FREEWAVE

Fixing the Access Issue While Securing the Floor

Today's manufacturing engineers are required to physically access equipment on the plant floor up to several times daily to collect data or make programming adjustments. This results in engineers making multiple round trips to facilities throughout the day. Some engineers claim to log a mile or more on foot when the shop floor is located far from their office.

Over the course of the year, that's more than 50,000 steps – or 26.2 miles, the length of a marathon.

Yet, instead of earning a medal, operations personnel face even more time inefficiency. They must then contact their IT department for access before connecting to the equipment with a flash drive or USB port to make updates, collect data, or load new programs. Using flash drives to extract the data they need is the most common method. But that poses additional issues like procurement challenges; if they lose the flash drive, it's a big deal, and if there are updates, sometimes they can get locked out. Third-party users extracting machine data poses extra challenges: their access to machinery becomes a hackable event.

The Zentry™ solution from FreeWave gives manufacturing teams secure, remote control of manufacturing equipment to save time, money – and steps.

The Technology Behind the Solution

The Freewave Zentry solution is a robust zero trust security solution that strengthens edge asset connectivity by protecting industrial and enterprise IoT networks. The Zentry solution enables remote access for systems management and protects the data residing in machines. Advanced cybersecurity gives organizations the ability to address threats like endpoint vulnerabilities, system disruptions, and data breaches before they impact operations.

Zentry technology leverages zero trust architecture to shift cybersecurity from reactive to proactive and secures networks of any size or complexity. Unlike traditional perimeter-based defenses, the platform authenticates every user and device at every connection point, reducing vulnerabilities and containing potential threats with precision. It also makes remote access to machinery on the factory floor possible without the intervention of the IT department. FreeWave brings Zentry technology to the manufacturing environment. Organizations gain dependable protection with seamless integration, future-ready scalability, and regulatory compliance support.

Connecting Engineers With Machine Data

While connecting devices remotely can be simple in some environments, doing so for high-security, isolated networks is complicated. The Zentry solution is a Remote Engineering Access Platform (REAP) that is ideal for AS9100 or ISO 9001 facilities operating on isolated or restricted networks due to ITAR (International Traffic in Arms Regulation) and EAR (Export Administration Regulations) data protection. The platform's robust technology maintains invisibility and end-to-end network protection while enabling secure connections and bypassing firewalls.

FreeWave Zentry solution offers auditable, scalable remote access for engineers. It boosts productivity and reduces downtime by eliminating the need for physical access to equipment. The solution keeps engineers productive while simultaneously freeing the IT Department of routine and repetitive access control duties.

Key benefits of remote connectivity for engineers include:

- Faster access to data without IT intervention
- Smooth navigation through security restraints
- Simple, fully remote file transfer to equipment
- Quicker diagnostics through remote data collection
- Enabled after-hours and off-site engineering support
- Scalable to hundreds of controlled devices for increased efficiency

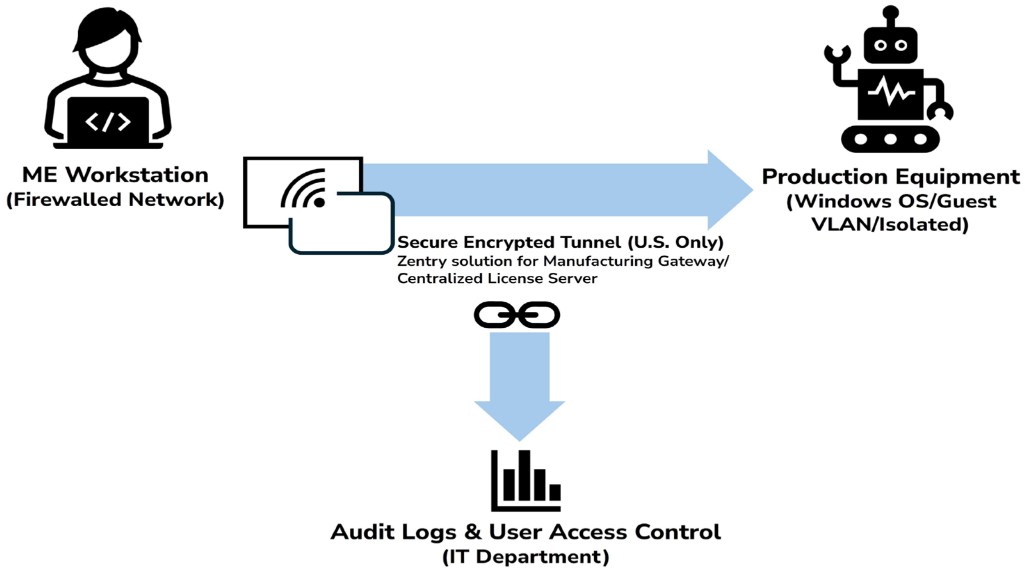
Endless Uses for Manufacturing Engineers

The Zentry solution maintains security compliance with remote capabilities. Once connected, manufacturing engineers can remotely view, control, and update equipment software in compliance with regulatory standards and corporate IT security policies. With the Zentry solution, it's simple to connect engineers with a diverse range of production equipment. Examples include:

- Laminate laser projectors
- Robotic systems
- Dispensing and welding controllers
- Robotic tube benders
- Precision Welders
- Chemical processing control computers
- Autoclave systems
- SMT pick and place machines
- Automated optical inspection equipment
- Oven control systems

System Overview

- **Requirement:** Executed via the Freewave Zentry solution. Secure connection from the engineer workstation to the equipment on the guest VLAN or isolated network.
- **Operating System:** Works on most legacy Windows operating systems and limited Linux or proprietary systems.
- **Network Structure:** Air-gapped or segmented networks with isolated VLANs and guest Wi-Fi for equipment access. Engineering workstations reside on firewalled internal networks.


ME Workstation
(Firewalled Network)
Production Equipment
(Windows OS/Guest
VLAN/Isolated)
Secure Encrypted Tunnel (U.S. Only)
Zentry solution for Manufacturing Gateway/
Centralized License Server
Audit Logs & User Access Control
(IT Department)

- **Access Method:** Fully remote. Replicates the full user interface.
- **File Transfer:** Possible through limiting the access to functions like SMB in Windows to identities. If users have the ability in the Zentry console, then they can do it on the machine.
- **Session Control:** Allow one or many users for different types of sessions. As an example, with VNC it allows multiple sessions to be working simultaneuously, and each session can be controlled to who has abilities within the session.
- **Logging:** Full audit trail.
- **Encryption:** AES-256 or higher.
- **Access Scope:** Internal LAN or U.S.-restricted VPN.
- **Admin Roles:** IT controls users; Manufacturing Engineering controls devices.
- **Performance:** Latency <100ms typical.
- **IT Oversight:** Minimal IT involvement beyond initial security vetting and user account management.

Security and Compliance Considerations

- **Data Jurisdiction:** All connections and stored data remain in compliance with the U.S. ITAR/EAR compliance.
- **Air-Gap Preservation:** REAP functions across approved VLANs and does not bridge external networks.
- **IT Vetting:** One-time approval process for engineering workstation installation. IT maintains user permissions while ME manages node enrollment.
- **Audit and Monitoring:** Automated session logs retained for compliance review.
- **AS9100 Compliance:**
  - Clause 8.5.1 – Control of production and service provision.
  - Clause 9.1.2 – Monitoring and measurement of processes.

Deployment That Grows With Your Enterprise

The FreeWave solution is modular and easy to expand with minimal IT dependency. Enterprises can pilot the system with one engineer and three devices, with deployments of more than 200 engineers in one facility using 1,000+ devices.

The IT Department is responsible for security review, licensing, and user control. The Manufacturing Engineering Department or Operations is responsible for configuration, installation, and operation. Authorized engineers can add or remove authorized users.

The entire solution has been designed to streamline data exchange between engineers and equipment, relieving the IT department of repetitive, unnecessary access control activities.

Are You Ready?

Learn what FreeWave can do for your operation. Contact sales@freewave.com or call 866-923-6168 to schedule a demo. Unleash the data in your machines for faster decision-making – and less steps.

Schedule a demo at www.FreeWave.com/contact or reach out at sales@freewave.com. Together, let's make your industrial world simple, secure, and connected.

SCHEDULE A DEMO →

FREEWAVE CORPORATE HEADQUARTERS

5395 Pearl Parkway
Boulder, CO 80301

Email: insidesales@freewave.com
Visit: freewave.com

Toll Free +1 866.923.6168
Local +1 303.381.9200
FW_ZUC002_0126