SOLUTION BRIEF

Secure IT/OT Convergence

Defending OT Operations with Zero Trust Security Segmentation and Controls

May 2022

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 Sector[2]

36%
Share of all OT Attacks from Ransomware[1]

2,204%
Increase in Reconnaissance Against OT, Jan-Sep 2021[1]

Potential Risks of OT Attacks

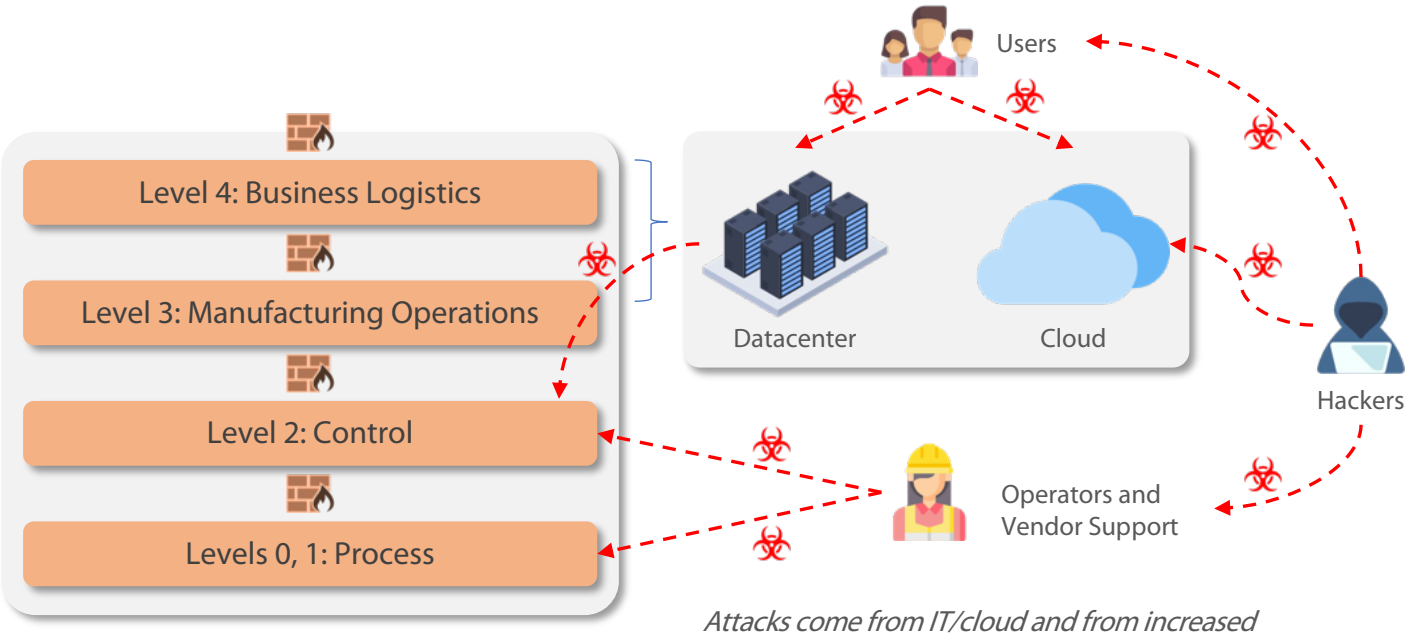
- Financial losses from production downtime and lost work in progress
- Costs to remediate and recover
- Loss of customer confidence and brand image
- Safety and environmental hazards
- Fines, lawsuits, and liability
- Bad publicity with shareholders and stakeholders
- Non-renewal of insurance coverage

[1]IBM Security, X-Force Threat Intelligence Index 2022
[2]IBM 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 in1992. 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 2021[1].

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 Traditional OT Segmentation Has Fallen Short

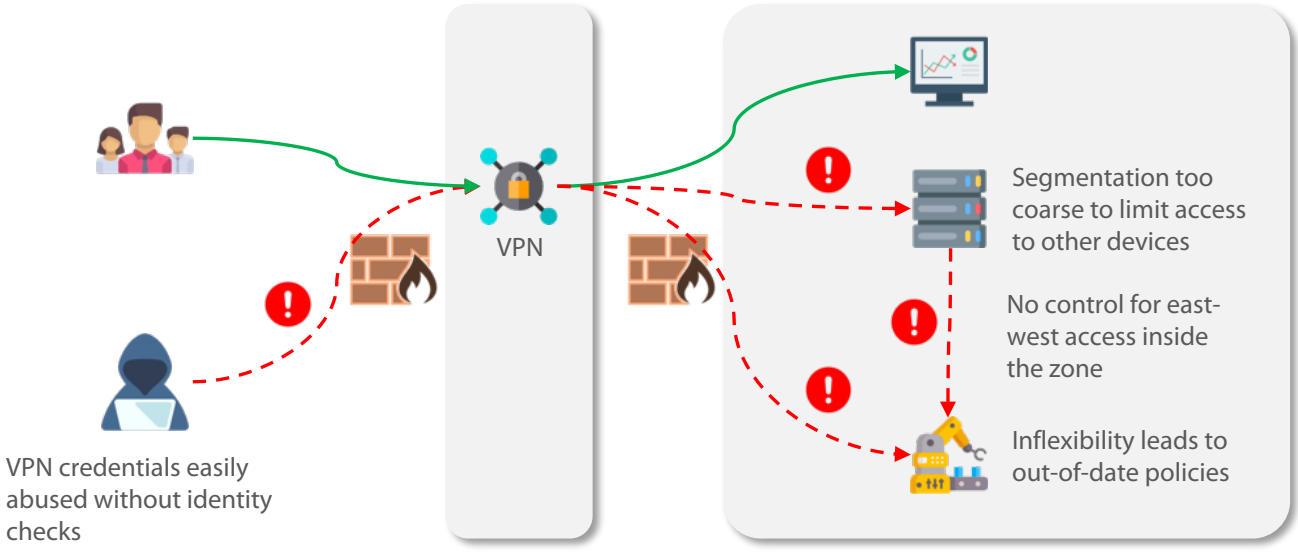
The fundamental concept behind the Purdue Reference Model is sound. It makes complete sense to group OT assets into different levels based on application and criticality and control access to them. The problem is not in the concept – it's in the execution.

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.



How Zentera Zero Trust Security Defends Converged IT/OT

Zentera Systems' CoIP® Access Platform is an advanced cybersecurity solution capable of layering application-scale segmentation and controls over existing IT and OT networks. Companies may use CoIP Access Platform as the basis of their Zero Trust plans in accordance with NIST 800-207 guidelines.

Once onboarded to CoIP Access Platform, IT and OT assets can be immediately assigned to logical zones called Application Chambers. Traffic flow into, out of, and between Chambers is controlled by identity-based policies that are easy to program and change. All policies are defined in a centralized orchestrator and enforced at users and applications for tight security control. The Zero Trust implementation completely overlays existing networking and firewall architectures without disruption.

Strong Zero Trust Security

Chamber and Access policies implement NIST 800-207 Zero Trust Security based on user, server, and application identity – not on IP address – and are applied properly even as users move and servers migrate across network environments

Workload Micro-Segmentation

Application Chambers provide granular segmentation, cloaking, and isolation of individual OT processes to cover the Detect and Protect categories of the NIST Cybersecurity Framework

Zero Trust Network Access

Least-privilege, application-aware, and VPN-free access with users, vendors, and contractors authenticated against your IdP

Overlay Application Network

Secure and application-aware direct access for cloud-based business applications and intelligence to Chambered OT assets without exposing the OT network to the cloud

Zero Touch Deployment

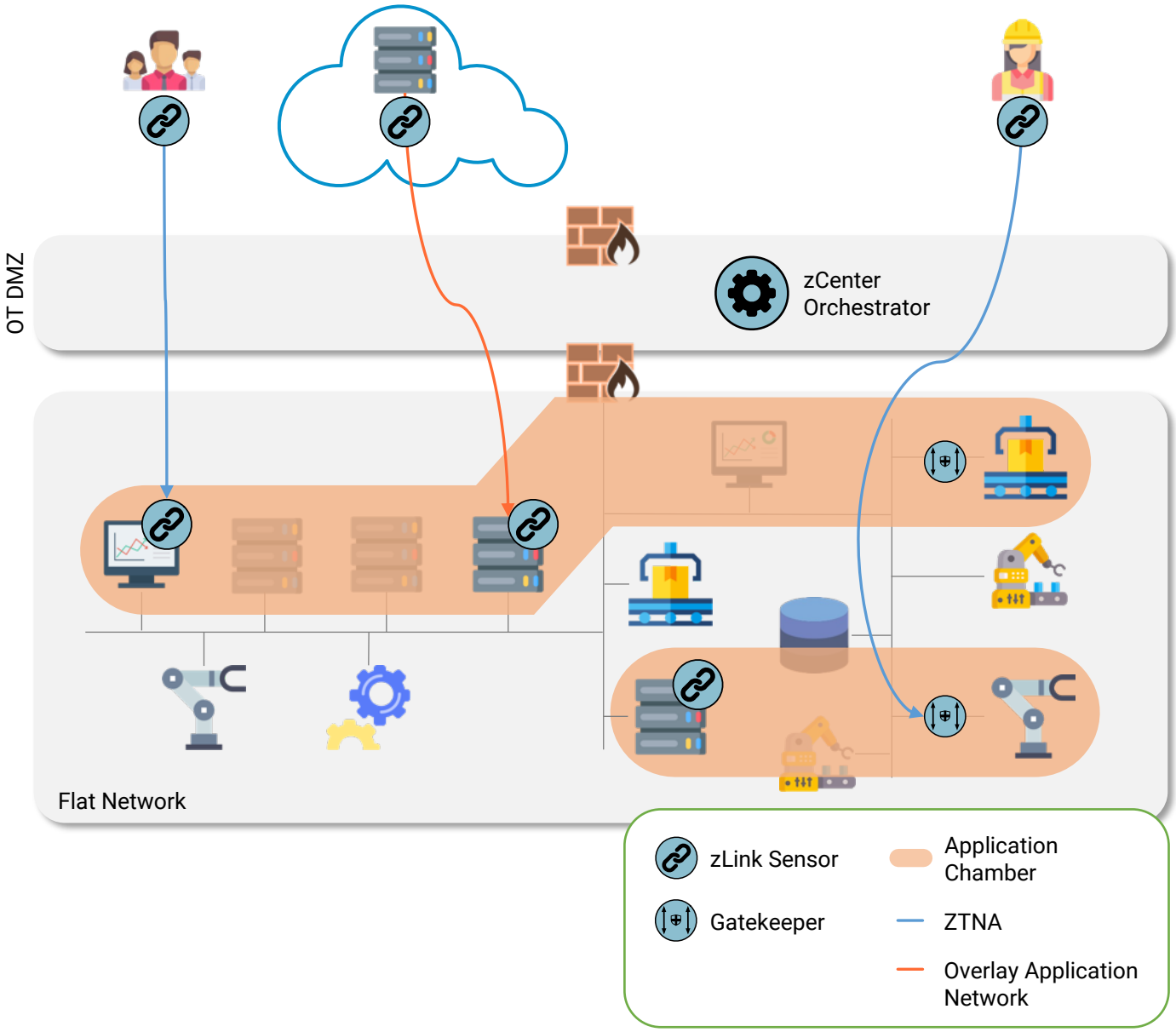
With onboarding options ranging from the Micro-Segmentation Gatekeeper for agentless protection of OT workloads to the powerful zLink agent for computers and servers, there's no need to disrupt or change existing applications or networks to deploy

Simple Operations and Change Management

Moving segmentation policies and flow control to CoIP Access Platform makes it simple and easy to onboard new users and devices or change policies without impacting already enforced policies

Apply Modern Segmentation and Controls to Any IT/OT Network

CoIP Access 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 secure developer access doesn't have to be complex.

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

- Install CoIP Access Platform
- Onboard servers with zLink agents and devices with Micro-Segmentation Gatekeeper

- Create Chambers
- Configure Chamber and access policies
- Turn on policies in Detection mode
- Create user roles and onboard users

- Enforce policies in Prevention mode
- Monitor logs
- Optimize Chamber assignments and policies as needed

Secure IT/OT Convergence

Defending OT Operations with Zero Trust Security Segmentation and Controls

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™