



# 知易行難的網路隔離在工控網路安全的問題與挑戰

許育誠 (Steven Hsu) Product Marketing Director

Adaptive Cybersecurity Solutions for OT Shop Floor Protection

# WHO WE ARE

A joint venture company of



and



30 years+ Cybersecurity Threat Intelligence

30 years+ OT Network Expertise



Industry  
Adaptive  
Solution

Threat  
Defense  
Expertise

OT-Focused  
Technology

Keep the Operation Running

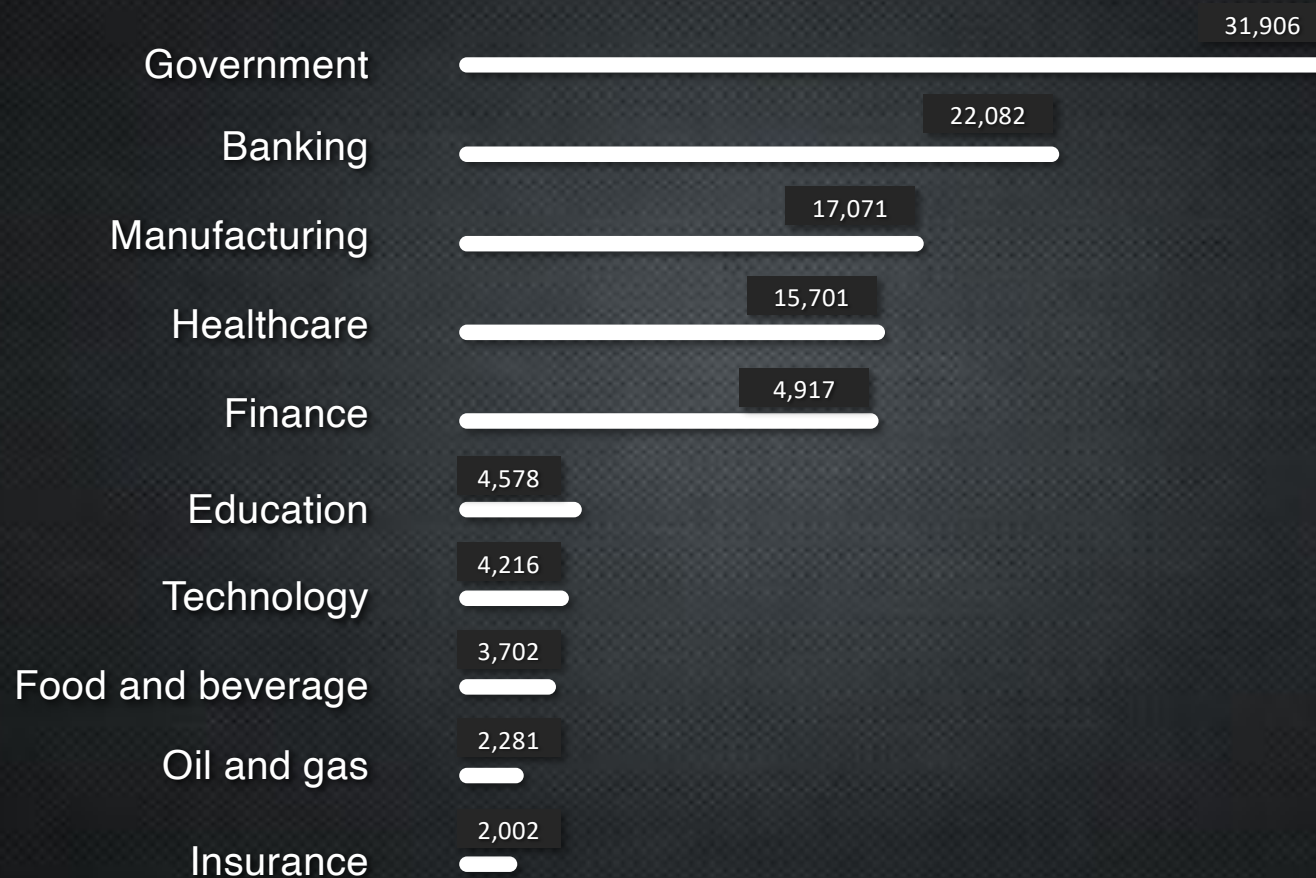
# ICS Threat Overview



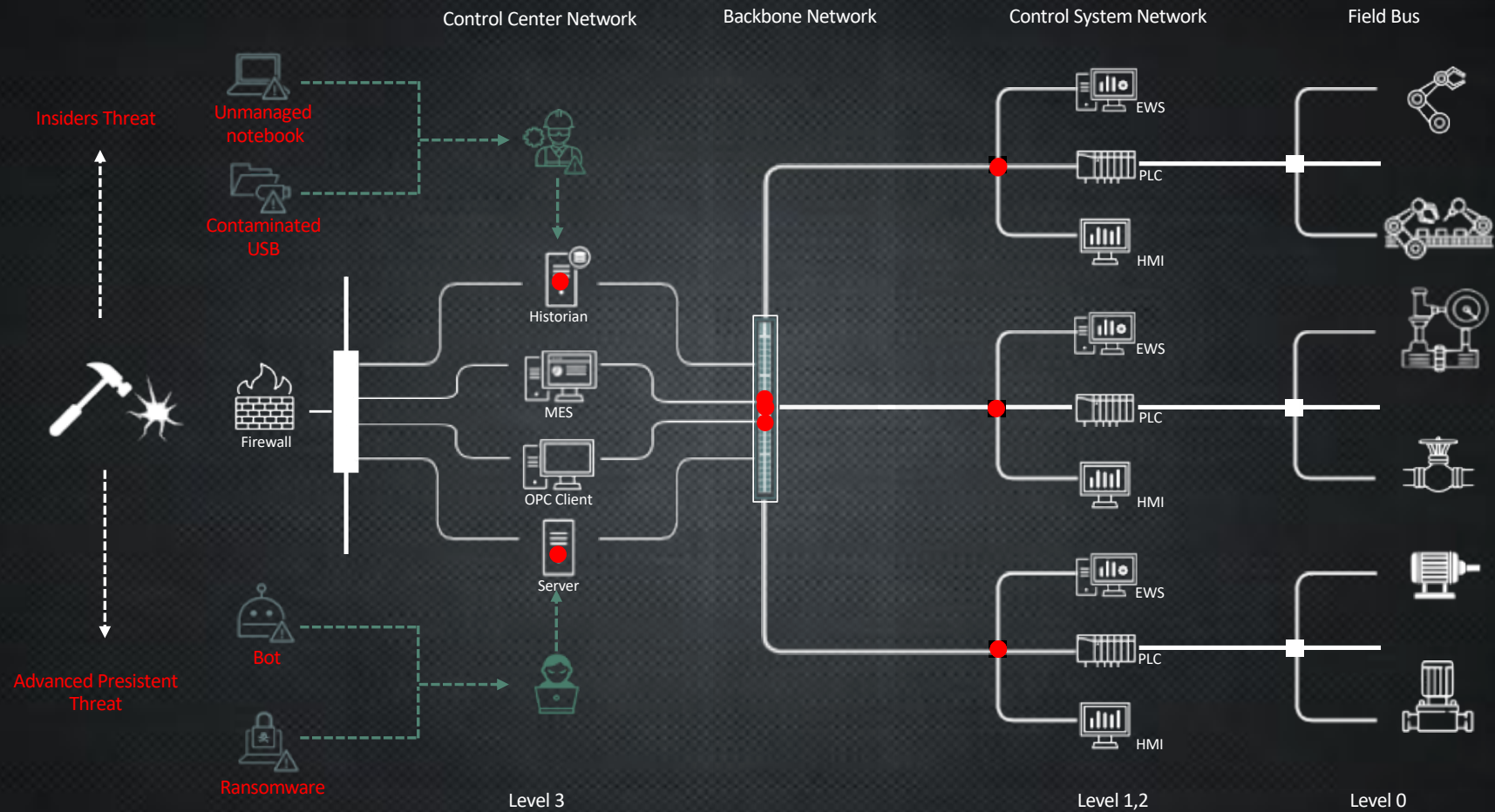
# OT is under a significant cyber attack in 2020

## The 10 industries most targeted by ransomware attacks in 2020

*Trend Micro 2020 Annual Cybersecurity Report*



# Typical ICS Attack Method



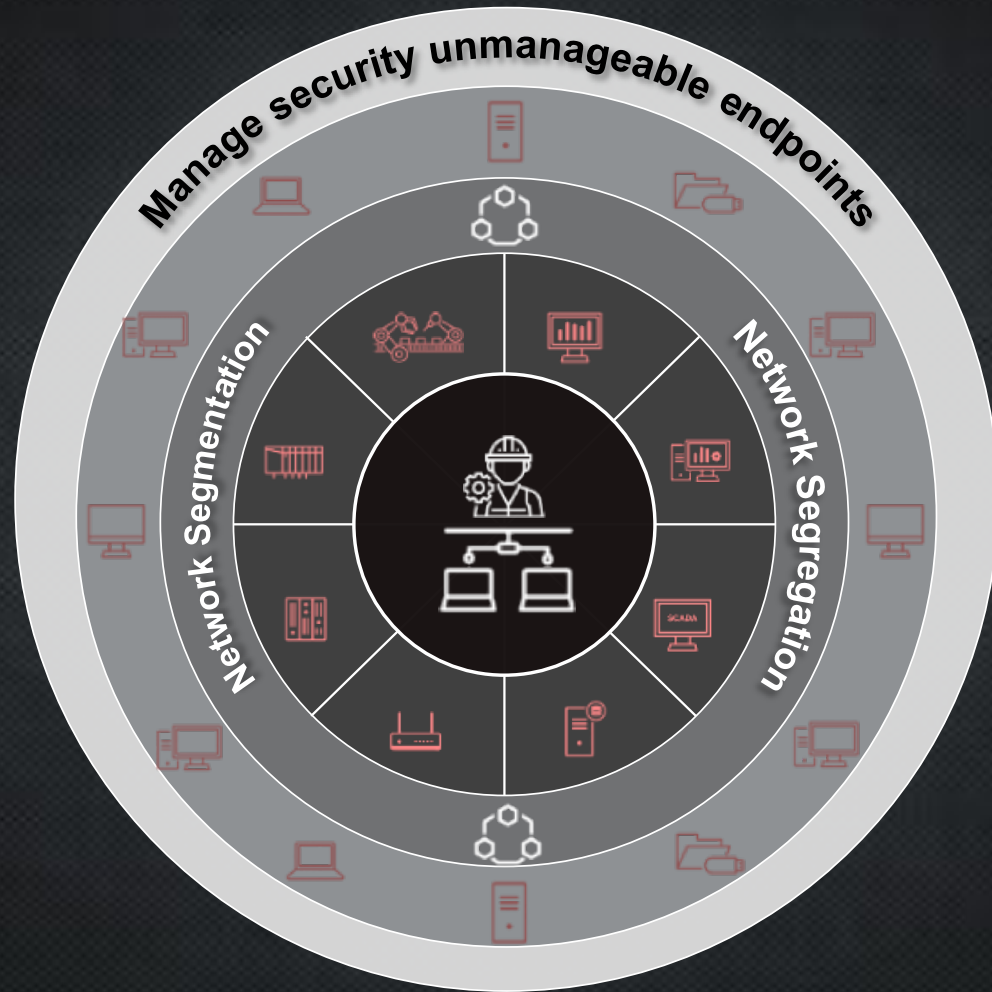
# ICS Cybersecurity Weakness – How and Why



# The nature of ICS - Variance, Volume, Vastitude

## Networks

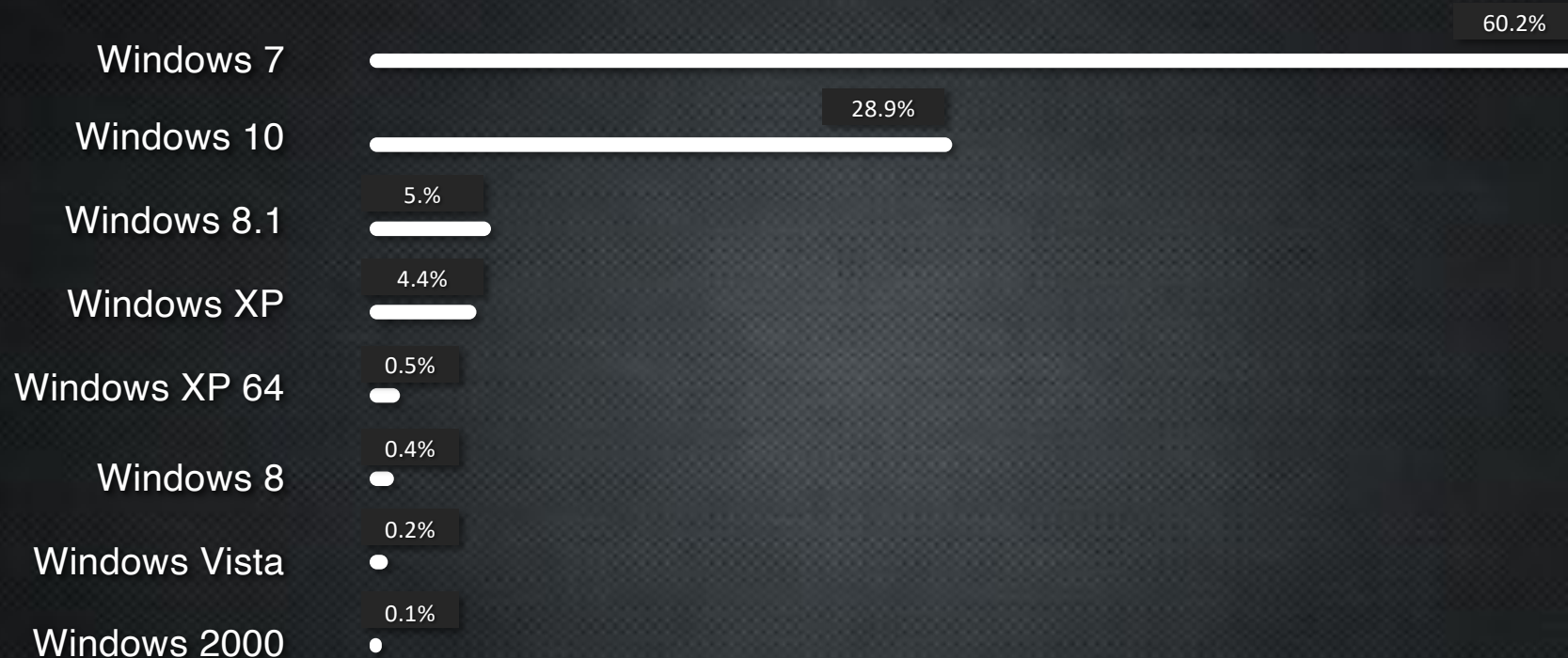
- ICS Proprietary Protocols
- Existing architecture is not designed for the security-centric purpose



## Endpoints

- Diversity of OS
- Mixture of legacy and modernize devices
- Seldom to update

# Top operating systems in the manufacturing industry



EOL

Source: Trend Micro Securing Smart Factories Threats to Manufacturing Environments in the Era of Industry 4.0



# Variant ICS Protocols

More than 69 proprietary OT protocols

Process Automation, Industrial control system, Building automation, Power-system automation

- S-I
- BSAP
- CC-Link Industrial Networks
- CIP
- CAN bus
- CANopen,
- DeviceNet
- ControlNet
- DF-1
- DirectNET
- EtherCAT
- Ethernet Global Data (EGD)
- Ethernet Powerlink
- EtherNet/IP
- Factory Instrumentation Protocol
- FINS
- FOUNDATION fieldbus
- H1
- HSE
- GE SRTP
- HART Protocol
- Honeywell SDS
- HostLink
- INTERBUS
- IO-Link
- INTERBUS
- IO-Link
- MECHATROLINK
- MelsecNet
- Modbus
- Optomux
- PieP
- PROFIBUS
- PROFINET
- RAPIEnet
- SERCOS interface
- SERCOS III
- Sinec H1
- SynqNet
- TTEthernet
- MTConnect
- OPC DA
- OPC HDA
- OPC UA
- 1-Wire
- BACnet
- BatiBUS
- C-Bus
- CEBus
- DALI
- DSI
- DyNet
- EnOcean
- EHS
- EIB
- FIP
- KNX
- LonTalk
- oBIX
- VSCP
- X10
- xAP
- xPL
- Z-Wave
- ZigBee
- IEC 60870-5
- IEC 60870-6
- DNP3
- Factory Instrumentation Protocol
- IEC 61850
- IEC 62351

[https://en.wikipedia.org/wiki/List\\_of\\_automation\\_protocols](https://en.wikipedia.org/wiki/List_of_automation_protocols)

# As the result - OT/ICS is so vulnerable

Worm/Malware brought in,  
or Misuse of PLC and  
critical assets, by  
Intentional or  
unintentional insiders.

Unknow  
Attack

Legacy  
Assets

Massive number of  
assets with complex and  
mixture systems included  
legacy, EOL operating  
systems



No network  
segmentation, in many  
cases the whole network  
is a big flat L2 network

Flat  
Network

Patching  
Absent

Difficult to conduct the  
patching and updating  
process due to several  
practical reasons

# ICS Segmentation Overview



# ICS Segmentation – A little bit history briefing here



Zones & Conduits

The diagram illustrates the Zones & Conduits model. It features a central hexagonal area labeled 'Zones & Conduits'. Surrounding this are several rectangular blocks representing different zones (e.g., Zone A, Zone B) and conduits (e.g., Conduit 1, Conduit 2). Arrows indicate the flow of data between these zones and conduits, showing a segmented network structure.



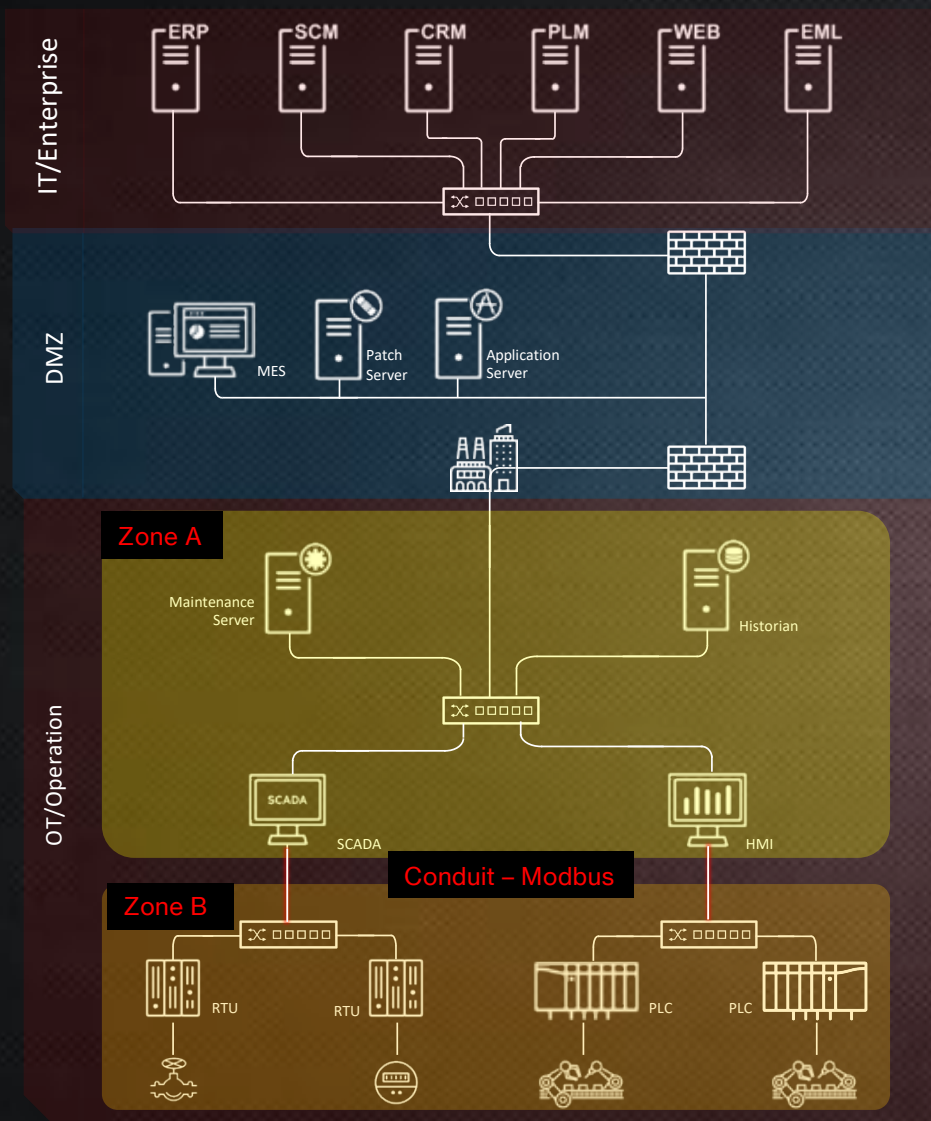
Purdue Model

The diagram illustrates the Purdue Model. It shows a central hexagonal area labeled 'Purdue Model'. The model is structured into layers, with a central layer for control systems and outer layers for enterprise IT and field devices. Arrows indicate the flow of data between these layers, showing a hierarchical network structure.



Zero-Trust Model

The diagram illustrates the Zero-Trust Model. It shows a central hexagonal area labeled 'Zero-Trust Model'. The model is structured into layers, with a central layer for control systems and outer layers for enterprise IT and field devices. Arrows indicate the flow of data between these layers, showing a hierarchical network structure.

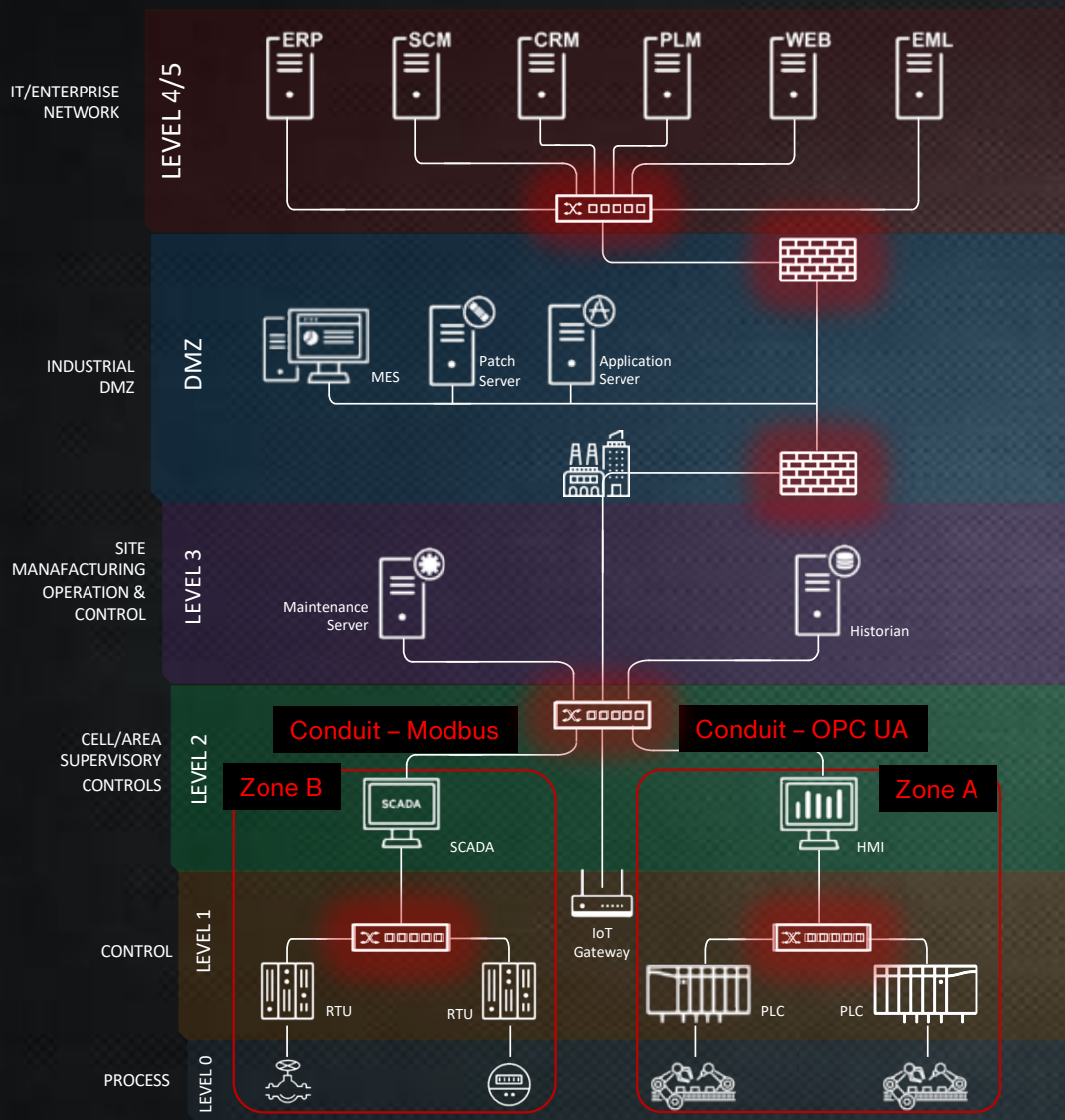


- *Traditional Three Tiers Approach*
- *Air gapped concept – introduce DMZ*
- *Zones and Conduits basic network segmentation for control network - introduced in the ANSI/ISA-99 security standard*

- *Zone: grouping of logical or physical assets that share common security requirements (ANSI/ISA99.01.01-2007-3.2.116)*
- *Conduit: a path for the flow of information between two zones*

- *Difficult to deploy the same security requirement within the same zone due to increasing of assets amount and diversities of OS*
- *Reply on Conduit segmentation is very easy to break*



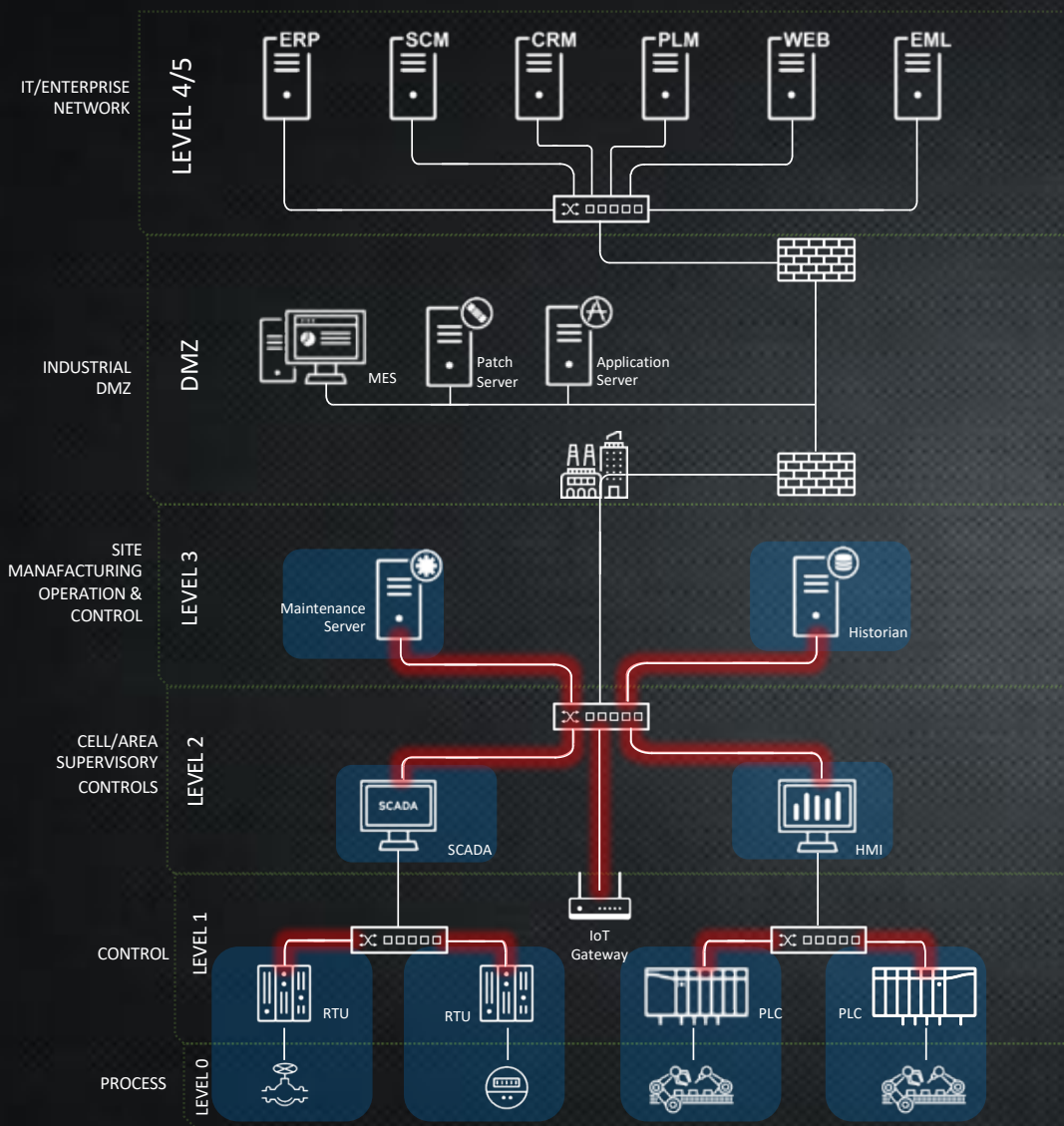


- *Extend the Zones and Conduits concepts*
  - *A zone can have sub-zones*
  - *A zone can have more than one conduit.*
  - *A conduit cannot traverse more than one zone*
  - *A conduit can be used for two or more zones to communicate with each other*

- *ICS network appliances play a very important roles – VLANs, Routing, Firewall or SDN*

- *ICS network architecture needs to be modified*
- *ICS network appliances need to be upgraded*
- *Required network administrator for configuration and setup*

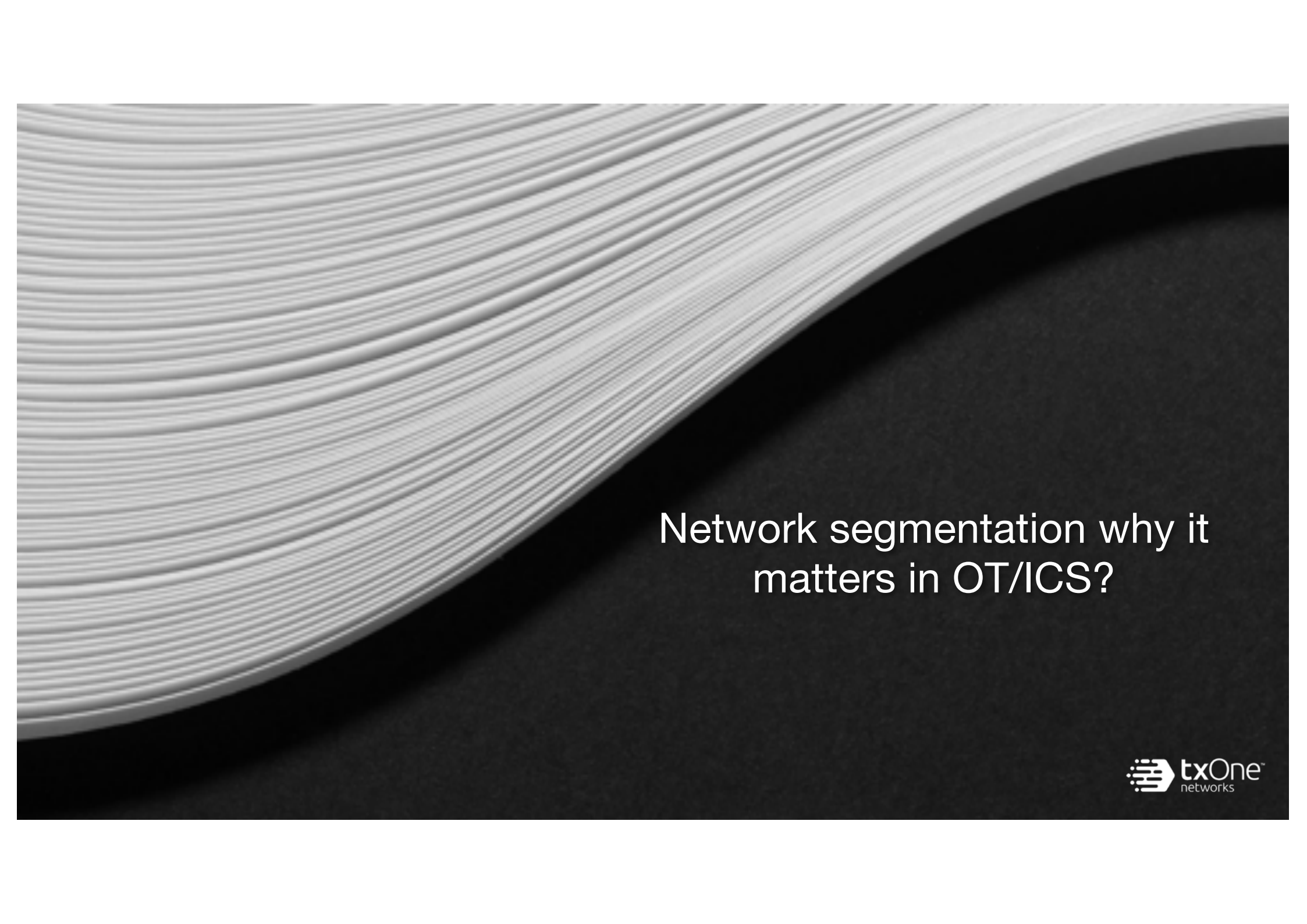




- Zero-Trust model based on the least privilege access apply to both endpoints and networks
- A Micro-segmentation concept has been introduced for the perimeter-centric defense

- Trust-list approach for policy management
- It is more related to business or operation intension for the network architecture

- Solutions across multiple assets owners (endpoints, networks)
- The management efforts v.s. operation continually
- ROI will be the main decision to assets owners



# Network segmentation why it matters in OT/ICS?

## With Segmentation



## Without Segmentation



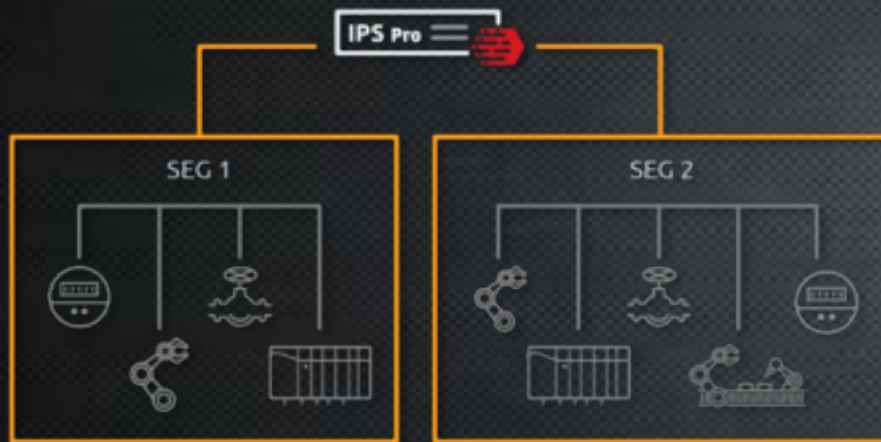
Network Segmentation has been highly addressed in the following ICS standard

- IEC 62443
- NIST SP 800-82
- NERC CIP



# Network Segmentation Benefits

- Security purpose
- Management purpose



Risk Mitigation



Prevent Lateral Movement



Outbreak Prevention



Deal with Massive IoT Adoption

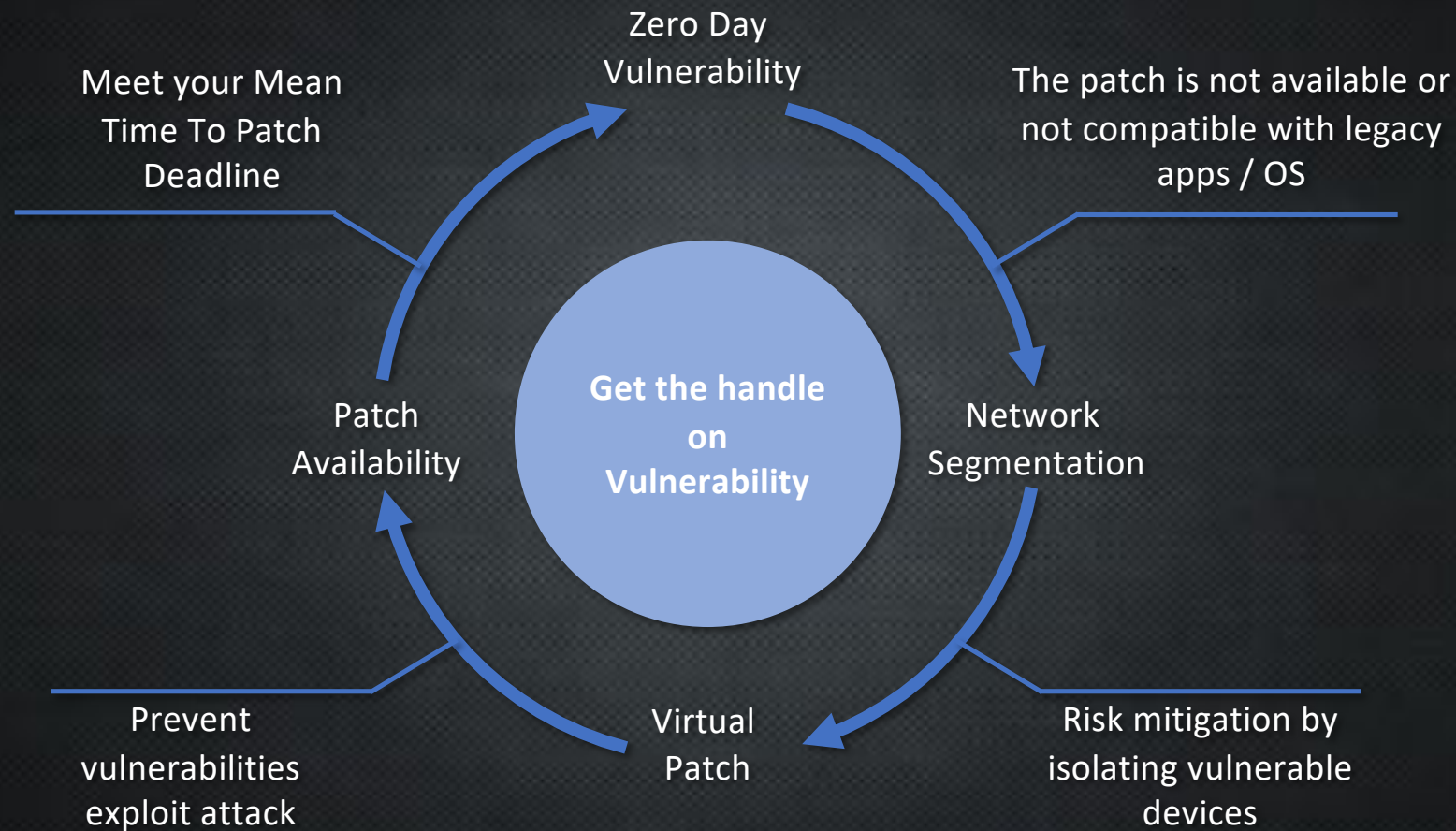


Future Private 5G Connection



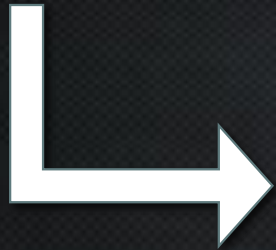
Zero Trust Network

# To prevent the unknow attack by network segmentation and virtual patch



# COVID-19 as the example for the unknow attack – Segmentation

Zero-day  
Vulnerability



## QUARANTINE

You Had Contact  
With Someone Who  
Tested Positive

Stay Home for  
14 Days Even if You  
Don't Feel Sick



## ISOLATION

You are Diagnosed  
With COVID-19

Stay Away From People  
& Household Members

Do Not Leave Home Except  
for Medical Treatment

Attack by the  
Vulnerability



<https://www.tlu.edu/covid-updates/staying-healthy-on-campus/quarantine-and-self-isolation-protocols>



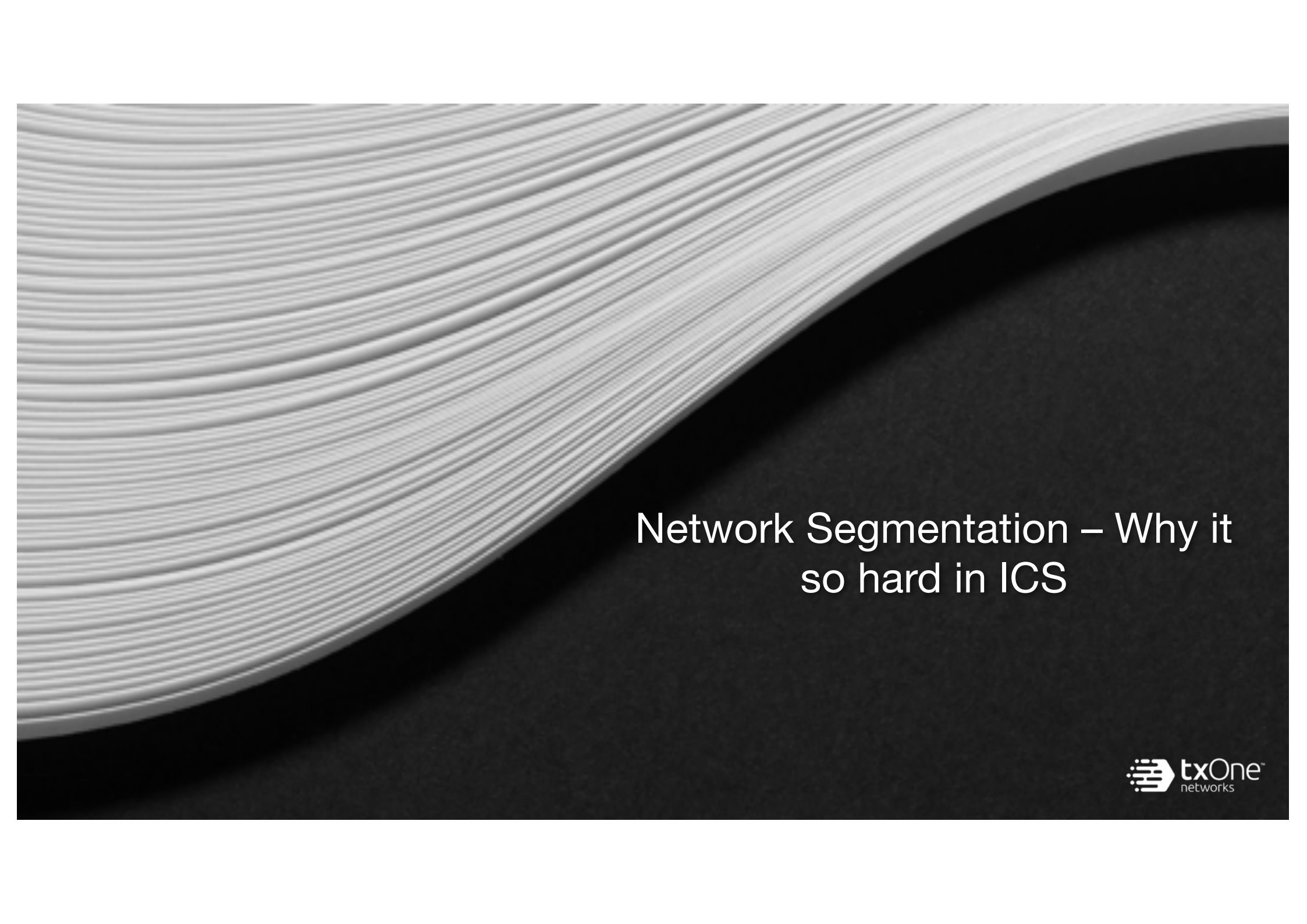
# COVID-19 as the example for the unknow attack– Virtual Patch

## Mask – Virtual Patch

Before vaccine is available

## Vaccine – Patch

Upgrade your system for future immune



# Network Segmentation – Why it so hard in ICS

# IT network segmentation does not work in ICS

1

## VLANs

- Complicated and time-consuming setup
- Chance to miss configuration
- Not able to automate for new segmentation is needed

2

## Routing

- NOC is needed
- Difficulty in network issue trouble shooting
- Configuration only available during the maintenance

3

## Firewall

- Not support multiple and proprietary OT protocols and commands

4

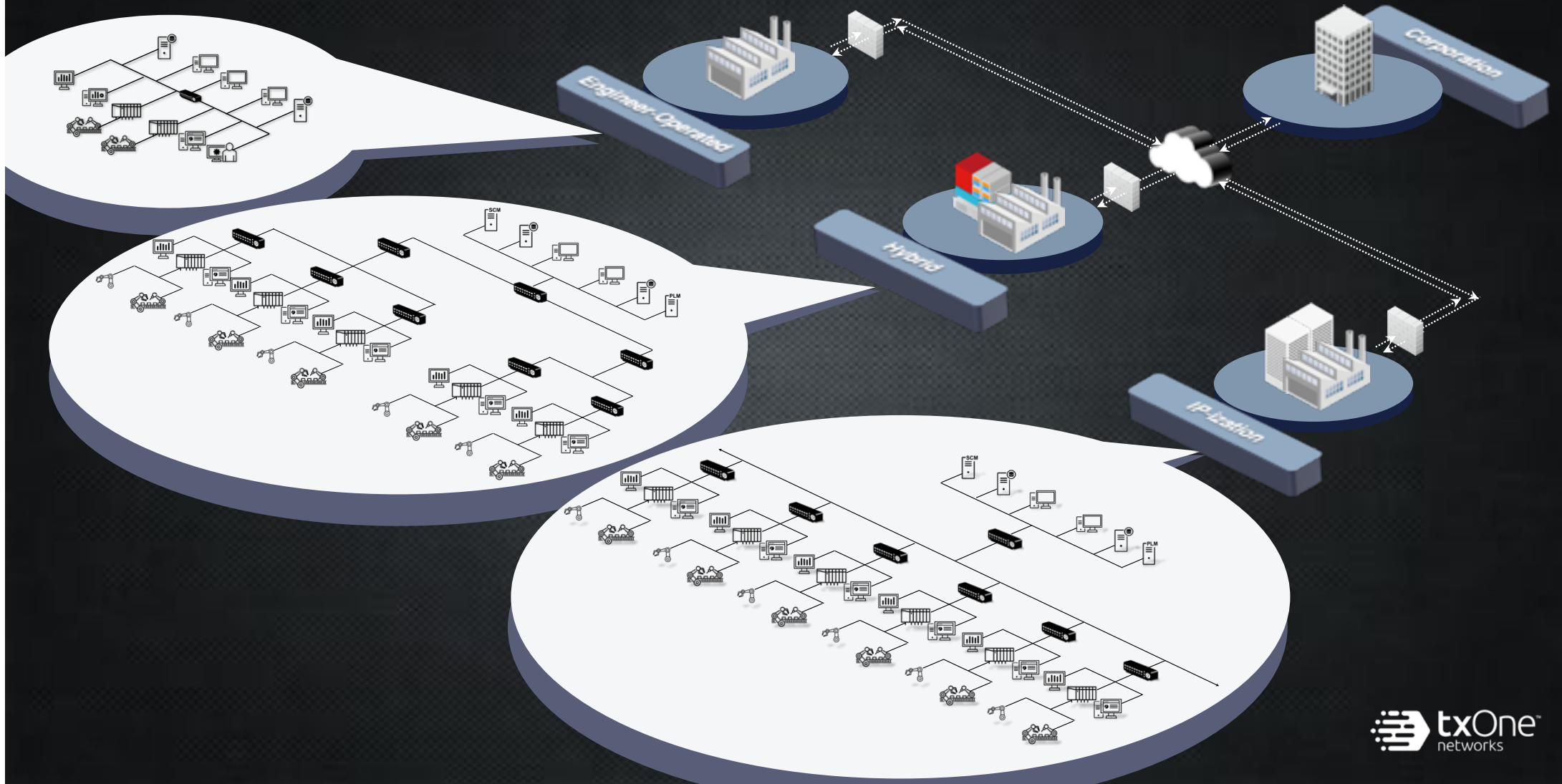
## SDN

- Expensive to change the entire network architecture

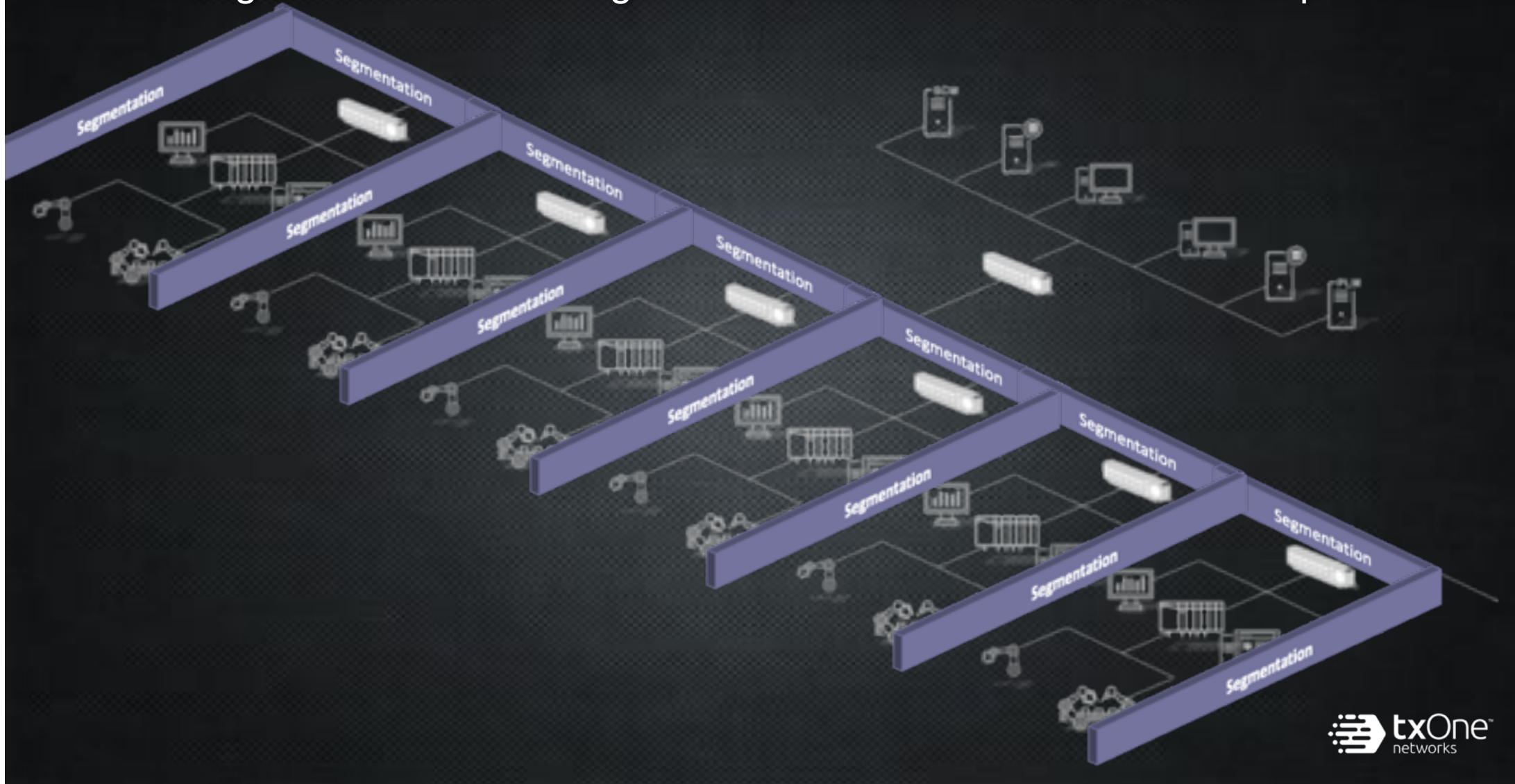
»»» It needs to change existing OT network architecture «««



# Different scale of manufacturer required different network segmentation method



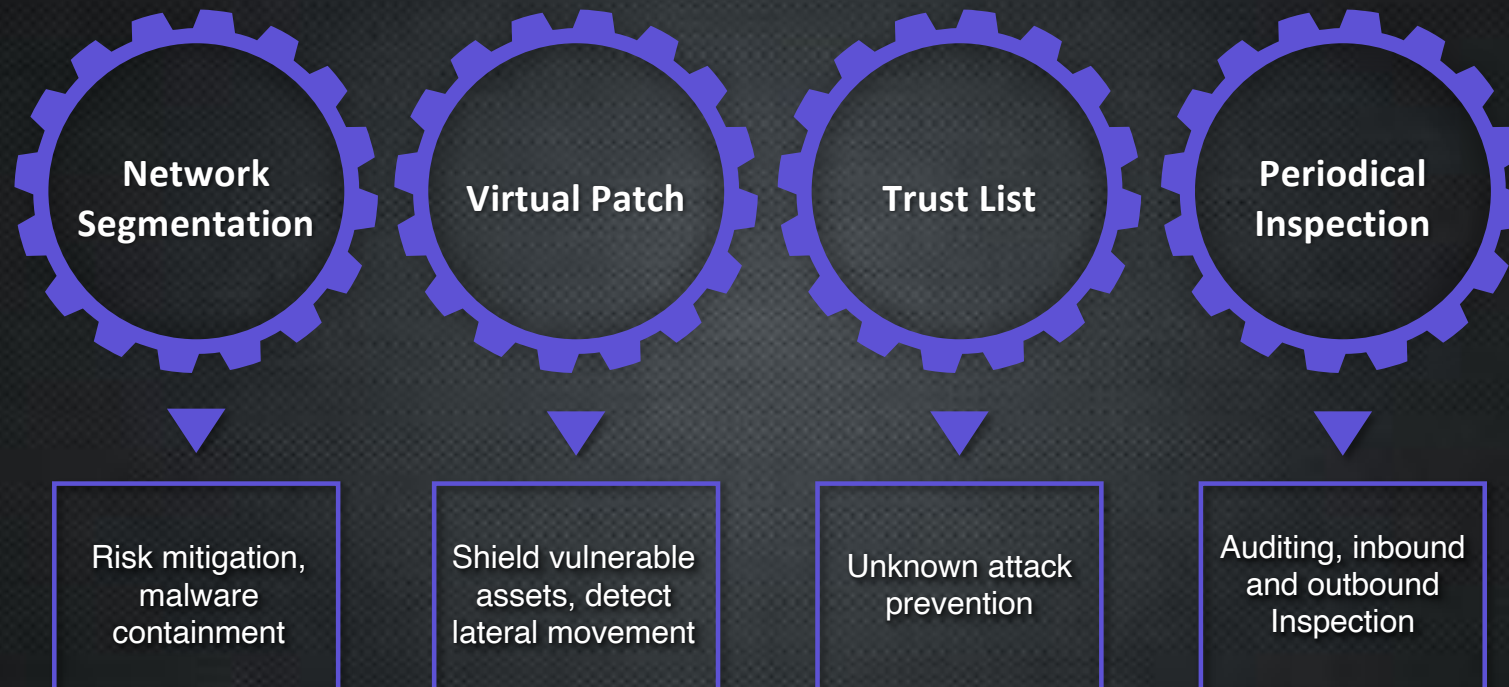
Network Segmentation to the large-scale manufacturer is a mission impossible



How TXOne can help?



# Best Practices for ICS Cybersecurity Resilience



# Adaptive ICS Cybersecurity Solutions for Shop Floor Protection

Hassle-free,  
installation-free malware inspection

Security  
Inspection

The Edge series, industrial  
IPS in multiple form factors



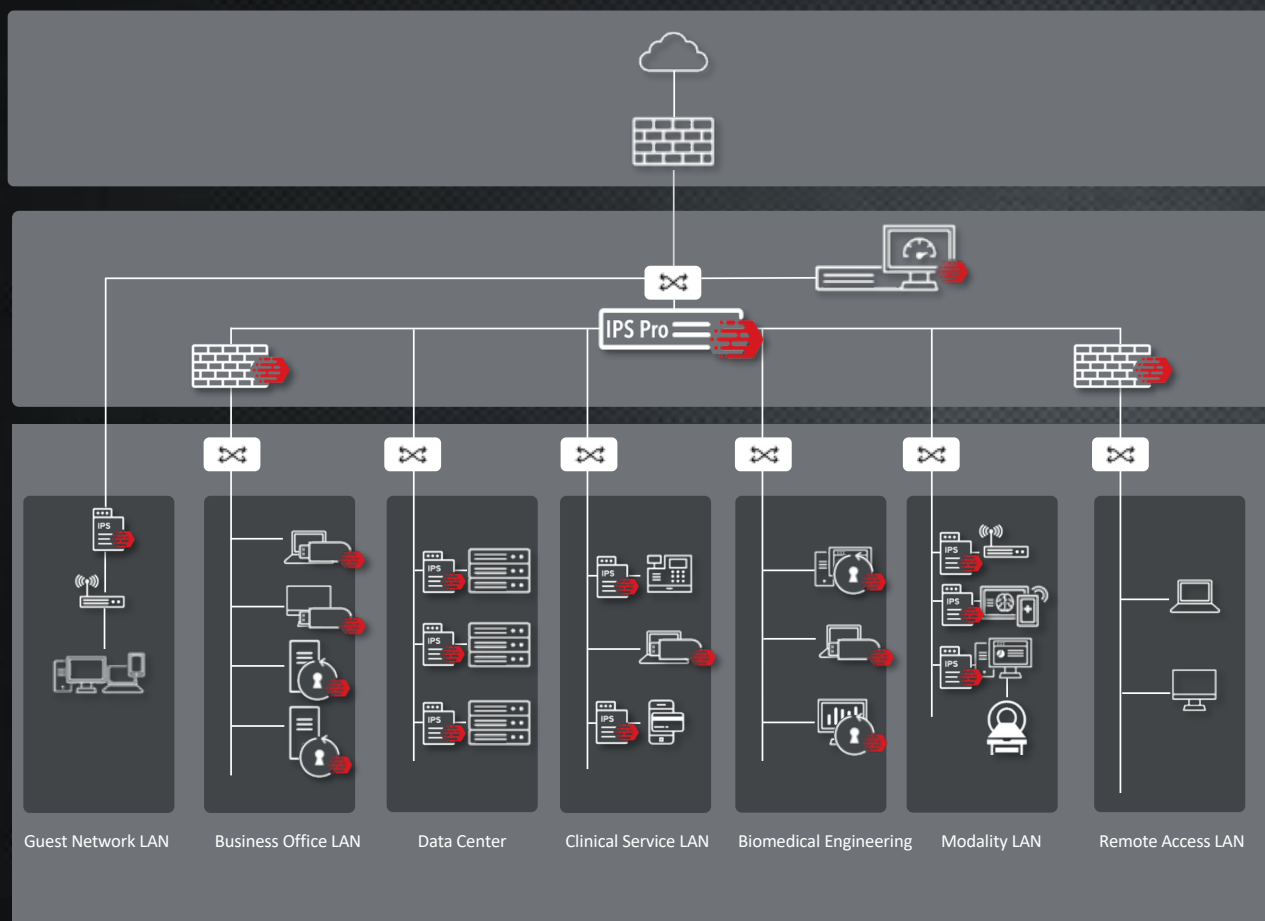
Network  
Defense

The Stellar series, all-terrain  
NGAV & lockdown



Endpoint  
Protection

## *Example - Helping several medical centers to deal with vulnerable legacy modalities*



- *Hardening the modalities*
- *Virtual patch shields legacy OS endpoints*
- *Network segmentation to reduce other attack surfaces*





*Contact us if you have more question about  
OT/ICS network segmentation*



© 2021