



Secure IT/OT Convergence

Defending OT Operations with
Zero Trust Security Segmentation and Controls

zentera™

Hackers Are Increasingly Targeting OT Networks

Information technology (IT) and operational technology (OT) networks have traditionally been separate domains. IT networks, which support enterprise computing and applications, prioritize *confidentiality* of the data they contain – financial performance, customer lists, and so on. OT networks, on the other hand, drive revenue production for the business, and therefore prioritize *availability* – any downtime instantly results in lost revenue and may even present a safety hazard.

These details haven't escaped hackers, who have figured out how motivated OT companies are in keeping facilities operational. With ransomware and cryptocurrency making cyber extortion simpler than ever, the surge in reconnaissance activity against OT networks is bad news.

\$4.24M

Average Cost of a Breach
in Industrial Sector²

36%

Share of all OT Attacks
from Ransomware¹

2,204%

Increase in
Reconnaissance Against
OT, Jan-Sep 2021¹

Potential Risks of OT Attacks

- Financial losses from production downtime and lost work in progress
- Costs to remediate and recover
- Loss of customer confidence and brand image
- Safety and environmental hazards
- Fines, lawsuits, and liability
- Bad publicity with shareholders and stakeholders
- Non-renewal of insurance coverage

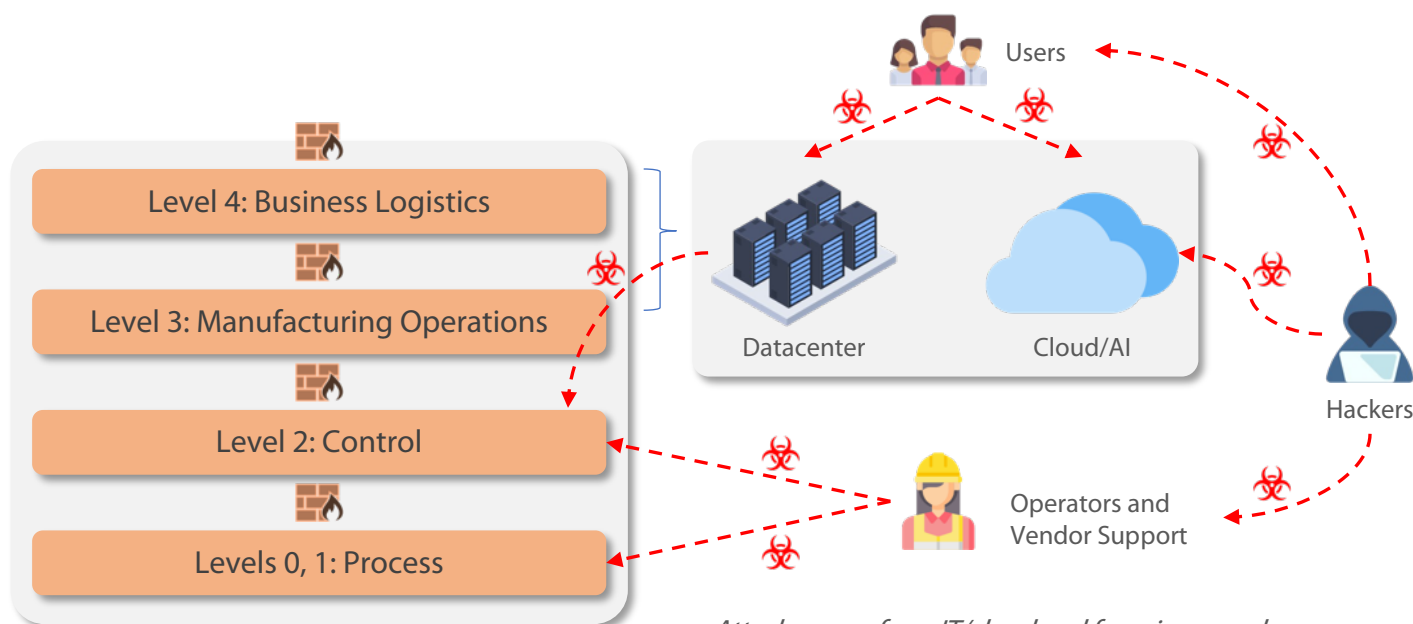
¹IBM Security, X-Force Threat Intelligence Index 2022

²IBM Security, Cost of a Data Breach Report 2021

The Divide Between IT and OT is Shrinking, and OT is More Exposed than Ever

The Purdue Reference Model for OT segmentation and security controls to protect mission-critical production assets was first proposed in 1992. While it provides a useful logical model, it is often difficult to implement using traditional, inflexible networking technologies. As a result, many OT environments are flat and even mixed with IT today. This weak cyber defense for OT is showing signs of age in today's interconnected world: IBM Security's X-Force Threat Intelligence Index 2022 reports that manufacturing was the top attacked industry in 2021¹.

It's not that the production assets have changed – in fact, most OT assets and networks are designed to last for decades. But as companies embrace Digital Transformation – adopting work from home policies and migrating business intelligence into the cloud – the expanded attack surface brings this decades-old technology face-to-face with today's modern threats.



IT/OT with Purdue Reference Model Segmentation

Attacks come from IT/cloud and from increased application access. Digital Transformation gives hackers new options to attack critical production workloads through the expansion of Level 3/4 infrastructure, as well as through compromised remote users and 3rd parties

¹<https://www.ibm.com/downloads/cas/ADLMYLAZ>

²<https://www.ibm.com/downloads/cas/OJDVQGRY>

Why OT Has Been Slow to Segment Using Traditional Techniques

The fundamental concept behind the Purdue Reference Model is sound. It makes complete sense to group OT assets into different levels based on application and criticality and control access to them. The problem is not in the concept – it's in the execution.

Network segmentation has been traditionally implemented by creating separate zones (e.g. VLAN) connected by a firewall or ACL as control points to control all cross-zone communications for devices. This approach creates many operational challenges:

Coarse Segmentation

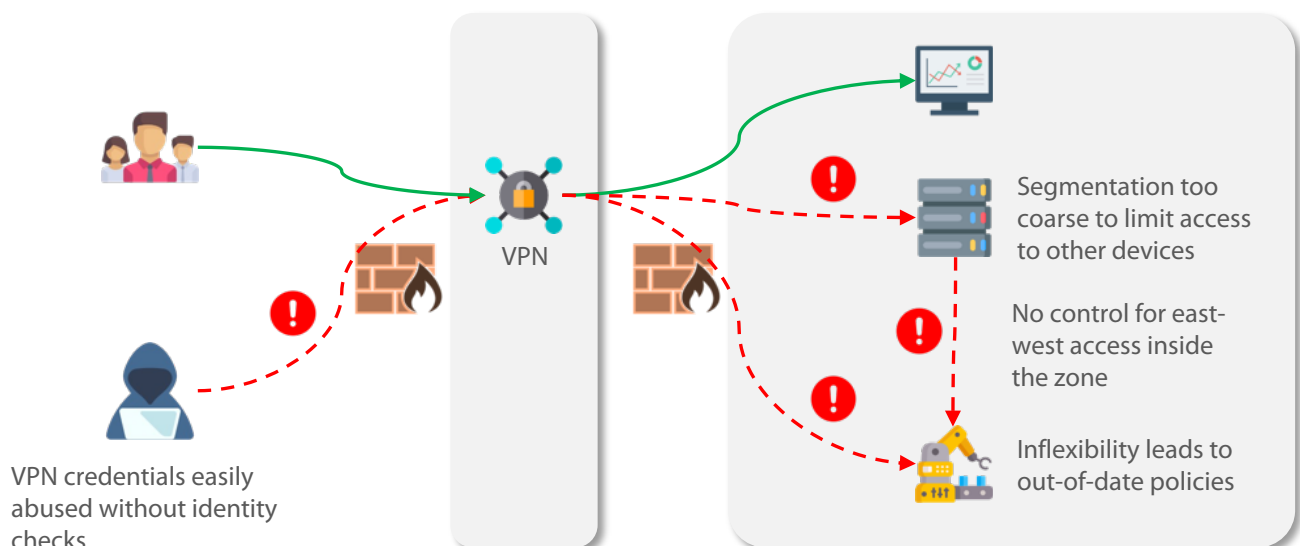
Firewalls can be prohibitively expensive. Architects may choose to reduce cost and management overhead by implementing large zones, but this makes it difficult to specify access to specific devices or workloads in the OT environment. Detailed zones using VLAN/ACL create other challenges for policy implementation and management.

Lack of Identity-Based Controls

With traditional filtering, an unauthorized user can bypass the filters simply by launching the attack from any authorized server – potentially one in the cloud or inside the OT environment.

Inflexibility

With traditional segmentation, a device's zone is tied to the network topology. Policy updates mean network reconfiguration that can trigger downtime and so are discouraged, making it hard to keep security filtering up-to-date with the needs of the business.



Zentera Defends Converged IT/OT Without a Rip and Replace

Zentera Systems' CoIP® Platform is an advanced software-defined network security solution that overlays advanced segmentation and policy-based controls across OT, IT, and cloud without an expensive rip and replace.

Once onboarded to CoIP Platform, OT assets can be protected with a Zero Trust DMZ, which enforces whitelist-based policies to allow authenticated and authorized application traffic, automatically blocking malware and ransomware. A centralized orchestrator provides a single pane of glass management experience.



"Zero Trust DMZ" for Protected Assets

CoIP Platform applies Zero Trust security policies to every single network packet to or from a protected asset, creating a virtual Zero Trust DMZ.



Strong, Policy-Driven Security

CoIP Platform policies incorporate information you can't get from the network – like user, device, and software identities. CoIP Platform makes it possible to tie every network packet to an authentication and authorization decision.



No Rip and Replace

The Micro-Segmentation Gatekeeper provides agentless deployment inline with protected OT assets, avoiding any change to network configuration or application behavior.



Unprecedented Visibility and Control

CoIP Platform learns existing traffic flows, suggesting identity-based policies for whitelisting and highlighting deviations from the defined policies.



Integrated ZTNA

Built-in secure remote access for employees, contractors, and vendors eliminates security holes created by VPN.

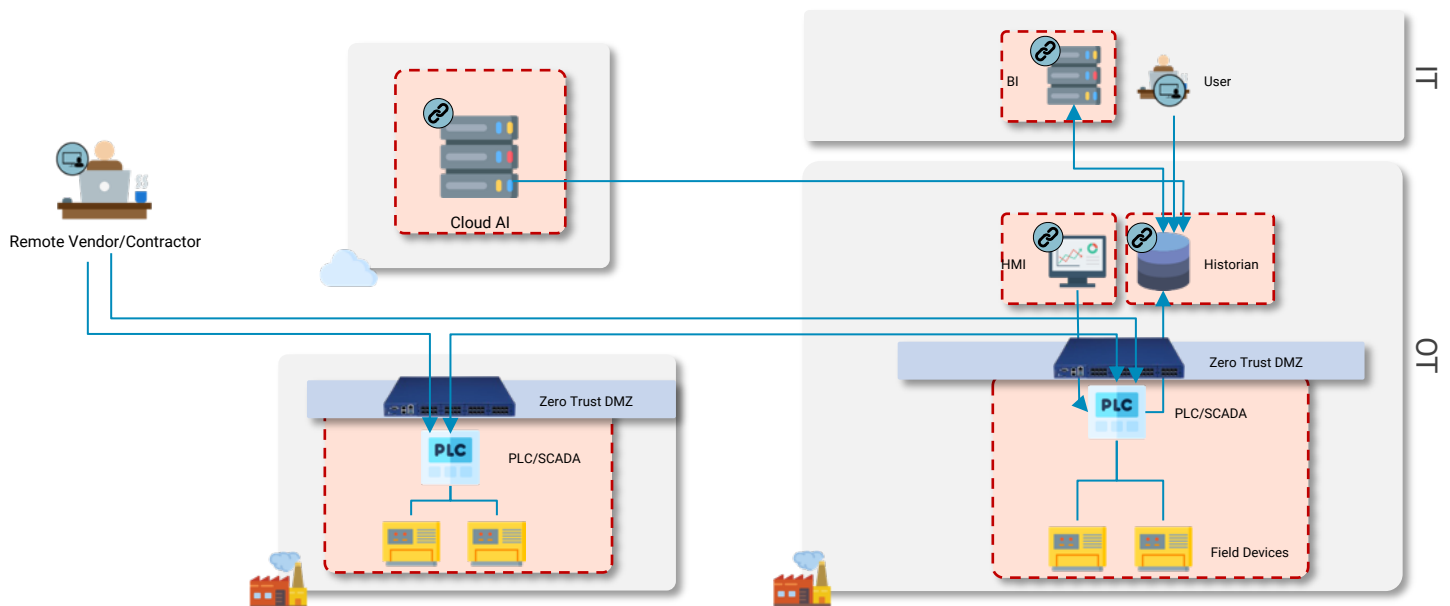


Application Network

Supports applications in IT or cloud to connect directly to specific OT assets without exposing the OT network to malware in those environments.

Apply Modern Segmentation and Controls to Any IT/OT Network

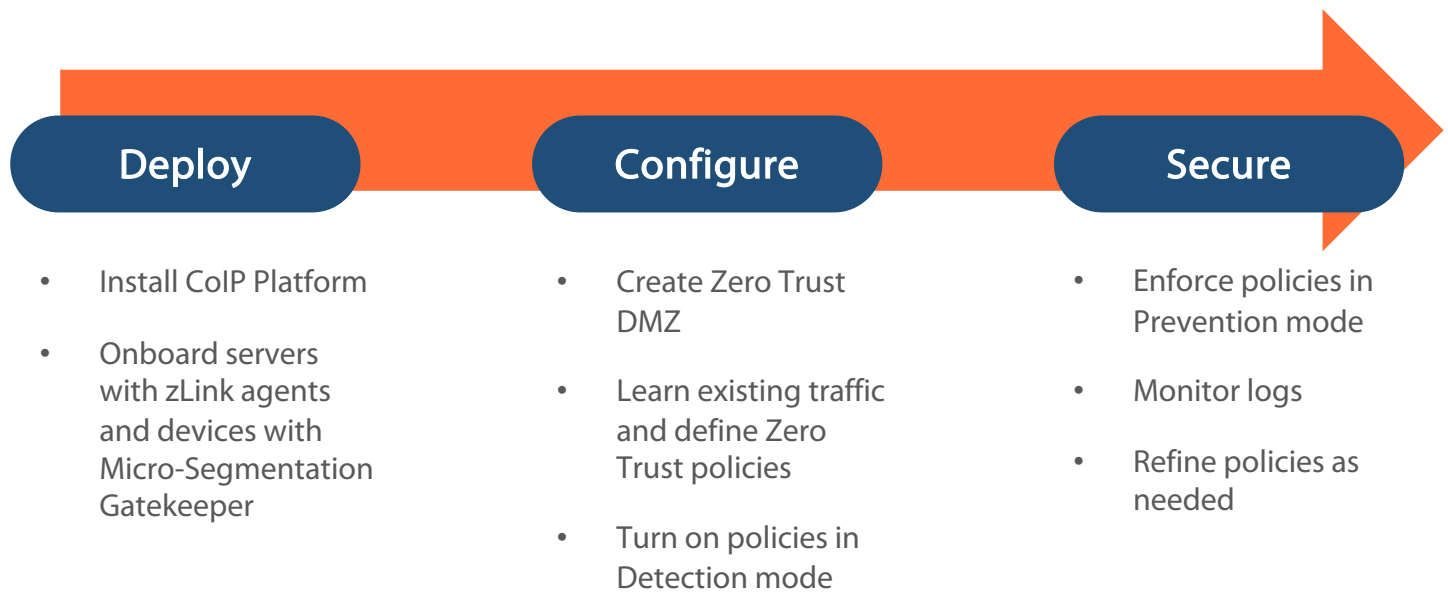
CoIP Platform enables OT administrators to create segmentation in any environment without VLANs, ACLs, or other network changes. Its combination of Application Chambers, ZTNA, and Overlay Application Network enable Zero Trust Security segmentation and controls for any converged IT/OT environment – even flat networks without any existing controls.



Advanced, Yet Simple to Adopt and Use

Adopting leading-edge network security solutions for OT doesn't have to be complex.

All it takes to get up and running is a simple 3-step process. Once in place, CoIP Platform makes it easy to build powerful Zero Trust security policies to improve your security posture.





About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

More Resources



On the web:
www.zentera.net



Email:
sales@zentera.net



Phone:
+1 (408) 436-4811

zentera™