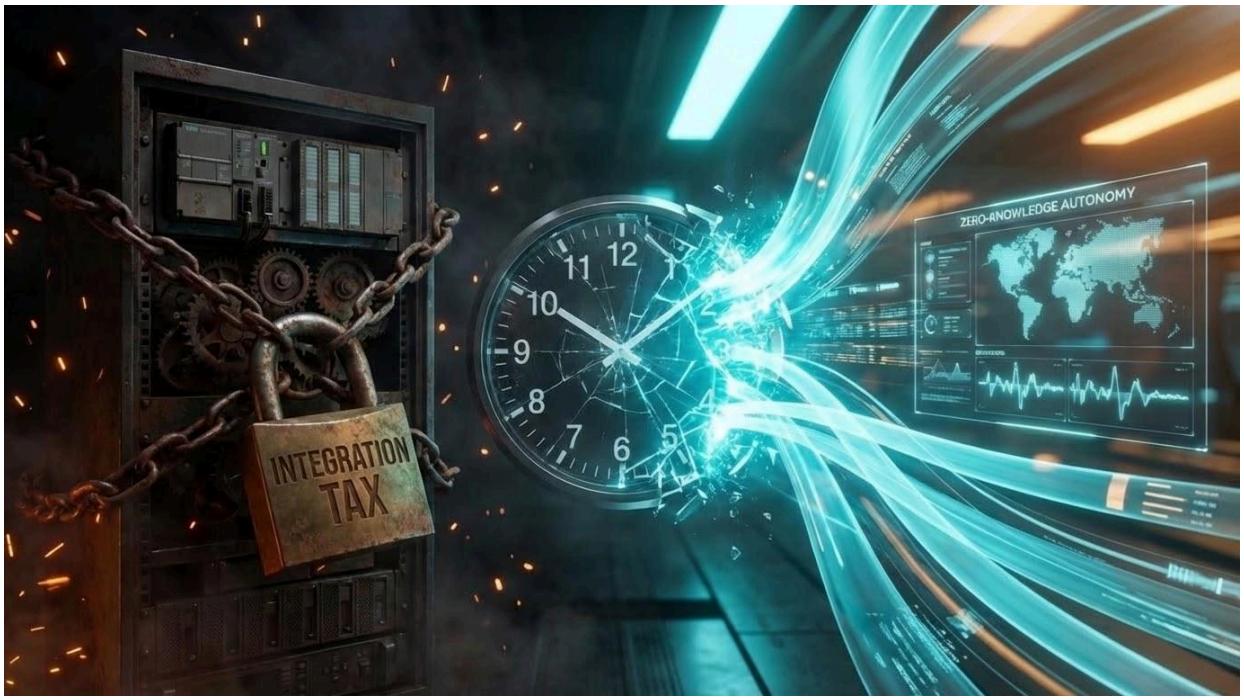

◆ COFRESÍ CONSULTING SERVICES · THOUGHT LEADERSHIP

The Integration Tax:

Why Time-to-Value Is the Only Metric That Matters

By José A. Cedeño · Cofresí Consulting Services · 2026

> ***Every network has a price of admission. The question is who pays it – your engineer, or your adversaries.***

I have spent over 25 years evaluating security and IT technologies across some of the most demanding environments in the world — the National Security Agency, the Department of Energy, and critical infrastructure operations where downtime is measured not in dollars but in consequences. In every one of those environments, I watched the same pattern repeat itself with exhausting consistency.

The tool gets purchased. The demo was flawless. Leadership is confident. And then the real work begins — months of manual engineering, custom parser development, environment-specific configuration, and data normalization — before the platform produces a single useful insight. By the time the tool is finally operational, the analysts who were supposed to benefit from it are burned out, the budget is strained, and the threat landscape has already moved on.

This is the Integration Tax. And it is the single most underacknowledged barrier to security value in the industry today.

The Problem: Feature-Rich, Value-Poor

Pillar One: The Parser Debt

If your environment uses a protocol that is not natively supported by your new platform — and in OT environments, it almost certainly does — your analysts become developers. They spend weeks, sometimes months, building custom ingestion logic for 30-year-old PLCs, proprietary SCADA systems, and legacy industrial protocols that were never designed with interoperability in mind.

This is not a minor inconvenience. It is a fundamental misallocation of your most scarce resource: analyst attention. Every hour spent writing a Modbus parser is an hour not spent hunting threats.

Pillar Two: The Stale Inventory

Legacy tools see only what they are told to see. The moment a new VLAN is provisioned, an IoT device is plugged in, or a contractor connects a laptop to the OT network, the tool becomes blind to that activity — not because the threat has changed, but because no one updated the configuration.

In rapidly evolving environments, this creates a perpetual gap between the network that exists and the network that the security tool thinks exists. Attackers understand this gap intuitively. The 200+ day average dwell time in OT environments is not a technology failure. It is the predictable consequence of an inventory model that requires constant human maintenance to remain accurate.

Pillar Three: The Cognitive Load

When a tool requires constant tuning, configuration updates, and parser maintenance just to remain relevant, it does not reduce the burden on your analysts. It increases it. The platform that was supposed to free your team to focus on judgment instead becomes another system that demands their attention.

This is how alert fatigue begins — not from too many alerts, but from too much noise generated by a system that was never properly calibrated to the environment it is supposed to protect. Analysts stop trusting the tool. They begin working around it. And eventually, the platform that costs seven figures to procure is generating PDF reports that no one reads.

The Cost of Inaction: What the Tax Buys Your Adversary

The Integration Tax is not merely an operational inconvenience. It is a strategic gift to anyone who wants to compromise your network.

Consider the arithmetic. The industry average dwell time in OT environments before detection is 200 days or more. That is not an accident. It is the direct result of monitoring gaps created by tools that were never fully deployed, parsers that were never written, and assets that were never added to the inventory. Attackers do not need to be sophisticated to exploit a monitoring gap. They simply need patience.

> **THE REAL COST**
>
> ***200+ days of undetected dwell time is not a technology problem. It is an Integration Tax problem. Every day your tool is not operational is a day your adversary is mapping your environment, identifying your failsafes, and planning their next move.***

Colonial Pipeline. The Ukraine power grid. The Oldsmar water treatment facility. These incidents did not succeed because the attackers were uniquely capable. They succeeded because the defenders were operating with incomplete visibility — visibility that was incomplete not because the technology did not exist, but because the Integration Tax had never been paid.

The question is not whether you can afford to eliminate the Integration Tax. The question is whether you can afford to keep paying it.

The Operator's Solution: Zero-Knowledge Autonomy

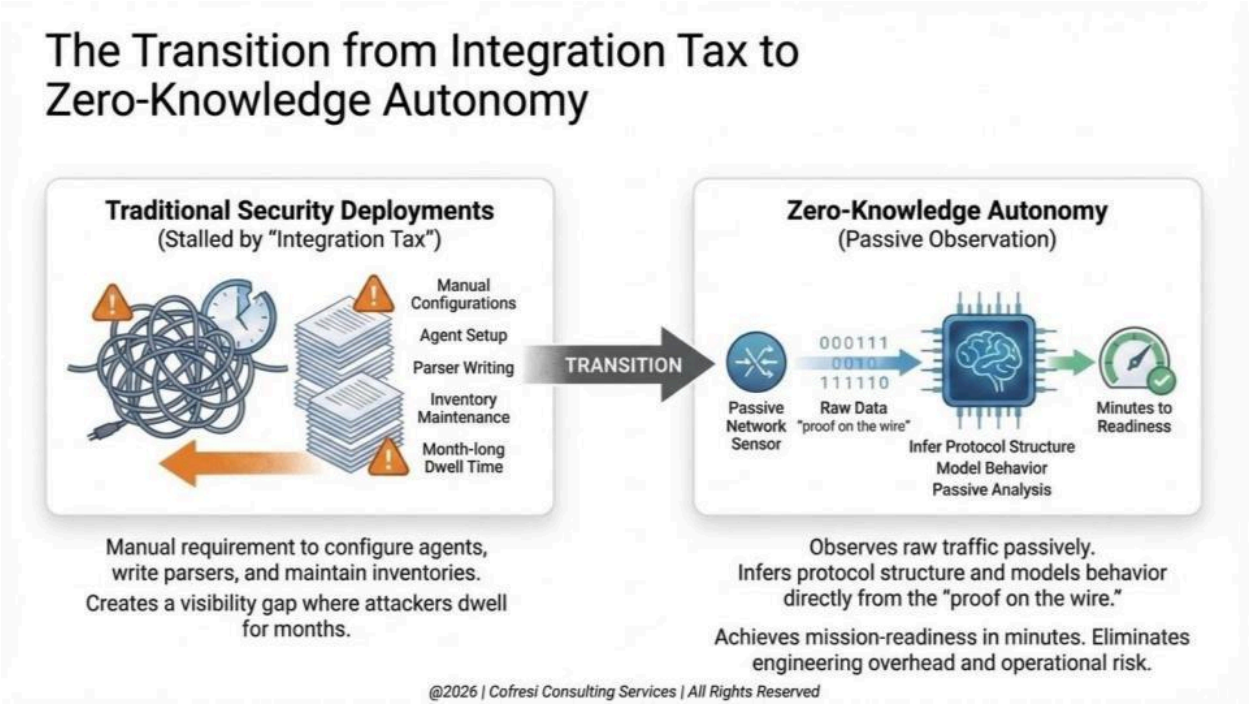

Figure 1: The next generation of security tools must stop asking operators to explain the network to the platform. The platform should infer it.

> ***If it emits a packet, it should be on the map. No exceptions. No tax required.***

This is the principle of Zero-Knowledge Autonomy — a system that can enter any environment and immediately begin modeling structure, behavior, and communication patterns directly from observable traffic, without pre-configuration, without parser libraries, and without prior protocol knowledge.

Instead of asking 'What will a device tell us about itself?' — which requires agents, active scanning, and cooperation from hardware that may be decades old and incapable of supporting modern security tooling — the question becomes: 'What does the wire prove this device is actually doing?'

Network traffic cannot be faked. A PLC communicating via Modbus to an HMI is generating packets regardless of whether any security tool is installed on it. A dormant controller that has been online for 847 days without appearing in any asset inventory is still emitting traffic. The evidence exists. The question is whether your platform can see it without requiring six months of engineering work to get there.

What This Looks Like in Practice

An autonomous ingestion layer should accomplish several things without human intervention:

- Identify hosts, classify their roles, and map communication relationships from raw traffic within minutes of deployment
- Recognize structural patterns in unknown protocols — fixed headers, sequence counters, timestamp fields, checksums — and generate reverse engineering scaffolding that analysts can immediately work from
- Correlate behavioral changes across systems to build a model of normal operations that does not require a human to define 'normal' in advance
- Flag deviations from that baseline with enough context — device identity, communication partners, blast radius — that an analyst can make a decision in minutes rather than days

This is not science fiction. Foundational technology exists today. What has been missing is the discipline to apply it specifically to the OT problem — to build systems that treat the absence of prior knowledge not as a limitation but as the design requirement.

The Strategic Outcome: Operational Continuity and Security Are Not a Trade-Off

For decades, industrial organizations have accepted a false choice between security and operational continuity. Active scanners crash legacy PLCs. EDR agents introduce latency into millisecond-sensitive control loops. The security team is not allowed on the factory floor. And so the floor becomes a black box, monitored by assumption rather than evidence.

The elimination of the Integration Tax changes this equation entirely. When a platform requires no agents, no active scanning, and no pre-configuration to begin producing value, the IT/OT conflict dissolves. Security teams can finally operate in environments that were previously off-limits — not because the rules changed, but because the tools no longer pose operational risk.

When that happens, something else changes too: the conversation between the security team and the board. Operator-grade findings — specific devices, specific behaviors, specific blast radii — become the evidence base for executive-ready recommendations. The CISO stops presenting threat landscapes and starts presenting decisions.

THE COFRESÍ STANDARD

We evaluate every tool against one question before we recommend it: How long from deployment to the first actionable insight? If the answer requires more than days, the Integration Tax has not been eliminated. It has been renamed.

The organizations that will avoid the next Colonial Pipeline are not necessarily the ones with the largest security budgets. They are the ones that stopped tolerating the Integration Tax — that demanded platforms capable of seeing their full environment from day one, without months of engineering overhead standing between deployment and value.

Time-to-certainty is the only metric that matters. Everything else is overhead.

ABOUT THE AUTHOR

José Cofresí is the founder of Cofresí Consulting Services, an IT strategy and cybersecurity advisory firm serving federal, critical infrastructure, and enterprise clients. He brings 25+ years of operator experience from the Intelligence Community and Department of Energy, where he evaluated emerging technologies against the reality of mission-critical operations. He can be reached at info@cofresi-consulting.net or at cofresi-consulting.net.