SCADA Systems as Target of Cyber Attacks

Jan Václavík, Systems Engineer CEE, Fortinet

jvaclavik@fortinet.com

OT Infrastructure Attacks – The Risk is Real

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

- Ukraine power grid knocked offline

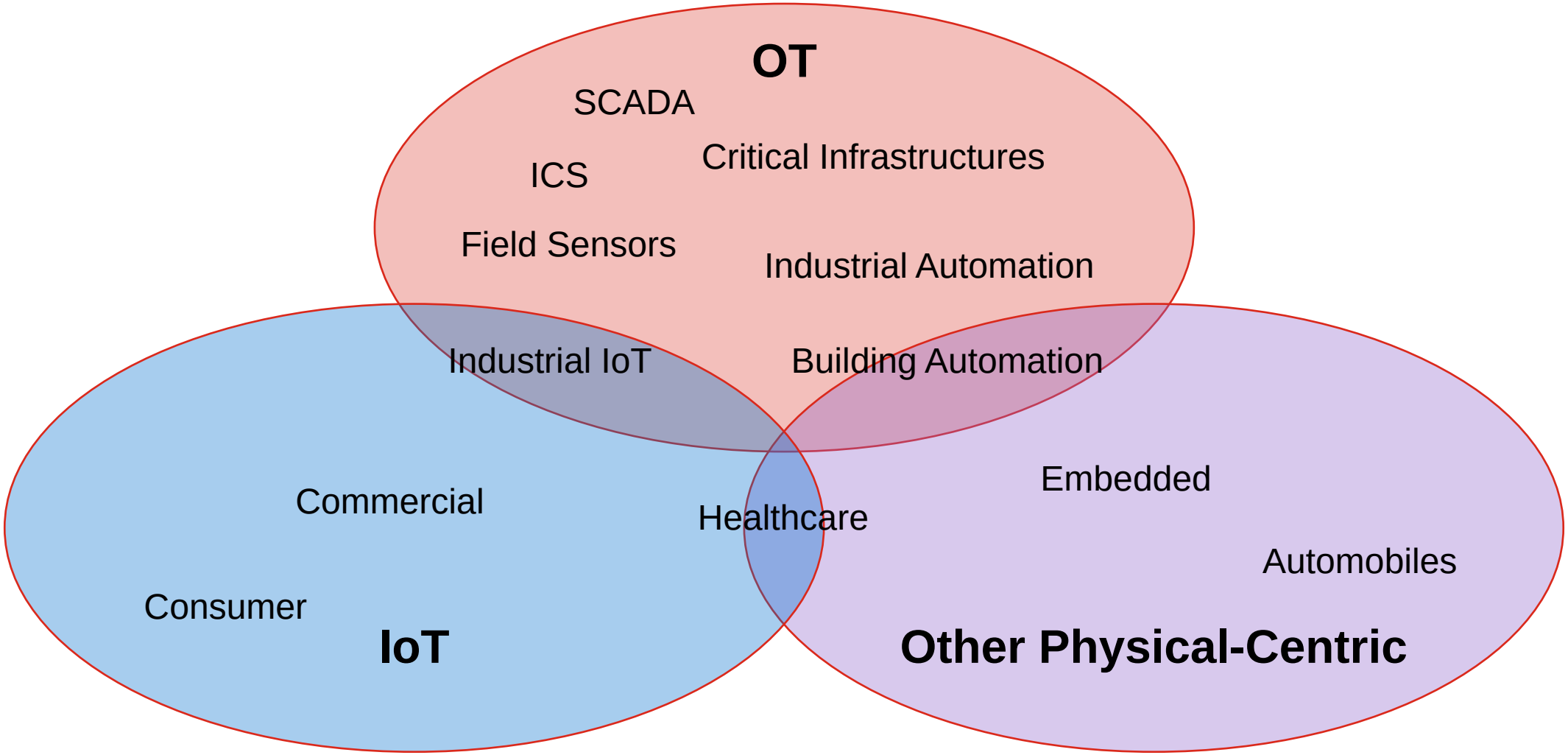
2017
- Merck pharma global production shutdown by ransomware ($1B loss)

- Maersk Shipping global shutdown by ransomeware ($250M loss)

2018
- Trisis/Triton: Malware designed to compromise Safety

2019
- Global Aluminum producer shutdown by ransomware

Cyber-physical Oriented Domains



Operational Technology

Industrial Control Systems (ICS)

ALL Industries

Often “Critical” Infrastructures

All Environmental Conditions

Harsh (Heat, Moisture, Vibration); Office

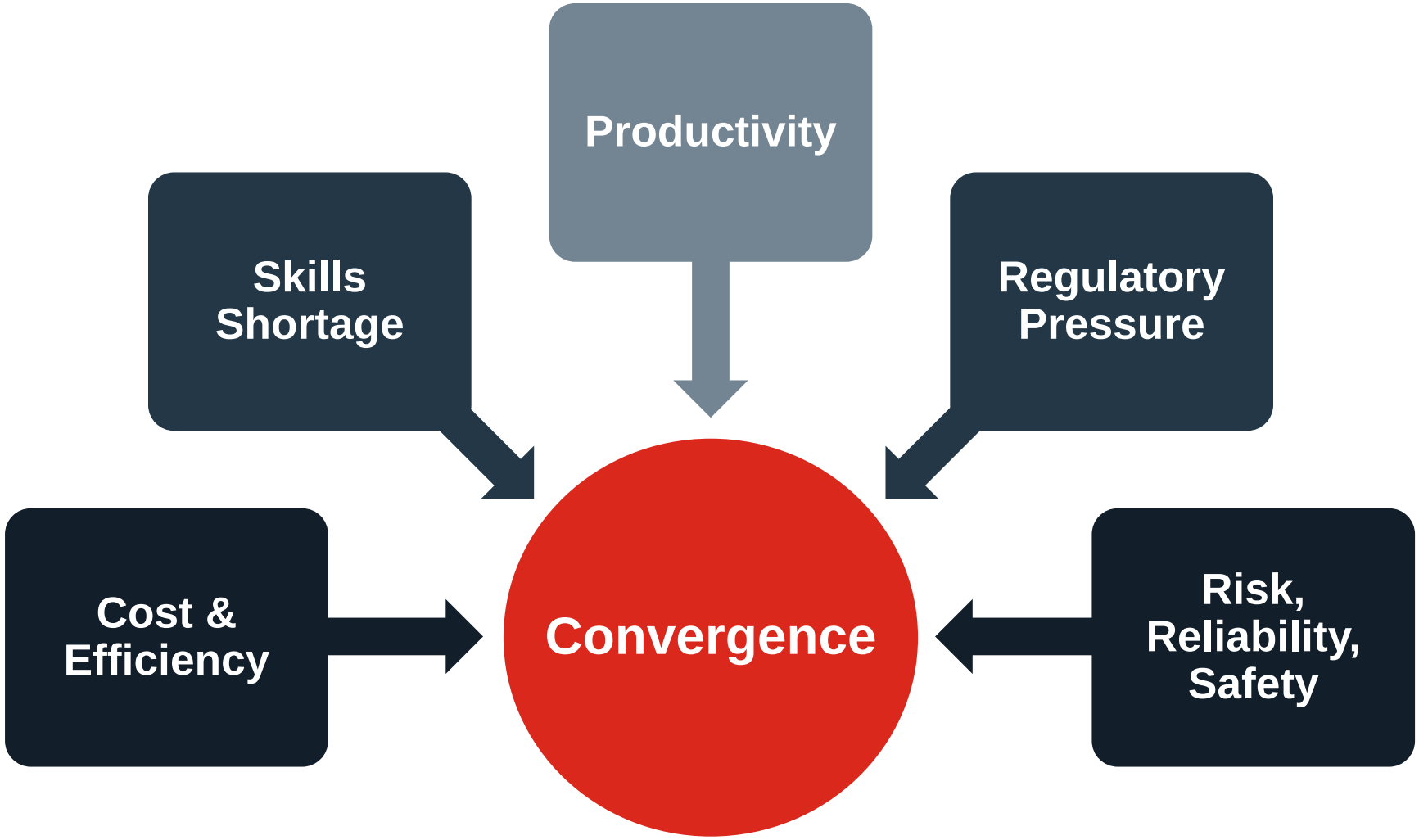
Critical Infrastructure Sectors, Operational Technology Opportunity

Critical Infrastructure Security and Resilience for the Following Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector


DX
[Digital Transformation]
is the integration of digital technology into all areas of a business, resulting in fundamental changes to how businesses operate and how they deliver value to customers

Forces Driving Growth IT/OT Convergence



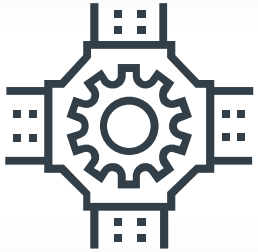
SX

[Security Transformation]

is the integration of security into all areas of digital technology, resulting in a Security Architecture that provides a Continuous Trust Assessment

Fortinet Critical Infrastructure Perspective

Fortinet seeks to improve countries' national security and economic competitiveness via critical infrastructure security solutions



- Critical Infrastructures have become the 21st century's Cold War ground
- Operational Technology and IT solutions are converging

Differences in technology, architectures, and culture require specialized expertise and solutions

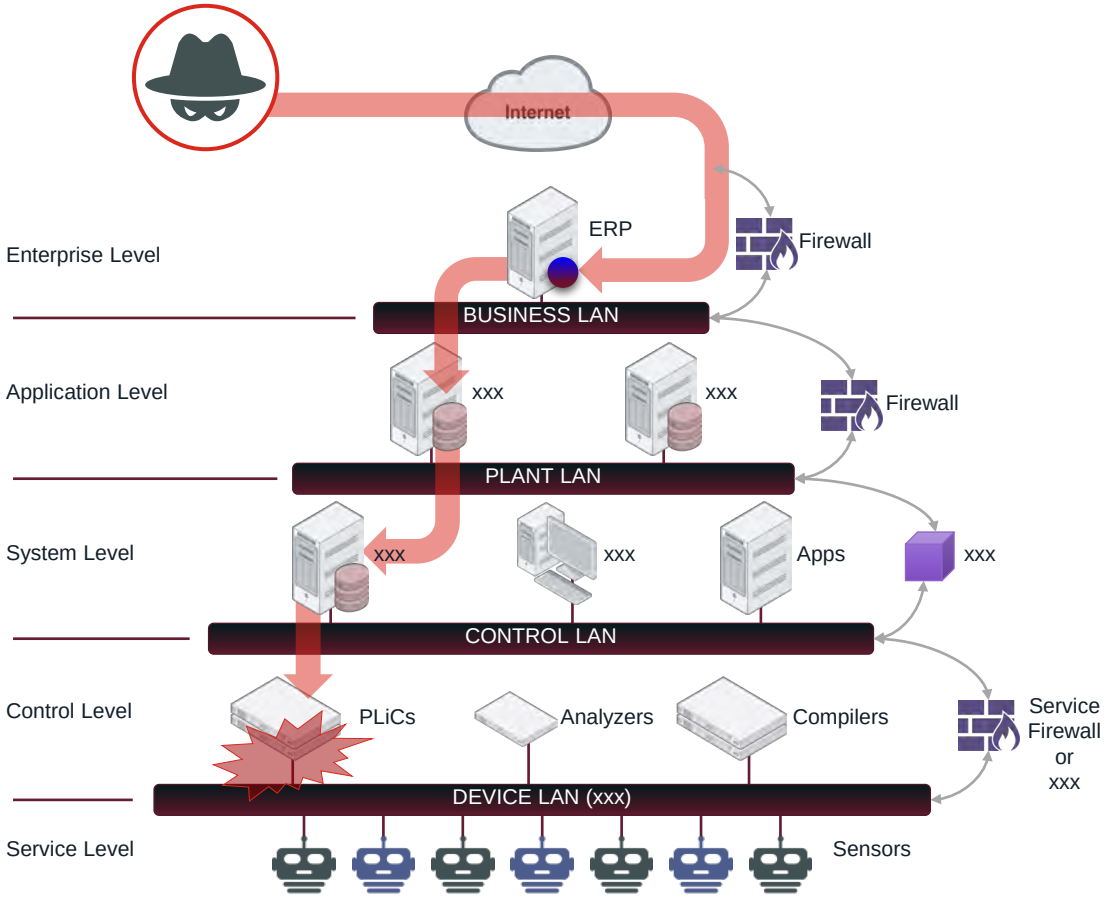
- Fortinet has directly-applicable solutions now; new solutions will meet growing demand
- Fortinet technical expertise built-up & integrated worldwide

We seek strategic alliances with channel partners and makers of OT, as well as the exposure necessary to signal our expanded role in the market

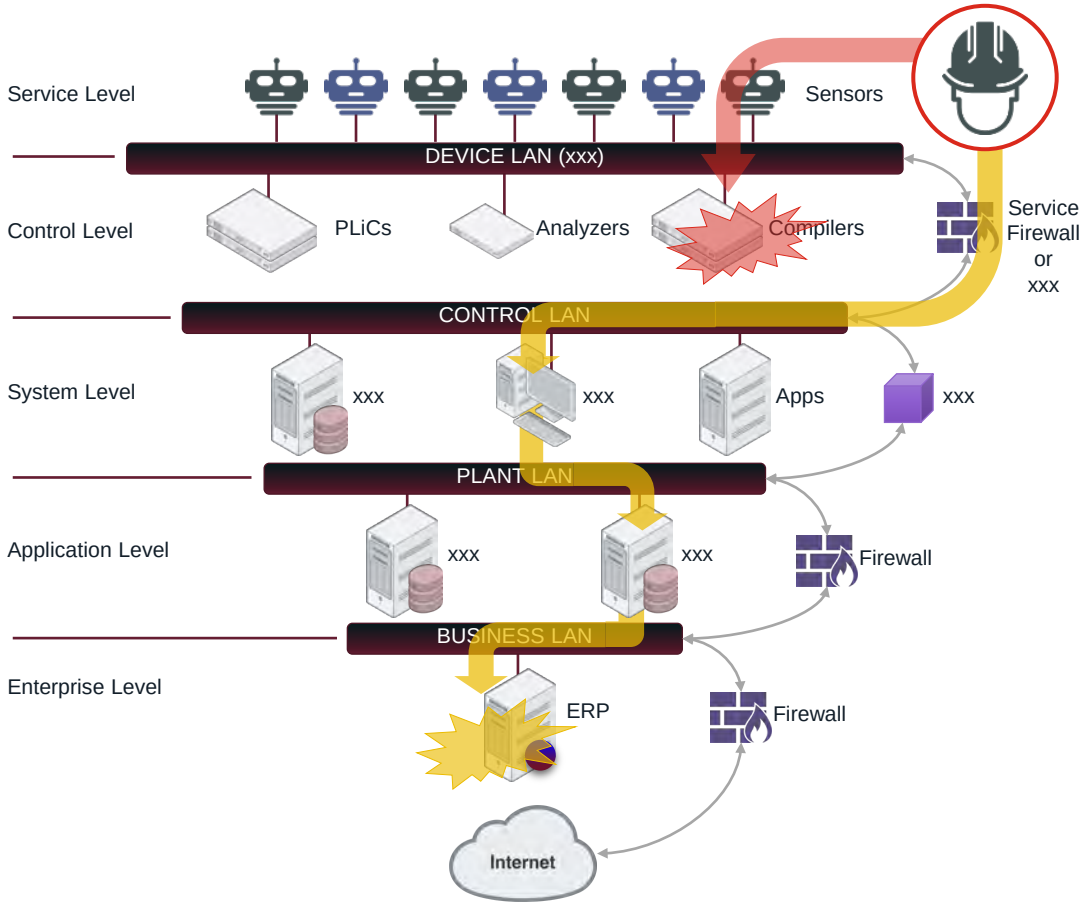
- Leverage existing relationships and create new ones
- Consulting Services and Pre-sales support available

Segmentation vectors:
Black Hat Attack vs Hard Hat Attack (Kojo-in)

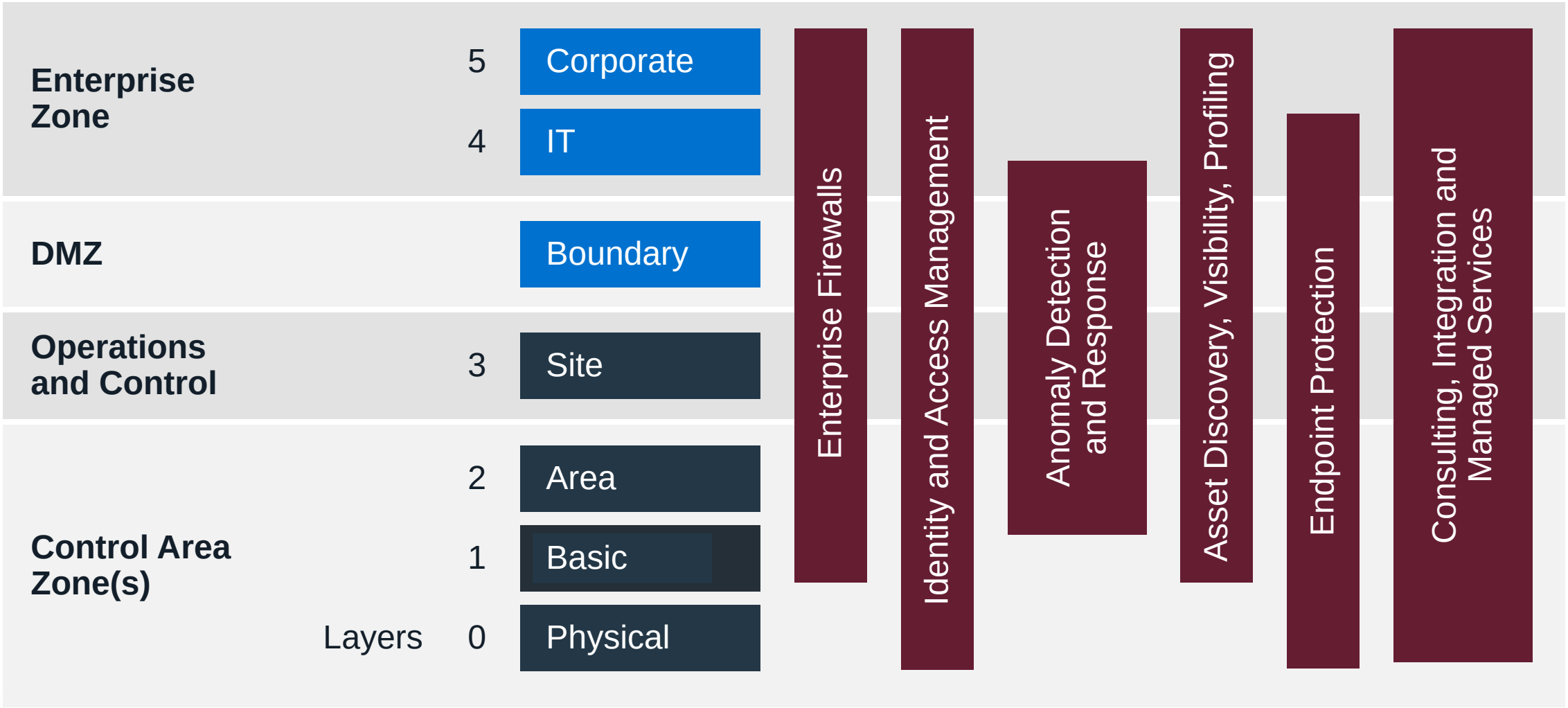
Information Technology
"Black Hat Attack"



Operational Technology
"Hard Hat Attack"

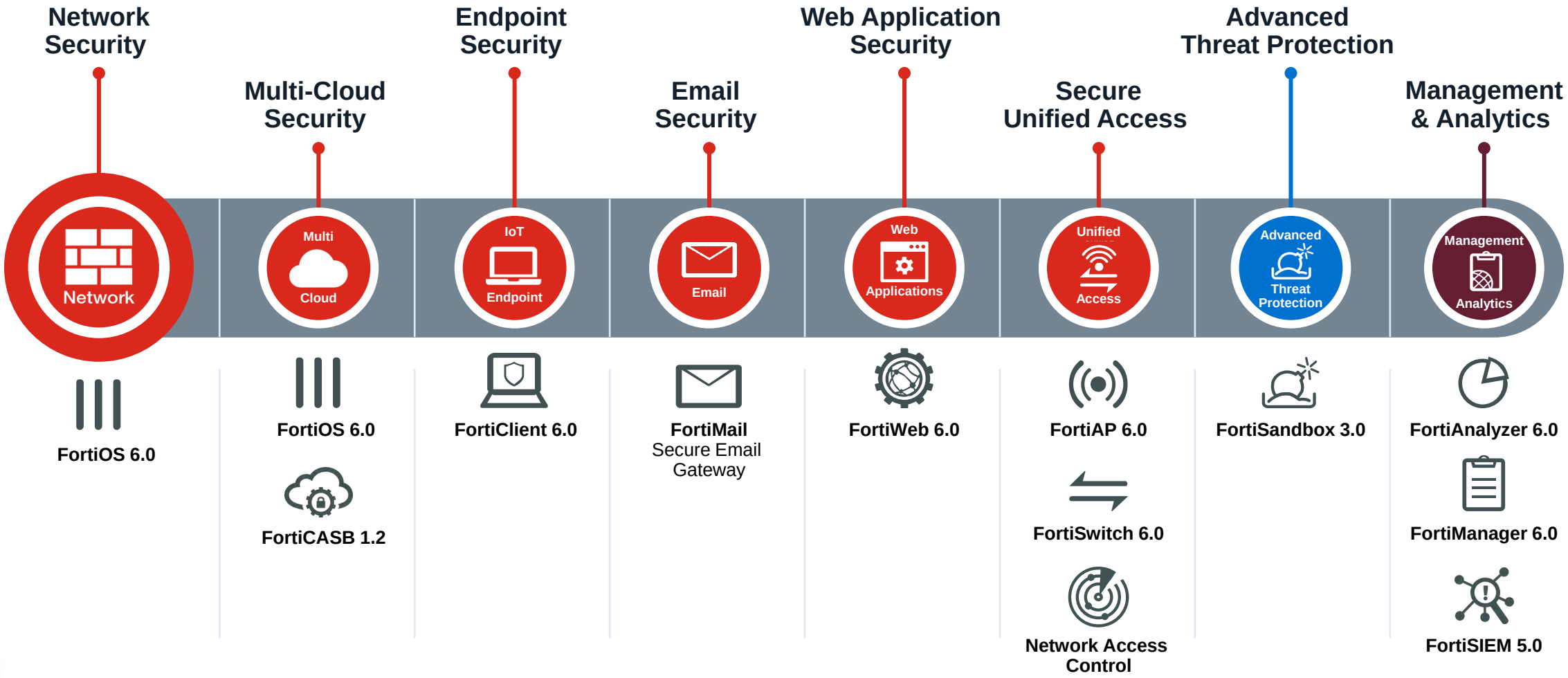


Purdue Model with Mapped IT Security Capabilities



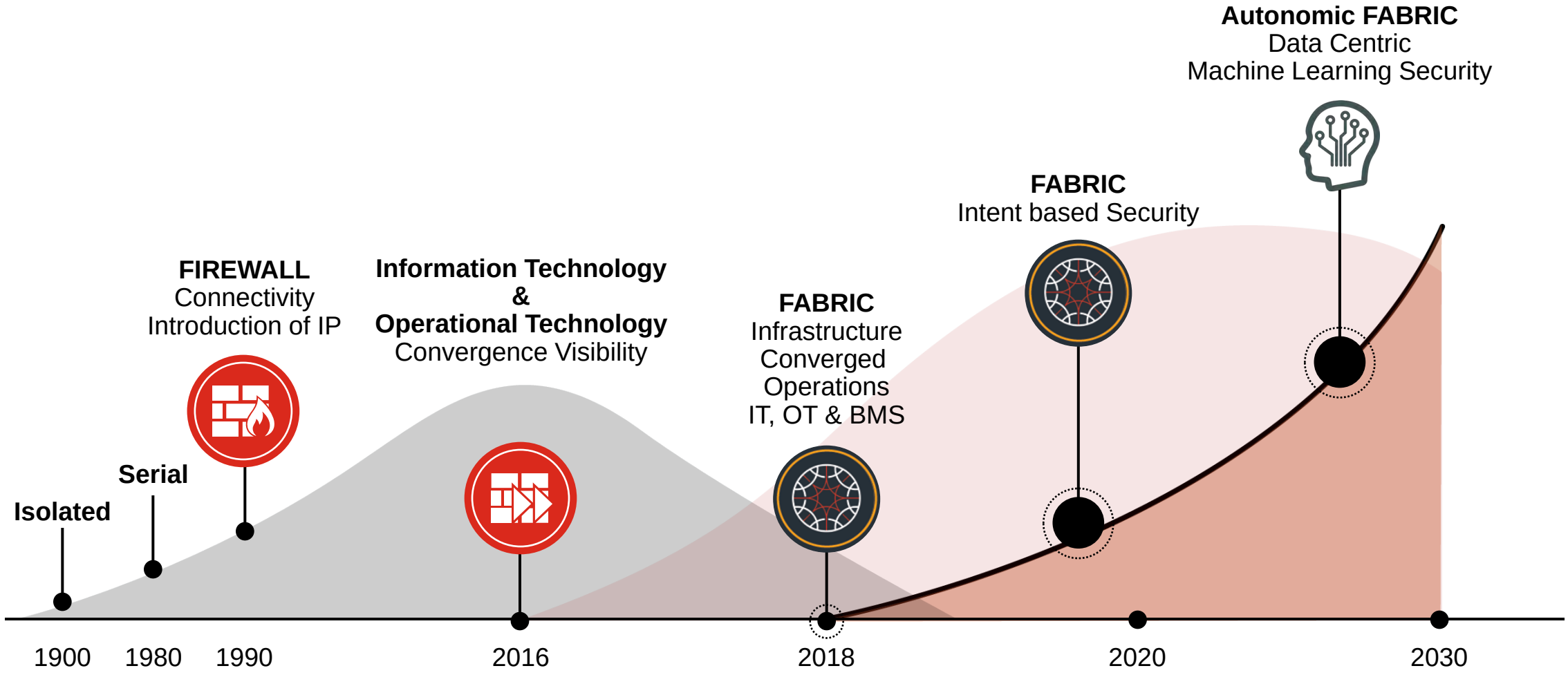
The Broadest Security Portfolio in the Industry

Built from the ground up to deliver true integration end-to-end

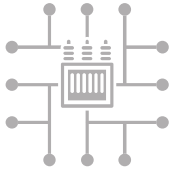


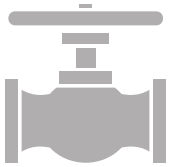
Physical to Digital Evolution of Operational Technology Environments

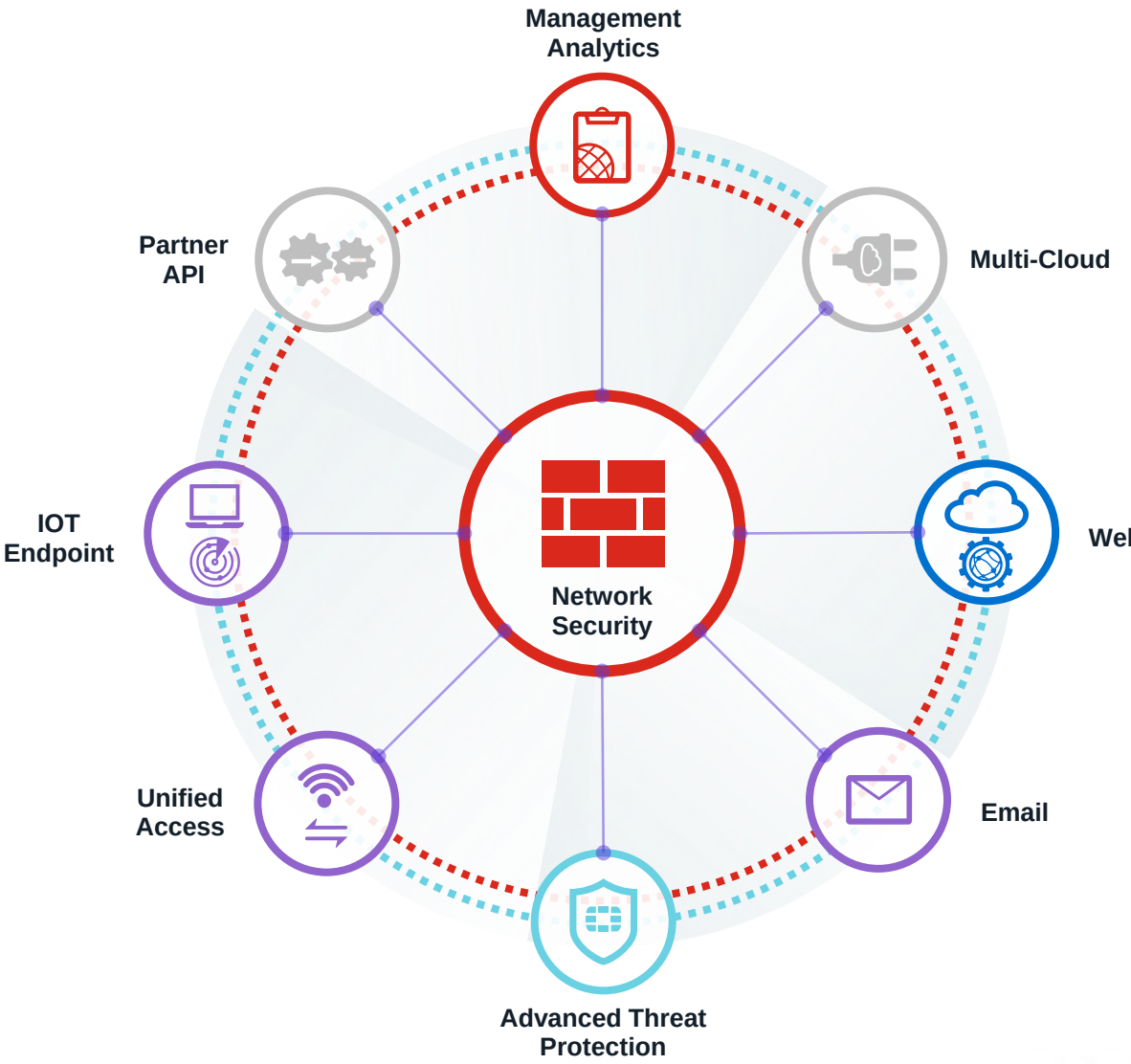
Security Evolution of Operational Technology



Fortinet Security Fabric for Protecting OT







OT Specific Solutions

Specialized Hardware

FortiGate Rugged 60D

FortiGate Rugged 90D

- Line of Rugged Firewalls
- Line of Rugged Switches
- Line of IPS-rated wireless access points

Specialized Threat Info

- Industrial Control Services
- OT-specific protocols
- OT-specific vulnerabilities
- More signatures than any other cybersecurity vendor

Specialized Team

- Experienced professionals
- Decades in Industry
- Decades of customers

Fortinet Defense in Depth Strategy: Components

Perimeter and Extranet

NETWORK SECURITY

MANAGEMENT AND ANALYTICS

VIRTUAL/CLOUD

Intranet and Host

ACCESS

INDUSTRIAL

USER

Data and Applications

MAIL

WEB

DATABASE

Industrial Standard and Compliance Ready

EMI

Unprotected devices can fail or be destroyed when exposed to high levels of electromagnetic interference

- A strong electromagnetic compatibility **(EMC) design is required**

Thermal

A wide (-20 to +75C) operating temp can be expected in a hash environment.

- Requires efficient heat dissipation system and self warming

Vibration

- Devices must survive being dropped from a cabinet rack mount
- 50G anti-shock & 5-500 Mhz anti-vibration requirement is present
- Protective components are used to cushion the device

IEC-61850 describes a unified communications system design for use in electrical sub-stations. **IEC-61850-3** provides guidance on the hardware requirements of equipment deployed in this demanding environment.

IPS/ Application Control for Industrial Systems

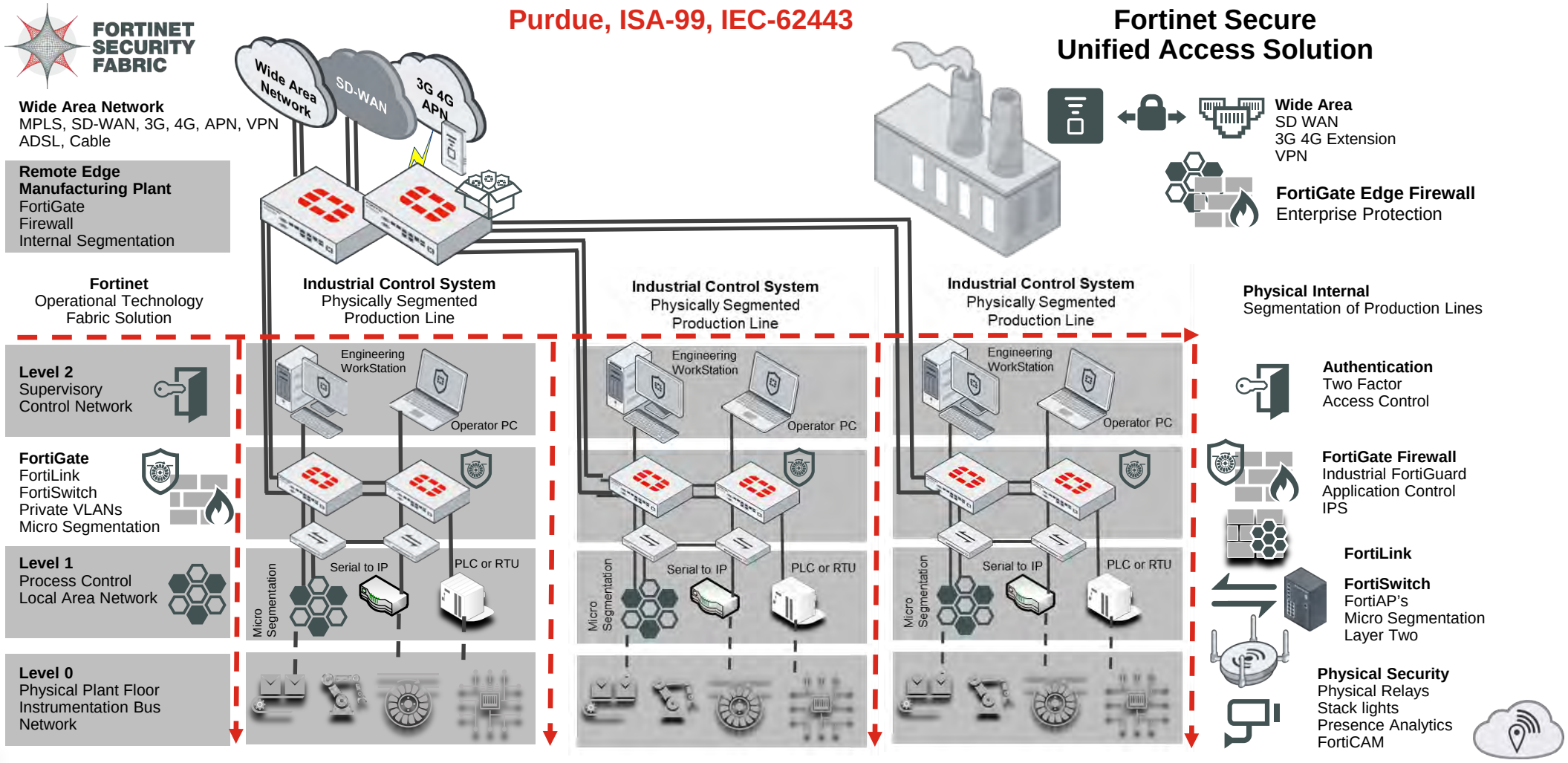
Some of the Supported Protocols

- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

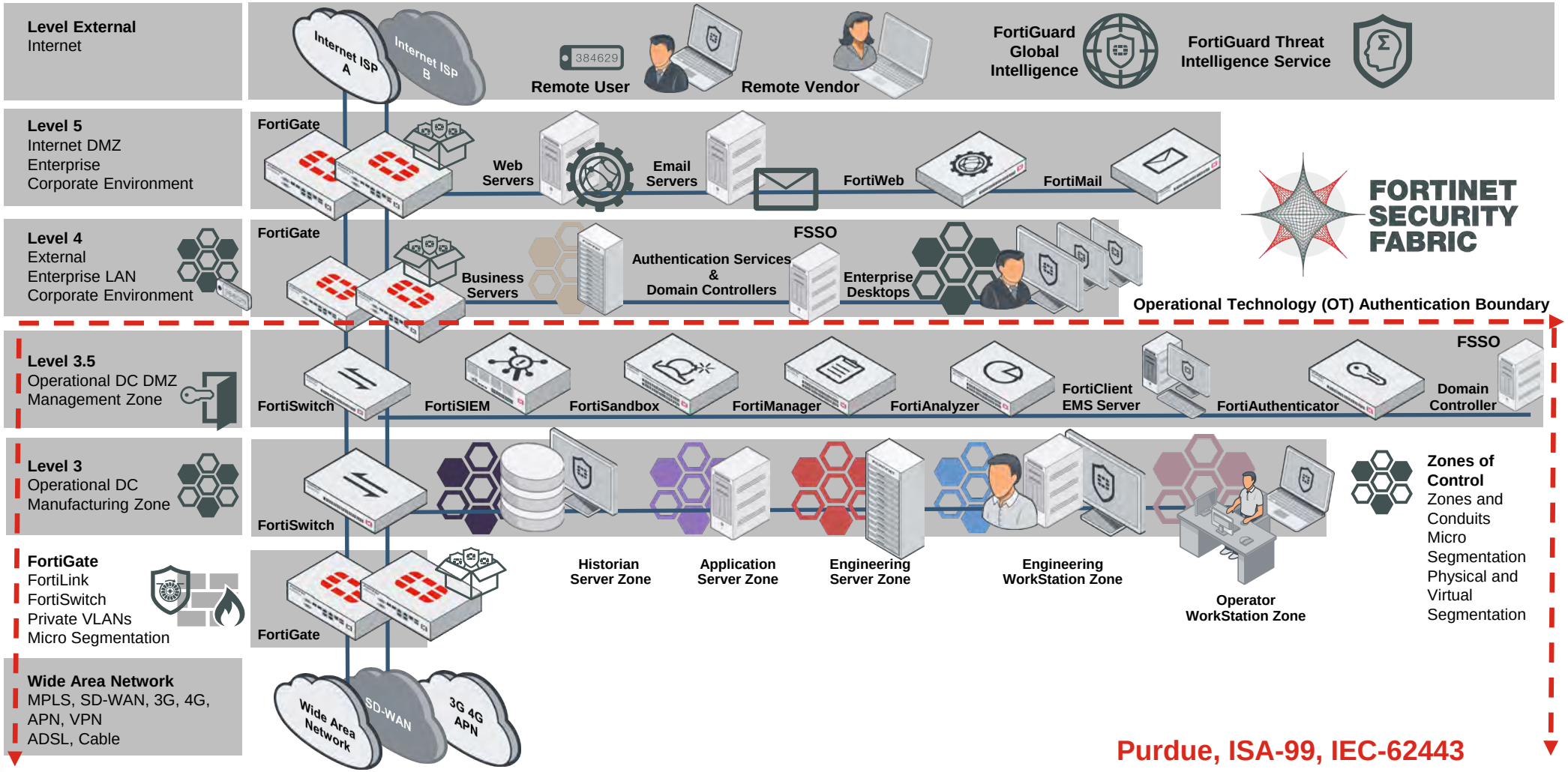
Supported Applications and Vendors

- 7 Technologies/ Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa

Critical Manufacturing Plant Floor



Applying Fortinet's Reference Architecture to Purdue




FORTINET