OT Security in 2026 –

a tale of ignorance, compliance and submarines

State of Legacy OT Environments

60%

Approximately 60% of industrial organizations rely on legacy systems that have been in operation for over 20 years, significantly increasing vulnerability to cyber threats.

Source: Deloitte Report on Cybersecurity in Industrial Control Systems.

20 %

of all ICS systems are relying on outdated operating systems

Source: Censys State of the Internet Report

OT Sector Attack Overview

January

Sector
Manufacturing
Victim
Schneider Electric
ICS Supplier

Sector
Automotive
Victim
Hyundai Motor Europe

Sector
Semiconductor
Victim
Foxsemicon

February

Sector
Pharmaceutical & healthcare
Victim
Change Healthcare
BlackCat

Sector
Manufacturing
Victim
Battery Maker Varta

Sector
Manufacturing
Victim
Thyssenkrupp

March

Sector
Pharmaceutical & healthcare
Victim
Crinetics Pharmaceuticals

Sector
Automotive
Victim
Nissan Oceania

Sector
Public Transportation
Victim
Liverpool Airport
Indirect Factor

April

Sector
Water
Victim
Russian wastewater

Sector
OT
Victim
Black Sea & Mediterranean
APT War

May

Sector
Food & Beverage
Victim
Meat Processing
Ransomhub

Jun - Jul

Sector
Pharmaceutical & healthcare
Victim
U.S. Healthcare Providers

Sector
Pharmaceutical & healthcare
Victim
Major Hospitals in London

Sector
Water
Victim
U.S. water and wastewater systems
Indirect Factor

August

Sector
Semiconductor
Victim
Microchip Technology

Sector
Public Transportation
Victim
Seattle Airport

Sector
Water
Victim
Arkansas Water Treatment

September

Sector
Pharmaceutical & healthcare
Victim
UMC Health System

Sector
Water
Victim
Arkansas Water Treatment

Oct - Dec

Sector
Water
Victim
American Water

Sector
Oil & Gas
Victim
Costa Rica's State Oil Refinery

Sector
OT
Victim
OT devices in the US and Israel
ICS Malware

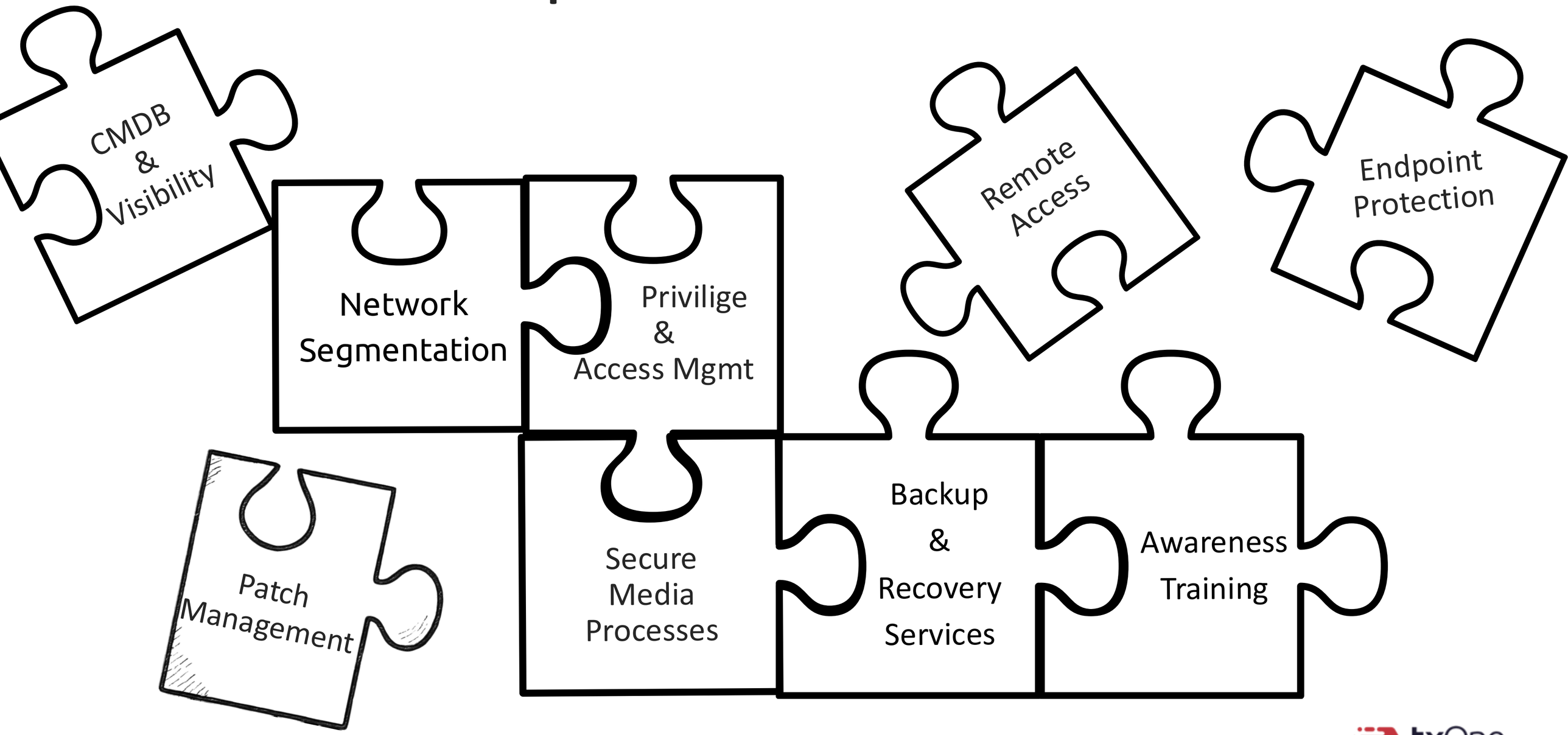
Ransomware Attack

Geopolitical Conflict

Keep the Operation Running

txOne networks

We have product XYZ – our OT is secure!



txOne networks

We are not allowed to implement endpoint protection on our machines

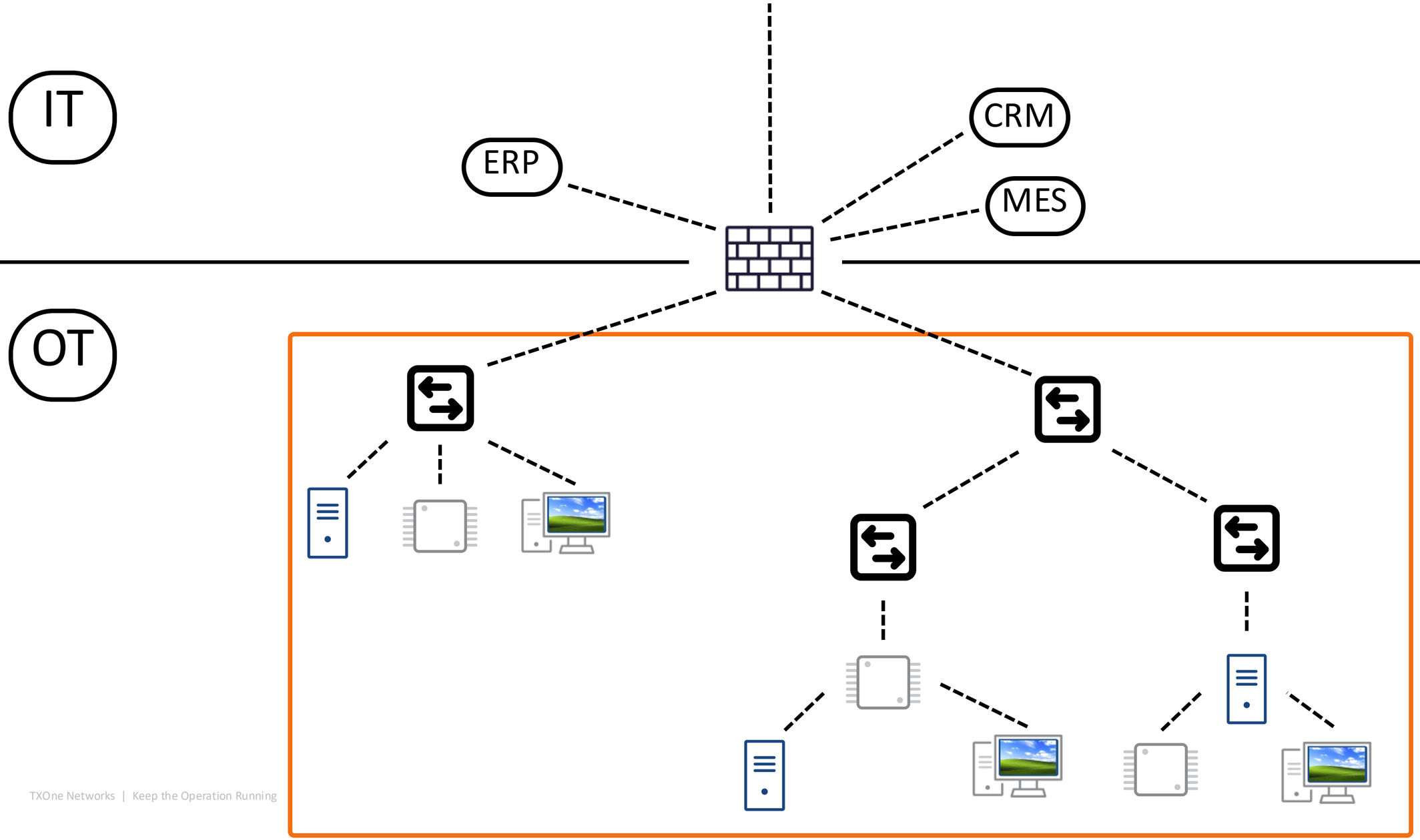
Operations

Service Technician

Machine Builder

txOne networks

We have implemented an OT-segmentation firewall



We banned all removeable media in the shopfloor

What is removable media?

Challenges in OT

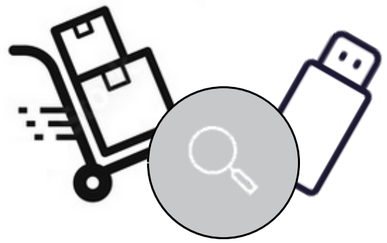
Microsoft Windows xp

Windows Embedded Standard 7

No support for old operating systems

```
IPv4-Adresse  . . . . . : 192.168.2.15
Subnetzmaske  . . . . . : 255.255.255.0
Standardgateway . . . . : 192.168.2.1
```

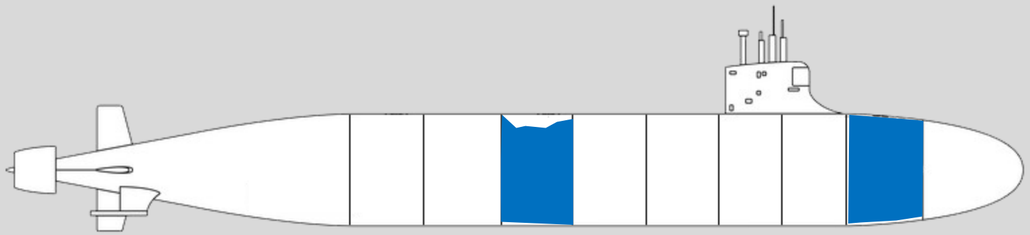
Network Segmentation „easier said than done“



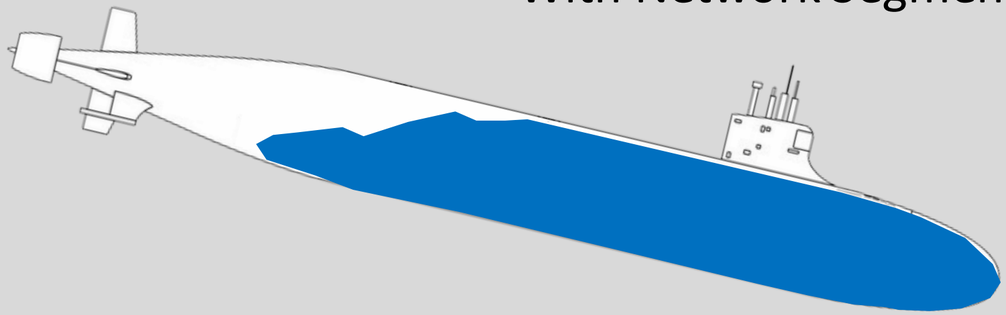
Onboarding & media handling

txOne networks

The submarine example



With Network Segmentation



Without Network Segmentation