SOLUTION OVERVIEW

Zero Trust Networking for Smart Manufacturing

Adding Security Segmentation for the Factory IT/OT Environment

Industry 4.0 Exposes Factories to New Threats

Manufacturers are constantly looking to upgrade their factories; infrastructure improvements and automation can bring down costs, improve yields, and help the manufacturer beat the competition. Most of the time, upgrading involves plugging new and intelligent computing or even cloud-based services into existing factory networks. However, many factories were designed with shared flat networks for legacy reasons, which provides an ideal platform for cybersecurity attack proliferation. With costs of idling a production line potentially exceeding $1 million per *hour*, manufacturers need effective ways to segment and protect this converged IT/OT environment.

Enter CoIP Platform: Zero Trust Networking

Incorporating the latest security best practices to make the factory a hard target and to limit the scope of potential damage are among the best ways for manufacturers to add defense-in-depth to existing factories. Zentera's Zero Trust Networking (ZTN) has been selected by major enterprises to secure IT applications; those same capabilities also enable secure IT/OT convergence. CoIP Platform's segmentation dramatically reduces the attack surface, blocking malware propagation from new applications to legacy applications, enabling secure connectivity as well as segmentation to cloud services without opening firewalls, and reducing the chance for data exfiltration.

CoIP® Platform for Smart Manufacturing

- Industry best-practice Zero Trust Networking
- Secures data in motion, from the server all the way to the client
- Layers on existing networks to protect both modern as well as legacy devices
- Blocks malware and other threats from spreading in shared flat networks
- Creates virtual micro-segmented zones
- Granular protection down to the app or container level

CoIP Platform deploys into a factory environment to protect legacy and modern equipment with device-level controls. Its powerful policy engine enables access permissions to be defined based on a combination of certificates and packet header information, with mutually-authenticated and encrypted tunnels protecting application traffic against snooping as it travels through the network. And, critically important, a CoIP-based ZTN can be set up in a factory without requiring rewiring or reconfiguration of the existing network and firewall infrastructure.

zentera™

CoIP Platform: Zero Trust with Overlay Networking Technology

Zentera's CoIP Platform allows enterprises to build an overlay network to meet the Zero Trust Security model without network redesign. This overlay ZTN is a proxy-based Layer 5 session network, built on top of the underlay L3 IP network. All core components of CoIP Platform are implemented as servers on the existing IP network, connected by "web proxy"-style SSL tunnels, enabling Zero Trust Security to be added to existing networks without changing the underlying IP network.

All applications inside a ZTN are cloaked and invisible to other applications running on the same network, with centrally-defined communication and security policies.

Manufacturers can use Zentera's CoIP Platform to:

- Segment sensitive manufacturing applications and devices from other applications
- Securely extend application connectivity from the factory floor to datacenters, office environments, and private/public clouds
- Establish zero trust connections that span across multiple segmented network regions
- Enable remote user access with strong role-based access controls that enforce principles of least privilege and minimal access

CoIP Platform Zero Trust Networking for Manufacturing