

## 01 · EXPOSE — ASSET INTELLIGENCE &amp; MEASUREMENT

# You Cannot Secure What You Cannot See

Incomplete, stale, or manually maintained OT asset inventories leave critical infrastructure exposed. ConsoleWorks delivers a continuous, authoritative view of every asset — without agents, without disruption, without replacing the tools you already have.

## THE CHALLENGE

## OT Asset Visibility Is Broken

**Most OT environments operate with fundamentally incomplete asset knowledge.**

- Asset inventories built from spreadsheets or manual walk-downs are outdated before they are finished.
- Multiple point tools each maintain their own asset view — none agree, and none are authoritative.
- Engineering, security, and compliance teams often work from different asset lists for the same environment.
- New devices, firmware changes, and configuration drift go undetected between audit cycles.

**Without accurate inventory, risk scoring, compliance mapping, and remediation prioritization are all built on a flawed foundation.**

## THE SOLUTION

## Inventory Is the Starting Point — Not the Finish Line

Most OT asset inventory tools stop at discovery — they give you data, but not intelligence. What you get is a collection of disconnected records from disparate tools, each with its own view of the same device. ConsoleWorks goes further: it aggregates that data into a single authoritative inventory and continuously measures every asset against your security and compliance requirements.

ConsoleWorks combines passive aggregation from your existing tools with active collection through its Continuous Configuration Monitor (CCM) — capturing device state directly from the source. The result is an inventory that ConsoleWorks alone can produce — a single, normalized, continuously updated record that security, compliance, and operations teams can trust.

### Zero-Agent Discovery

No agents on OT devices. ConsoleWorks aggregates existing tool feeds — zero production impact. There is nothing to install, patch, or maintain on managed devices.

### Multi-Source Aggregation

Ingests data from existing security tools, network sensors, and manual inputs. Reconciles into one asset record per device.

### Continuous Inventory Maintenance

Inventory updates on every measurement cycle. New devices and configuration drift are captured without manual intervention.

### Rich Asset Classification

Captures device type, vendor, firmware, criticality, location, communication paths, and compliance obligations — plus any additional attributes your organization requires.

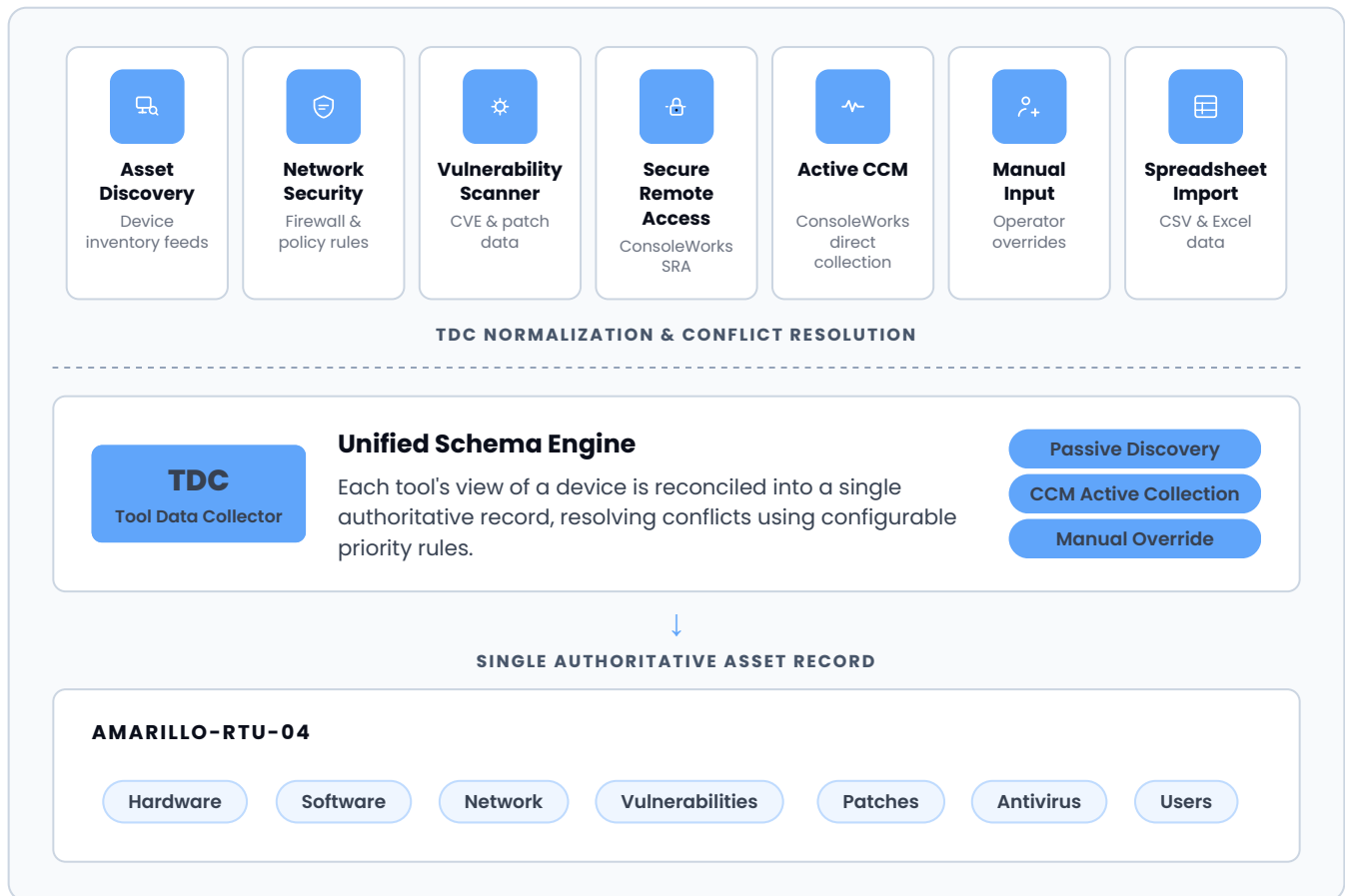
### HOW CONSOLEWORKS COLLECTS ASSET DATA

ConsoleWorks uses the Tool Data Collector (TDC) framework to ingest asset information from tools already deployed in your environment. Rather than deploying agents or running active scans that could disrupt OT devices, the TDC connects to existing data sources — vulnerability scanners, network sensors, SIEM feeds, historian exports, and manual inputs — and normalizes their output into a unified schema. Each tool's view of a device is reconciled into a single authoritative record, resolving conflicts using configurable priority rules.

Not every source knows the same things about a device — and not every source can be trusted equally for every field. The TDC handles this through configurable Mapping Rules that define how each tool's data maps to the ConsoleWorks asset schema. When two sources report conflicting values for the same field — firmware version from a scanner versus firmware version collected directly by CCM — priority rules determine which value wins. CCM-collected data carries the highest trust, followed by purpose-built discovery tools, with manual inputs and spreadsheet imports available to fill gaps that automated sources cannot reach. The result is a single record per device that reflects the most authoritative data available, not simply the most recent.

Passive discovery runs continuously, detecting new devices and changes as they appear in tool feeds. Where passive discovery cannot capture sufficient detail, operators supplement records through manual override — adding criticality ratings, site locations, or compliance obligations.

Where passive aggregation captures what existing tools already see, ConsoleWorks Continuous Configuration Monitor (CCM) goes further — actively collecting configuration state directly from each managed device. Firmware versions, running configurations, and device-level attributes collected by CCM are not estimates or approximations — they are ground truth.



The result is a single, normalized record per device — built from the most authoritative data available across every connected source. No manual reconciliation. No conflicting lists. Every field reflects the highest-confidence value ConsoleWorks has collected, from the tool best positioned to provide it. When new data arrives — from a scan, a session, or a direct collection cycle — the record updates automatically, without operator intervention.

### ● **Passive Aggregation**

Captures what existing tools already see. Runs continuously — new devices and changes appear as tool feeds update, with no production impact to OT devices.

### ● **CCM Active Collection**

Collects configuration state directly from each managed device. Firmware versions and device-level attributes are ground truth — not estimates inferred from network traffic.

**Passive discovery tools infer device state from network traffic. ConsoleWorks CCM collects configuration data directly from the source — the most trusted and comprehensive asset inventory.**

#### ASSET RECORD STRUCTURE

Every device in ConsoleWorks is represented as a structured asset record — a unified view built from the most trusted data available across all connected sources. Hardware attributes such as firmware version, model, running configuration, and communication paths are aggregated from the sources best positioned to provide them. Software and vulnerability data, operational context, criticality, site location, functional classification, and compliance obligations are drawn from whichever connected tools and operator inputs have the most authoritative view.

#### BEYOND DISCOVERY

### How Measurements Work

Most asset inventory tools stop once they have a list. ConsoleWorks goes further — every asset in the inventory is continuously evaluated against the measurements applicable to it, producing a Pass/Fail result on every cycle. This is not a point-in-time assessment. The status of every device always reflects current state.

#### **Operational**

- Running approved firmware version
- Configurations within defined policy
- No unauthorized software installed
- Services and ports within baseline

#### **Security**

- Latest known vulnerabilities addressed
- Patches applied within required window
- Antivirus definitions current
- No known high-severity CVEs unmitigated

#### **Compliance**

- Meets specific NERC CIP control
- IEC 62443 requirement satisfied
- Logging and audit trail active
- Access control policy enforced

Organizations configure which measurements apply to which devices — ensuring measurement reflects what actually matters to them, not a generic baseline. Results are generated at the device level — specific, actionable, and unambiguous. When a device fails a measurement, ConsoleWorks surfaces the result immediately in the inventory view, alongside the full context of the device. For assets under ConsoleWorks Secure Remote Access management, operators can connect directly to the affected device to investigate or remediate. For assets not under SRA management, ConsoleWorks generates notifications and reports to ensure the right teams are informed and can act.

The Pass/Fail results produced by ConsoleWorks measurement are the foundation of everything that follows. They feed directly into the Risk Analysis engine, where they are aggregated and weighted to produce a continuous view of security and compliance posture — for every stakeholder that needs to act on it.

### THE INVENTORY VIEW

The asset record is the foundation of what operators see. ConsoleWorks surfaces every record in a unified inventory view — a single, searchable list of every managed device, with its current measurement status visible at a glance. Operators can filter by site, device type, criticality, or measurement status to focus on exactly what needs attention.

For each device, the full asset record is available in a single click — firmware version, communication paths, compliance obligations, and current Pass/Fail status for every applicable measurement. There are no separate tools to query, no manual correlation required. Everything ConsoleWorks knows about a device is in one place.

| ASSET RECORD — AMARILLO-RTU-04 <span style="float: right;">Connect</span> |   |  |  |
|---|---|--|--|
| <b>DEVICE TYPE</b><br>RTU / PLC   | <b>VENDOR</b><br>Schneider Electric         | <b>FIRMWARE</b><br>v3.1.2 — Drift Detected | <b>OS / PLATFORM</b><br>EcoStruxure v4.2               |
| <b>PATCH STATUS</b><br>2 Critical — Unpatched                             | <b>ANTIVIRUS</b><br>Definitions 47 days old | <b>UNAUTHORIZED SOFTWARE</b><br>1 Detected | <b>PASSWORD POLICY</b><br>Default Credentials Detected |

For assets under Secure Remote Access management, operators can initiate a direct connection to the device from within the inventory view — moving from exposure to elimination without leaving the platform.

### WHY CONSOLEWORKS

| Capability                       | Point Inventory Tools                 | ConsoleWorks                                    |
|----------------------------------|---------------------------------------|---|
| Asset Discovery                  | Yes — per-tool view only              | ✓ Unified, multi-source, single record          |
| Multi-Source Aggregation         | Not typically included                | ✓ TDC normalizes all feeds into one schema      |
| Active Configuration Collection  | Passive inference only                | ✓ CCM collects directly from the device         |
| Security Measurement             | Not typically included                | ✓ Continuous Pass/Fail via SCF hierarchy        |
| Compliance Mapping               | Limited or manual                     | ✓ Auto-mapped to 100+ frameworks                |
| Firmware & Patch Tracking        | Snapshot only                         | ✓ Continuously updated every measurement cycle  |
| Unauthorized Software Detection  | Not included                          | ✓ Detected and flagged per measurement policy   |
| Conflict Resolution              | No — each tool maintains its own view | ✓ Configurable priority rules resolve conflicts |
| Remediation Guidance             | Not included                          | ✓ Impact-ranked, assigned work items            |
| Secure Remote Access Integration | Separate tool required                | ✓ Connect directly from inventory view via SRA  |
| Stakeholder Views                | Single view, single audience          | ✓ Three Lenses — CISO, compliance, ops          |