FORTINET

Cybersecurity for Industry 5.0: Protecting OT and IIoT in a Connected Era

Dr. Rattipong Putthacharoen, Com. Eng.

Senior Manager, Systems Engineering

Agenda

1 Industry 5.0 and Industrial Threats

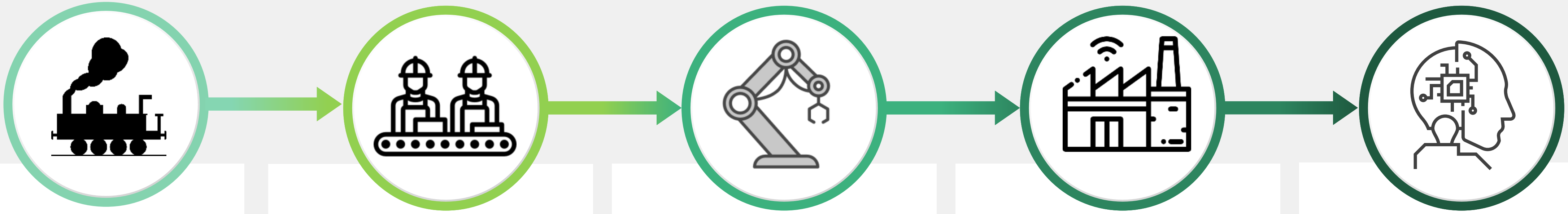
2 OT Security Standards for Industry 5.0

3 OT Security for Industry 5.0

4 Industrial IoT (IIoT) Security for Industry 5.0

Industry 5.0 and Industrial Threats

Industrial Revolutions



1800

Mechanization, water and steam powers

INDUSTRY 1.0

1900

Mass production, electric power, assembly line

INDUSTRY 2.0

2000

Computers, automated production, electronics

INDUSTRY 3.0

2010

Cyber-physical systems, IoT, networking, machine learning

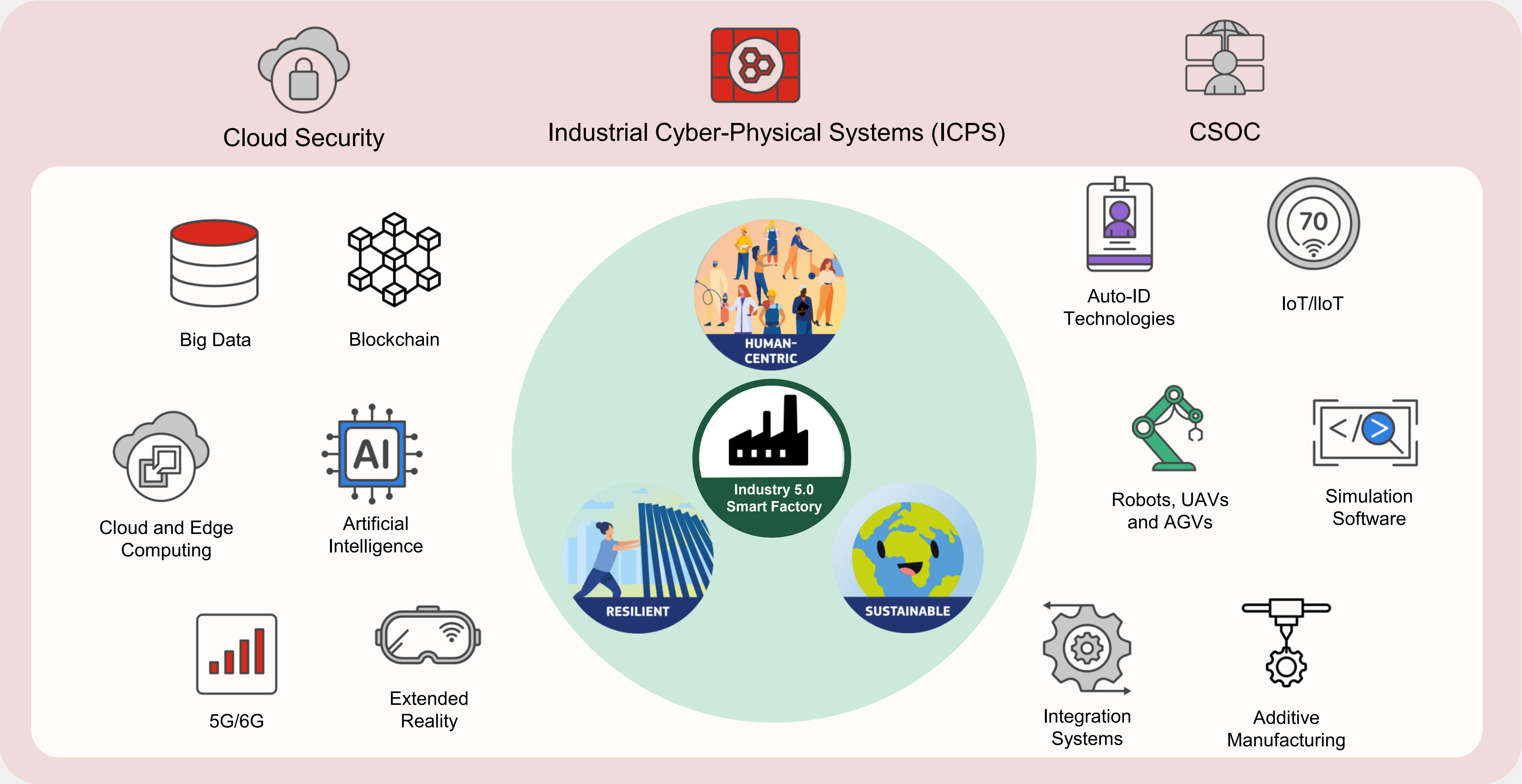
INDUSTRY 4.0

2020

Human-robot collaboration, cognitive systems, customization

INDUSTRY 5.0

Industry 5.0 Smart Factory



Cloud Security

Industrial Cyber-Physical Systems (ICPS)

CSOC

Big Data

Blockchain

Cloud and Edge Computing

Artificial Intelligence

5G/6G

Extended Reality

HUMAN-CENTRIC

Industry 5.0 Smart Factory

RESILIENT

SUSTAINABLE

Auto-ID Technologies

IoT/IIoT

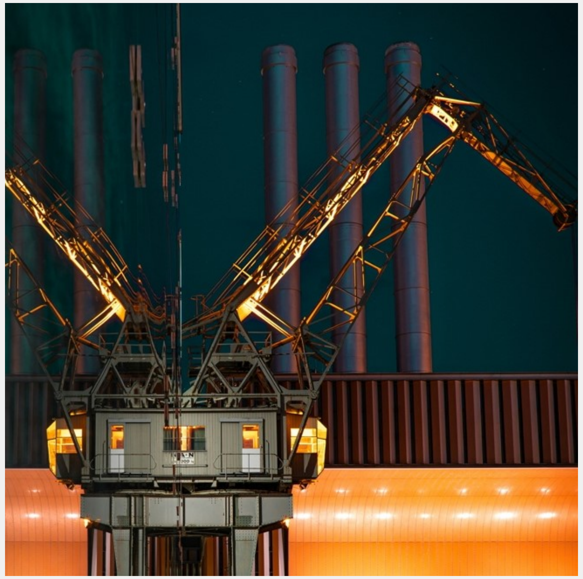
Robots, UAVs and AGVs

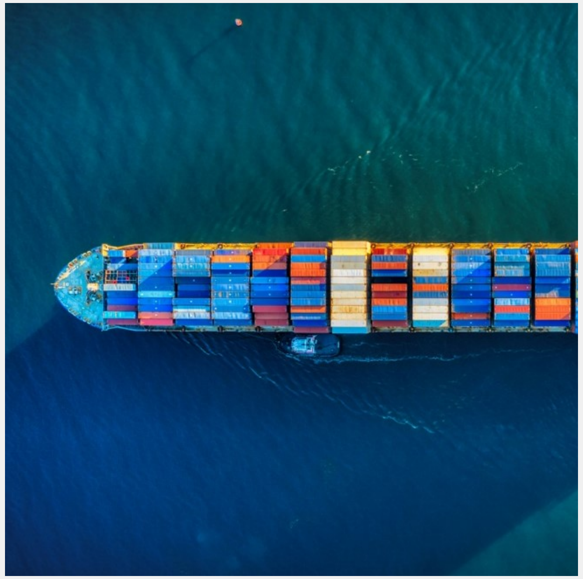
Simulation Software

Integration Systems

Additive Manufacturing

Securing Operational Technology Challenges





Most industrial control systems lack security by design and are sensitive to change

The attack surface for cyber-physical assets is expanding, dependence on air-gap protection is diminishing

Digital transformation (Industry 4.0) initiatives driving IT-OT network convergence

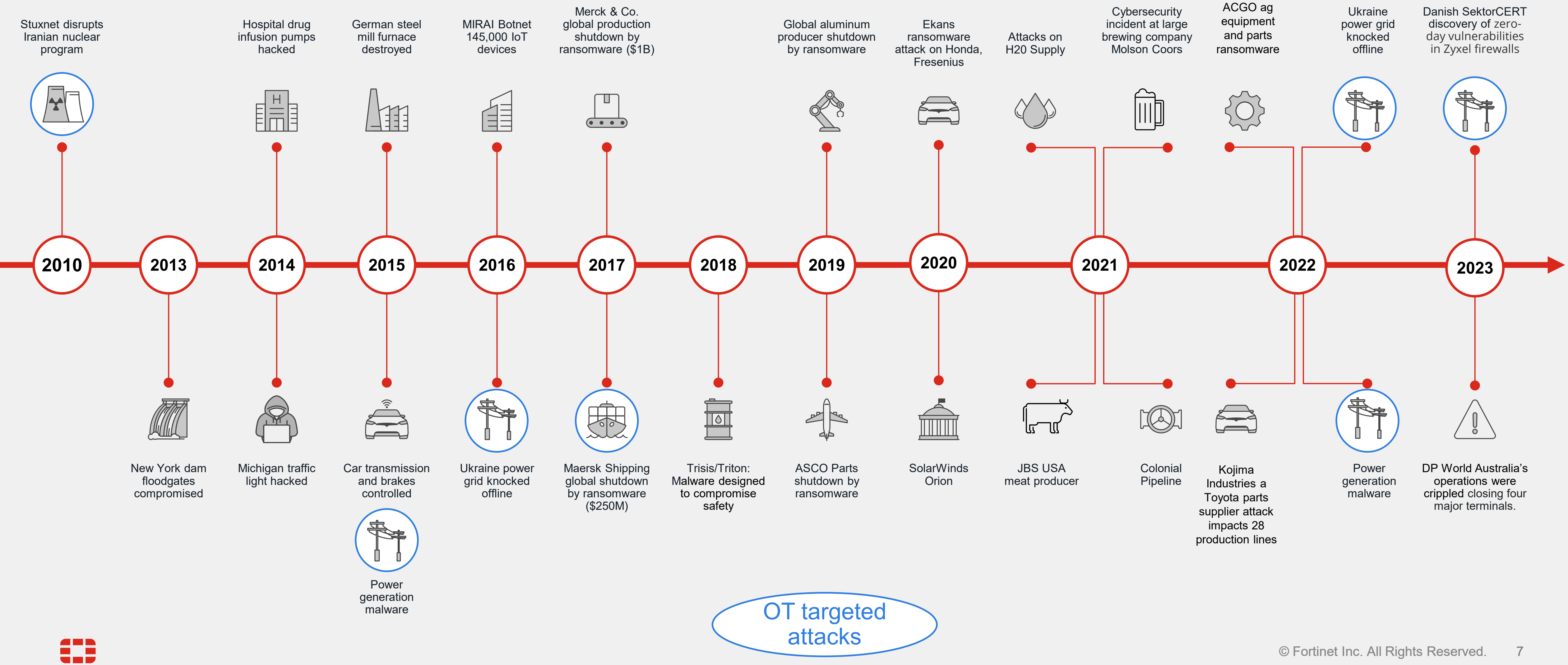
Increasing adoption of new technologies, such as 5G, IoT, and Cloud

Remote access requirements for third-parties and employees causing additional risks

Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks

OT Infrastructure Attacks Are Getting Worse

Attacks are increasing in frequency and impact



2010

Stuxnet disrupts Iranian nuclear program

2013

New York dam floodgates compromised

2014

Hospital drug infusion pumps hacked

Michigan traffic light hacked

2015

German steel mill furnace destroyed

Car transmission and brakes controlled

Power generation malware

2016

MIRAI Botnet 145,000 IoT devices

Ukraine power grid knocked offline

2017

Merck & Co. global production shutdown by ransomware ($1B)

Maersk Shipping global shutdown by ransomware ($250M)

2018

Trisis/Triton: Malware designed to compromise safety

2019

Global aluminum producer shutdown by ransomware

ASCO Parts shutdown by ransomware

2020

Ekans ransomware attack on Honda, Fresenius

SolarWinds Orion

2021

Attacks on H20 Supply

Cybersecurity incident at large brewing company Molson Coors

JBS USA meat producer

Colonial Pipeline

2022

ACGO ag equipment and parts ransomware

Ukraine power grid knocked offline

Kojima Industries a Toyota parts supplier attack impacts 28 production lines

Power generation malware

2023

Danish SektorCERT discovery of zero-day vulnerabilities in Zyxel firewalls

DP World Australia's operations were crippled closing four major terminals.

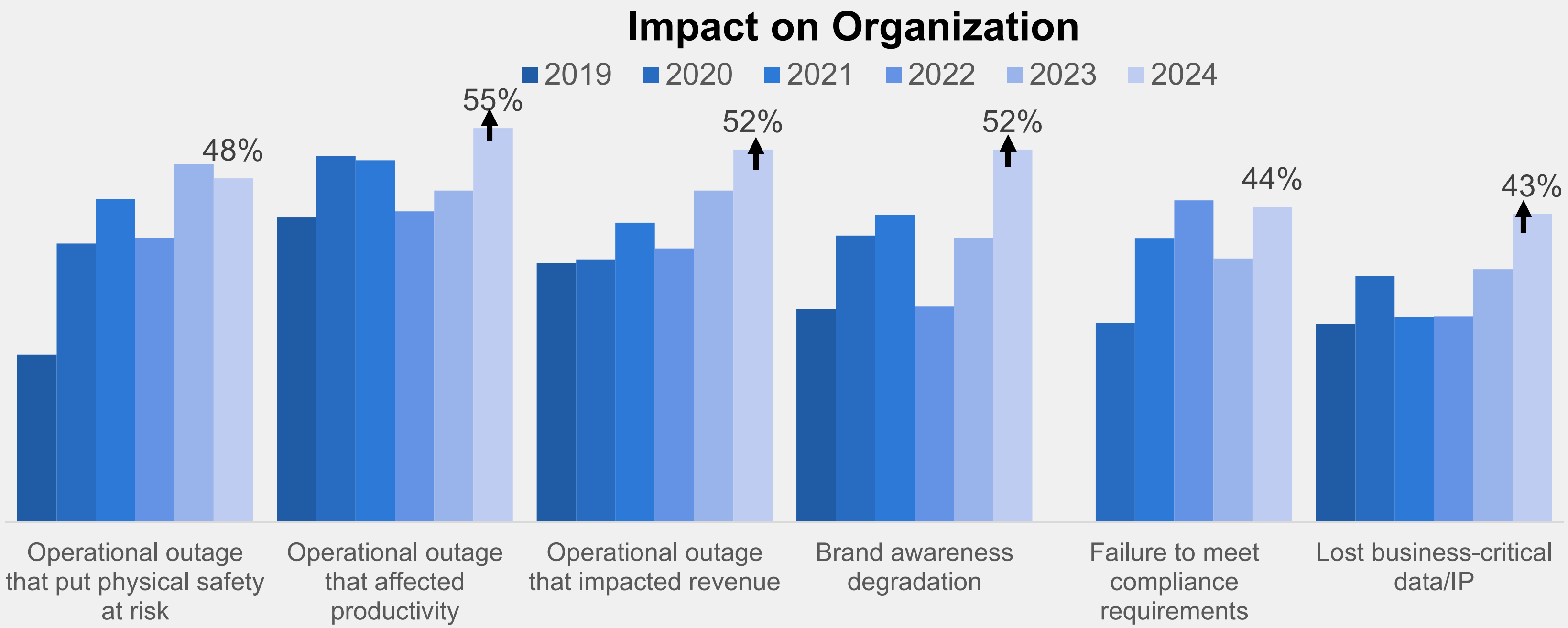
OT targeted attacks

OT Risk Is Proportional to OT Connectivity

CISO assuming responsibility for OT Cybersecurity

6 out of 10

OT organizations experienced 3 or more intrusions in the past year



Critical Insights…

62% **Mobile security breaches** ranked **highest** in techniques involved in intrusions

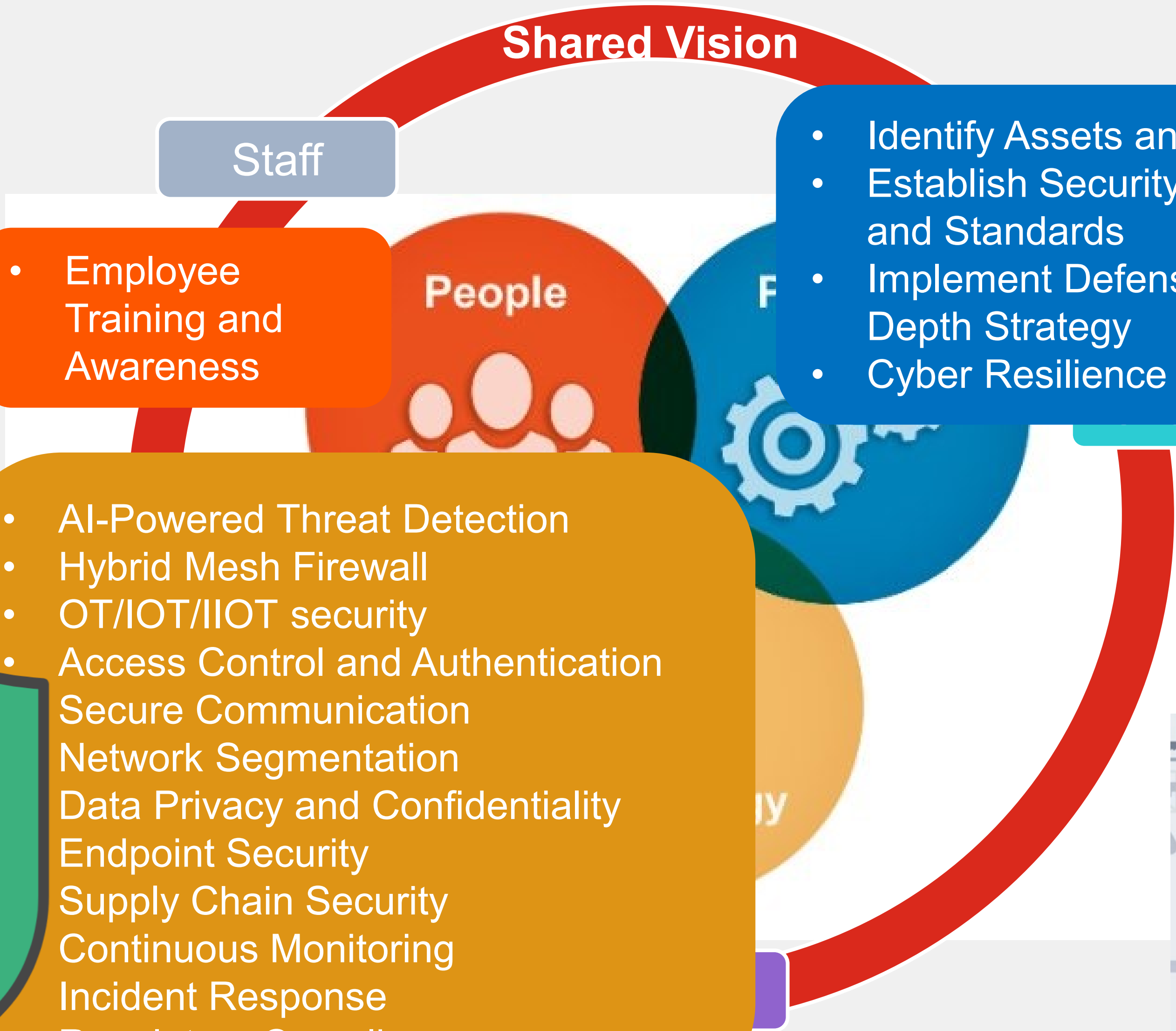
49% Both **IT and OT systems were impacted by an intrusion**, 24% OT only, 28% IT only

…**network segmentation, security training, and role-based access** are the areas that show the most significant growth this year.

Source: 2024 State of Operational Technology and Cybersecurity Report

OT Security Standards for Industry 5.0

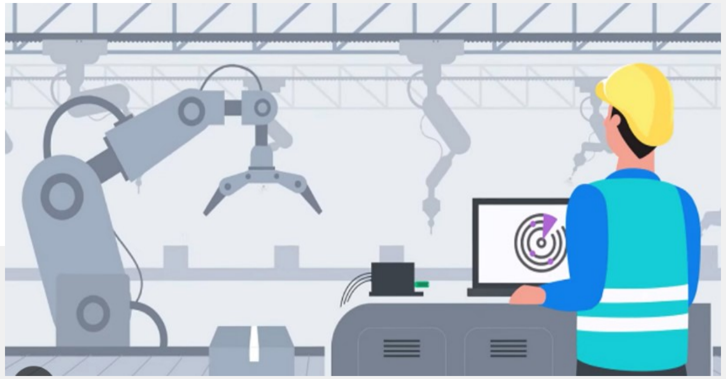
Cybersecurity in Industry 5.0



- Employee Training and Awareness

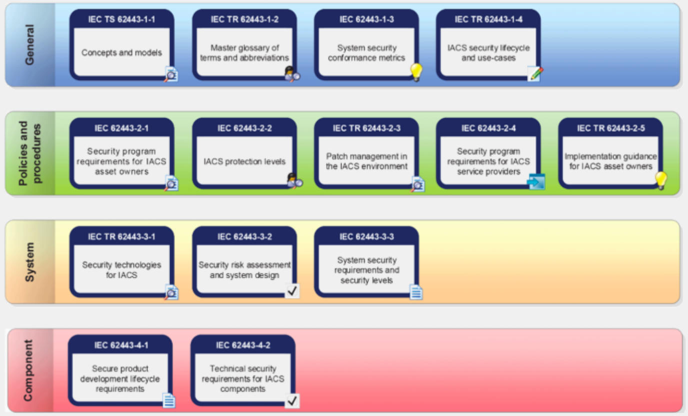
- Identify Assets and Risks
- Establish Security Policies and Standards
- Implement Defense-in-Depth Strategy
- Cyber Resilience Planning

- AI-Powered Threat Detection
- Hybrid Mesh Firewall
- OT/IOT/IIOT security
- Access Control and Authentication
- Secure Communication
- Network Segmentation
- Data Privacy and Confidentiality
- Endpoint Security
- Supply Chain Security
- Continuous Monitoring
- Incident Response
- Regulatory Compliance



Industry Standards for OT

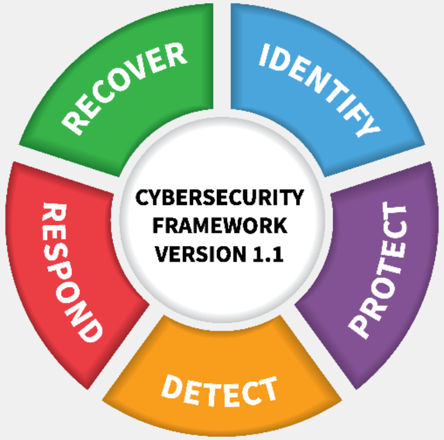
Globally accepted standard best practices for cybersecurity



General	IEC TS 62443-1-1 Concepts and models	IEC TR 62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR 62443-1-4 IACS security lifecycle and use-cases	
Policies and procedures	IEC 62443-2-1 Security program requirements for IACS asset owners	IEC 62443-2-2 IACS protection levels	IEC TR 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Security program requirements for IACS service providers	IEC TR 62443-2-5 Implementation guidance for IACS asset owners
System	IEC TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security risk assessment and system design	IEC 62443-3-3 System security requirements and security levels		
Component	IEC 62443-4-1 Secure product development lifecycle requirements	IEC 62443-4-2 Technical security requirements for IACS components			

IEC 62443

Cybersecurity Standards



NIST SP 800-82r3

Guide to OT Security

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC- CIP

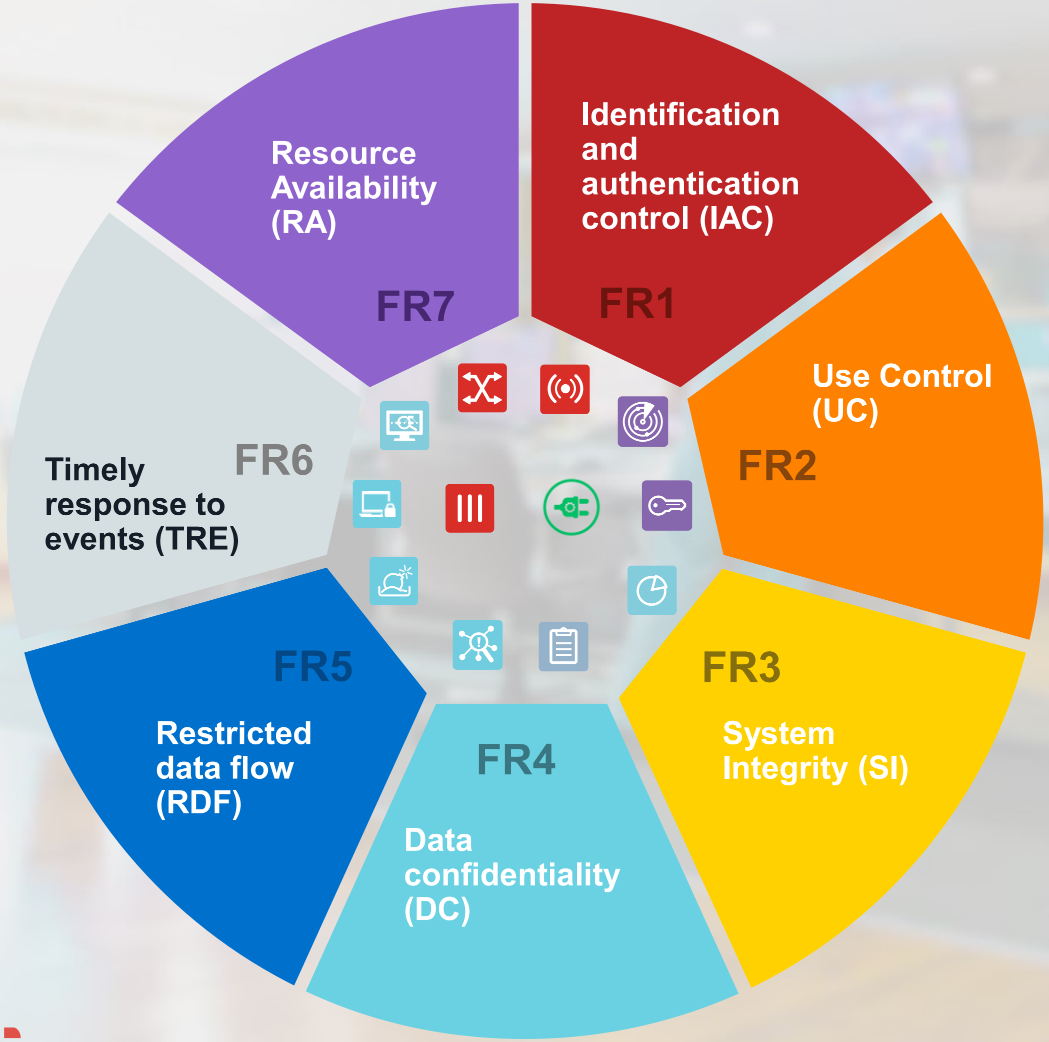
Critical Infrastructure Protection

มอก. 62443

Integrity, Availability, Confidentiality and Safety (IACS)

IEC 62443

Contain methods encompassing People, Processes and Technology to attain required IACS Security Levels (SL's)


Identification and authentication control (IAC)
FR1
Use Control (UC)
FR2
FR3
System Integrity (SI)
FR4
Data confidentiality (DC)
FR5
Restricted data flow (RDF)
Timely response to events (TRE)
FR6
Resource Availability (RA)
FR7

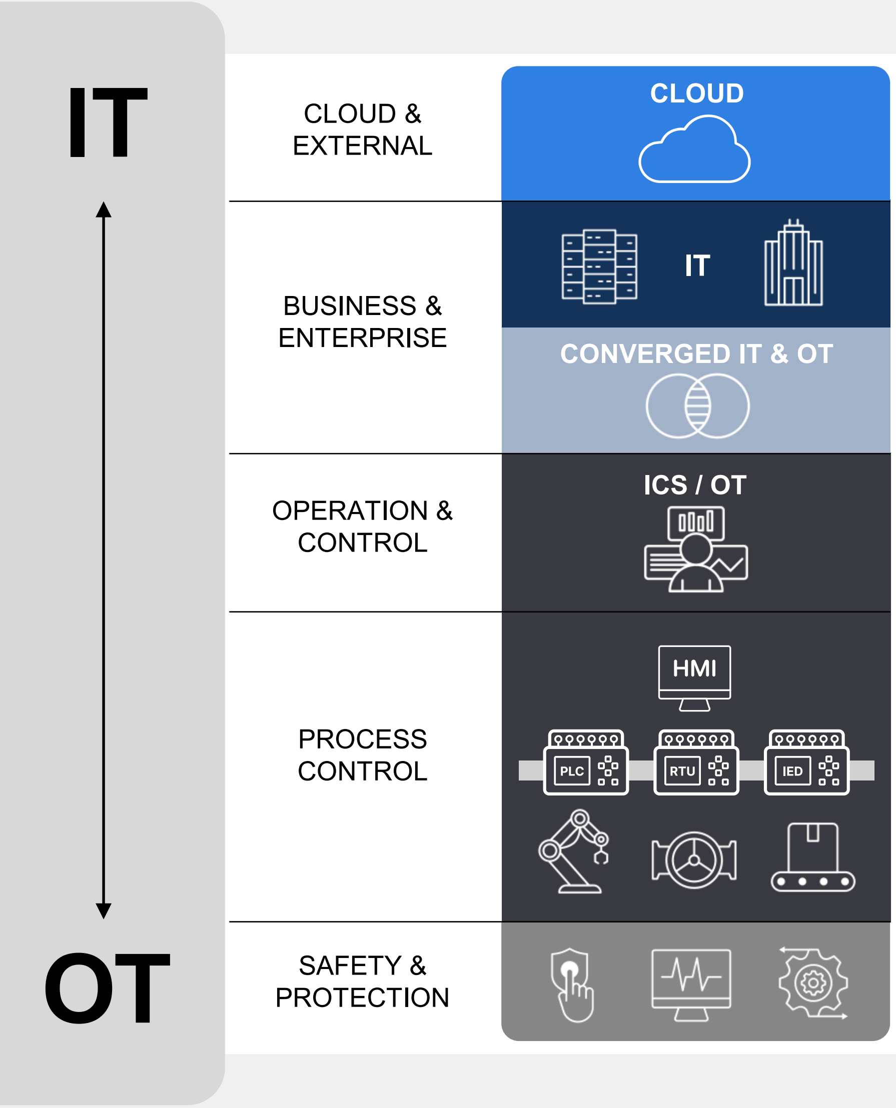
IEC 62443-3-3 System Requirements

Foundational Requirements	Mitigation Techniques
FR1. Access Control (AC) Identify and authenticate all entities attempting to access the ICS.	• Multi Factor Authentication
FR2. Use Control (UC) Enforce privileges of an authenticated Entity, monitoring the proper use and actions.	• Restrict Data to External Zones • Time of Day Access Restrictions
FR3. System Integrity (SI) Ensure integrity, prevent unauthorized manipulation.	• Advanced Threat Protection
FR4. Data Confidentiality (DC) Ensure confidentiality on communication channels and data repositories, prevent data disclosure.	• Encryption • Continuous Monitoring
FR5. Restricted Data Flow (RDF) Segment the control system via zones and conduits to limit the unnecessary flow data.	• Network Segmentation
FR6. Timely Response to Events (TRE) Response to security violations, notifying and reporting evidence and taking timely corrective actions.	• Audit System Logs • Alert & Monitoring
FR7. Resource Availability (RA) Ensure the availability of the control system against the degradation or denial of essential services.	• High Availability • DDoS Protection

What controls are essential to secure OT environments?

Zones and Conduits	Segmentation protects OT from mistakes and bad actors.
Secure Remote Connectivity	Enable secure access for employees and third-parties who connect to your OT environment.
Deep OT Visibility	Detect abnormal activities and attacks, and collect the security events in OT.
Role-based Access Control	Limit access to only those who need it.
Endpoint Security	Apply endpoint security protection to the servers at and near the secure perimeter.
NOC / SOC	Synergistic benefits of managing everything in one place.
Advanced Persistent Threat	Advanced Persistent Threats (APT) require advanced solutions.

Lead with Fortinet OT Security Platform



IT

OT

CLOUD & EXTERNAL	CLOUD
BUSINESS & ENTERPRISE	IT CONVERGED IT & OT
OPERATION & CONTROL	ICS / OT
PROCESS CONTROL	
SAFETY & PROTECTION	

Secure Networking

Secure Digital Networks

- FortiGate
- FortiSRA
- FortiNAC
- FortiExtender
- FortiAP
- FortiSwitch

Unified SASE

Secure Service Edge

- FortiSASE
- FortiPAM
- FortiClient
- FortiClient EMS
- FortiAuthenticator
- 384629 FortiToken

Security Operations

Secure IT/OT Convergence

- FortISOAR
- FortiSIEM
- FortiManager
- FortiAnalyzer
- FortiDeceptor
- FortiNDR
- FortiEDR

Security Services

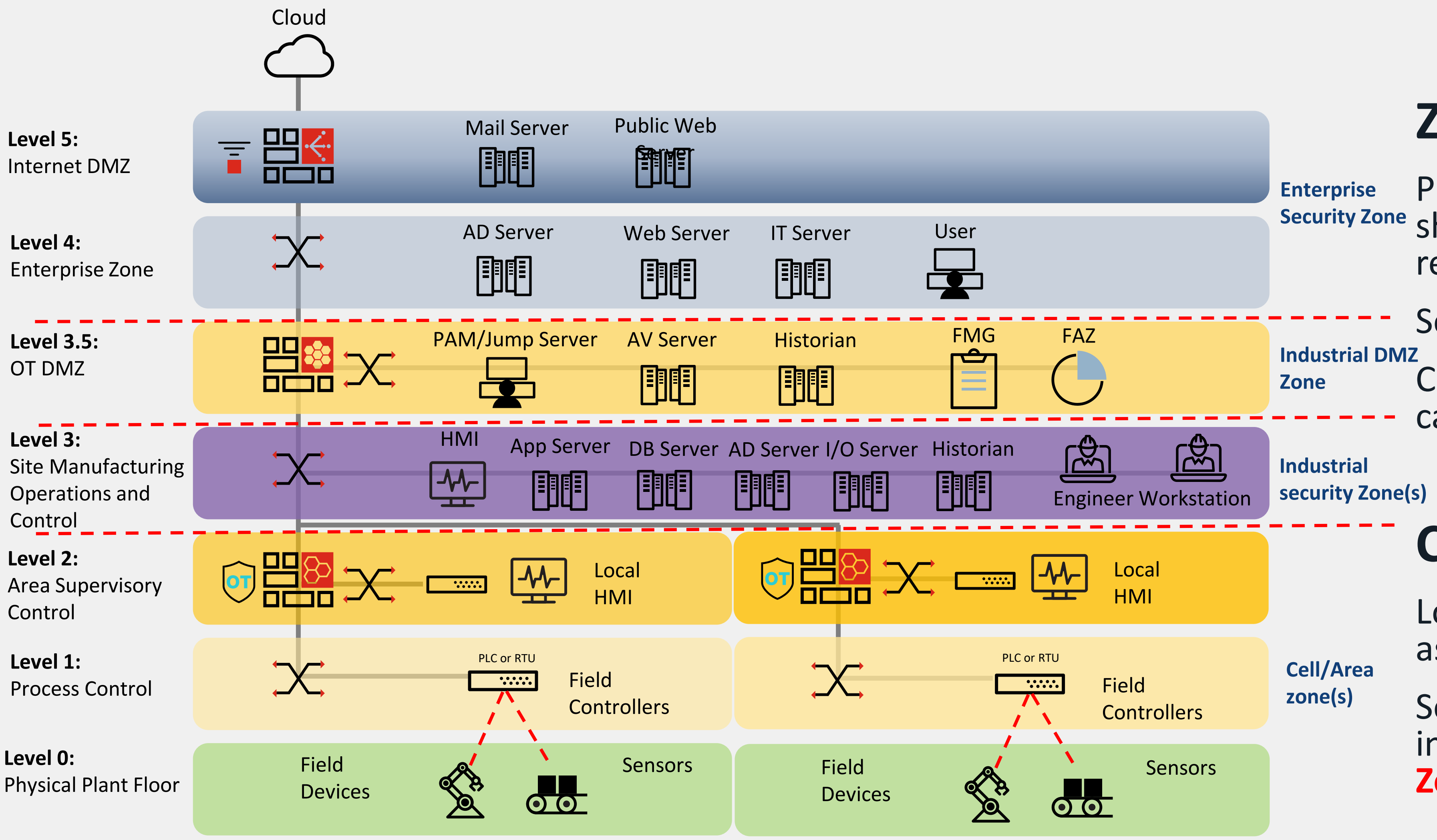
- OT Security Service
- OT Virtual Patching
- OT Device Detection

Ecosystem Partners

Fabric-Ready Partner Solutions

OT Architecture design: Purdue Model

Purdue Enterprise Reference Architecture (PERA)



Zones

Physical or logical grouping of assets sharing common security requirements

Security zones are never isolated

Connections between the zones are called **Conduits**

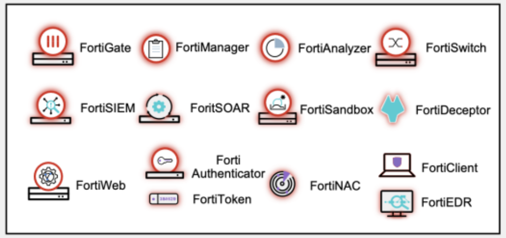
Conduits

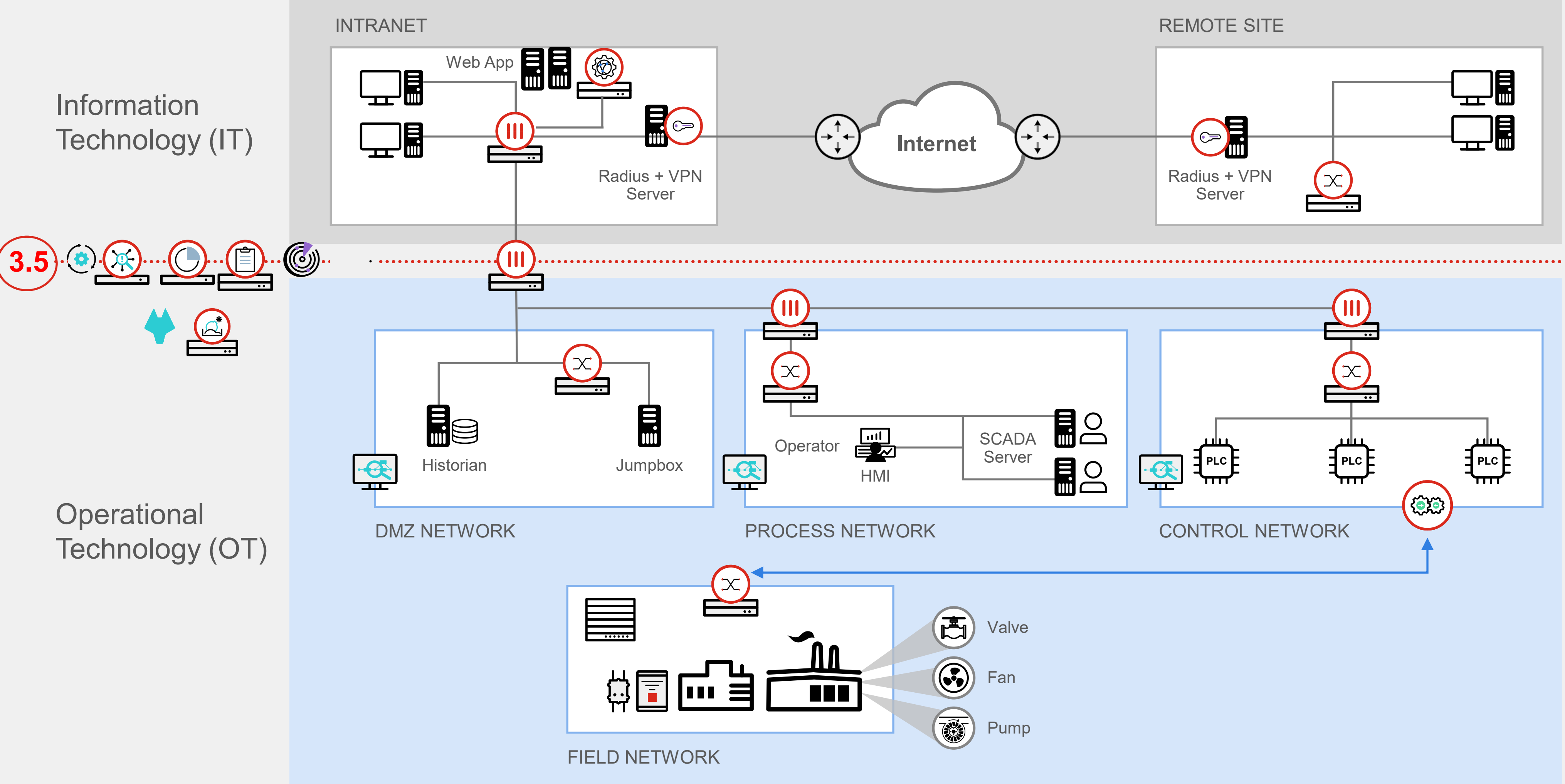
Logical grouping of communication assets

Secure the channels where information is flowing intra and extra **Zone**

Access Control, Network Segmentation, Least Function and Least Privilege

Critical Controls for IT and OT Integration

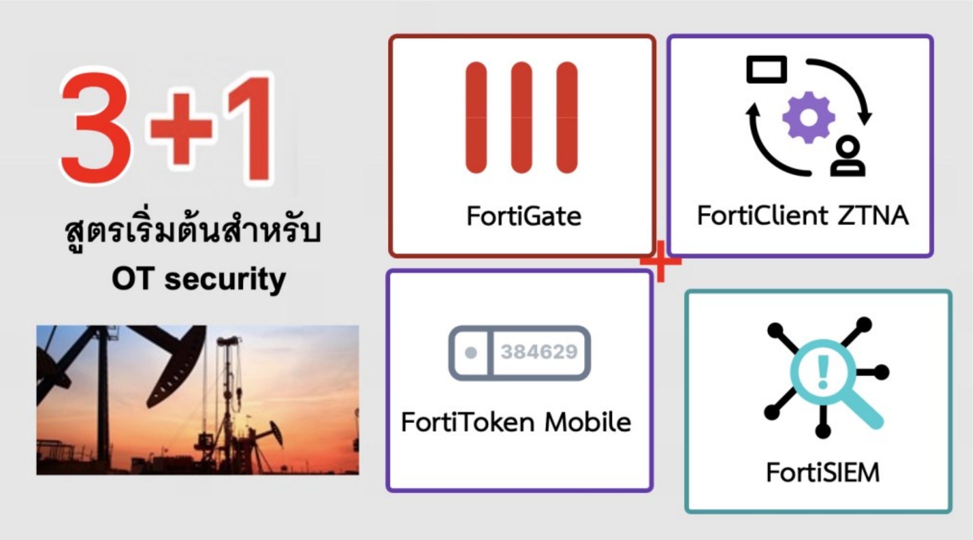




- Zones and Conduits
- Secure Remote Connectivity
- Deep OT Visibility
- Role-based Access Control
- Endpoint Security
- SOC
- Advanced Persistent Threat

OT Security for Industry 5.0

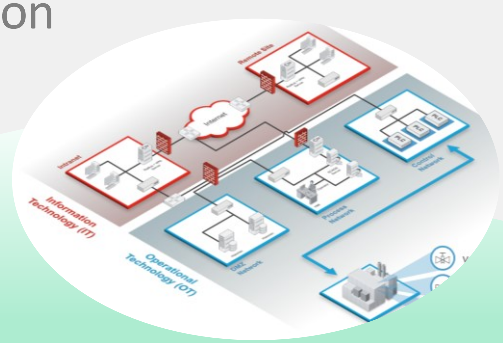
Basic 3 Steps for OT security

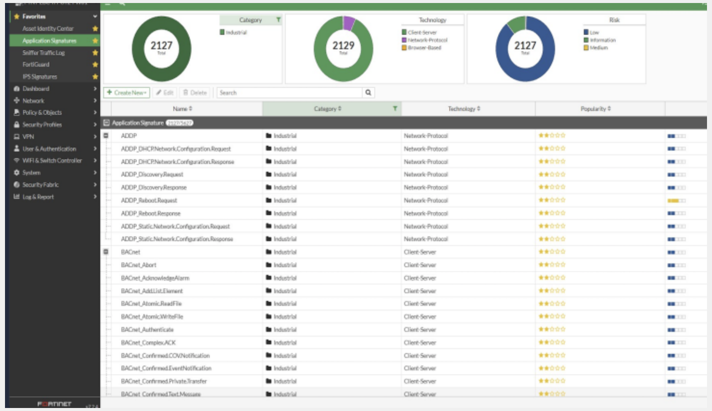


Zones and Conduits	Segmentation protects OT from mistakes and bad actors.
Secure Remote Connectivity	Enable secure access for employees and third-parties who connect to your OT environment.
Deep OT Visibility	Detect abnormal activities and attacks, and collect the security events in OT.
Role-based Access Control	Limit access to only those who need it.
Endpoint Security	Apply endpoint security protection to the servers at and near the secure perimeter.
SOC	Synergistic benefits of managing everything in one place.

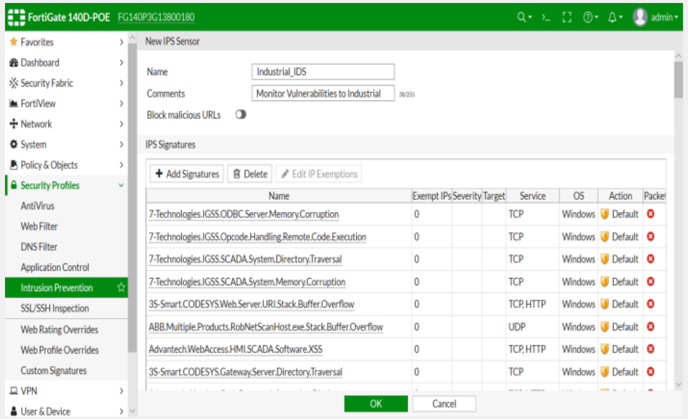
1. Segmentation using FortiGate

Provides Segmentation, Visibility and Protection





Name	Category	Technology	Popularity
Application Signature			
ADDP	Industrial	Network-Protocol	★★☆☆☆
ADDP_DHCP.Network.Configuration.Request	Industrial	Network-Protocol	★★☆☆☆
ADDP_DHCP.Network.Configuration.Response	Industrial	Network-Protocol	★★☆☆☆
ADDP_Discovery.Request	Industrial	Network-Protocol	★★☆☆☆
ADDP_Discovery.Response	Industrial	Network-Protocol	★★☆☆☆
ADDP_Reboot.Request	Industrial	Network-Protocol	★★☆☆☆
ADDP_Reboot.Response	Industrial	Network-Protocol	★★☆☆☆
ADDP_Static.Network.Configuration.Request	Industrial	Network-Protocol	★★☆☆☆
ADDP_Static.Network.Configuration.Response	Industrial	Network-Protocol	★★☆☆☆
BACnet	Industrial	Client-Server	★★☆☆☆
BACnet_Abort	Industrial	Client-Server	★★☆☆☆
BACnet_AcknowledgeAlarm	Industrial	Client-Server	★★☆☆☆
BACnet_AddList.Element	Industrial	Client-Server	★★☆☆☆
BACnet_Atomic.ReadFile	Industrial	Client-Server	★★☆☆☆
BACnet_Atomic.WriteFile	Industrial	Client-Server	★★☆☆☆
BACnet_Authenticate	Industrial	Client-Server	★★☆☆☆
BACnet_Complex.ACK	Industrial	Client-Server	★★☆☆☆
BACnet_Confirmed.COVNotification	Industrial	Client-Server	★★☆☆☆
BACnet_Confirmed.EventNotification	Industrial	Client-Server	★★☆☆☆
BACnet_Confirmed.Private.Transfer	Industrial	Client-Server	★★☆☆☆
BACnet_Confirmed.Text.Message	Industrial	Client-Server	★★☆☆☆



New IPS Sensor

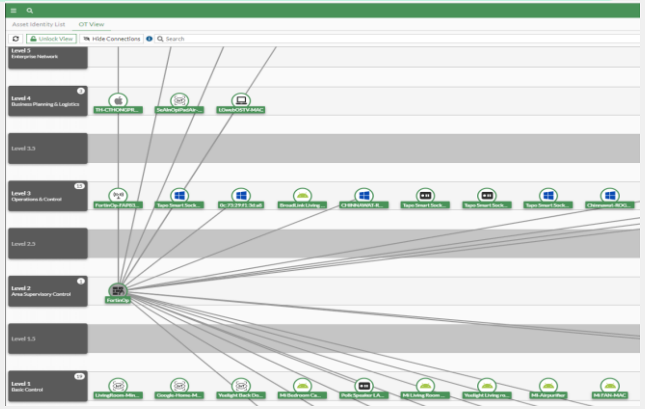
Name: Industrial_IDS

Comments: Monitor Vulnerabilities to Industrial 38/255

Block malicious URLs

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet
7-Technologies.IGSS.ODBC.Server.Memory.Corruption	0			TCP	Windows	Default	⊗
7-Technologies.IGSS.Opcode.Handling.Remote.Code.Execution	0			TCP	Windows	Default	⊗
7-Technologies.IGSS.SCADA.System.Directory.Traversal	0			TCP	Windows	Default	⊗
7-Technologies.IGSS.SCADA.System.Memory.Corruption	0			TCP	Windows	Default	⊗
3S-Smart.CODESYS.Web.Server.URI.Stack.Buffer.Overflow	0			TCP, HTTP	Windows	Default	⊗
ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow	0			UDP	Windows	Default	⊗
Advantech.WebAccess.HMI.SCADA.Software.XSS	0			TCP, HTTP	Windows	Default	⊗
3S-Smart.CODESYS.Gateway.Server.Directory.Traversal	0			TCP	Windows	Default	⊗



ICS/OT Applications & Protocols

FortiGuard Industrial Security Service provides broader coverage for Industrial Control System and Operational Technology protocols and application through Application Control and IPS signatures.

ICS/OT Intrusion Prevention

- Protect Known Vulnerability
- Prevent Zero day exploits
- Detect Protocol abnormalities
- Supports major ICS manufactures to provide vulnerability protection

Asset awareness and classification

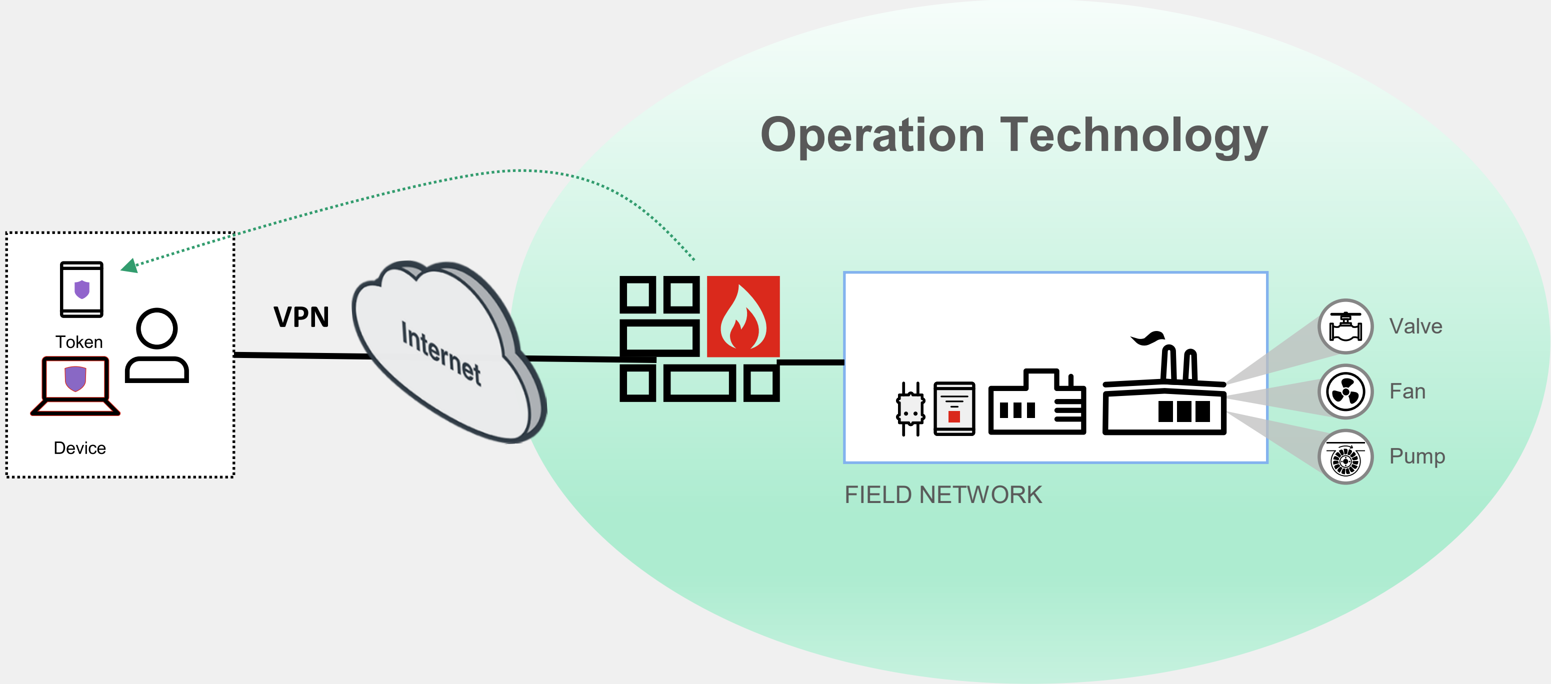
The Asset Identity Center page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend

2. Secure Remote Access with Zero Trust

FortiGate with FortiClient ZTNA and FortiToken Mobile

Simplified Secure Remote Access

- Built-in Remote Access Server in FortiGate
- Combination of Zero Trust Network Access and Endpoint Protection Platform in FortiClient
- Two Factor Authentication with FortiToken Mobile



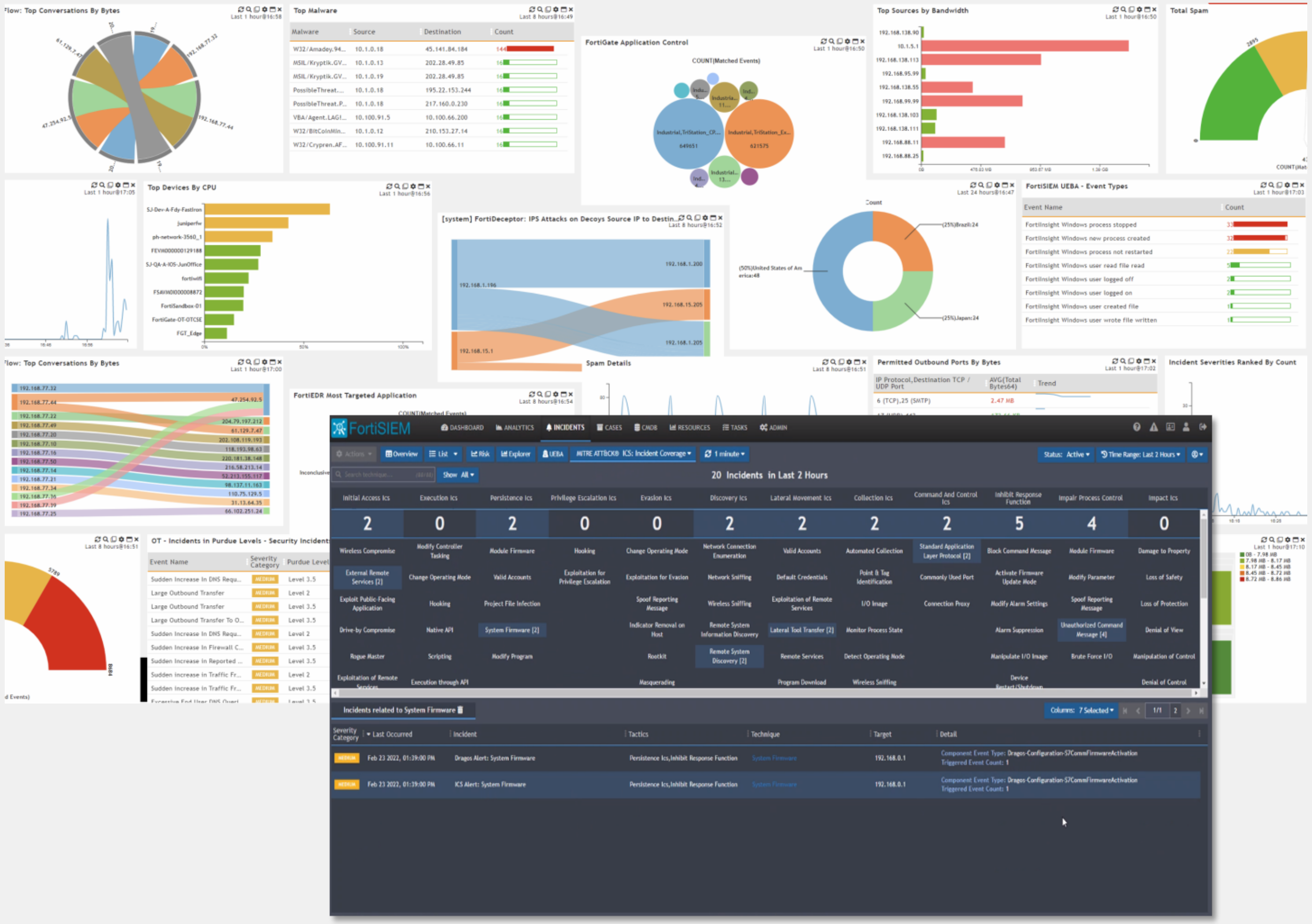
FortiToken Mobile

Multi-platform OATH OTP application with PUSH notification of login attempts and one tap approval

3. Continuous OT Security Monitoring using FortiSIEM

FortiSIEM ATT@CK Technique rules for ICS/OT

> *Three new MITRE ATT&CK dashboards for ICS are created to show Rule coverage, Incident coverage and Kill Chain analysis for ICS Techniques.*
>
> *Currently 84 ICS ATT&CK Technique detection rules are provided out of the box and similar support for other vendors can be added.*



Flow: Top Conversations By Bytes
Top Malware
FortiGate Application Control
Top Sources by Bandwidth
Total Spam
Top Devices By CPU
[system] FortiDeceptor: IPS Attacks on Decoys Source IP to Destin
FortiSIEM UEBA - Event Types
Spam Details
Permitted Outbound Ports By Bytes
Incident Severities Ranked By Count
FortiEDR Most Targeted Application
OT - Incidents in Purdue Levels - Security Incidents
FortiSIEM
DASHBOARD
ANALYTICS
INCIDENTS
CASES
CMDB
RESOURCES
TASKS
ADMIN
Actions
Overview
List
Risk
Explorer
UEBA
MITRE ATT&CK® ICS: Incident Coverage
1 minute
Search technique...
Show All
Status: Active
Time Range: Last 2 Hours
Columns: 7 Selected
1/1
2

20 Incidents in Last 2 Hours

Initial Access Ics	Execution Ics	Persistence Ics	Privilege Escalation Ics	Evasion Ics	Discovery Ics	Lateral Movement Ics	Collection Ics	Command And Control Ics	Inhibit Response Function	Impair Process Control	Impact Ics
2	0	2	0	0	2	2	2	2	5	4	0
Wireless Compromise	Modify Controller Tasking	Module Firmware	Hooking	Change Operating Mode	Network Connection Enumeration	Valid Accounts	Automated Collection	Standard Application Layer Protocol [2]	Block Command Message	Module Firmware	Damage to Property
External Remote Services [2]	Change Operating Mode	Valid Accounts	Exploitation for Privilege Escalation	Exploitation for Evasion	Network Sniffing	Default Credentials	Point & Tag Identification	Commonly Used Port	Activate Firmware Update Mode	Modify Parameter	Loss of Safety
Exploit Public-Facing Application	Hooking	Project File Infection		Spoof Reporting Message	Wireless Sniffing	Exploitation of Remote Services	I/O Image	Connection Proxy	Modify Alarm Settings	Spoof Reporting Message	Loss of Protection
Drive-by Compromise	Native API	System Firmware [2]		Indicator Removal on Host	Remote System Information Discovery	Lateral Tool Transfer [2]	Monitor Process State		Alarm Suppression	Unauthorized Command Message [4]	Denial of View
Rogue Master	Scripting	Modify Program		Rootkit	Remote System Discovery [2]	Remote Services	Detect Operating Mode		Manipulate I/O Image	Brute Force I/O	Manipulation of Control
Exploitation of Remote Services	Execution through API			Masquerading		Program Download	Wireless Sniffing		Device Restart/Shutdown		Denial of Control

Incidents related to System Firmware

Severity Category	Last Occurred	Incident	Tactics	Technique	Target	Detail
MEDIUM	Feb 23 2022, 01:39:00 PM	Dragos Alert: System Firmware	Persistence Ics,Inhibit Response Function	System Firmware	192.168.0.1	Component Event Type: Dragos-Configuration-S7CommFirmwareActivation Triggered Event Count: 1
MEDIUM	Feb 23 2022, 01:39:00 PM	ICS Alert: System Firmware	Persistence Ics,Inhibit Response Function	System Firmware	192.168.0.1	Component Event Type: Dragos-Configuration-S7CommFirmwareActivation Triggered Event Count: 1

7 Steps for complying OT security standards

			IEC 62443-3-3 Mapping
1. Asset awareness and classification	Partner Consultant Service SIEM		
2. Segmentation	Switch NGFW WIFI Extender	Zones and Conduits	FR: 1,2,3,4,5
3. Identity/RBAC/Secure Remote	AC MFA Client PAM	Secure Remote Connectivity	FR: 1,2,3
4. Network Visibility	NAC	Deep OT Visibility	FR: 1,2,3,5
5. Endpoint Protection	EDR Client (EPP)	Endpoint Security	FR: 1,2,3,4,5,6,7
6. Sensors and Decoys	Sandbox Deception NDR	Advanced Persistent Threat	FR: 2,3
7. Analytics for anomaly & Infusing Threat Inte	Analyzer SIEM SOAR	NOC / SOC	FR: 1,2,3,5,7

Industrial IoT (IIoT) Security for Industry 5.0

IIoT Use Cases Enabled by 5G

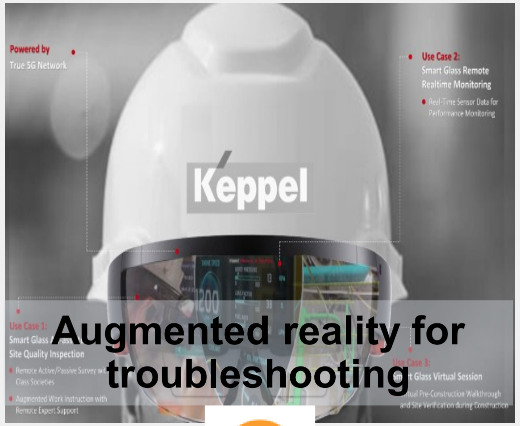
Enabled by seamless mobility inside & outside the factory and by connecting different locations

Intelligent AGV

Singtel

Connected logistics

Discover
Delivered by DHL



Augmented reality for troubleshooting

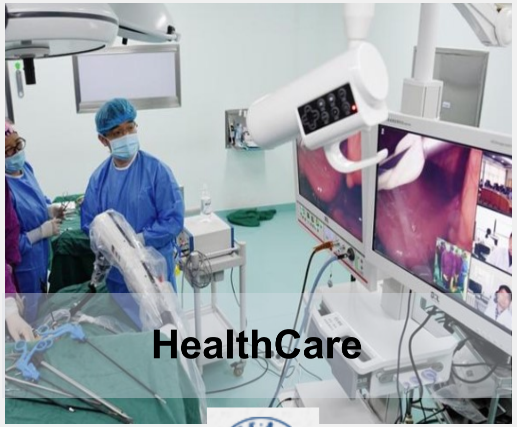
M1

Connected Tooling

ABB

Distributed sensors

ENVIROTECH
Online



HealthCare

Remote Mining

CMOC

Industrial IoT Organization

IIoT Functional Domains mapped to the 3-Tier Technology Architecture

Domains

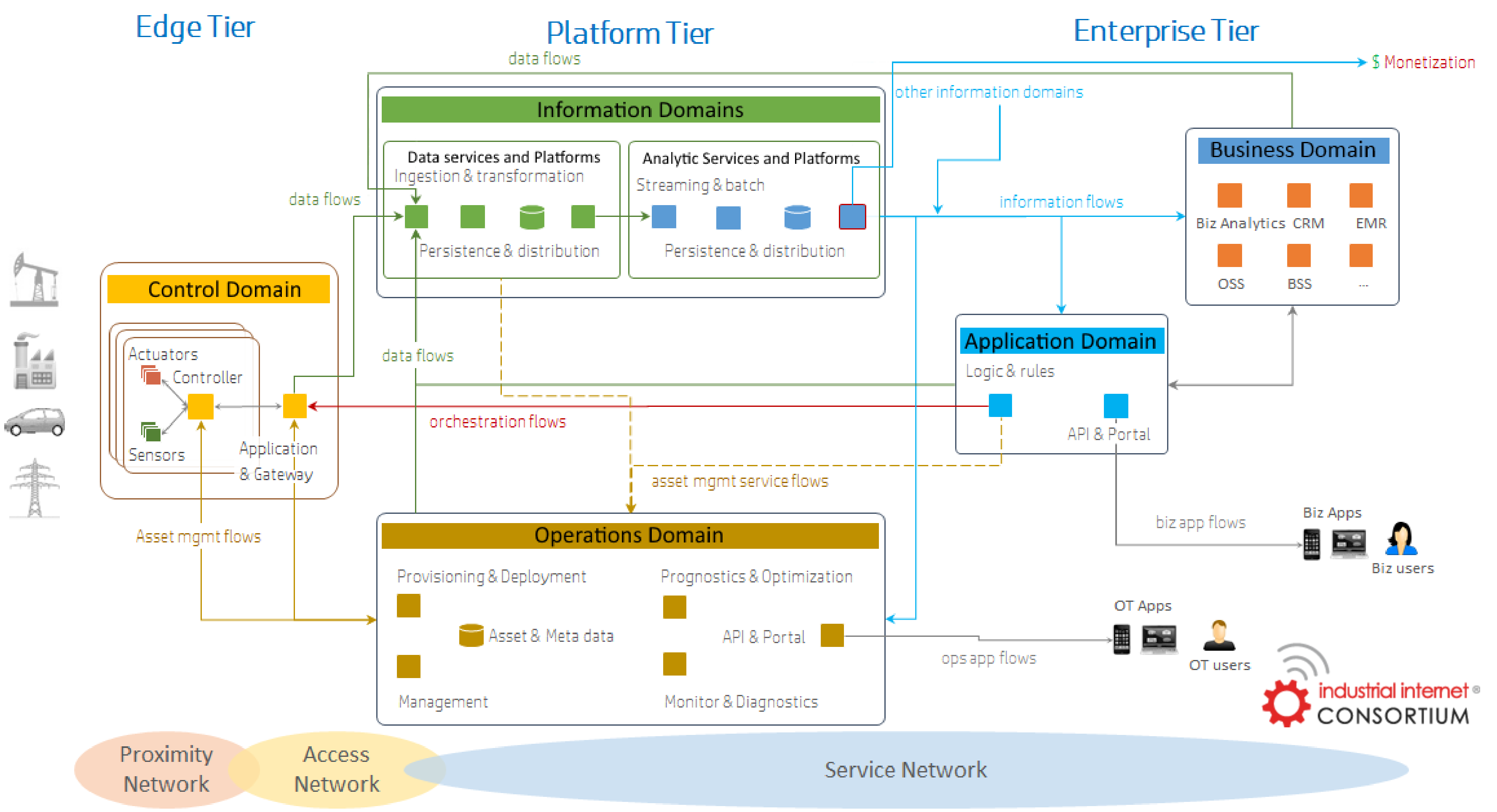
- Control Domain
- Operations Domain
- Information Domain
- Application Domain
- Business Domain

Technology Tiers

- Edge Tier
- Platform Tier
- Enterprise Tier

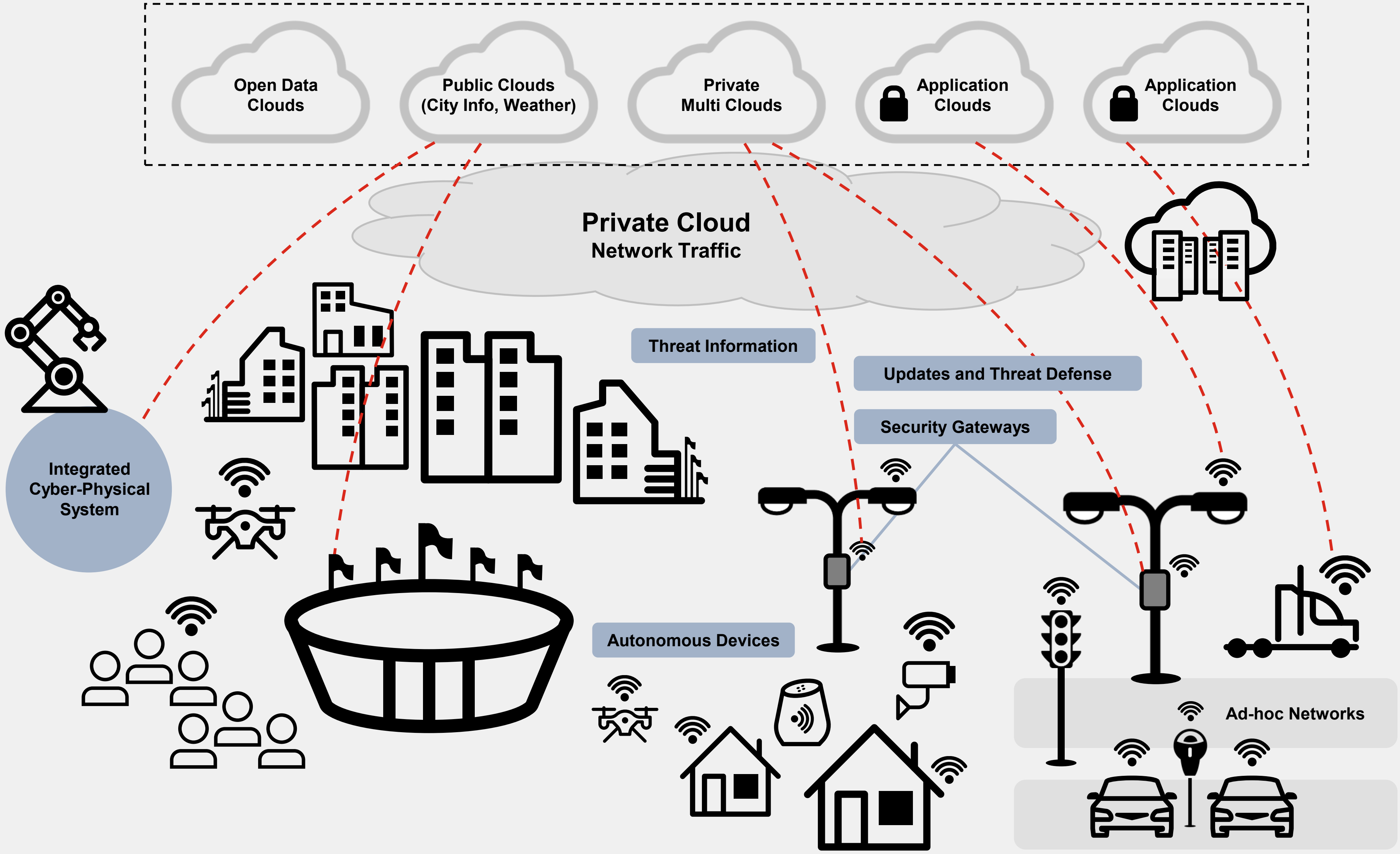
Networks

- Proximity Network
- Access Network
- Service Network



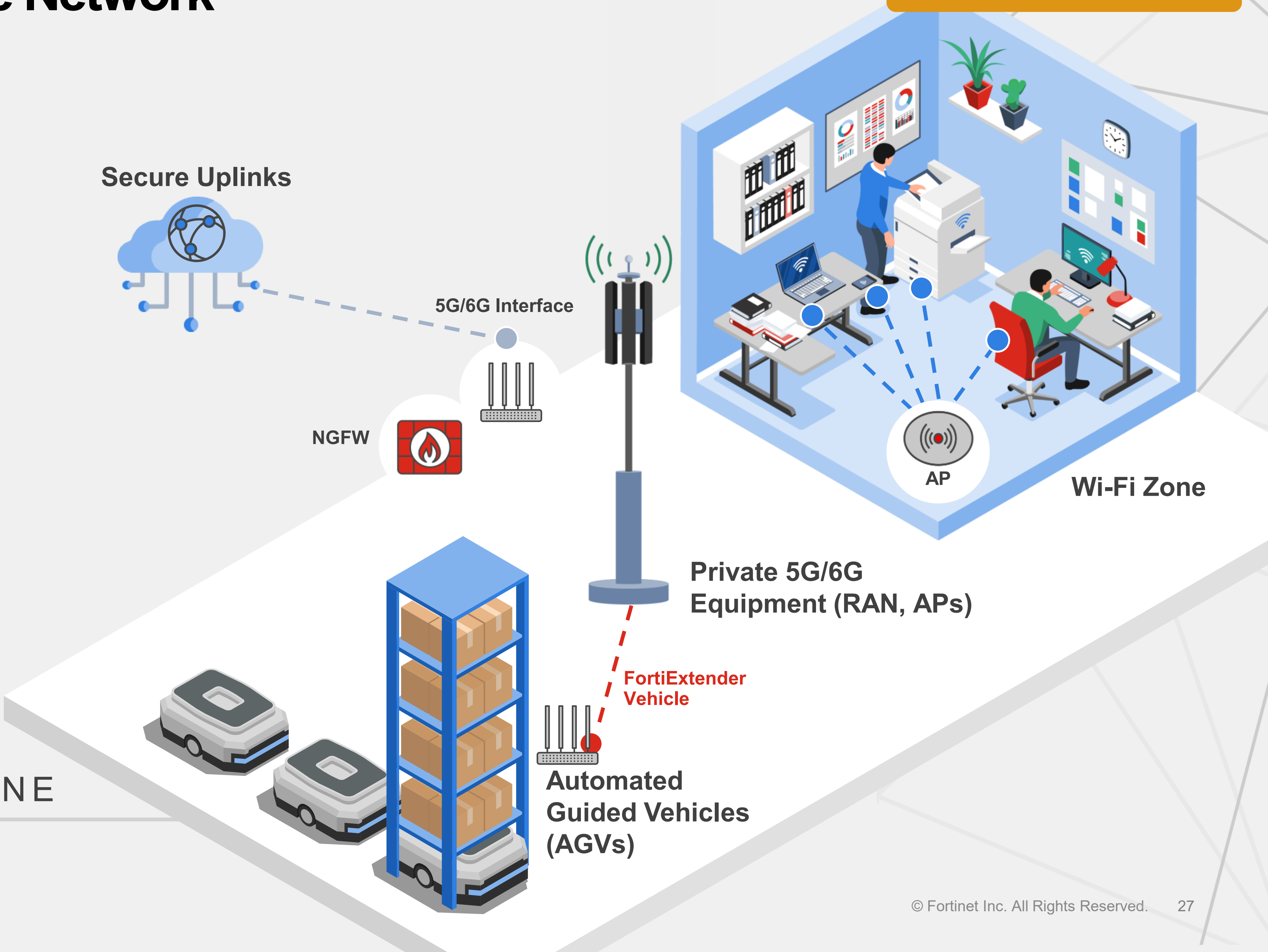
IIC – Industrial Internet Reference Architecture (IIRA)

Interconnected Ecosystem for IIoT



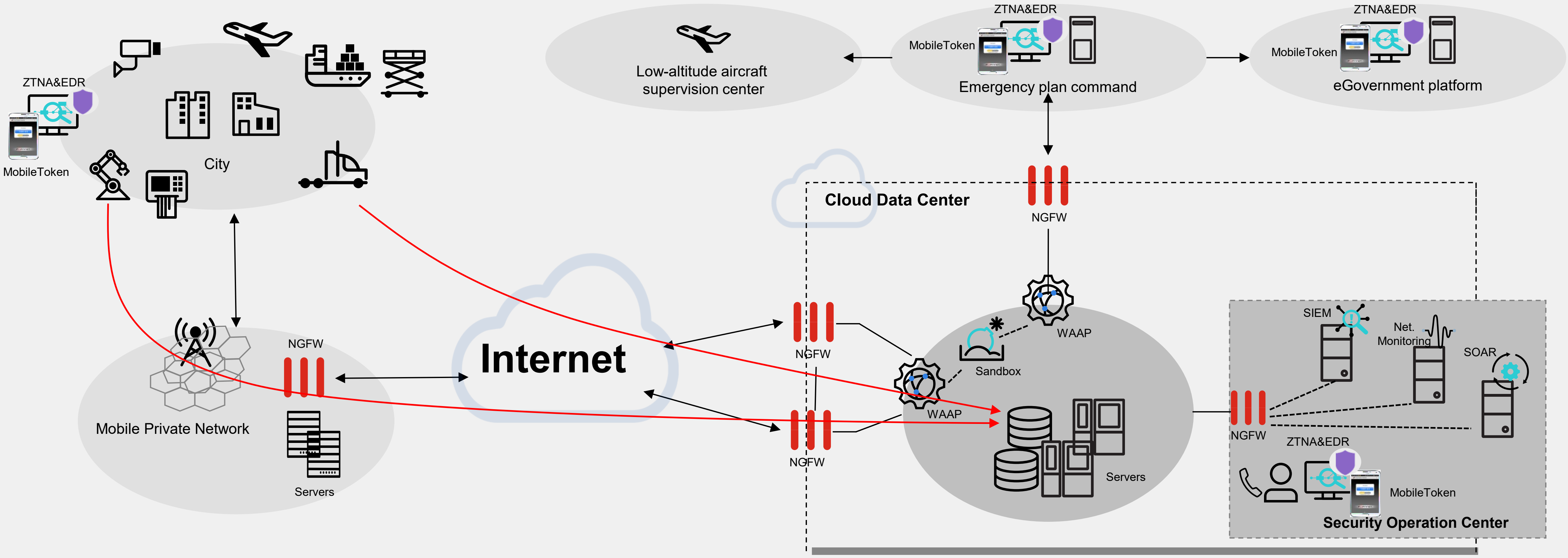
Secure Mobile Private Network

- ✓ Supports 3G/4G/5G/6G
- ✓ Deploy as Secure Uplink
- ✓ Deploy as AGV Client
- ✓ Implement NGFW policies over the air



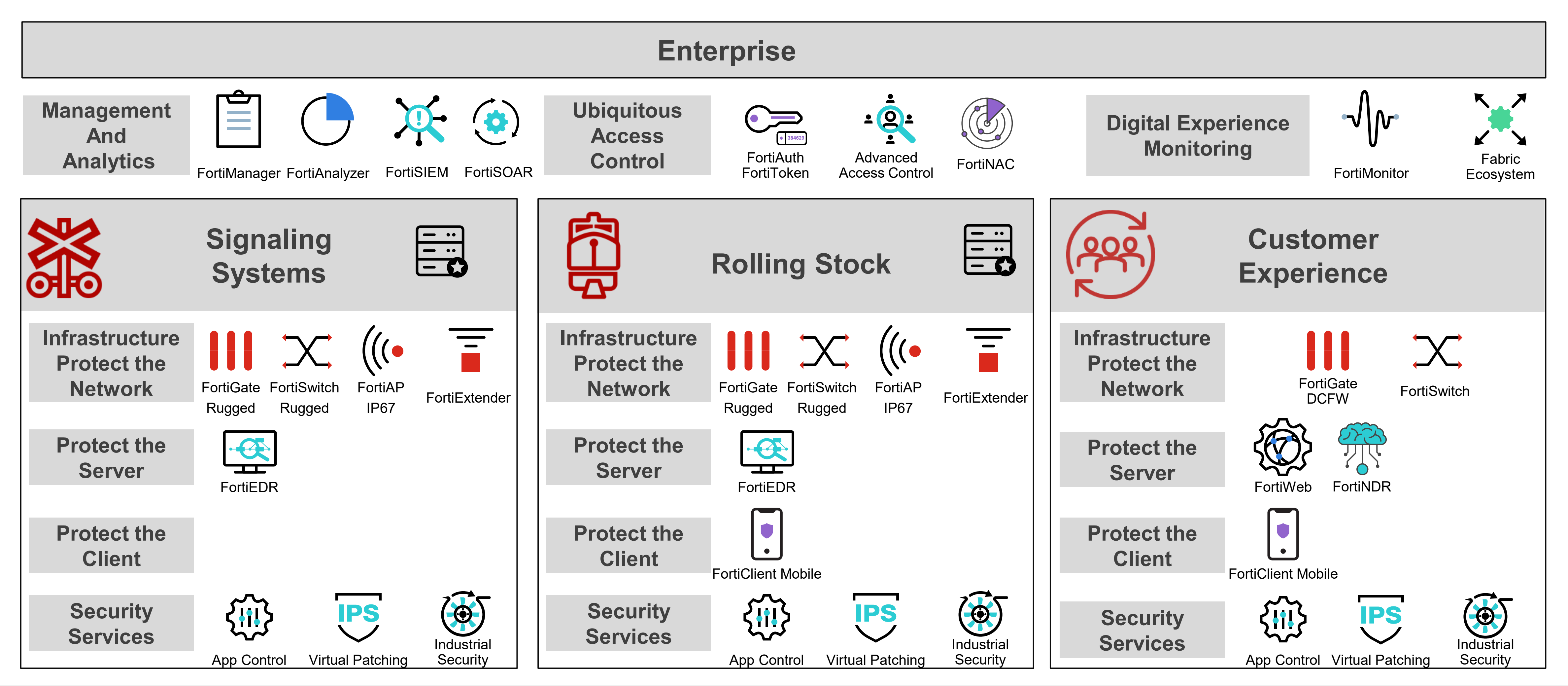
PRIVATE **5G/6G** ZONE

Security Implementation for IIoT



Starting Your Cybersecurity Journey

Cybersecurity Maturity Applied to Key Areas



Enterprise

Management And Analytics

FortiManager FortiAnalyzer FortiSIEM FortiSOAR

Ubiquitous Access Control

FortiAuth FortiToken

Advanced Access Control

FortiNAC

Digital Experience Monitoring

FortiMonitor

Fabric Ecosystem

Signaling Systems

Infrastructure Protect the Network

FortiGate Rugged FortiSwitch Rugged FortiAP IP67 FortiExtender

Protect the Server

FortiEDR

Protect the Client

Security Services

App Control Virtual Patching Industrial Security

Rolling Stock

Infrastructure Protect the Network

FortiGate Rugged FortiSwitch Rugged FortiAP IP67 FortiExtender

Protect the Server

FortiEDR

Protect the Client

FortiClient Mobile

Security Services

App Control Virtual Patching Industrial Security

Customer Experience

Infrastructure Protect the Network

FortiGate DCFW FortiSwitch

Protect the Server

FortiWeb FortiNDR

Protect the Client

FortiClient Mobile

Security Services

App Control Virtual Patching Industrial Security

Why Fortinet?

Fortinet is one of the largest cybersecurity companies in the world.

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500 Indices**

Member of: **2023 Dow Jones Sustainability World and North America Indices**

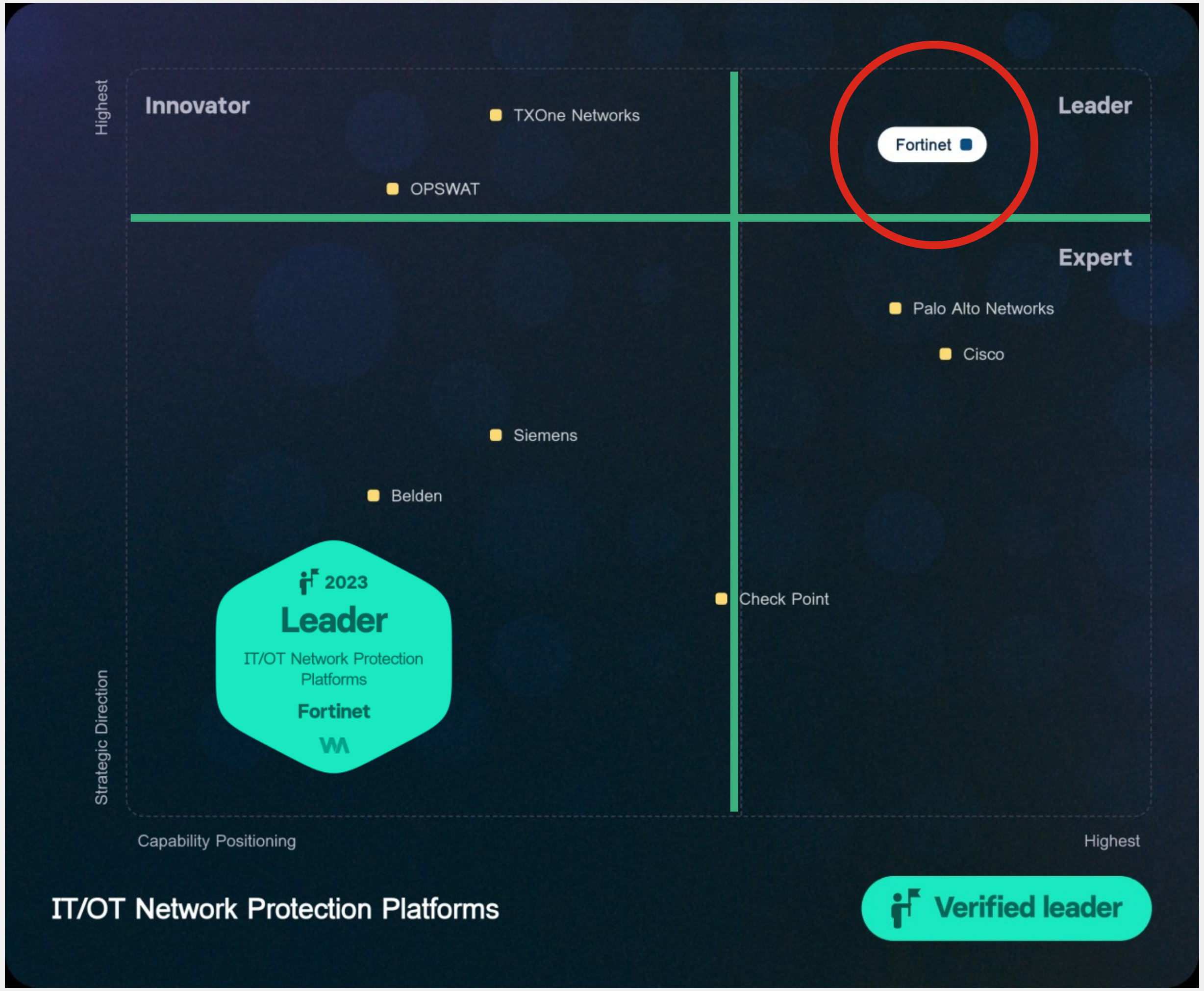
Global Customer Base **775K+** Customers	**>50%** Global Firewall Shipments
2023 Billings **$6.4B+** *(as of Dec. 31, 2023)*	**~$2.5B+** Investment in Innovation since 2017, with 91% R&D *(as of Dec. 31, 2023)*
Market Capitalization **$57B** *(as of Aug 21, 2024)*	Security Investment Grade Rating: **BBB+ Baa1**

Fortinet Is the Sole Leader in the IT/OT Security Platforms Navigator 2023

Fortinet OT Security Platform identified as a **Navigator Leader** for two consecutive years

“Fortinet is a leading IT and OT cybersecurity solutions provider to the industrial and critical infrastructure sectors, with a high customer base and strong coverage of all industrial verticals.”

Westlands Advisory, Industrial Cybersecurity Outlook 2023-2030



FORTINET