Cybersecurity in the Digital Transformation Journey

Eva Chen, Trend Micro CEO
Terence Liu, TXOne Networks CEO

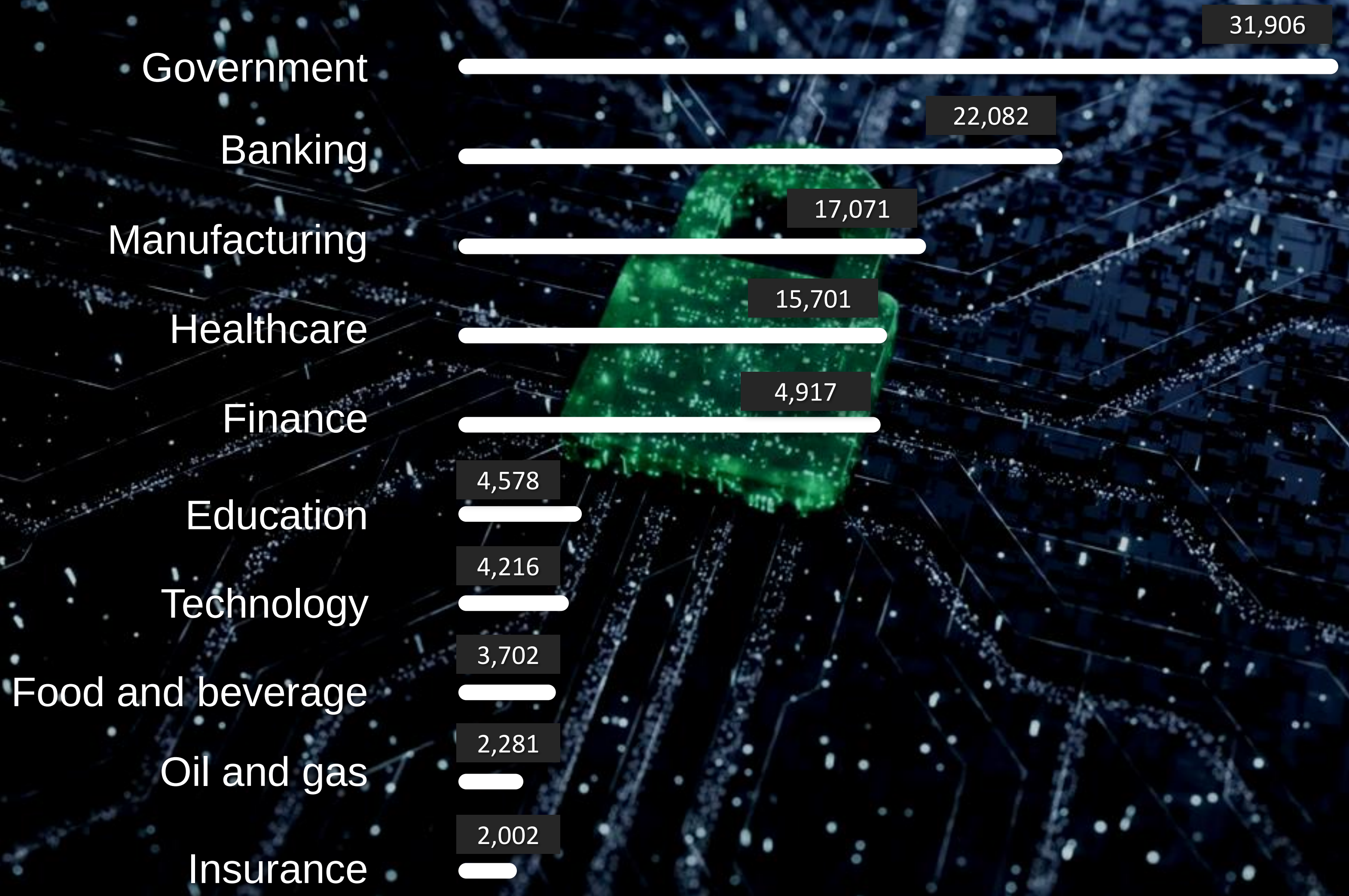
The pandemic accelerated digital transformation

The threat landscape changed

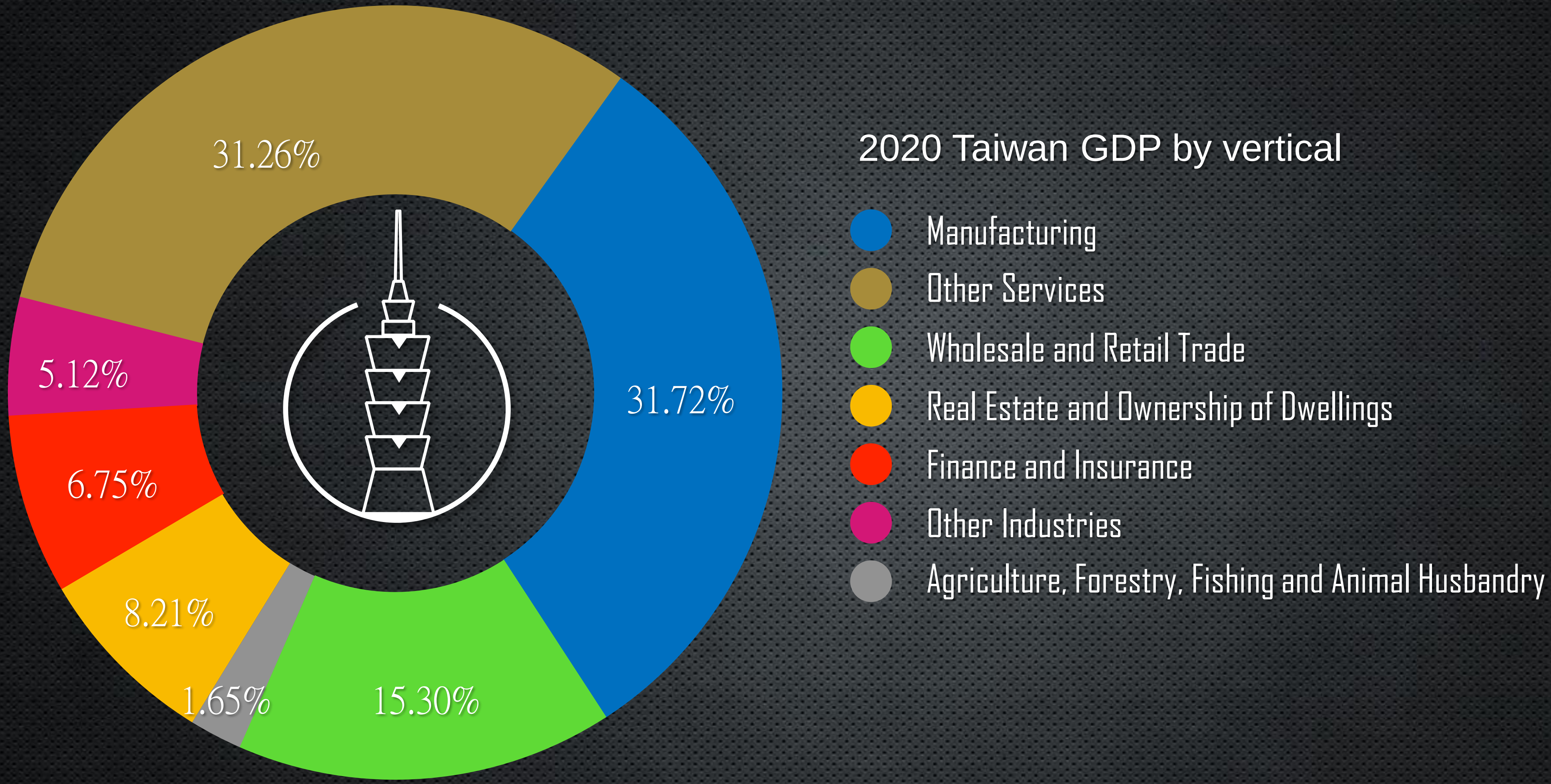
Cybersecurity solutions need to be transformed

The 10 industries most targeted by ransomware attacks in 2020

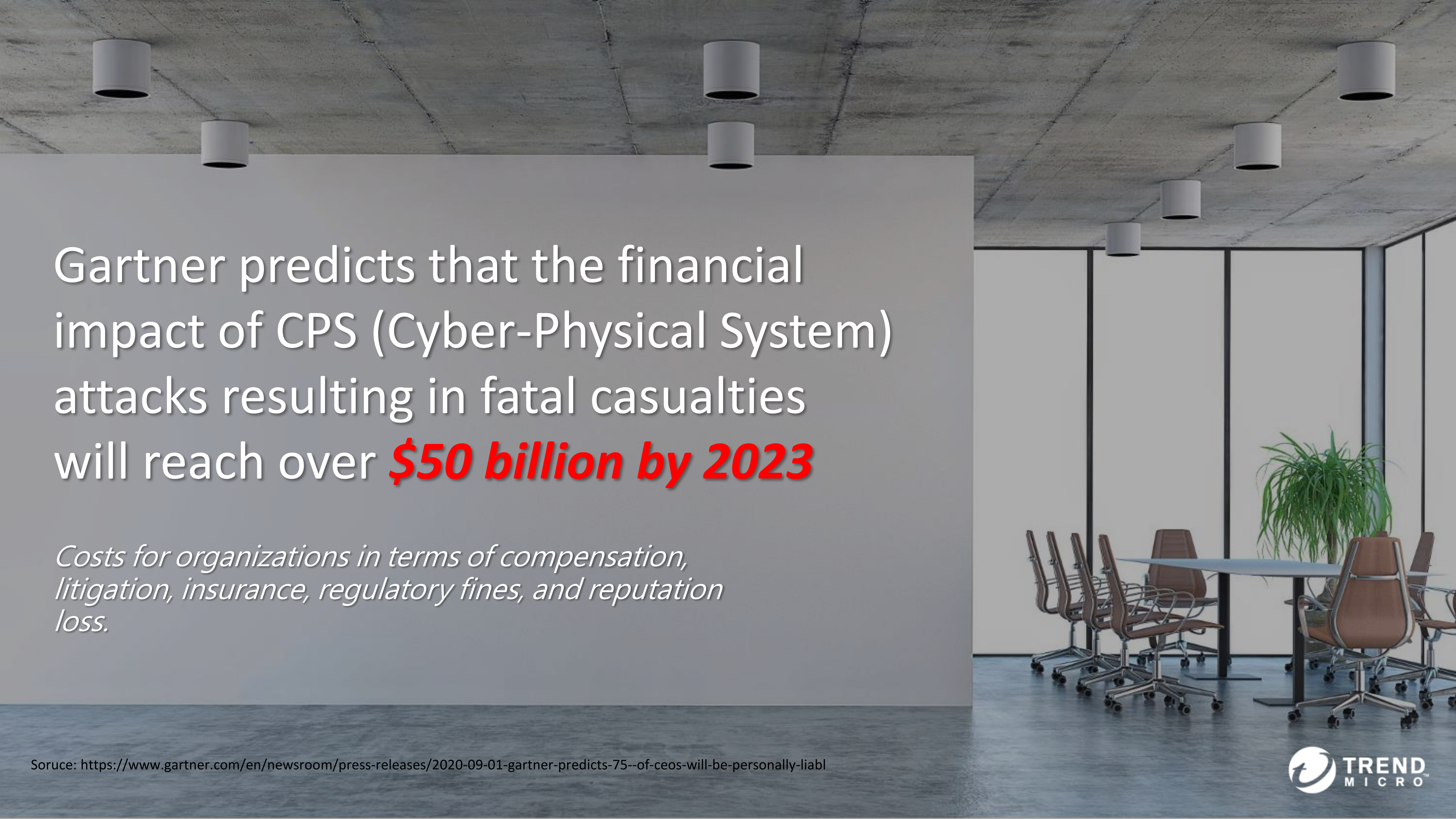
Trend Micro 2020 Annual Cybersecurity Report



Why it matters to Taiwan?



Source: Directorate General of Budget, Accounting and Statistics, Executive Yuan, R.O.C..



Gartner predicts that the financial impact of CPS (Cyber-Physical System) attacks resulting in fatal casualties will reach over **$50 billion by 2023**

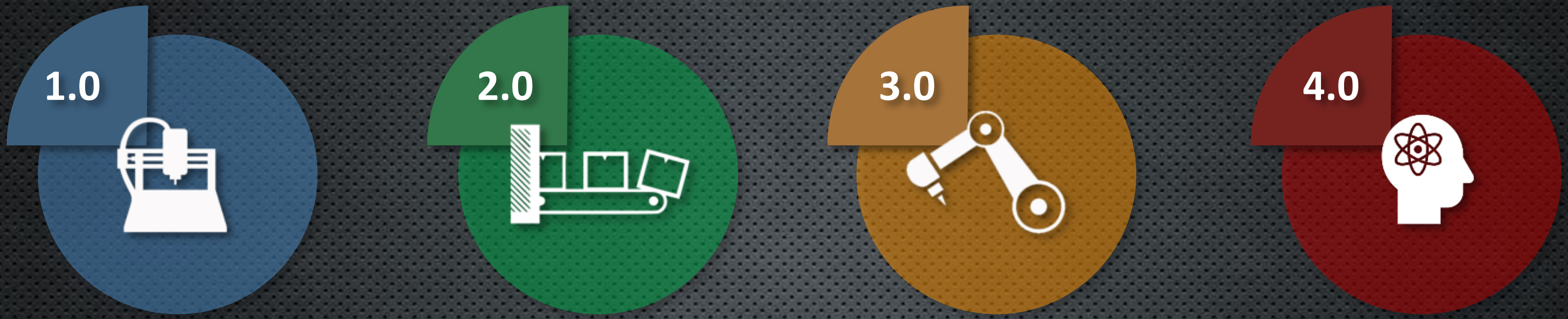
Costs for organizations in terms of compensation, litigation, insurance, regulatory fines, and reputation loss.

Soruce: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

What is the Digital Transformation Value Stream?

Data to Decision

Industry 4.0 is the Digital Transformation



Mechanical Manufacturing

Steam engines replace human labor

Mass Production

Electricity and the development of large capital goods industries

IT Automation

IT system deployment in the production line

Cyber-Physical Systems

Smart factories with decentralized decision-making through IoT technologies

Data to Decision for Cyber-Physical Systems

The Data to Decision Value Stream for Corporations

Data-driven, data first – a long and challenging journey

Data Acquisition

Automation creates operational continuity

Data Silos

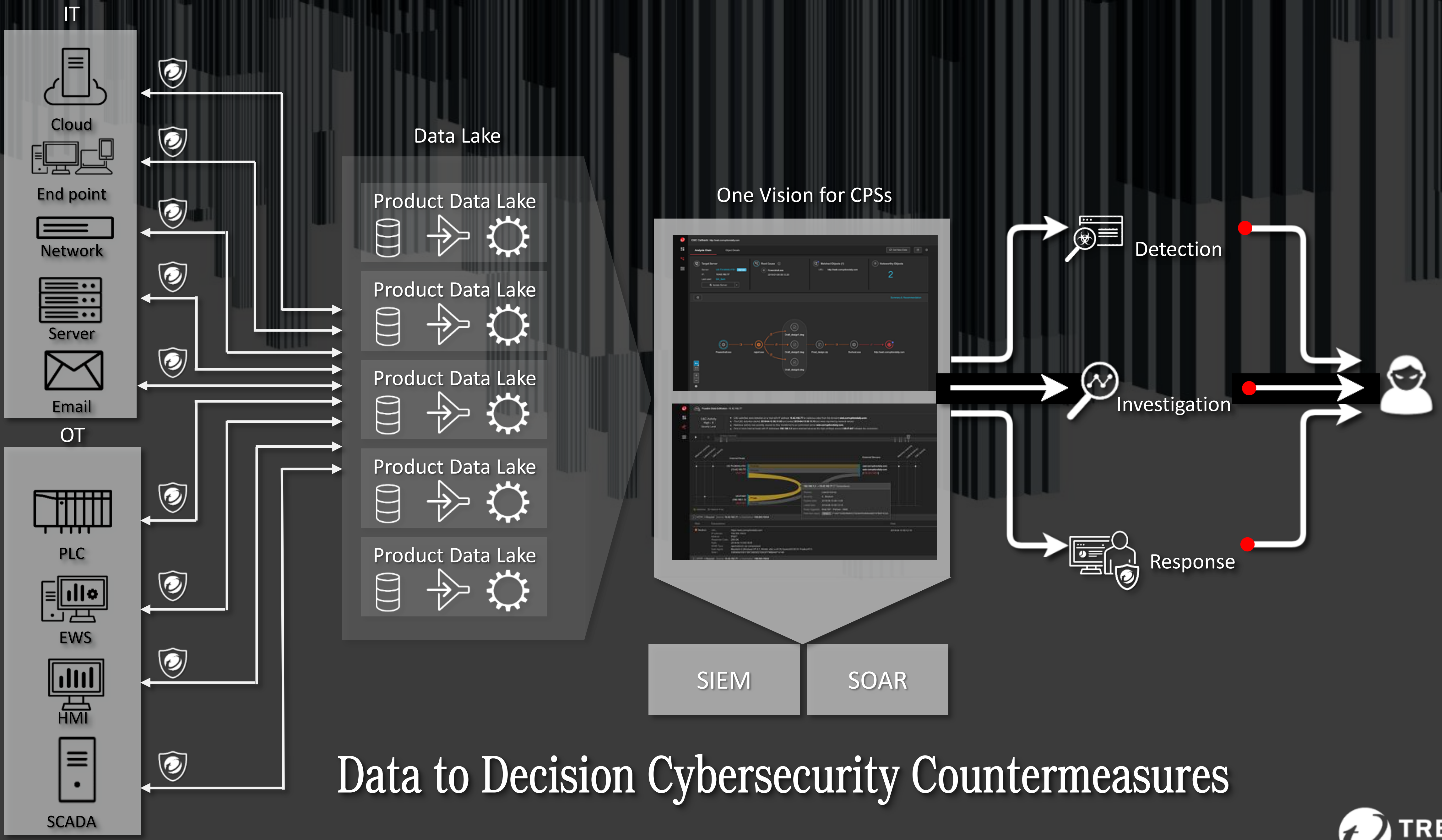
Cross-department cooperation

Data Depth

Critical data under the surface

Data Analysis

Where is the computation? On-premises or the cloud?



Data to Decision Cybersecurity Countermeasures

TREND MICRO

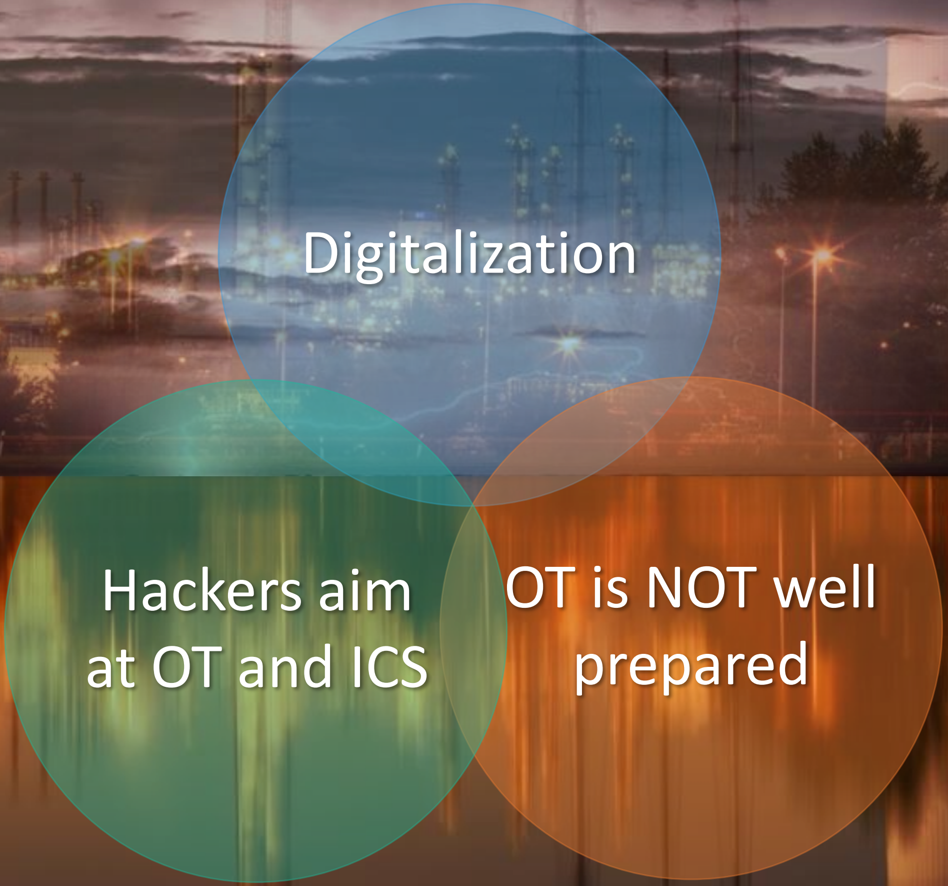
Cybersecurity for ICS

ICS Cybersecurity Challenges

From Taiwan to the World

The Perfect Storm for OT Cybersecurity

- OT is NOT air-gapped anymore – modern enterprises collect data for analysis over the cloud (IIoT)
- Industry 4.0, 5G, AI/ML, Edge Computing, Digital Twin

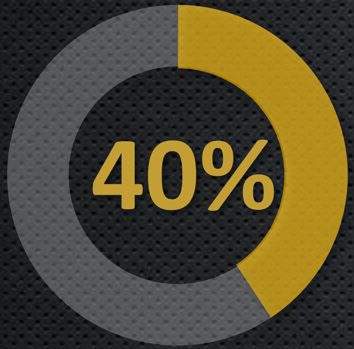


- Hackers are aware of OT weaknesses and conduct targeted ransomware attacks accordingly
- Paying ransoms is often illegal -- the money could go to terrorists
- Cybersecurity insurance may exclude nation-sponsored cybercrime

- Limited number of experts who understand both OT and cybersecurity
- Lack of OT-specific products and playbooks

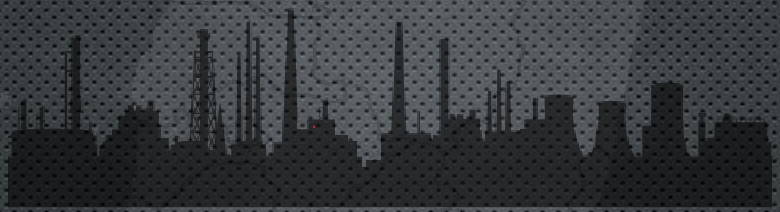
Ransomware in Taiwan OT/ICS in 2020

According to June 2020, “Research of Cyber Security Industry in Taiwan”

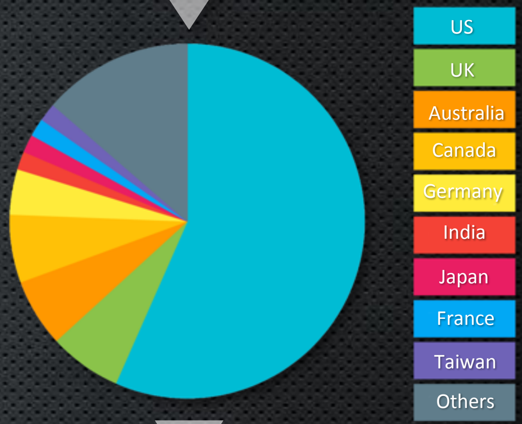


of manufacturing companies on average must enhance access control, data security, and system security

Taiwan manufacturers are upgrading their intelligence in response to competition and customer demands



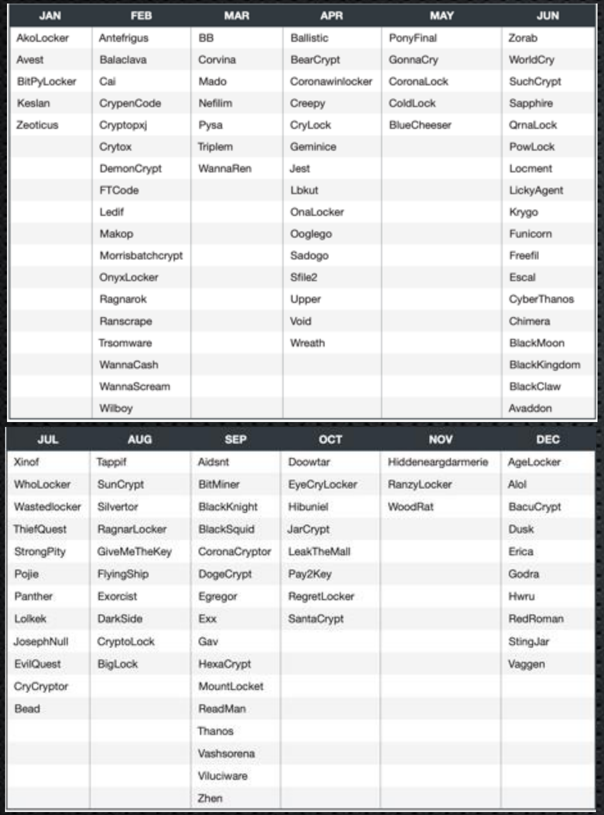
In 2020 Q4 there were more than 10 manufacturers/critical infrastructures suffering from ransomware attacks



Taiwan is #9 for most ransomware attacks by country

Ransomware in Global OT/ICS in 2020

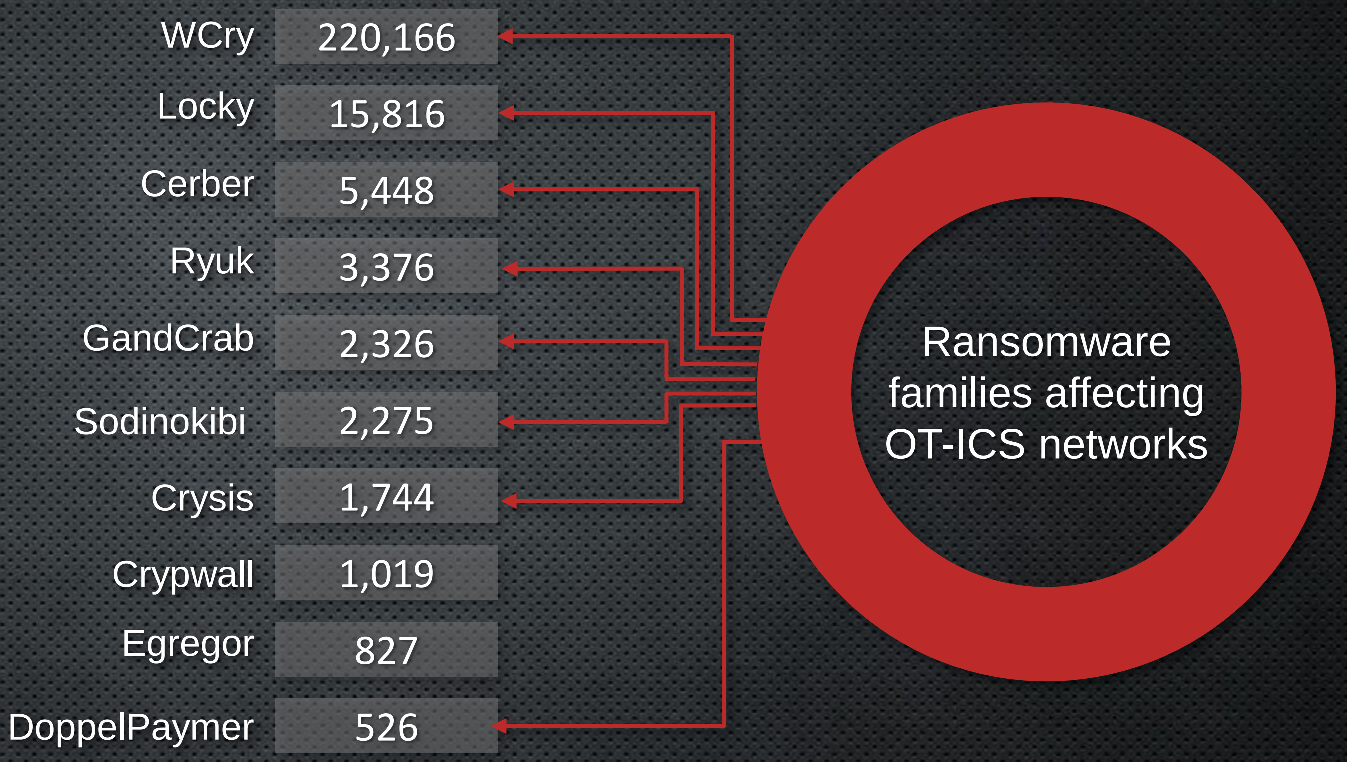
127 new ransomware families detected in 2020



JAN	FEB	MAR	APR	MAY	JUN
AkoLocker	Antefrigus	BB	Ballistic	PonyFinal	Zorab
Avest	Balaclava	Corvina	BearCrypt	GonnaCry	WorldCry
BitPyLocker	Cai	Mado	Coronawinlocker	CoronaLock	SuchCrypt
Keslan	CrypenCode	Nefilim	Creepy	ColdLock	Sapphire
Zeoticus	Cryptopxj	Pysa	CryLock	BlueCheeser	QrnaLock
	Crytox	Triplem	Geminice		PowLock
	DemonCrypt	WannaRen	Jest		Locment
	FTCode		Lbkut		LickyAgent
	Ledif		OnaLocker		Krygo
	Makop		Ooglego		Funicorn
	Morrisbatchcrypt		Sadogo		Freefil
	OnyxLocker		Sfile2		Escal
	Ragnarok		Upper		CyberThanos
	Ranscrape		Void		Chimera
	Trsomware		Wreath		BlackMoon
	WannaCash				BlackKingdom
	WannaScream				BlackClaw
	Wilboy				Avaddon

JUL	AUG	SEP	OCT	NOV	DEC
Xinof	Tappif	Aidsnt	Doowtar	Hiddeneargdarmerie	AgeLocker
WhoLocker	SunCrypt	BitMiner	EyeCryLocker	RanzyLocker	Alol
Wastedlocker	Silvertor	BlackKnight	Hibuniel	WoodRat	BacuCrypt
ThiefQuest	RagnarLocker	BlackSquid	JarCrypt		Dusk
StrongPity	GiveMeTheKey	CoronaCryptor	LeakTheMall		Erica
Pojie	FlyingShip	DogeCrypt	Pay2Key		Godra
Panther	Exorcist	Egregor	RegretLocker		Hwru
Lolkek	DarkSide	Exx	SantaCrypt		RedRoman
JosephNull	CryptoLock	Gav			StingJar
EvilQuest	BigLock	HexaCrypt			Vaggen
CryCryptor		MountLocket			
Bead		ReadMan			
		Thanos			
		Vashsorena			
		Viluciware			
		Zhen			

The 10 most detected ransomware families in 2020

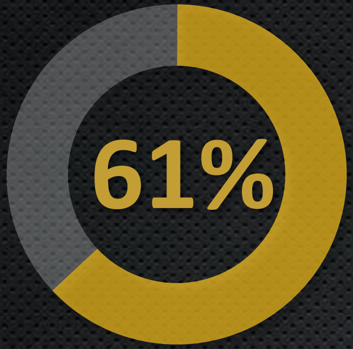


WCry	220,166
Locky	15,816
Cerber	5,448
Ryuk	3,376
GandCrab	2,326
Sodinokibi	2,275
Crysis	1,744
Crypwall	1,019
Egregor	827
DoppelPaymer	526

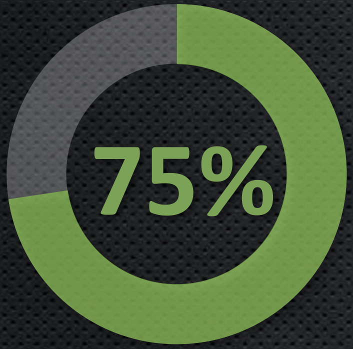
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report

Many manufacturers have experienced critical cyber breaches

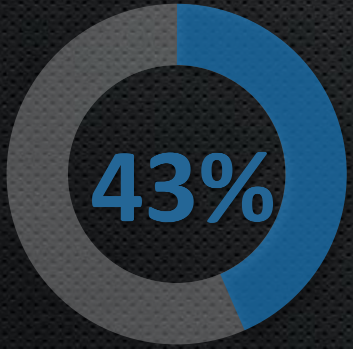
Trend Micro 2020 OT security survey with 500 respondents in US (200), Germany (150), and Japan (150)



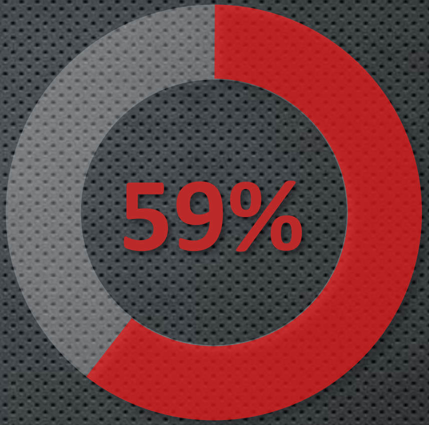
of manufacturers encounter cybersecurity incidents



of incidents caused production line stop



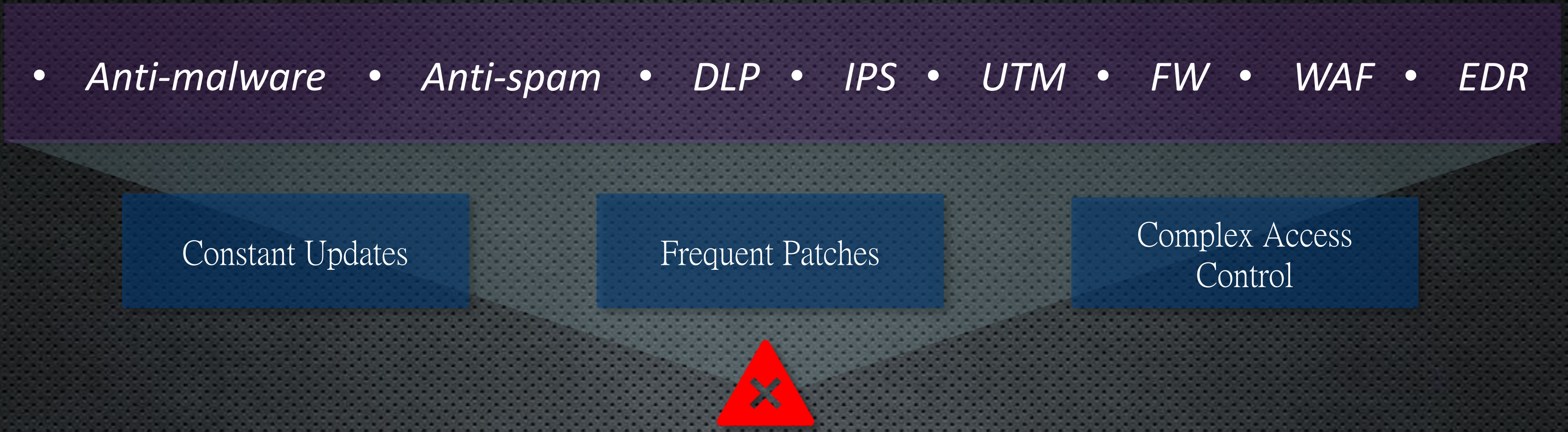
of incidents stopped the production line for more than 4 days



of respondents indicated the greatest challenge in OT cybersecurity is the lack of ICS cybersecurity solutions designed for their systems and devices

Source: https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

IT security products can’t meet the needs of OT



- *Anti-malware*
- *Anti-spam*
- *DLP*
- *IPS*
- *UTM*
- *FW*
- *WAF*
- *EDR*

Constant Updates

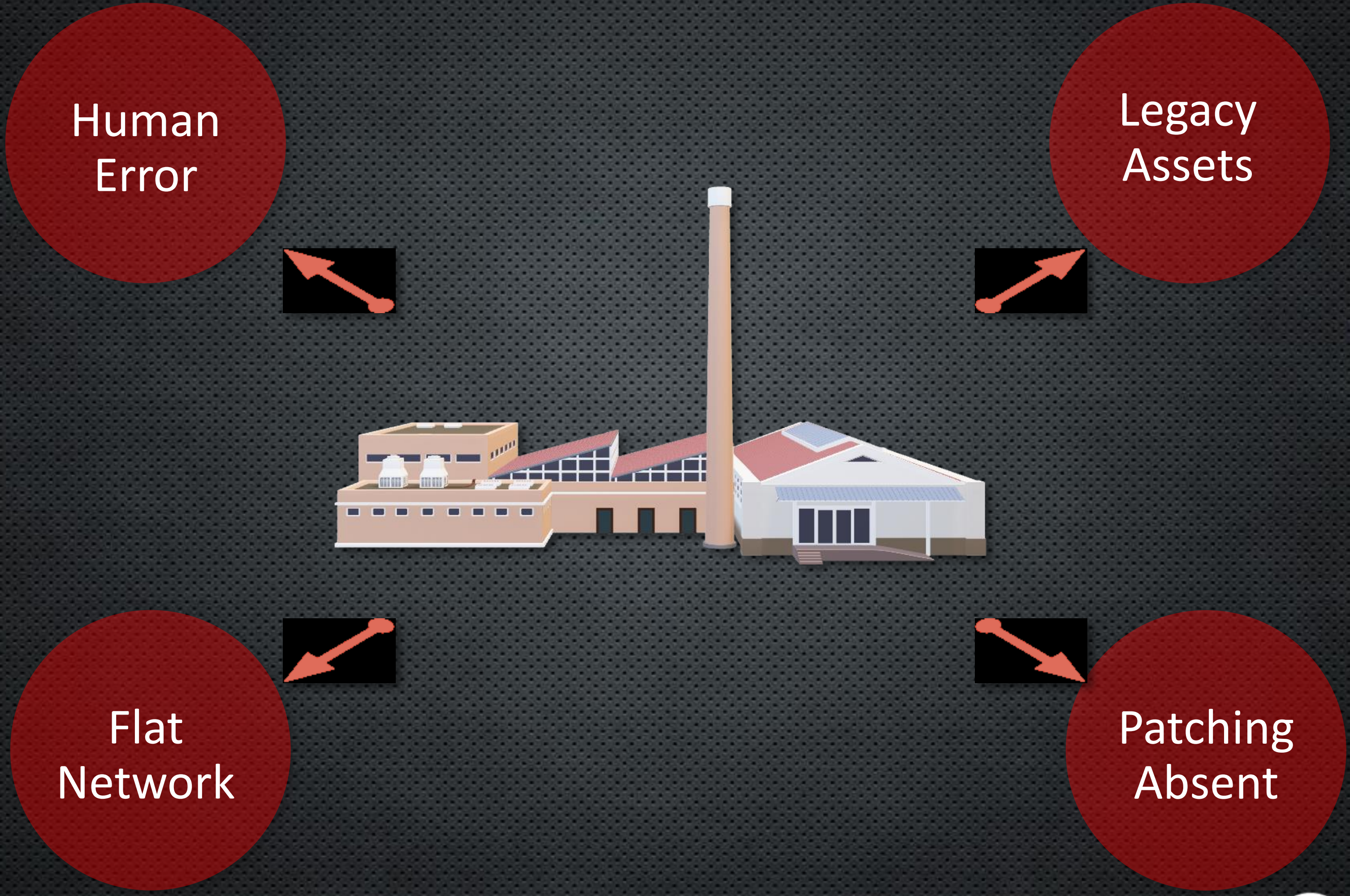
Frequent Patches

Complex Access Control

- Automation system downtimes must not exceed a few milliseconds
- The mean time to patch (MTTP) for SCADA is around 146 days
- Harsh working environments include high temperature, vibration, and humidity

- Typical IT approaches and solutions conflict with OT-related security objectives
- ICS cybersecurity solutions must be adaptative enough for industrial operations

Typical reasons OT/ICS is so vulnerable



Human Error

Intentional or unintentional insiders can bring in malware or mis-operate the PLC and critical assets

Legacy Assets

Massive number of assets with mixed, complex systems including legacy and EOL operating systems

Flat Network

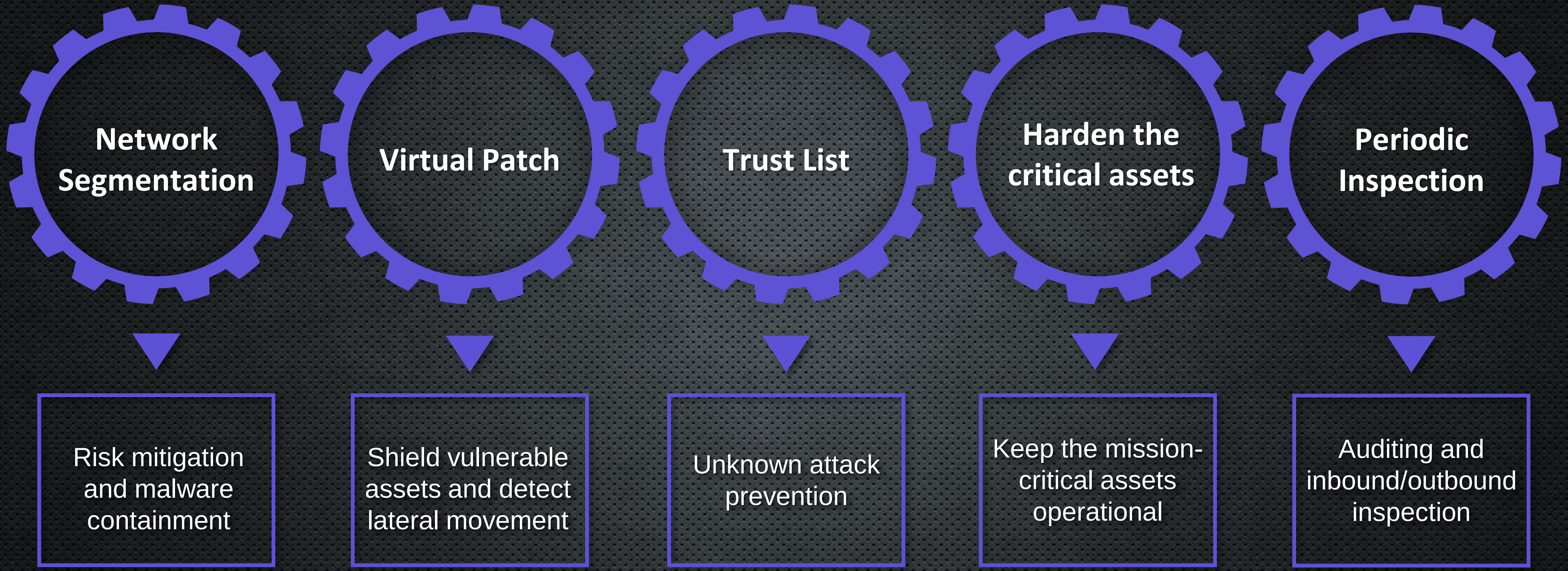
No network segmentation, in many cases the whole network is a big flat L2 network

Patching Absent

Difficult to conduct the patching and updating process while maintaining high productivity

Best Practices and Real Cases

Best Practices for ICS Cybersecurity Resilience



Network Segmentation

Risk mitigation and malware containment

Virtual Patch

Shield vulnerable assets and detect lateral movement

Trust List

Unknown attack prevention

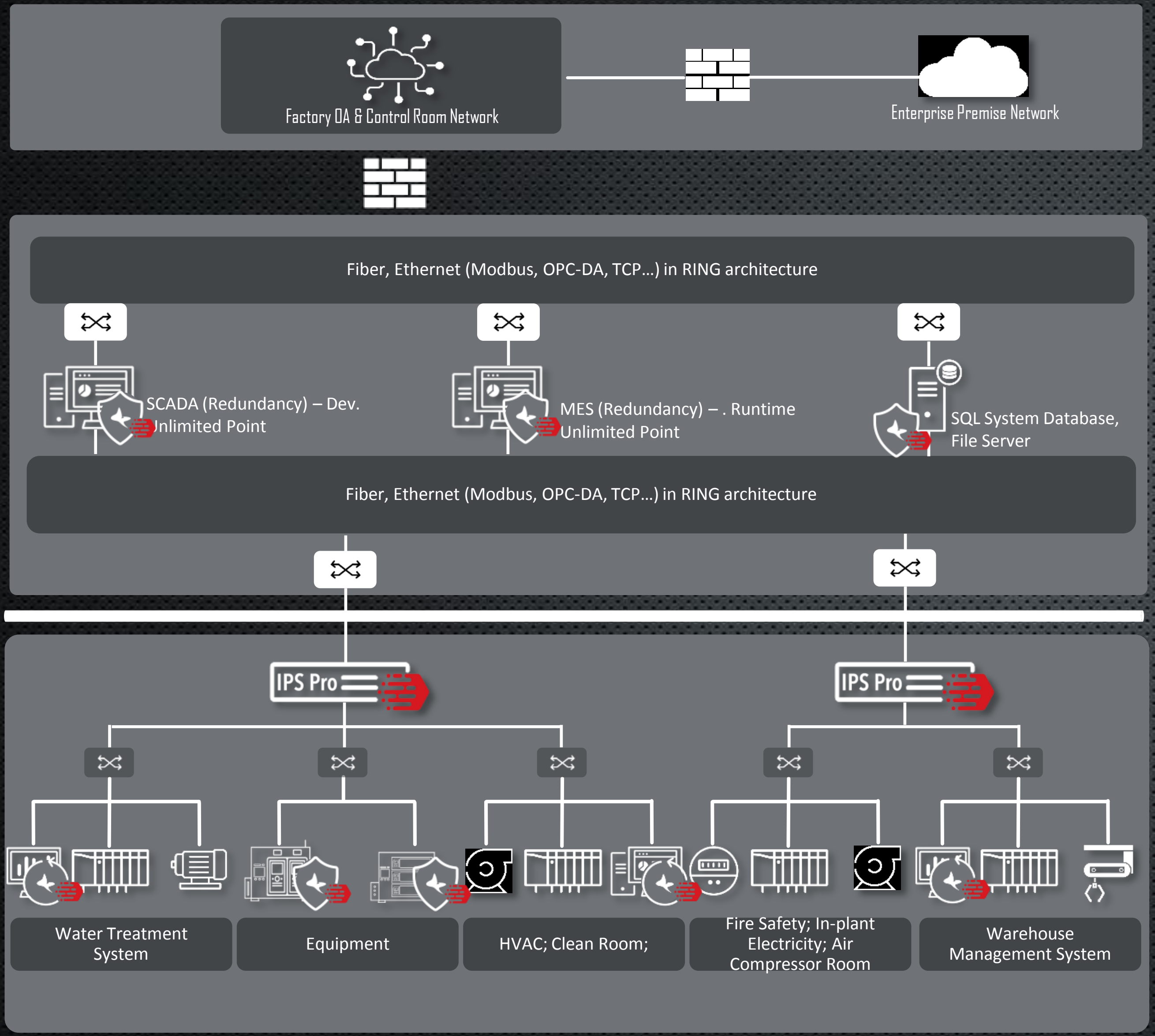
Harden the critical assets

Keep the mission-critical assets operational

Periodic Inspection

Auditing and inbound/outbound inspection

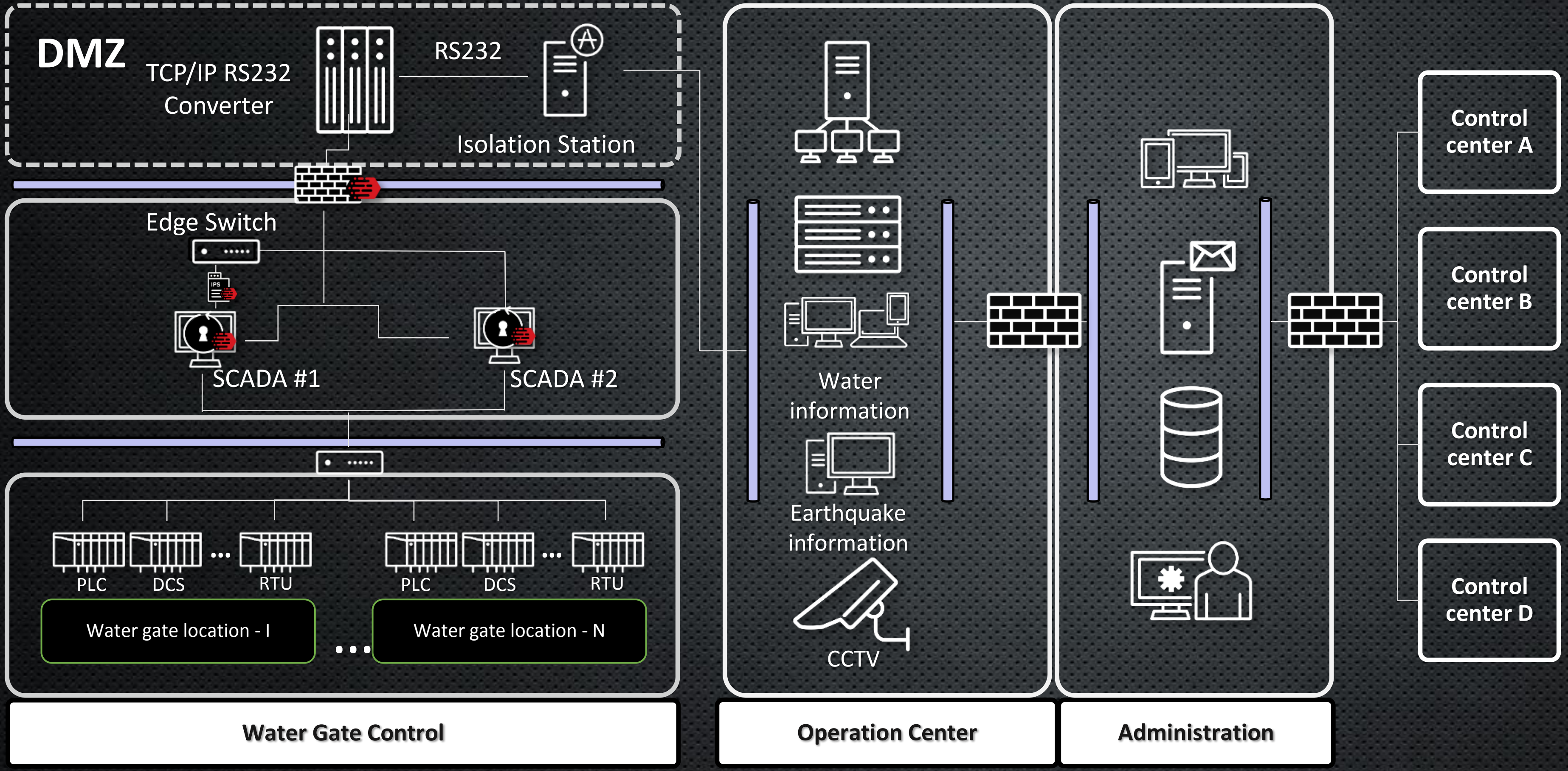
Using semiconductor foundries as an example



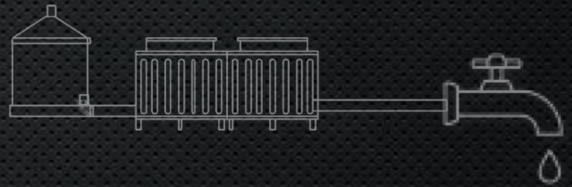
Factory OA & Control Room Network
Enterprise Premise Network
Fiber, Ethernet (Modbus, OPC-DA, TCP…) in RING architecture
SCADA (Redundancy) – Dev.
Unlimited Point
MES (Redundancy) – . Runtime
Unlimited Point
SQL System Database,
File Server
Fiber, Ethernet (Modbus, OPC-DA, TCP…) in RING architecture
IPS Pro
IPS Pro
Water Treatment System
Equipment
HVAC; Clean Room;
Fire Safety; In-plant Electricity; Air Compressor Room
Warehouse Management System

- *Network segmentation to prevent worm propagation and mitigate lateral movement*
- *Hardening OT-ICS endpoints*
  - *Lockdown fixed-function devices as well as legacy OS*
  - *Secure servers, workstations, and frequently-updated tools*
- *Equipment suppliers must ensure to comply with Virus-Free Policy*

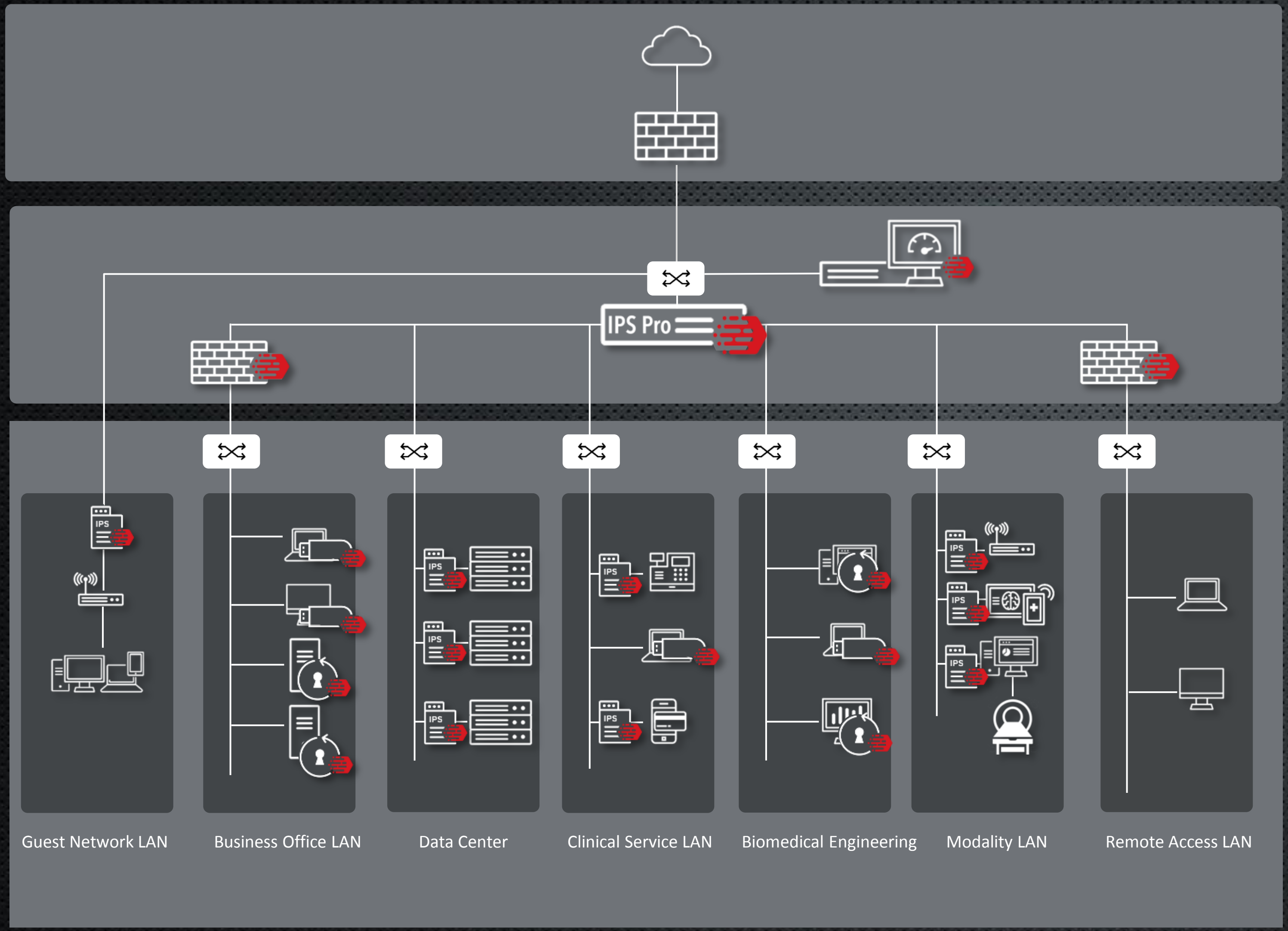
Preventing misuse and mis-operation at critical infrastructure



- *Deployed a trust list for both the network and endpoints to avoid human errors and possible insider attacks*



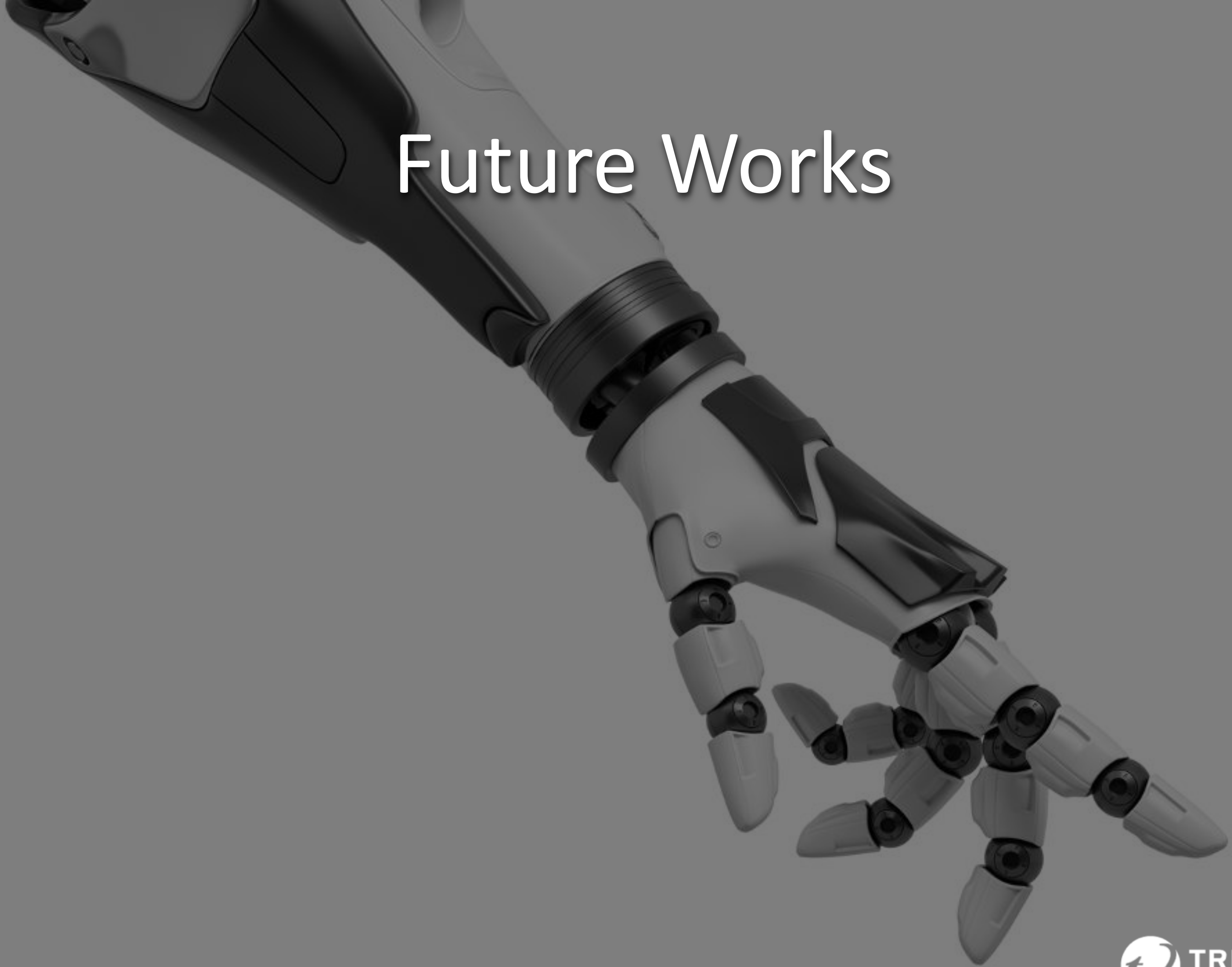
Helping several medical centers to deal with vulnerable legacy modalities



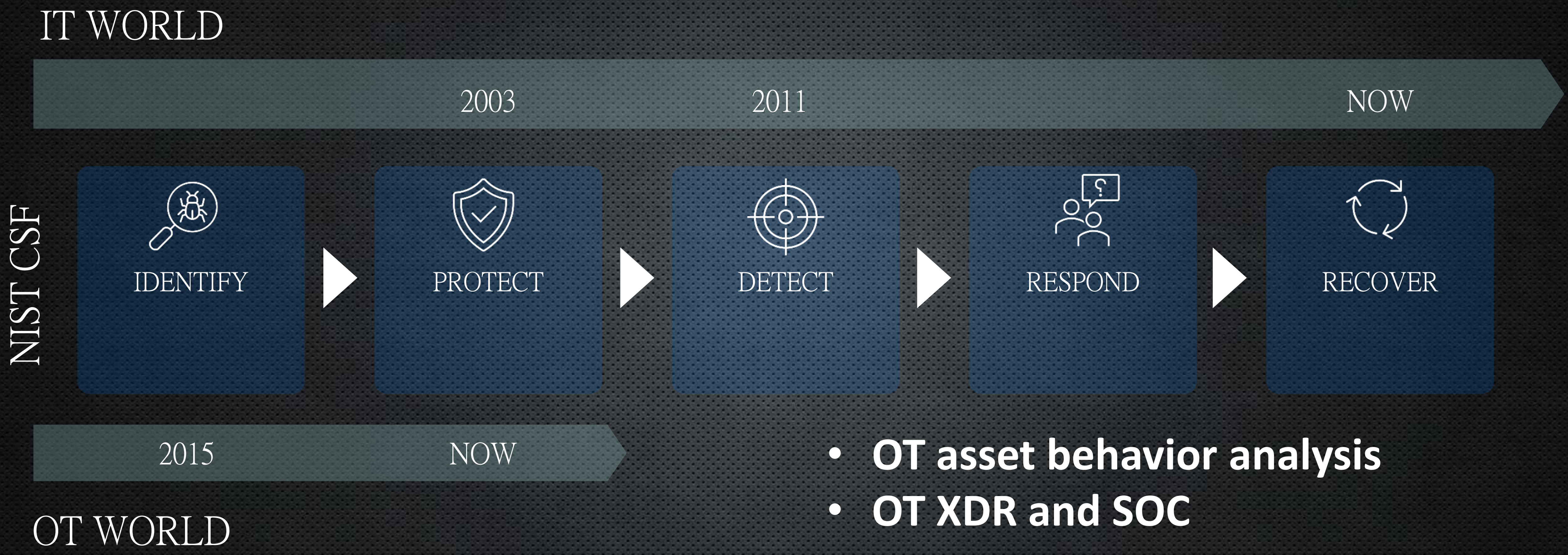
- *Hardening the modalities*
- *Virtual patch shields legacy OS endpoints*
- *Network segmentation to reduce other attack surfaces*

TREND MICRO™ txOne™ networks

Future Works



Following the path of IT cybersecurity functions



IT WORLD

2003 2011 NOW

NIST CSF

IDENTIFY → PROTECT → DETECT → RESPOND → RECOVER

2015 NOW

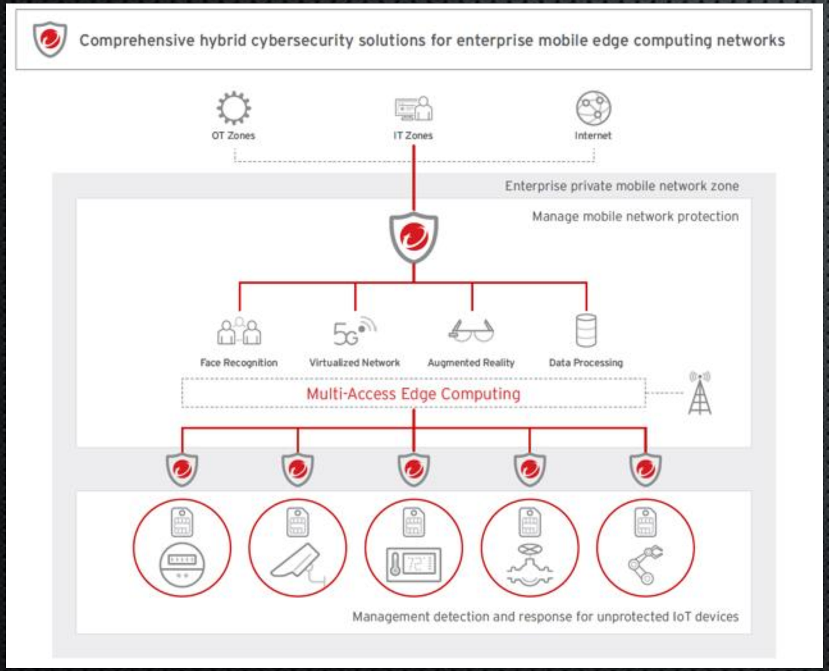
OT WORLD

- **OT asset behavior analysis**
- **OT XDR and SOC**

COMPUTING

Virtualization, Private Cloud, and Edge Computing

- OT servers, all workstations, and even PLCs will be virtualized and running on COTS hardware
- Edge Cloud


Comprehensive hybrid cybersecurity solutions for enterprise mobile edge computing networks
OT Zones
IT Zones
Internet
Enterprise private mobile network zone
Manage mobile network protection
Face Recognition
Virtualized Network
Augmented Reality
Data Processing
Multi-Access Edge Computing
Management detection and response for unprotected IoT devices

Adapting to Infrastructure changes

CONNECTIVITY

Time-Sensitive Network (TSN), 5G, Wifi6

Remotely controlling

- High Bandwidth (5G eMBB)
- Low Latency (5G URLLC)

Communication inside the digital factory

- Wifi6

Time-critical, reliable process optimization

- Low Latency - TSN

Cost-saving for outdoor connectivity

- High Coverage – 5G mMTC

Summary

IT-OT convergence drives changes to OT security

Hackers are aiming at manufacturers and critical infrastructure

Take practical and effective approaches to ensure operational resilience

TREND MICRO

txOne networks