

MANUFACTURING SOLUTION GUIDE

The Zero Trust Factory



THE CHALLENGE

Six challenges for manufacturing CISOs

Most teams securing factories and OT know what an incident would do to the plant. They want to make the change. The hard part is doing it without impacting production.

REDUCE THE RISK OF A FACTORY SHUTDOWN 01

Most OT networks are flat below Purdue Level 3.5. Malware on a single workstation can reach the historian, the PLCs, then the next line.

AI-DRIVEN ATTACKS ON LEGACY OT 02

Attackers use AI to find and chain weaknesses in minutes. Many OT systems on the floor are decades old. They can't run agents or be patched.

SLOW, RISKY CONTRACTOR ACCESS 03

OEM technicians need access to fix machines or update firmware. That usually means a vendor VPN with broad access, or someone gets on a plane.

SENSITIVE DATA IN PUBLIC AI TOOLS 04

Engineers already use AI. A process engineer pastes PLC fault logs into a chatbot to save time. Blocking AI doesn't work. People go around it.

RISING COMPLIANCE PRESSURE 05

EU CRA (2026) reporting duties are live. CIRCIA's final rule is in White House review. U.S. Zero Trust for OT guidance (2026) raises the bar.

SLOW, RISKY M&A INTEGRATION 06

Every acquired factory brings its own network and devices. Overlapping IPs and VLANs can stall integration for months. You inherit its risk on day one.



SECURE THE FACTORY FLOOR

Keep the factory floor running

Zero Trust Branch + Zscaler Cellular

Reduce the risk of a factory shutdown

CAPABILITY Discover and classify every OT and IoT device, then set which devices can talk by make, model, and zone. Zscaler Cellular brings the same policy to SIM-connected handheld scanners and devices.

WHY ZSCALER **No agents or VLAN changes.** Outbound-only connections, so nothing is exposed to the internet.

OUTCOME Isolate ransomware to a single device and shrink the blast radius.

90 device types segmented, zero agents

Kingston Technology

"The utilization of the platform, in terms of segmenting assets, can be done in minutes."

John Leitgeb, IT Director and CISO

Read the story →

Zscaler Deception

Catch AI-driven attacks on legacy OT

CAPABILITY Deploy decoy historians, HMIs, and workstations across IT and OT.

WHY ZSCALER **No SPAN ports or network changes.** No real user touches a decoy, so every alert counts, whether the attacker is a person or an AI agent.

OUTCOME Catch anything scanning your OT and IT environments, fast.

80+ high-priority attacks intercepted in 90 days

Persistent

"Zscaler Deception has detected more than 80 notable attacks over a 90-day period, including 31 high-risk attacks."

Debashis Singh, Chief Information Officer

Read the story →



SECURE ACCESS AND AI

Enable secure contractor access and safe AI use

Zscaler Privileged Remote Access

Fast, least-privilege contractor access

CAPABILITY Contractors reach only the one HMI or engineering workstation a work order needs, never the network. Browser-based RDP, SSH, and VNC, time-boxed and recorded.

WHY ZSCALER **Nothing to install.** No inbound firewall holes. Copy/paste and file-transfer controls inside the session.

OUTCOME Access in minutes, with recordings for IEC 62443 and NIS2 audits.

$500K+ travel saved across 100+ sites — **Eaton**

"Our playbook isn't exotic. What made it work was sequencing and trust as much as technology."

John Millsaps, Senior Manager, Cybersecurity Engineering

Read the story →

Zscaler AI Guard + Data Protection

Keep sensitive data out of public AI tools

CAPABILITY Discover every AI app in use, then allow, caution, or block it. Inspect prompts to stop PII, CAD files, and process data from leaving.

WHY ZSCALER **Policy per user, per app.** One unified platform for OT, users, and AI.

OUTCOME Engineers keep their AI tools. Designs and config files stay in-house.

GenAI caution pages coach employees on safe use — **BorgWarner**

"We want to empower our employees to use AI so that they can be more productive."

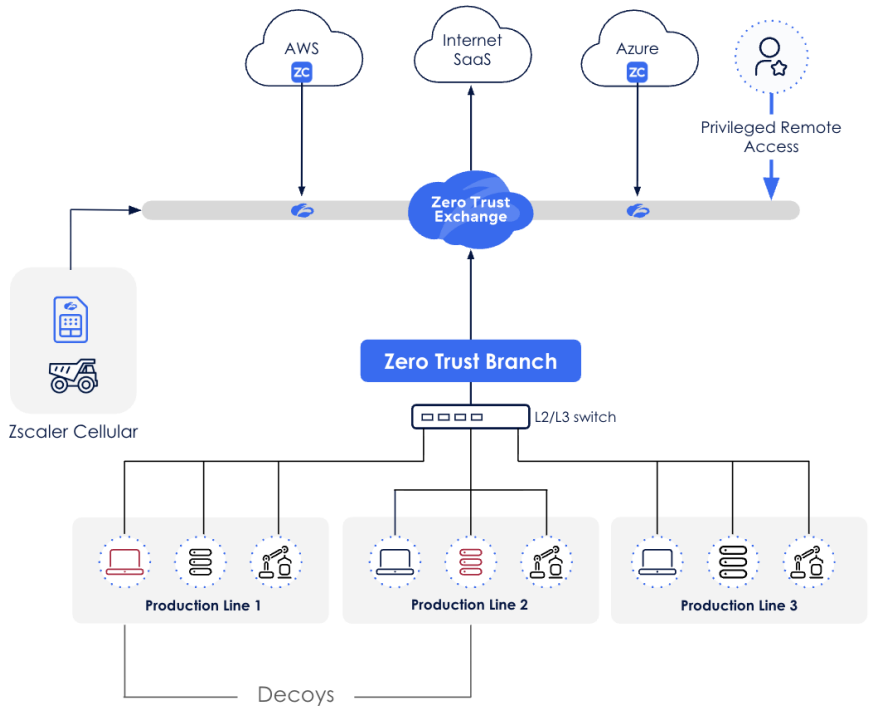
Mark Williams, IT Director, Global Network Engineering

Read the story →



HOW IT FITS TOGETHER

One Zero Trust Exchange, from cloud to PLC



Zero Trust Branch
Segments every device on each production line.

Zscaler Cellular
Same policy for SIM-connected equipment.

Privileged Remote Access
Contractors reach one asset, never the network.

Deception
Decoys on the line flag lateral movement.

AI Guard + Data Protection
Keeps sensitive data out of public AI apps.

OUTCOMES

75%
faster M&A integration
BorgWarner →

6 mo
faster M&A integration
Siemens →

~100%
attack surface reduction
AkzoNobel →

<1 hr
to onboard an acquisition
Sanmina →

Faster, safer M&A integration
Acquired sites get app access on day one, without merging networks.

Audit-ready compliance
Recorded contractor sessions and device-level policy give evidence for IEC 62443 and NIS2.

Build your Zero Trust Factory

No agents and no downtime to deploy.

Request a demo

Explore manufacturing