INDUSTRIAL DEFENDER®

CASE STUDY

Achieving Enterprise - Wide OT Visibility

Across 90+ Retail and Warehouse Locations

90+
Retail & Warehouse Locations Monitored

15,000+
OT & IT Assets Discovered

300+
OT Devices with Firmware Identified

INDUSTRIALDEFENDER.COM

When one of Southern Europe's largest department store and logistics operators set out to secure its operational technology environment, it faced a challenge shared by many large, distributed organizations: no one could see what was actually running across the network.

THE CHALLENGE

This major Southern European retailer operates one of the most complex commercial environments in Europe. Across more than 90 retail locations, storage facilities, and large-scale logistics warehouses — some comparable to Amazon fulfillment centers in automation sophistication — thousands of connected devices ran quietly in the background.

From simple label printers in a warehouse to complex HVAC/R systems used to store ready-to-eat food at retail locations, the environment was complex, diverse and dispersed across an entire country.

The challenge wasn't a lack of technology investment. It was a lack of visibility. HVAC controllers, refrigeration management systems, warehouse PLCs managing automated picking operations, label printers, building management systems, and networking infrastructure all operated across siloed, segmented networks.

No single team could see across all of them. No unified inventory existed.

And no one in the security function could answer the most basic question of OT security: what do we have, and is it vulnerable?

> **Industrial Defender was brought in to change that — delivering enterprise-wide OT asset visibility across 90+ locations without disrupting a single operational system.**

The security team had a specific, time-sensitive mandate:

- Identify all OT assets not covered by the corporate IT security program
- Surface firmware vulnerabilities across those assets
- Report findings to management and operational staff at individual locations
- Execute asset inventory without disrupting live retail and logistics operations

The constraints were equally clear.

The security team had limited authority over network access and device configurations – they would need to work within existing infrastructure without relying on cooperation from operational teams or network administrators at each site.

Any solution had to be 100% proven to support Building Management Systems in complex, distributed consumer-facing retail locations and highly orchestrated logistics and warehousing facilities. No risk of disrupting a picking robot, a cooler controller, or a point- of-sale system. With 90+ locations operating around the clock, unknown OT vulnerabilities represent a direct risk to operational uptime. Enterprise-wide OT visibility is the foundation for protecting the infrastructure that keeps product moving and customers happy.

Firmware vulnerability tracking was effectively impossible without first knowing what assets existed.

The retailer had grown rapidly across Spain and beyond, adding locations, warehouse automation systems, and building infrastructure faster than any manual inventory process could track. The gap between what the security team thought was on the network and what was actually there was unknown.

And that unknown was the risk.

THE SOLUTION

The retailer selected Industrial Defender to deploy its OT asset monitoring platform across the entire estate. Industrial Defender Collectors (IDCs) were installed at each retail and warehouse site, feeding data back to the Industrial Defender Central Manager (IDCM) — creating a unified, centrally managed view of the OT environment for the first time.

Every collector monitored the network traffic without disrupting any operational device providing the retailer with real-time telemetry.

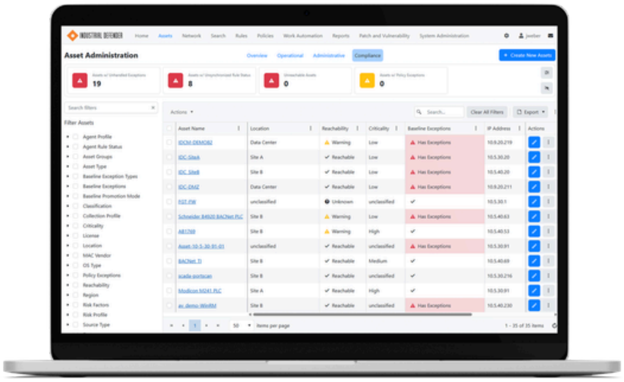
No coordination with on-site teams.

And no risk to live systems.

As traffic flowed across the retailer's networks, Industrial Defender began building the inventory:

- Johnson Controls building management equipment across department store locations
- Warehouse PLCs controlling automated logistics and pick-and-pack operations
- Refrigeration and cooler management controllers serving in-store grocery and food sections
- Label printers and shipping systems across logistics warehouse floors
- Windows-based servers and terminals across retail and back-office environments
- Networking infrastructure spanning dozens of sites

Where OT protocols were detectable on the wire, Industrial Defender extracted firmware version data automatically. For assets broadcasting via SNMP, the platform captured firmware and configuration data without any manual configuration.



For OT-specific devices -- PLCs, controllers, building management systems -- firmware versions were identified and cross-referenced against known vulnerability databases, generating an exportable report the security team could act on and distribute to site managers.

The IDC-to-IDCM architecture meant the security team in their central office had a single pane of glass across all 90+ locations -- a capability that previously required either on-site presence or complex, expensive tooling that was never deployed at this scale.

THE RESULTS

For the first time in the organization's history, the OT security team had a comprehensive, enterprise-wide view of their operational asset landscape. The results delivered immediate strategic and operational value.

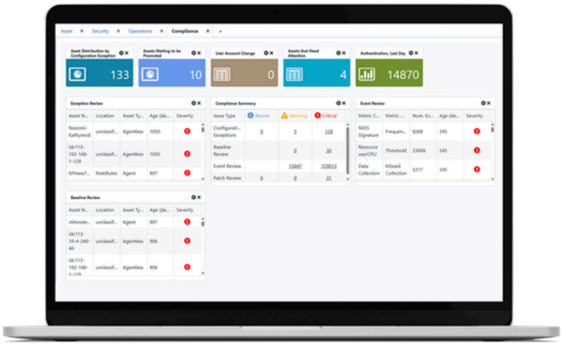
• **15,000+ assets discovered** across retail stores, warehouses, and logistics facilities – the vast majority previously untracked by any security program and unknown to the security function.

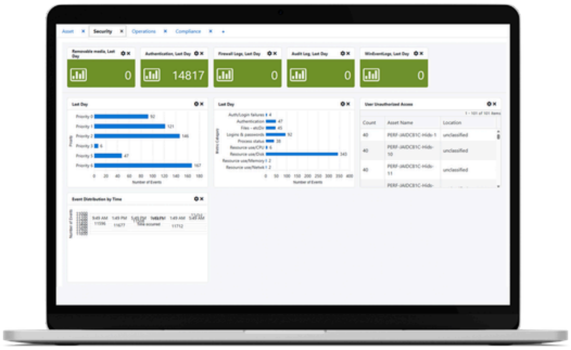
• **300+ OT-specific devices** with firmware version data identified and mapped to known CVEs — creating an actionable vulnerability baseline for PLCs, building management systems, refrigeration controllers, and industrial automation equipment.

• **Multi-site visibility achieved from a single central console**, enabling reporting to regional management and executive leadership without requiring on-site audits or manual data collection from individual locations.

• **Firmware vulnerability reports generated and distributed** to operational staff at individual locations, enabling targeted remediation planning against a baseline that simply didn't exist before.

• **Previously unknown OT asset classes identified** — including warehouse automation PLCs, refrigeration management systems, and smart building infrastructure that the security team had not known were network-connected.





"Before Industrial Defender, we had no way of knowing what was running across our stores and warehouses. We now have a single view of our entire OT landscape — from the department store floor to warehouse automation systems — and a clear roadmap for managing firmware vulnerabilities across all of it."

LOOKING AHEAD

The initial deployment established the foundation.

With a comprehensive, enterprise-wide asset inventory now in place, the retailer is positioned to activate Industrial Defender's active collection capabilities, enabling richer firmware interrogation via SNMP and agentless data collection to supplement its discovery and close the remaining visibility gaps on Windows assets.

Windows servers and terminals represent a significant portion of the discovered asset population. While passive monitoring identifies OS version groupings, active or agentless collection unlocks patch-level visibility and precise CVE matching -- ideal as the OT security program matures into baseline inventory and continuous vulnerability management.

As the program grows, Industrial Defender's platform scales with it: from asset inventory, to continuous vulnerability monitoring, to configuration change detection and policy compliance reporting -- all from the same unified platform already deployed and operational across the estate.

As regulatory frameworks governing critical infrastructure and large-scale retail operations continue to evolve across Europe — including NIS2 and equivalent national directives — the investment in OT visibility positions them well ahead of compliance timelines.

The asset inventory, network baseline, configuration monitoring, and anomaly detection capabilities already in place are precisely the controls these frameworks require. Rather than facing a compliance buildout under deadline pressure, an operational foundation can be mapped to regulatory requirements with minimal additional effort.

CUSTOMER PROFILE	
Organization	Major Southern European Retailer
Industry	Retail & Logistics
Headquarters	Southern Europe
Locations	90+ stores & warehouses
Challenge	Enterprise OT Asset Visibility & Firmware Vulnerability Management
Deployment	Multi-Site | Centrally Managed
Solution	Industrial Defender IDC + IDCM Platform

Learn how Industrial Defender can give your organization visibility into its OT environment.

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com 225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com