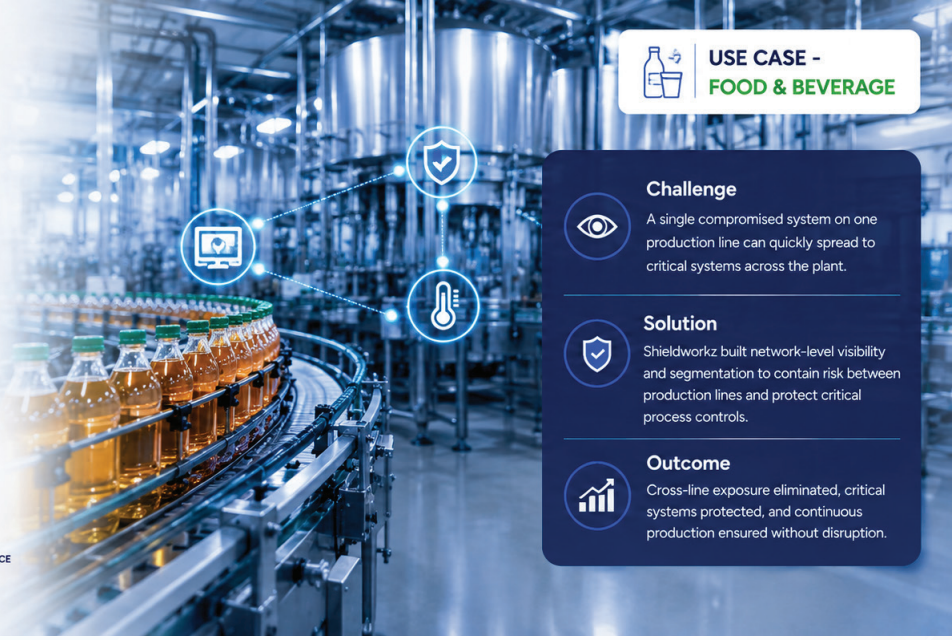
SHIELDWORKZ

Protecting Production Automation Systems from Cross-Line Exposure

> One infected HMI on the packaging line was ***three network hops away*** from the pasteurizer's temperature controls.

VISIBILITY ACROSS PRODUCTION LINES | ISOLATE & PROTECT CRITICAL SYSTEMS | DETECT LATERAL MOVEMENT | MAINTAIN UPTIME & COMPLIANCE | REDUCE RISK, INCREASE RESILIENCE



USE CASE - FOOD & BEVERAGE

Challenge
A single compromised system on one production line can quickly spread to critical systems across the plant.

Solution
Shieldworkz built network-level visibility and segmentation to contain risk between production lines and protect critical process controls.

Outcome
Cross-line exposure eliminated, critical systems protected, and continuous production ensured without disruption.

A beverage bottling and canning plant found malware on a packaging-line HMI and discovered, mid-investigation, that the packaging network had a direct path to the pasteurization and CIP systems responsible for food-safety-critical temperature holds. Shieldworkz confirmed the infection never reached those systems, then rebuilt the network so the next incident can't get as close.

THE CHALLENGE

The malware itself was contained quickly. What took longer was proving it had never reached the systems that actually keep the product safe.

Flat Production Network
Mixing, pasteurization, filling, and packaging automation shared a single network with no isolation between lines.

Food-Safety-Critical Systems Exposed
CIP and pasteurization temperature controls sat on the same segment as general packaging and labeling equipment.

Unpatched Packaging HMIs
Several packaging-line HMIs ran unsupported software, with no patch plan because the line couldn't stop to test updates.

No Containment Plan
When the infection was found, there was no fast way to confirm it hadn't reached process-critical controls.

HACCP Documentation Pressure
A compromised process control system could force a product hold, and the plant had no quick way to prove system integrity.

Use Case Overview
Confirm the packaging-line infection never reached pasteurization or CIP, then separate food-safety-critical process control from general packaging and labeling equipment so the next incident has nowhere to spread.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery
Every PLC, HMI, and controller across mixing, pasteurization, filling, and packaging mapped without stopping the line.

IEC 62443 Zone & Conduit Model
Food-safety-critical zones separated from general production equipment zones across the plant.

Network Segmentation
Pasteurization and CIP temperature controls isolated from general packaging and labeling equipment.

OT SOC & Managed Monitoring
Alerts routed to a team watching specifically for attempts to cross between zones.

OT NDR & Continuous Monitoring
Traffic watched for movement attempts between segments and activity tied to the infected HMI's history.

Incident Response Readiness
A tested isolation runbook for the packaging network that doesn't require shutting down pasteurization or CIP.

Malware Containment & Verification
Confirmed the infection never reached pasteurization or CIP before the incident was closed out.

HACCP Compliance Mapping
Controls documented to support food safety audits and prove system integrity quickly if asked.

OT Vulnerability Assessment
HMI and PLC software versions reviewed, with a patch plan built around existing production windows.

Patch Scheduling Governance
A documented process for updating packaging HMIs around planned production windows.

HOW IT WORKED

Discover

Mixing, pasteurization, filling, and packaging automation mapped across the plant.

Contain & Verify

Infected HMI isolated and traffic history reviewed to confirm no lateral spread.

Segment

Pasteurization and CIP separated from general packaging and labeling equipment.

Harden

HMI and PLC software reviewed, with patching scheduled around production windows.

Monitor

Cross-segment traffic and HMI activity handed to the managed OT SOC.

BUSINESS OUTCOMES

- Confirmed the packaging-line infection never reached pasteurization or CIP controls
- Food-safety-critical process control fully separated from general packaging and labeling equipment
- Full inventory of PLCs, HMIs, and controllers produced across all four production lines
- Cross-segment traffic attempts now flagged automatically instead of requiring a manual investigation
- HACCP audit documentation ready to demonstrate system integrity on short notice
- Patch plan in place for packaging HMIs with no new impact to the production schedule

Shieldworkz Threat Research Lab Insight

Food & Beverage is becoming a high-value target for industrial ransomware. Dragos recorded 75 ransomware incidents targeting the Food & Beverage manufacturing subsector in Q1 2025, representing 16% of reported manufacturing incidents. Shieldworkz Threat Research Lab's 2025 analysis, based on 50,000+ honeypots and wireless sensors, also found that automated attacks can reach critical networks in under 24 hours-making network segmentation and continuous OT monitoring essential for preventing cross-line exposure.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through containment, segmentation, and ongoing monitoring under one team.

Food & Beverage Expertise

Responders familiar with pasteurization, CIP, filling, and packaging line operations.

Zero-Downtime Segmentation

Network changes built around existing production schedules, not against them.

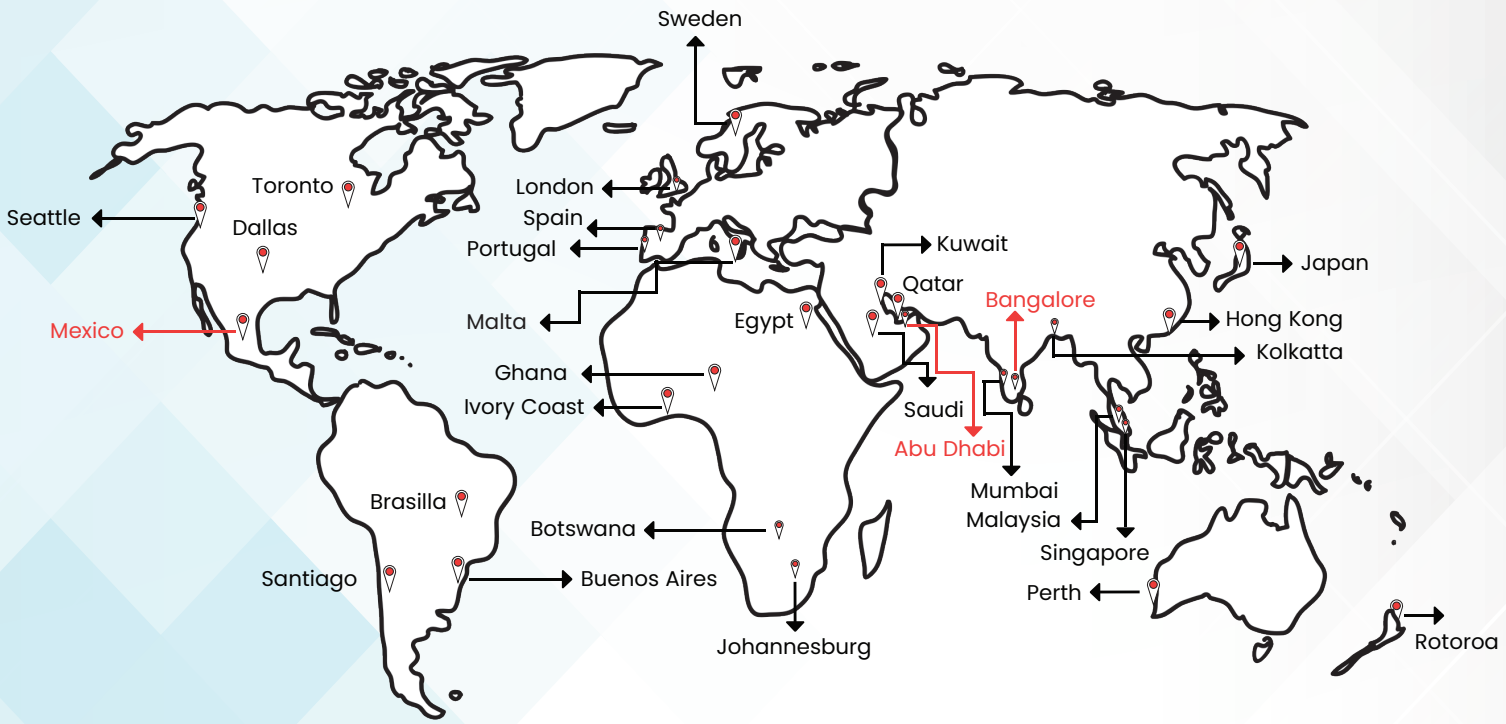
Standards-Based Approach

Zone and conduit separation aligned to IEC 62443 practice for process-critical systems.

Managed OT SOC

Ongoing monitoring handed to a team that watches OT traffic, not just IT alerts.

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us

GERMANY

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

CANADA

396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com

UAE

Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

INDIA

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com