Zero Trust Boundary Security for IT/OT Convergence

Enabling Industry 4.0 Without Increasing Risk

Industry 4.0 Exposes Factories to New Threats

The inexorable drive for competitive advantage is driving new IT business processes into existing Operational Technology (OT) environments. Most of the time, these new initiatives involve plugging new, intelligent and even cloud-based services into existing OT networks. However, OT networks are typically full of legacy servers, with far fewer protections than their IT server cousins. With costs of idling a production line potentially exceeding $1 million per *hour*, companies need effective ways to secure the boundary of the converged IT/OT environment to enable transformation without risk.

Enter Zero Trust Application Networks

Incorporating the latest Zero Trust Security best practices to harden the OT environment and to limit the scope of potential damage are among the best ways for manufacturers to add defense-in-depth to existing facilities. Zentera's CoIP Platform creates Zero Trust Application Networks (ZTAN), which provide zero trust connectivity for specific and sensitive applications. ZTAN enables application segmentation that dramatically reduces the attack surface, enabling only certain applications to communicate while blocking malware propagation across the OT boundary. Additionally, CoIP Platform's ZTAN allows the underlay firewall to implement a network "air gap," effectively protecting legacy servers against new zero day threats.

CoIP Platform's powerful policy engine enables access permissions to be defined across the IT/OT boundary based on application, user, and endpoint identity and policy. Mutually-authenticated and encrypted tunnels limit specific application traffic as it travels through the network. And, critically, CoIP Platform can overlay rapidly to add protection to brownfield facilities without requiring re-engineering or reconfiguration of the existing network and firewall infrastructure.

Zero Trust Boundary Security for IT/OT Convergence

- Rich visualization and risk scoring for application traffic crossing the IT/OT boundary
- End to end security for Industry 4.0 application traffic
- Protects legacy servers against zero day threats
- Continuous monitoring of the IT/OT security posture and alerting
- Zero Touch, non-disruptive deployment – no rip and replace

CoIP Platform: Zero Trust with Overlay Proxy Network Technology

CoIP Platform allows enterprises to build an overlay network to meet the Zero Trust Security model without network redesign. The overlay ZTAN it creates 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

zentera™

network, connected by “network proxy”-style SSL tunnels, enabling Zero Trust Security to be added to existing networks without changing or disrupting the underlying IP network.

All applications inside a ZTAN are securely protected as well. They are cloaked and invisible to other applications running on the same network, with centrally-defined communication and security policies.

CoIP Platform Protects the IT/OT Boundary by:

- Segmenting sensitive OT applications and devices from untrusted IT applications
- Securely extending application connectivity from the OT environment to datacenters, office environments, and private/public clouds
- Establishing zero trust application connections across multiple segmented network regions
- Enabling remote user access with strong role-based access controls that enforce principles of least privilege and minimal access