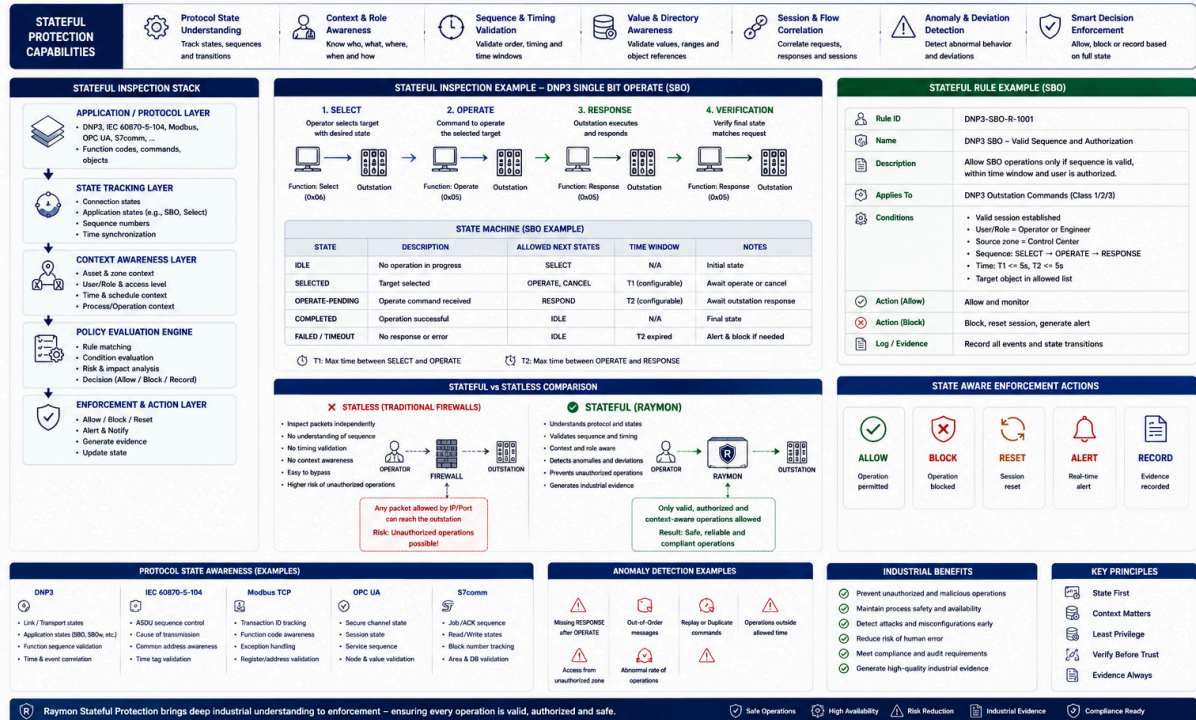
Dimension	Industrial question
Previous state	What has already happened?
Current operation	What is being requested now?
Identity/session	Is the same authorized context still valid?
Timing	Is the operation within its allowed window?
Fingerprint	Does the command match the earlier authorization/select?
Prerequisite	Is the required condition present?
Feedback	Did the process/device confirm the expected result?
Replay/duplication	Is this authorization or command being reused?

RAYMON STATEFUL PROTECTION

State Aware. Context Aware. Industrial Aware.

Raymon understands protocol states and enforces rules based on the behavior and context of industrial operations.

RAYMON
INDUSTRIAL SECURITY



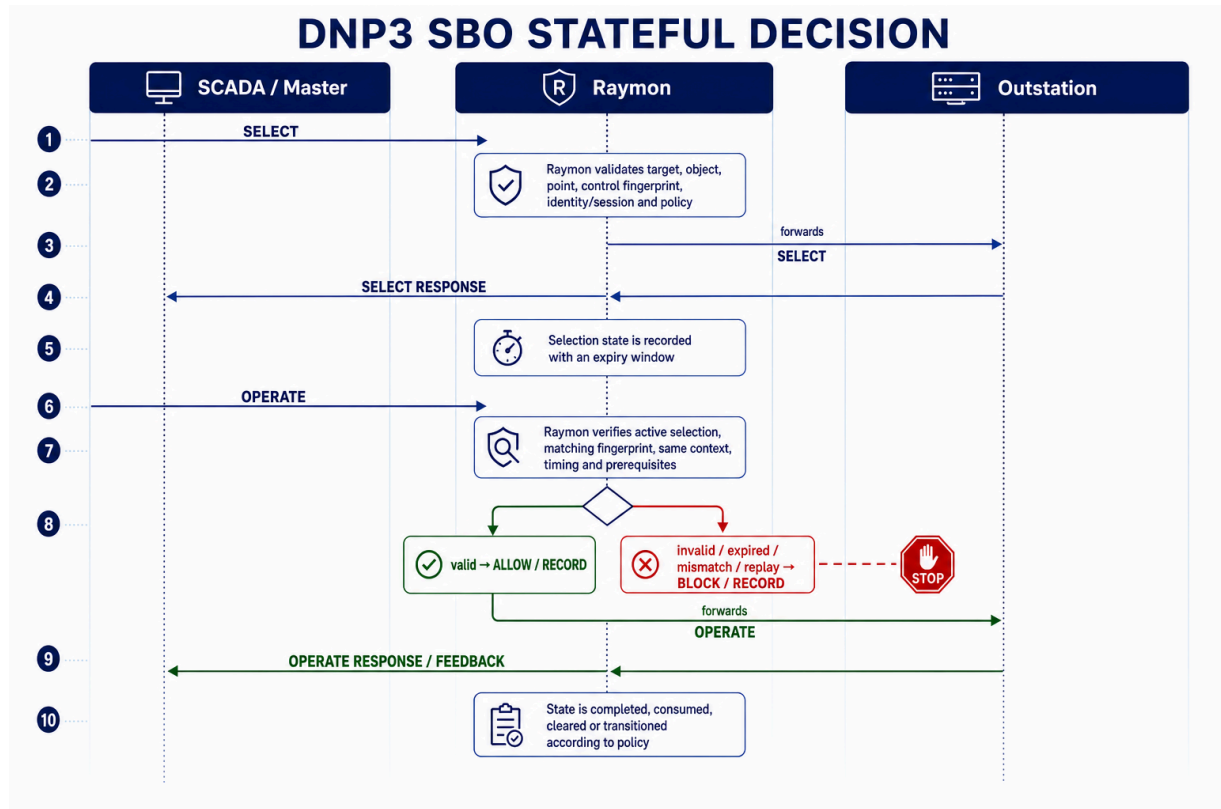
Stateful industrial protection using protocol state, context, sequence, timing, state machines, and smart enforcement

Figure 8 — Stateful Protection. Raymon correlates industrial operations across identity, sequence, timing, state, prerequisites, and feedback instead of evaluating each message in isolation.

9. DNP3 Select-Before-Operate protection

DNP3 Select-Before-Operate (SBO) is a concrete example of why state matters.

The expected sequence is more than four valid protocol messages. Raymon can retain and compare the context that binds them together.



DNP3 Select-Before-Operate stateful decision sequence

DNP3 SBO stateful decision — validating Select, response, recorded selection state, Operate context, timing, prerequisites, decision, and final feedback.

Conditions that can be evaluated

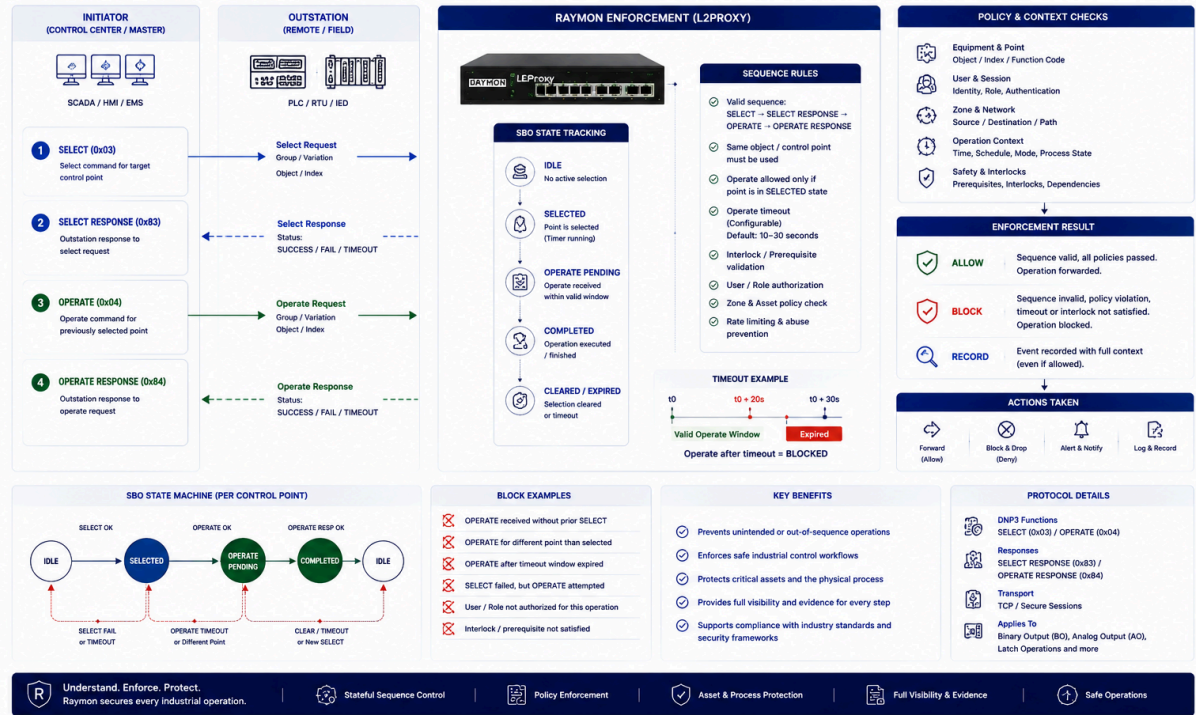
- missing Select;
- expired Select;
- Operate that does not match the selected control;
- wrong object/point/control code;
- session or identity drift;
- duplicate or replayed Operate;
- missing maintenance authorization;
- missing process prerequisite;
- absent or unexpected feedback;
- sequence timeout.

9 DNP3 SELECT-BEFORE-OPERATE (SBO) SEQUENCE

Safe Control of Critical Operations

Raymon understands and enforces the full DNP3 SBO workflow with state awareness, timing control and policy validation.

RAYMON
INDUSTRIAL SECURITY



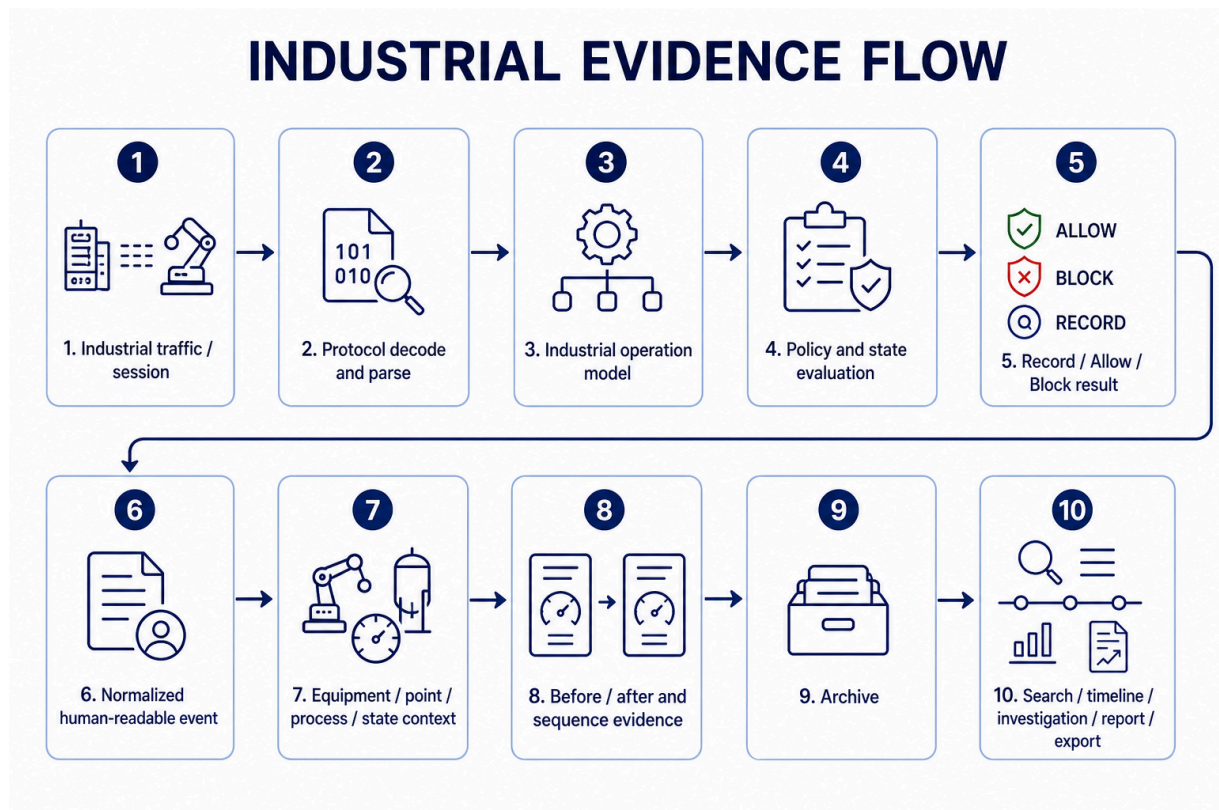
DNP3 select-before-operate sequence with state tracking, validation, timeout, and enforcement decisions

Figure 9 — DNP3 Select-Before-Operate Sequence. Raymon validates the complete DNP3 SBO control sequence—not only individual packets—and retains evidence for valid, expired, mismatched, replayed, and prerequisite-failing operations.

10. Industrial evidence — from protocol traffic to operational meaning

A blocked command without understandable evidence is difficult to operate, qualify, and investigate. Raymon therefore treats evidence as part of the control model rather than a separate logging feature.

The evidence pipeline can preserve multiple levels of detail:



Industrial evidence flow from traffic and protocol parsing to archive and investigation

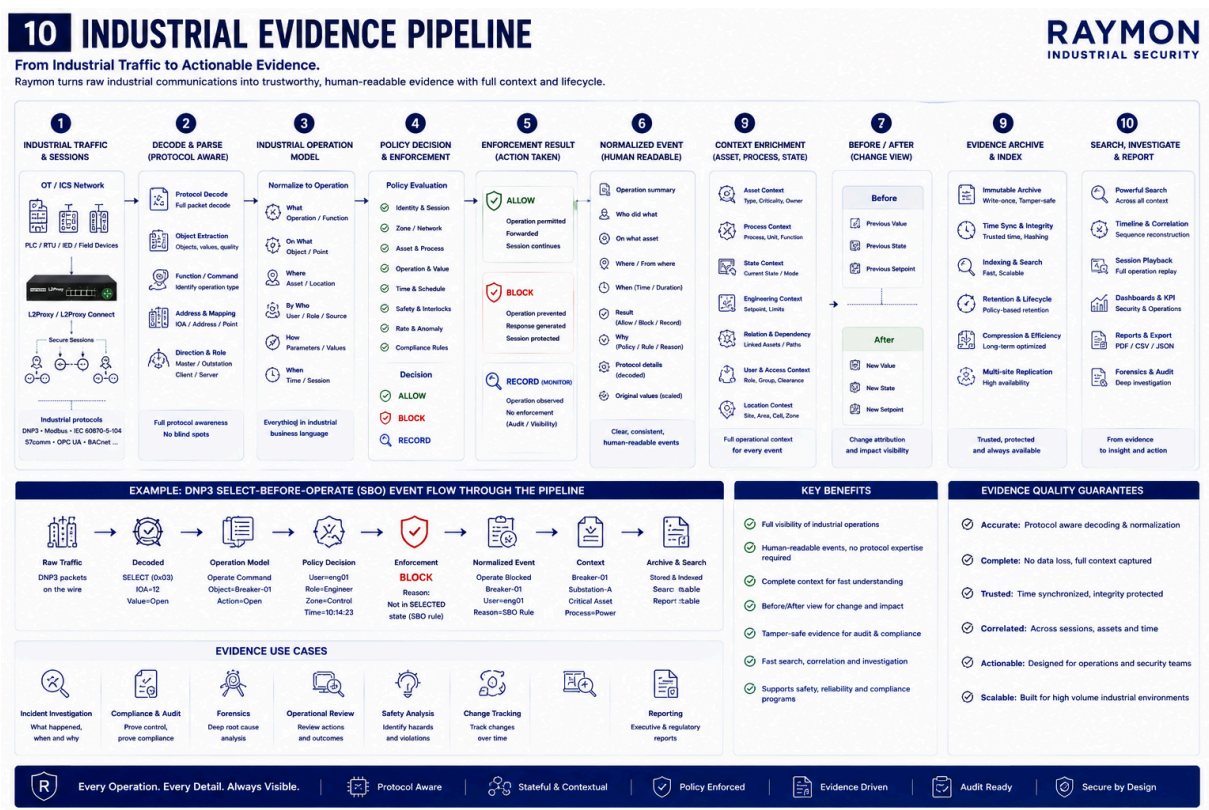
Industrial evidence flow — retaining the complete path from decoded traffic and policy decisions to readable events, context, sequence evidence, archive, and investigation.

Evidence can answer

- Who introduced the activity?
- Which session or access domain was involved?
- Which equipment and point were affected?
- What industrial operation was requested?
- Which value or control code was used?
- What policy and rule matched?
- Was the operation recorded, allowed, or blocked?
- Why was that decision made?
- What state existed before the decision?
- What state transition or timeout followed?
- What raw protocol evidence is available for drill-down?

Human-readable industrial events

A technical protocol tuple can be enriched into an event that operations can recognize without discarding the underlying facts. Asset and point mappings can add equipment names, roles, locations, units, operational intent, and criticality while retaining raw protocol fields for engineering and forensic review.



11. Deployment topologies and product placement

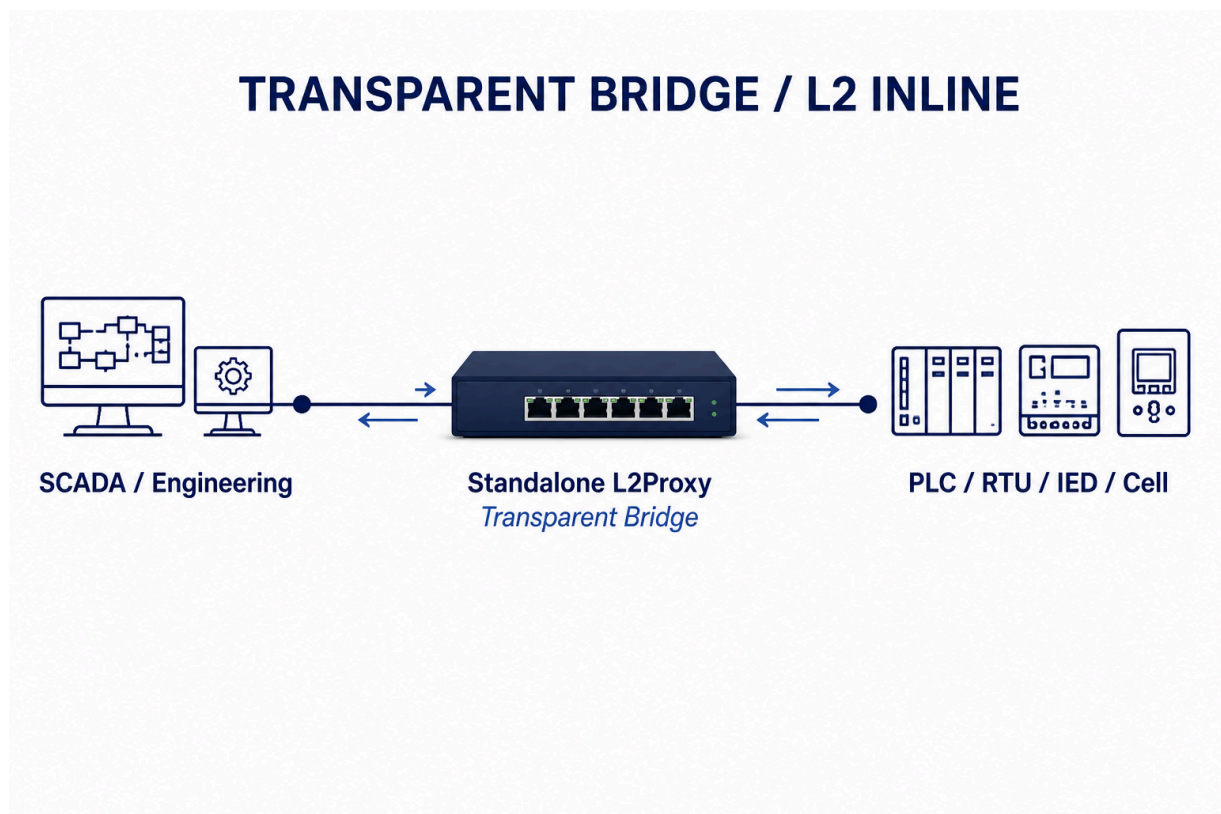
Raymon has **two primary enforcement forms**. Their distinction should remain explicit in all customer-facing architecture.

A. Standalone L2Proxy

Standalone L2Proxy operates as an independent enforcement service in the industrial network path.

Transparent Bridge / L2 inline

Use where policy must be inserted between industrial segments without changing the existing IP addressing plan.



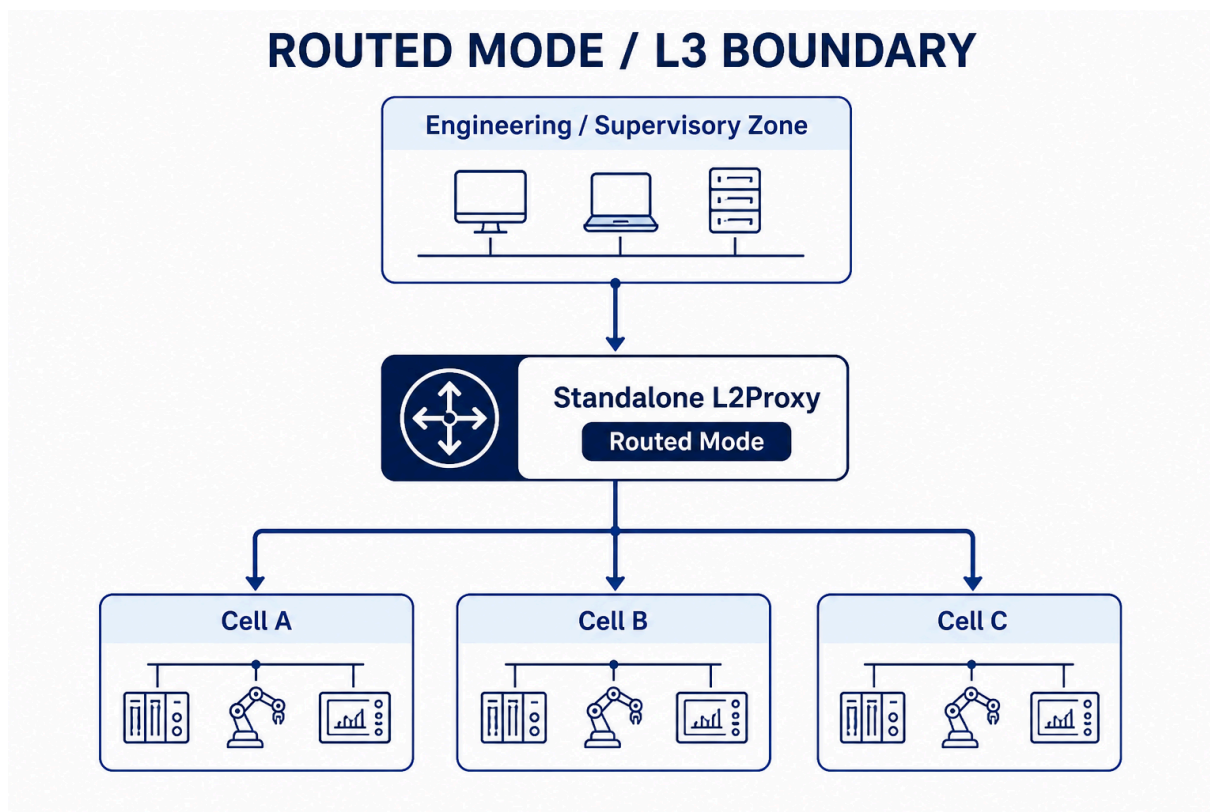
Standalone L2Proxy transparent bridge at an L2 inline boundary

Transparent Bridge / L2 inline — Standalone L2Proxy inserted between supervisory systems and industrial equipment without changing the addressing plan.

Routed Mode / L3 boundary

Use where Raymon acts at an established routed boundary between OT subnets, VLANs, sites, supervisory networks, or control cells.

ROUTED MODE / L3 BOUNDARY



Standalone L2Proxy routed mode between supervisory zone and industrial cells

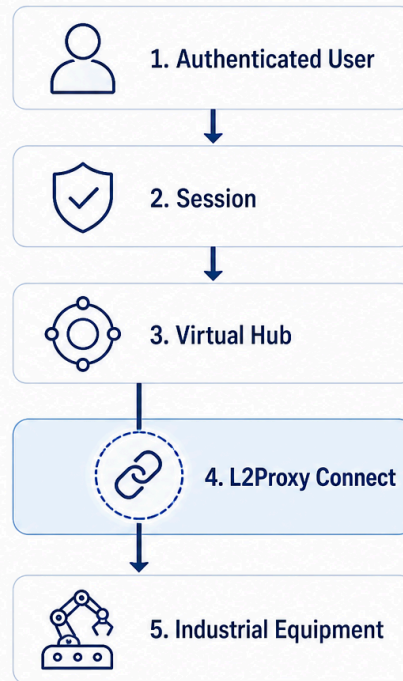
Routed Mode / L3 boundary — Standalone L2Proxy enforcing policy between the engineering or supervisory zone and multiple industrial cells.

Standalone deployment is **network-path enforcement**.

B. L2Proxy Connect

L2Proxy Connect places the industrial enforcement engine inside the authenticated session forwarding environment / Virtual Hub.

L2PROXY CONNECT SESSION PATH



L2Proxy Connect path from authenticated user and session to industrial equipment

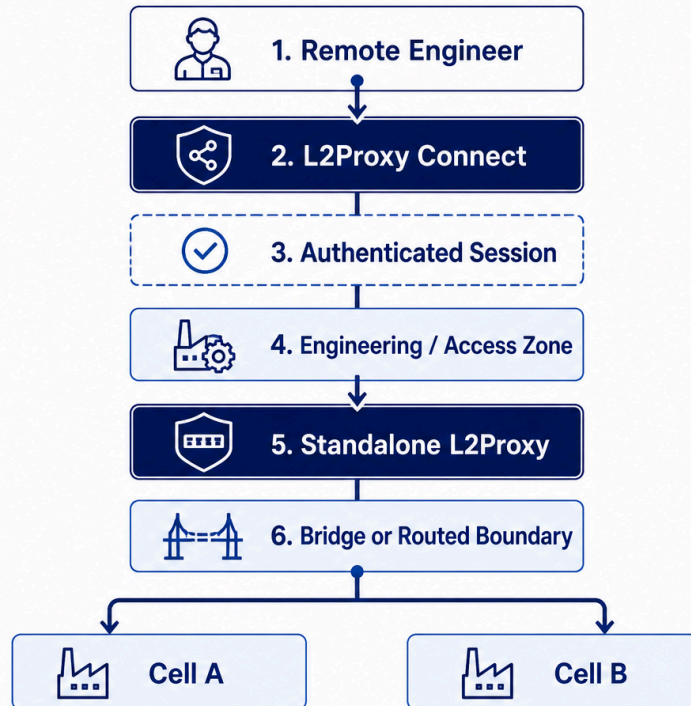
L2Proxy Connect — session-path enforcement from the authenticated user through the Virtual Hub to industrial equipment.

This is **session-path enforcement**. It can use identity, live session, access domain, equipment, industrial operation, state, and policy in the same decision path.

C. Hybrid deployment

Sites can combine the two forms:

HYBRID ENFORCEMENT



Hybrid Raymon enforcement combining authenticated-session and network-boundary controls

Hybrid enforcement — combining L2Proxy Connect session controls with Standalone L2Proxy at a bridge or routed boundary protecting industrial cells.

L2Proxy Connect constrains the authenticated session; Standalone L2Proxy can enforce at deeper plant, cell, area, or site boundaries.

Passive and offline postures

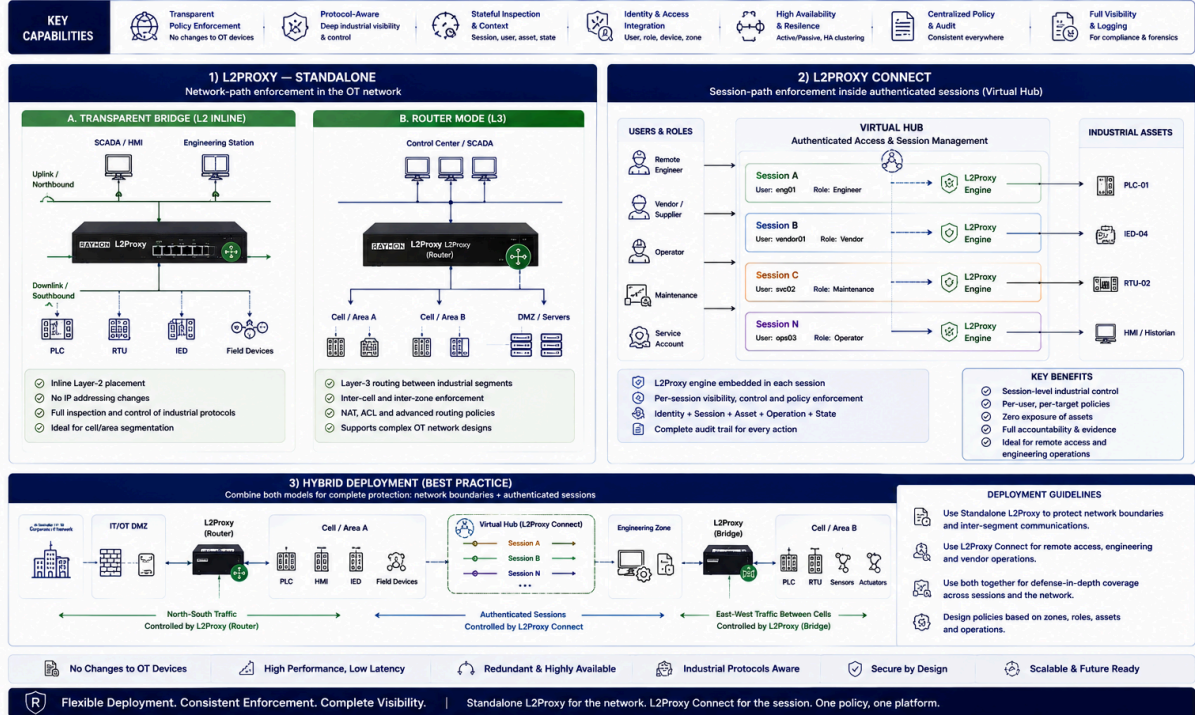
Passive observation and offline PCAP analysis are important commissioning, qualification, investigation, and policy-validation workflows. They are **operating postures**, not separate product forms equivalent to Standalone L2Proxy or L2Proxy Connect.

11 DEPLOYMENT TOPOLOGIES & PRODUCT PLACEMENT

RAYMON
INDUSTRIAL SECURITY

Deploy Raymon Enforcement Where It Matters Most

Two deployment models. One security architecture. Full control of industrial communications.



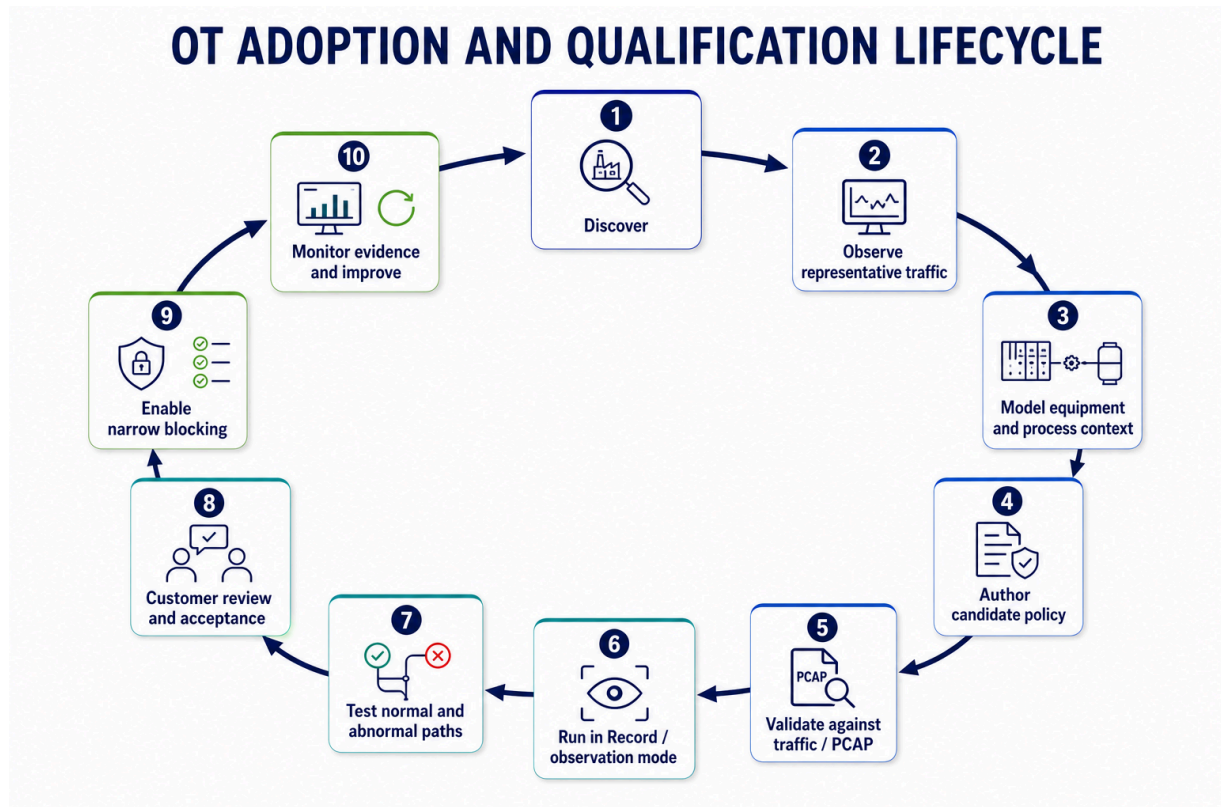
Raymon deployment topologies for standalone L2Proxy, L2Proxy Connect, and hybrid enforcement

Figure 11 — Deployment Topologies and Product Placement. Raymon can enforce directly at OT network boundaries through Standalone L2Proxy, inside authenticated sessions through L2Proxy Connect, or in a hybrid architecture that combines both control points.

12. Commissioning, qualification, and controlled adoption

Industrial enforcement should be introduced with evidence and operational acceptance. Raymon supports a progression from observation to narrowly scoped production control.

Recommended adoption lifecycle



OT adoption and qualification lifecycle from discovery to controlled blocking and improvement

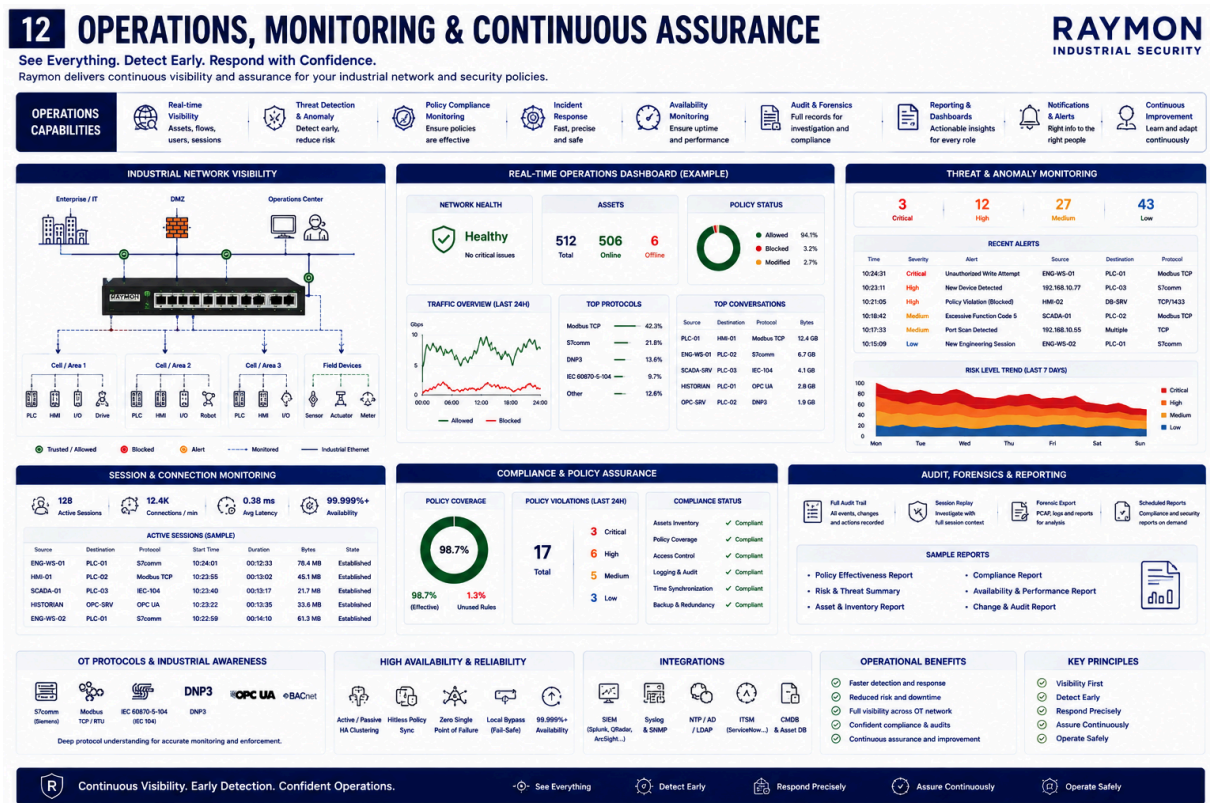
OT adoption and qualification lifecycle — progressing from discovery and representative observation to validation, customer acceptance, narrow blocking, and evidence-driven improvement.

Qualification should cover

- representative startup and shutdown;
- normal operation;
- maintenance behavior;
- retry and retransmission patterns;
- timeout and failure conditions;
- failover and redundancy behavior;
- process recovery;
- emergency or degraded operation;
- expected vendor-specific variations;
- bypass / rollback / fail-open / fail-closed decisions;

- evidence retention and investigation requirements.

A capability marked as supported or production-ready still requires qualification for the actual vendor implementation, topology, object variation, process behavior, and customer-approved policy.



OT adoption lifecycle with operational monitoring, qualification, enforcement readiness, and continuous assurance

Figure 12 — OT Adoption and Continuous Assurance. Raymon supports progressive OT adoption from observation and modeling through validation, acceptance, narrow enforcement, operational monitoring, and evidence-driven improvement.

13. Operating model by responsibility

Raymon is intended to support multiple plant responsibilities without forcing all users to work at packet level.

Responsibility	Primary Raymon view
Operations	Equipment, activity, decision, readable event, process relevance
Control / Automation Engineering	Equipment model, points, values, states, prerequisites, sequences
OT Security	Access domains, policy, enforcement, event classification, investigation
Maintenance	Approved work scope, identity/session, assigned equipment, evidence
System Integrator	Protocol fields, parser exposure, templates, validation, deployment modes
Qualification / Governance	Capability status, product boundaries, acceptance tests, retained evidence

One policy model — multiple enforcement locations

The value of the platform is not a single network position. Raymon carries a consistent industrial model across authenticated sessions and independent OT boundaries while preserving traceability from engineering intent to runtime evidence.

14. Protocol-aware protection portfolio

Raymon's platform architecture is designed to expose industrial protocol meaning to policy and evidence. Protocol maturity should be stated by capability level rather than by a single "supported / unsupported" label.

A useful qualification model is:

1. **Dissection** — decode protocol structure and fields.
2. **Field-aware policy** — evaluate decoded fields in rules.
3. **Semantic helpers** — expose stable industrial predicates and canonical values.
4. **Stateful protection** — correlate multi-message industrial behavior.
5. **Operational normalization** — convert protocol activity into readable industrial events.
6. **Qualification evidence** — representative tests, captures, examples, and known boundaries.

The existing public documentation currently presents **DNP3** in the greatest depth. Additional protocol portfolios should be documented with the same discipline before being represented in this catalog as equivalent customer-ready coverage.

Catalog maintenance note: Modbus, S7comm, and IEC 60870-5-104 coverage can be added to this section when their current product capabilities, examples, stateful use cases, event normalization, and qualification evidence have been written and reviewed. The platform story above does not need to change when those protocol portfolios are added.

15. Product boundaries

Clear boundaries are part of industrial trust.

Raymon provides industrial network inspection, policy enforcement, access-context correlation, stateful protection, segmentation controls, and retained evidence. It does **not** replace the safety or control logic owned by the plant.

Raymon is not a replacement for:

- PLC, RTU, DCS, or IED control logic;
- Safety Instrumented Systems (SIS);
- hardwired or controller-native process interlocks;
- engineering Management of Change;
- endpoint operating-system authorization;
- historian functionality;
- SIEM or enterprise log-management platforms;
- customer backup/retention policy;
- physical safety procedures.

Where Raymon evaluates a prerequisite or process condition, the policy must be based on customer-approved information and qualified against the actual plant behavior.

State lifecycle boundary

Stateful protection is designed for bounded runtime correlation. Persistent distributed state across engine restarts is not assumed unless explicitly implemented and qualified for the deployed build.

16. Why Raymon

Know the equipment

Start with equipment, points, operating limits, permitted commands, states, and protection knowledge rather than a blank packet rule.

Control industrial authority

Limit not only connectivity but the actual operations a user, session, system, or network path may perform.

Protect process-aware sequences

Evaluate timing, prerequisites, replay, feedback, and state transitions where one packet is not enough to understand the operation.

Deploy at the right control point

Use Standalone L2Proxy at transparent or routed OT boundaries, L2Proxy Connect inside authenticated session paths, or combine both.

Prove what happened

Retain operationally readable evidence with the underlying policy, state, identity, session, and protocol details available for drill-down.

Raymon Industrial Security Platform

Know. Control. Protect. Prove.

Industrial equipment knowledge → engineered policy → controlled enforcement → explainable evidence

For detailed engineering, qualification, capability status, protocol examples, and product boundaries, continue to the Raymon Industrial Security documentation set.

Appendix A — Master Diagram Placement Index

#	Master diagram	Primary catalog section	Usage
1	Raymon Platform Architecture	Opening / platform overview	Full-width

#	Master diagram	Primary catalog section	Usage
2	Industrial Operation Control Model	Industrial security problem	Two complementary full-width figures (2A and 2B)
3	L2Proxy Connect Session Path	L2Proxy Connect	Full-width
4	Industrial Microsegmentation	Segmentation	Full-width
5	Equipment Protection Model	Equipment-centric protection	Overview and derived-protection figures (5A and 5B)
6	Policy Engineering Lifecycle	Policy engineering	Full-width
7	Policy → Enforcement Traceability	Runtime traceability	Full-width
8	Stateful Protection	Stateful protection	Full-width
9	DNP3 SBO Sequence	DNP3 protection example	Full-width
10	Industrial Evidence Pipeline	Evidence	Full-width
11	Deployment Topologies & Product Placement	Deployment	Full-width
12	OT Adoption / Qualification Lifecycle	Qualification	Full-width

Appendix B — Figure Publication Checklist

Before publishing the customer-facing catalog:

1. proofread every label;
2. confirm all arrows and states match the current product behavior;
3. ensure Diagram #11 uses the exact Standalone / Connect / Hybrid taxonomy in this catalog;
4. ensure Diagram #9 is specifically DNP3 SBO, not generic anomaly detection;
5. ensure Diagram #10 is specifically the industrial evidence pipeline;
6. remove any text that exposes internal implementation platform names from L2Proxy Connect;
7. prefer final SVG/Figma redraws for dense text diagrams;
8. keep important product claims in Markdown text as well as the image;
9. retain the descriptive alt text and one-sentence caption under every figure;
10. verify that every referenced image is packaged beside this Markdown file in the published artifact.