SHIELDWORKZ

USE CASE | Manufacturing Industry

Secure
Remote Vendor Access
for Maintenance Engineers

Four vendors, four remote tools, one plant: that could not say who was connected.

A dairy and beverage processor running pasteurization, homogenization, and filling lines at a single site depends on four equipment vendors for ongoing maintenance support. Each vendor had set up its own remote access tool directly on plant systems, and plant IT had no consistent way to control, log, or revoke that access. The engagement centralized vendor remote access without slowing down maintenance response.

THE CHALLENGE

Manufacturers are increasingly targeted by ransomware operators looking to disrupt operations and force a payout. Once malware reaches the OT network, it can halt PLCs, corrupt recipe and configuration data, and stop a line mid-shift.

No Centralized Control
Four OEM vendors each ran their own remote access tool directly on plant systems.

Standing Connections
Remote clients stayed installed and reachable well outside any maintenance window.

Shared Credentials
Some vendor tools were accessed through logins shared across several technicians.

No Session Visibility
Plant IT could not say what a vendor actually did once connected.

Customer Audit Pending
A major retail customer's audit required proof of controlled third-party access.

Use Case Overview
Replace four independent vendor remote access tools with one controlled gateway, scoped to only the systems each vendor needed, without slowing down maintenance response.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery
Helps trace an incident to a specific change, not just a general alert.

Secure Access Gateway
Four separate vendor tools consolidated into one broker with approval workflows.

Least-Privilege Scoping
Each vendor's access limited to their own equipment, not the wider network.

Time-Bound Sessions
Connections tied to an approved maintenance window instead of standing access.

Session Recording
Every remote session logged for review, replacing informal vendor-side logs.

Network Segmentation
Remote access gateway separated from the rest of the control network.

Vulnerability Review
Workstations that had hosted the old remote tools reviewed for exposure.

Governance Documentation
Access policy and audit trail prepared for the customer's review.

OT SOC Alerting
Session activity outside an approved window triggers a flagged alert.

Vendor Onboarding Process
A repeatable process defined for adding or removing vendor access.

HOW IT WORKED

Discover

Every existing remote access path and vendor tool mapped across the plant.

Scope

Least-privilege access defined per vendor based on their actual equipment.

Architect

Gateway placement planned to avoid disrupting pasteurizer HMI access.

Deploy

Rollout to each vendor with old and new tools run in parallel.

Validate

A live test session run with each vendor during a scheduled visit.

BUSINESS OUTCOMES

- Four separate vendor remote access tools consolidated into a single controlled gateway
- 100% of vendor sessions now logged and tied to an approved time window
- Vendor access scope reduced to only the systems covered under each service contract
- Audit documentation delivered ahead of the retail customer's third-party access review
- No measurable increase in vendor response time recorded during the transition
- Standing, always-on remote connections eliminated across all four vendor relationships

> **Our vendors still get in when they need to. We just know who, when, and to what now.**
>
> Maintenance Manager, Beverage and Dairy Manufacturer

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through scoping, deployment, and monitoring under one team.

OT-Specific Expertise

Engineers who understand plant maintenance workflows, not just access tools.

Built Around Maintenance

Access controls designed to fit existing shift and vendor schedules.

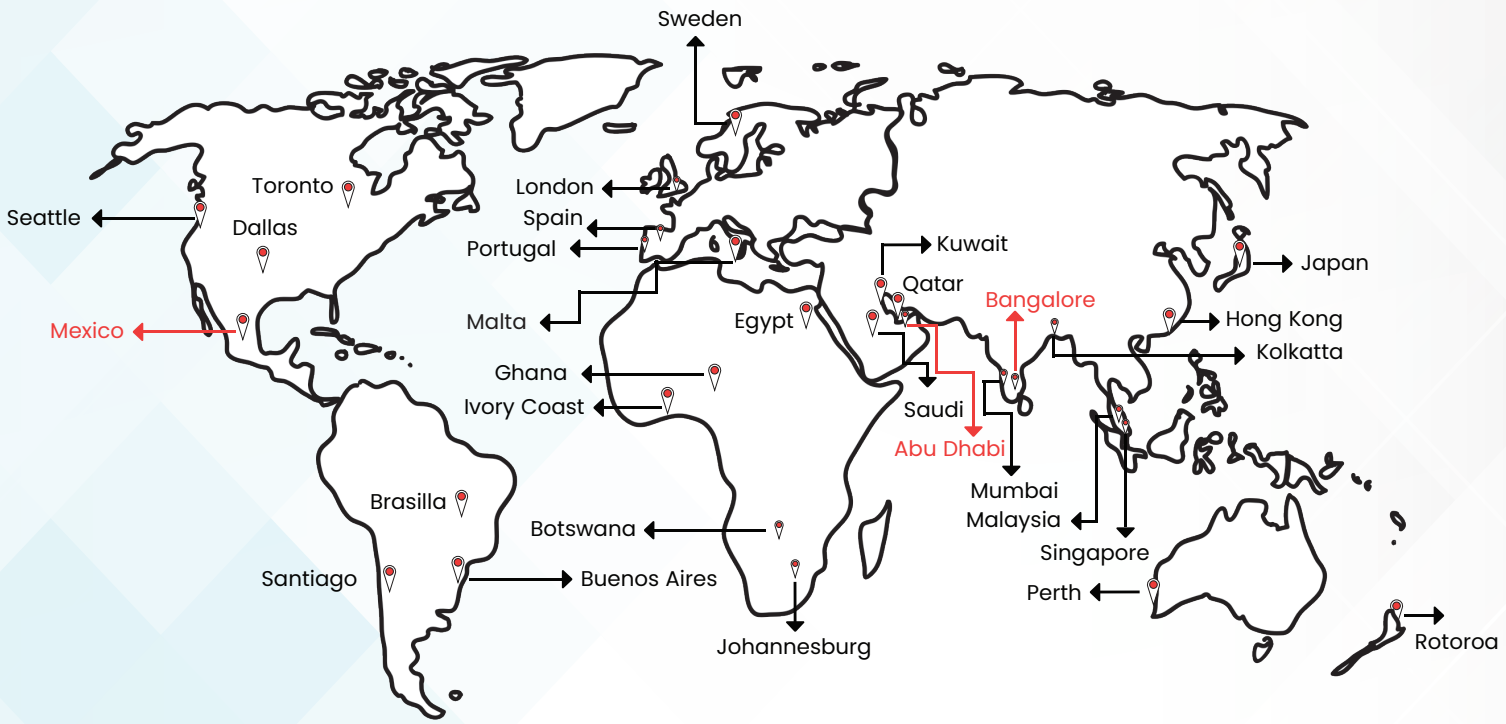
Vendor-Neutral Approach

Works across multiple OEM vendors instead of favoring one platform.

Standards-Based Records

Access policy and logs delivered in a form that supports customer audits.

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