IGEL Zero Trust Platform for OT Environments

Compliance Starts at the Endpoint. Immutability Makes It Continuous.

The Challenge: Compliance Without Disruption

Operational Technology (OT) organizations face increasing pressure to strengthen security and resilience across critical infrastructure systems, including SCADA, DCS, PLCs, and HMIs that support industrial and manufacturing operations. Many of these environments still depend on older technology that was never designed to withstand today's cyber threats or meet modern compliance standards.

IGEL addresses this challenge with its Preventative Security Model™, protecting OT endpoints at the source. Using a read-only, immutable endpoint operating system built on Zero Trust principles, organizations can meet compliance requirements such as CMMC 2.0, IEC 62443, and NIST 800-82 without introducing production risk or downtime.

IGEL ensures every session begins from a known, secure, validated state. Endpoints cannot drift, store local data, or accumulate unauthorized software, reducing attack surfaces and assuring compliance.

Key Benefits for OT Environments

Zero Trust Enforcement at Scale	IGEL extends Zero Trust into OT by validating every user, application, and connection before access is granted. Policy-based segmentation isolates critical assets while maintaining operational continuity without requiring an infrastructure overhaul.
Attack Surface Elimination	Reduces the attack surface through immutable OS architecture that prevents malware, ransomware, or unauthorized changes from persisting or executing on the endpoint even if perimeter defenses are breached. IGEL eliminates the need for traditional antivirus scanning that can interfere with real-time industrial control systems, simplifying endpoint operations and updates.
Centralized Operational Control	With IGEL's Universal Management Suite (UMS), organizations can enforce policies and maintain version control across thousands of distributed OT endpoints. Provides complete configuration auditability and change control—critical for CMMC 2.0, IEC 62443, and SOC 2 compliance requirements. Supports phased rollouts and instant rollback capabilities without production downtime.
Legacy Application Protection	Securely isolates legacy Windows applications, including SCADA clients, HMIs, and engineering workstations, through containerization. This extends the life of critical operational services while protecting the underlying OS from exposure to vulnerabilities.
Reduce Endpoint TCO	By extending hardware lifecycles and centralizing endpoint management, organizations can reduce maintenance costs, simplify operations, and minimize costly hardware replacement.

Why IGEL

IGEL is purpose-built to secure and modernize OT endpoints without disrupting industrial operations. Unlike traditional security approaches that rely on layered agents, patching cycles, and reactive controls, IGEL delivers compliance and resilience through an immutable, Zero Trust endpoint foundation.

By enforcing a known-good state, eliminating endpoint drift, and enabling centralized policy control at scale, IGEL helps OT organizations reduce risk, meet regulatory requirements, and protect critical infrastructure—while keeping production systems running safely and continuously.

Achieve compliance without compromise.

Talk to an IGEL OT security expert to see how Zero Trust endpoint OS can be deployed without disrupting production.