Securing Critical Infrastructure during Digital Transformation

Peter Newton- Sr. Director of Products and Solutions

Security Day, June 13, 2019

Agenda

- Critical Industries & Definitions
- Threat Evolution
- Journey to Security

Critical Infrastructure Sectors

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

Critical Infrastructure Sectors

Operational Technology

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**

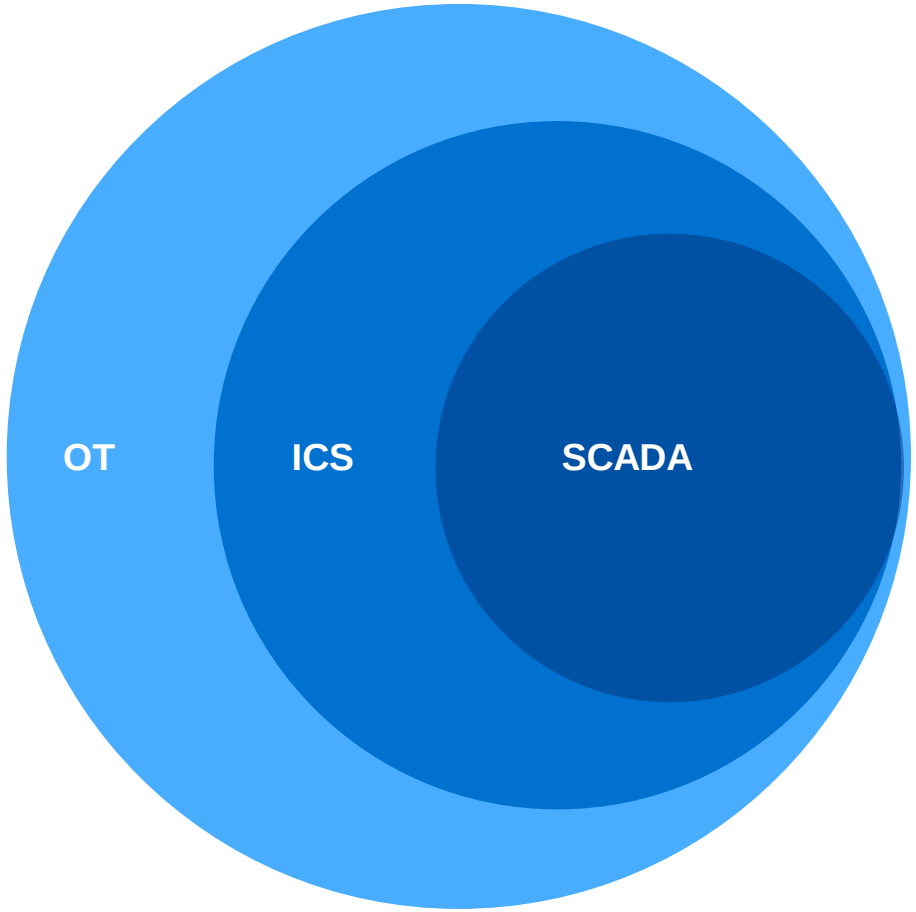
Terminology

Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the industrial environment.

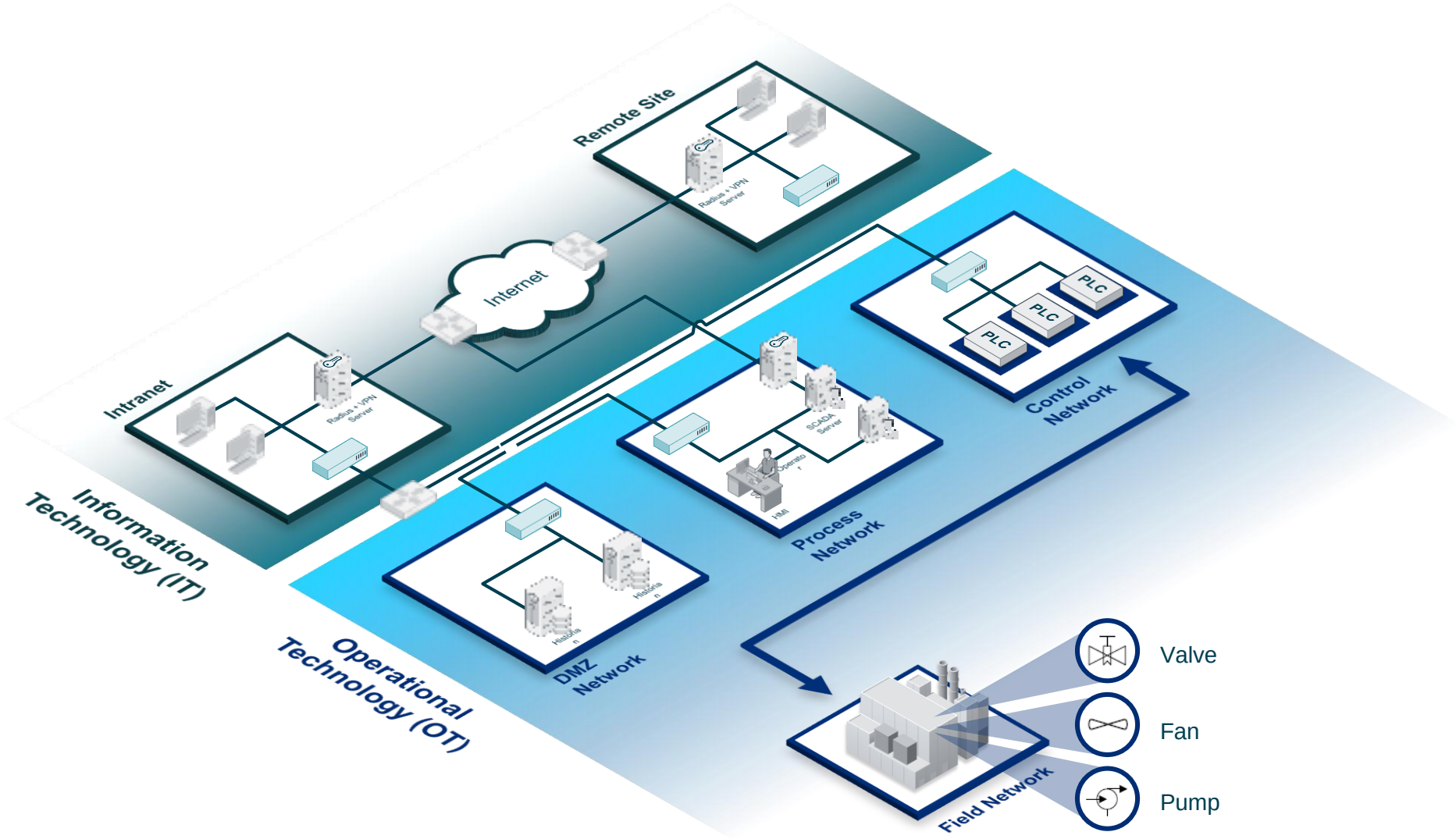
Industrial Control Systems (ICS) play a main role in OT and includes Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

Supervisory Control and Data Acquisition (SCADA) refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.

Field Sensors/Actuators are diverse physical devices that are deployed on or near physical devices and processes. They are sometimes referred to informally as the 'Industrial Internet of Things (IIoT)'.

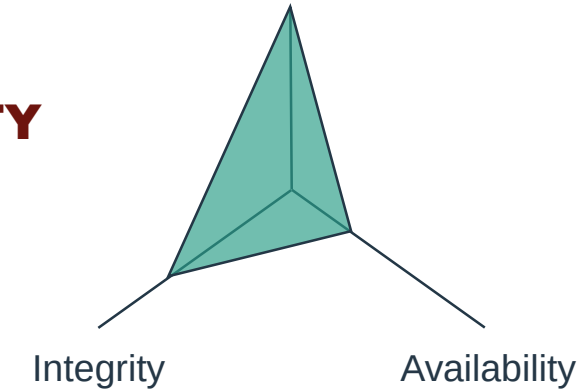


Common IT and OT Network



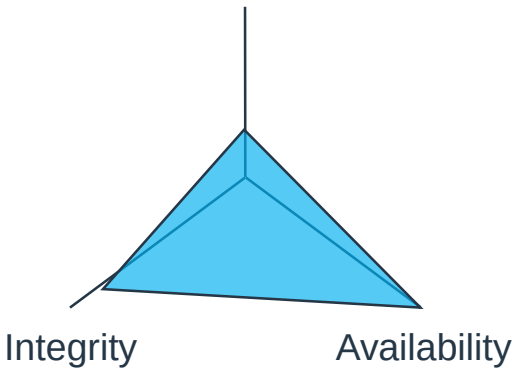
How are IT and OT Different?

IT



SECURITY

OT



SAFETY

Characteristics	Security objective priorities	
Medium, delays accepted	Availability requirement	Very High
Delays accepted	Real-time requirement	Critical
3-5 years	Component lifetime	Up to and over 20 years
Regular / scheduled	Application of patches	Slow / infrequent
Scheduled and mandated	Security testing / audit	Occasional
High / mature	Security awareness	Increasing

Industrial Control System Attacks are on the Rise

Cyber threats to industrial networks are a real and fast-growing challenge

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)

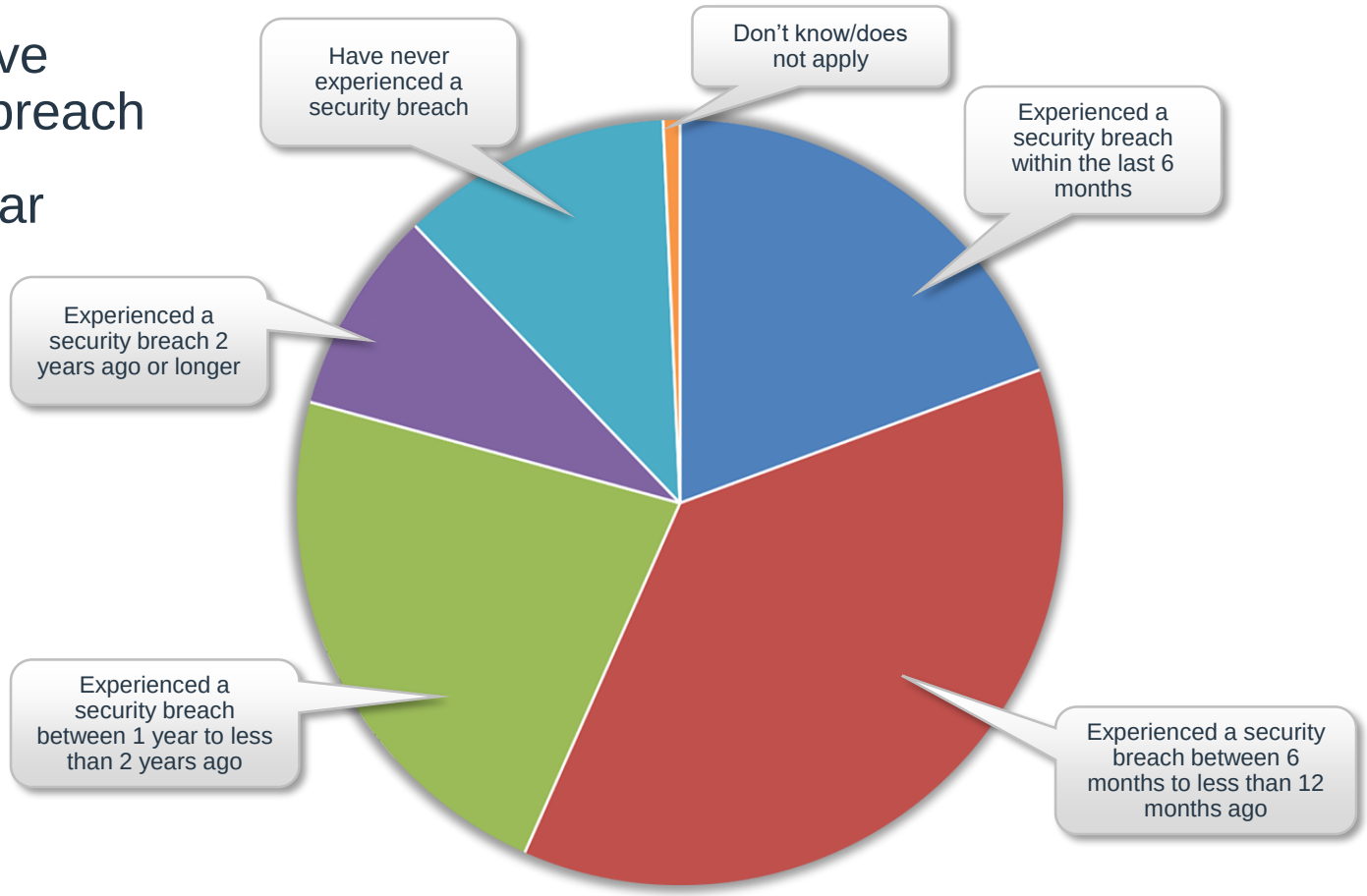
- Mersk Shipping global shutdown by ransomeware ($250M loss)

2018
- Trisis/Triton: Malware designed to compromise Safety

2019
- Global Aluminum producer shutdown by ransomware

Market Situation for OT/ICS/SCADA Cybersecurity

- Almost 90% have experienced a breach
- >50% in last year

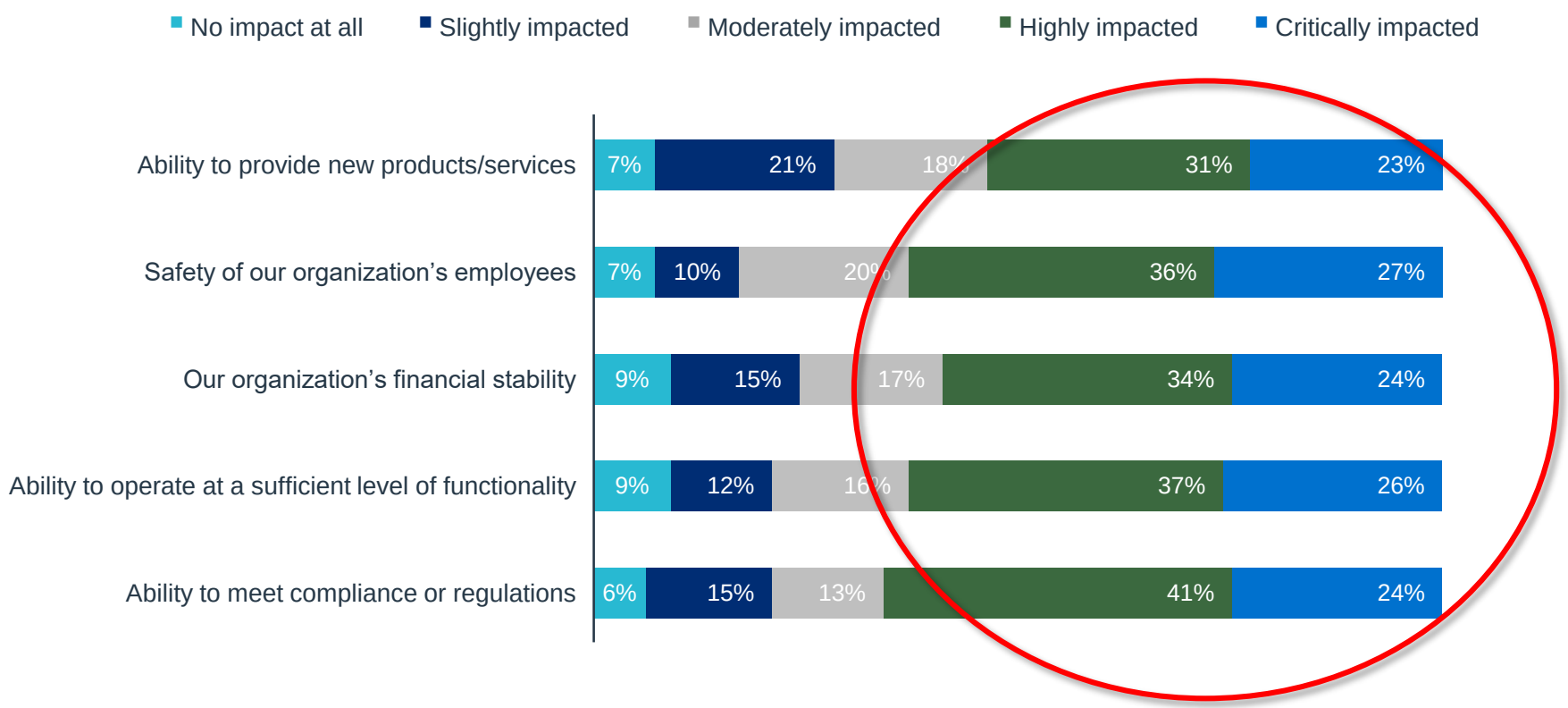


FORTINET + FORRESTER®

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Market Situation for OT/ICS/SCADA Cybersecurity

>50% of breaches had high/critical impact



FORTINET + FORRESTER®

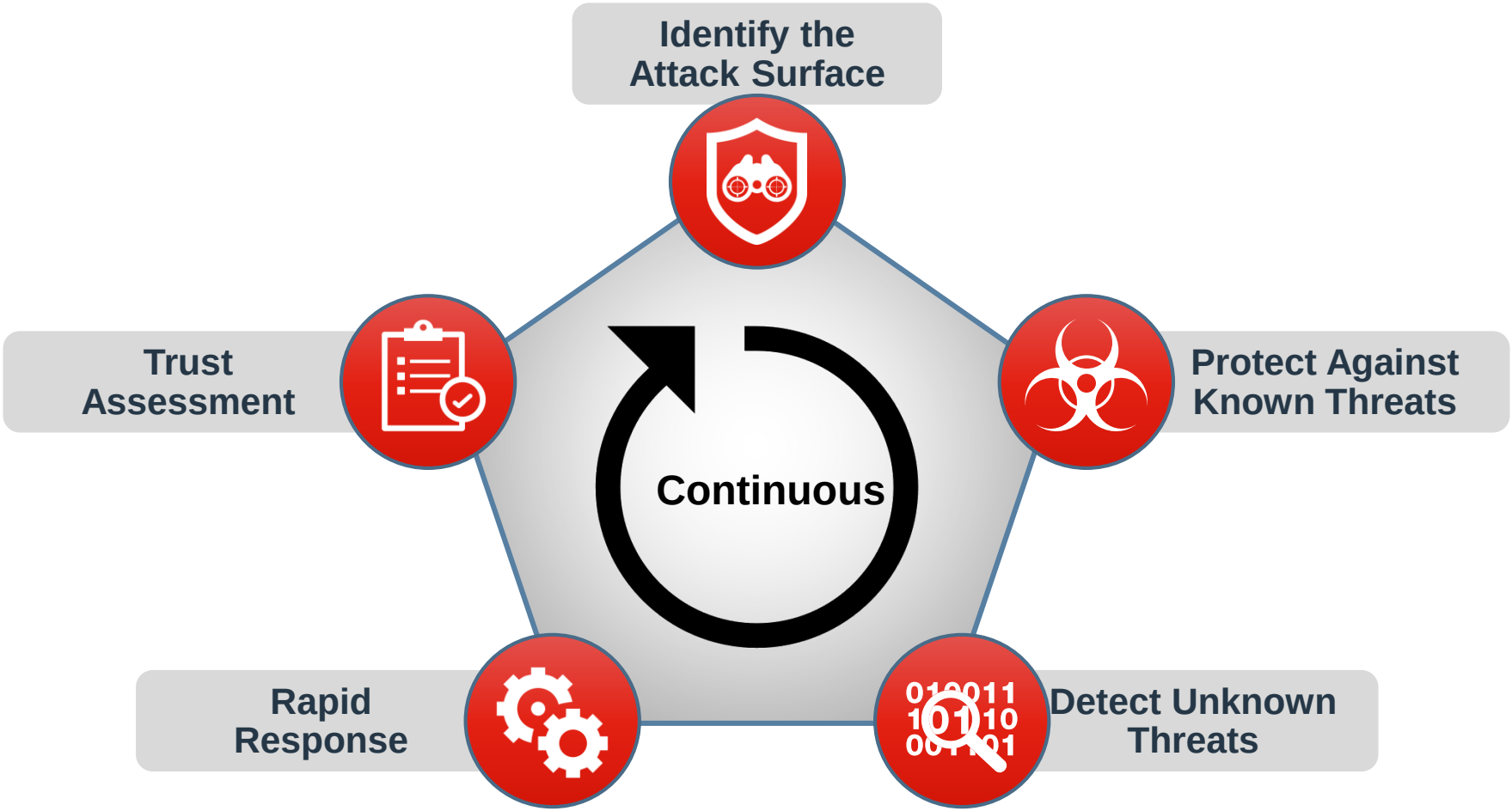
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Journey to Security

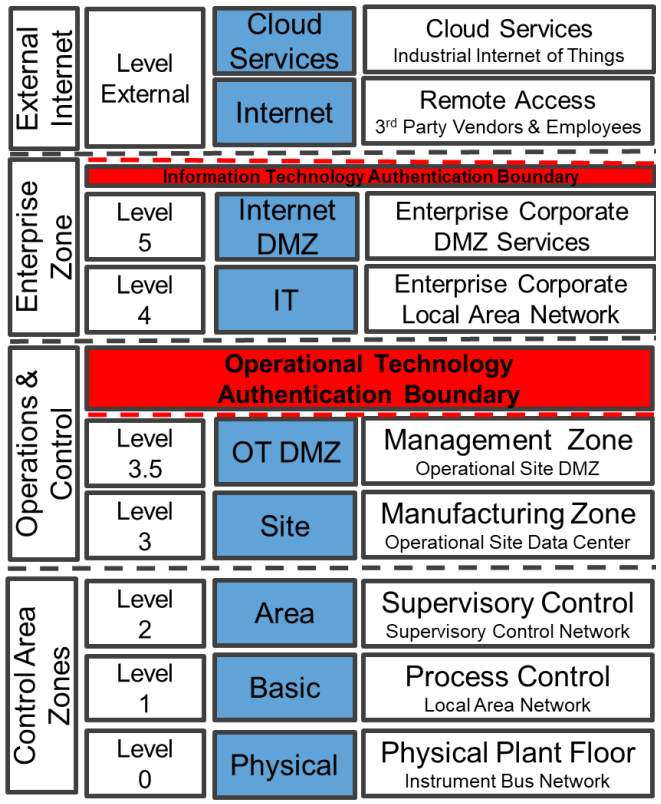
Maturity Model for Cybersecurity in OT

Security Framework for Digital Security

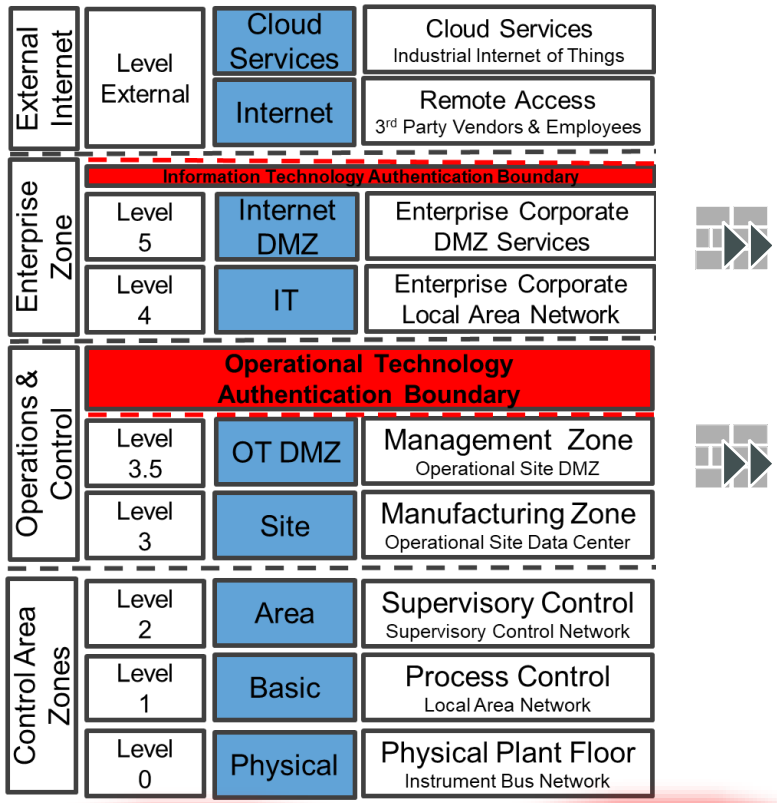
NIST Model



Customer Journey for Securing OT Infrastructure



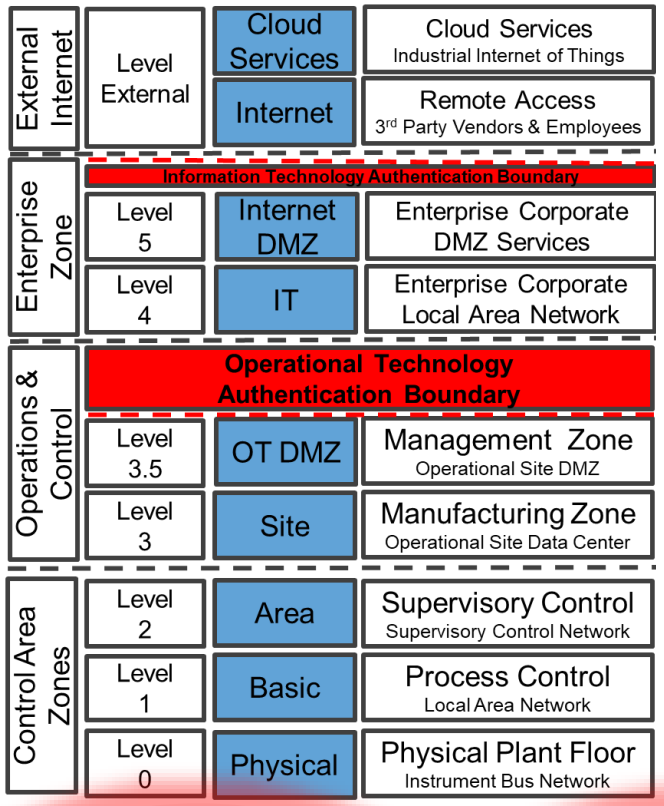
Customer Journey for Securing OT Infrastructure



Step 1. Basic Visibility & Control

- NGFW w/ OT protocol & vulnerability protection

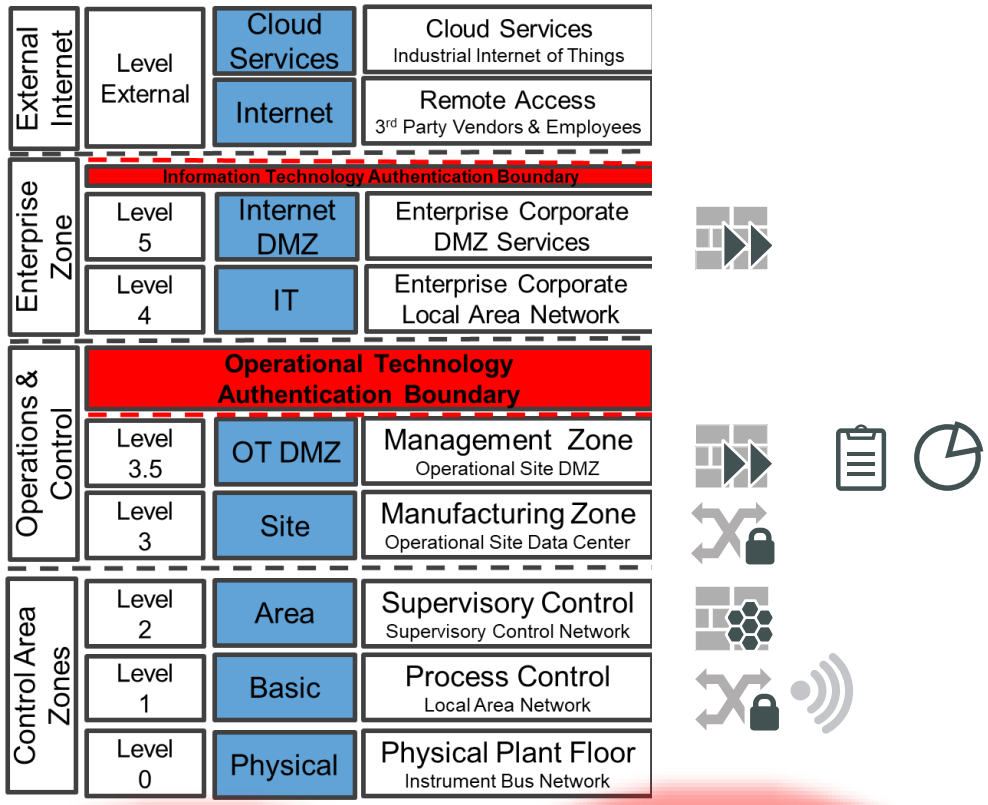
Customer Journey for Securing OT Infrastructure



Step 2. Visibility & Configuration

- Add Management & Analytics

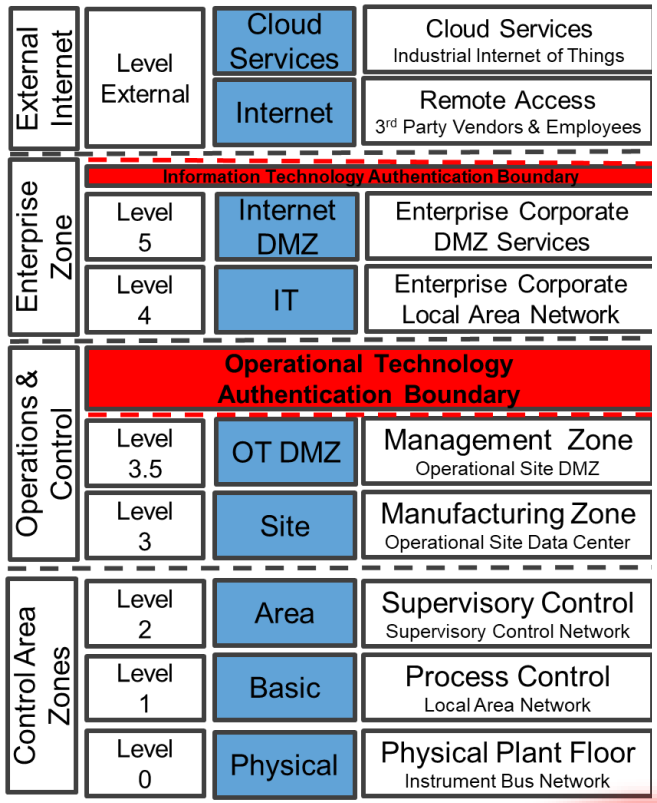
Customer Journey for Securing OT Infrastructure

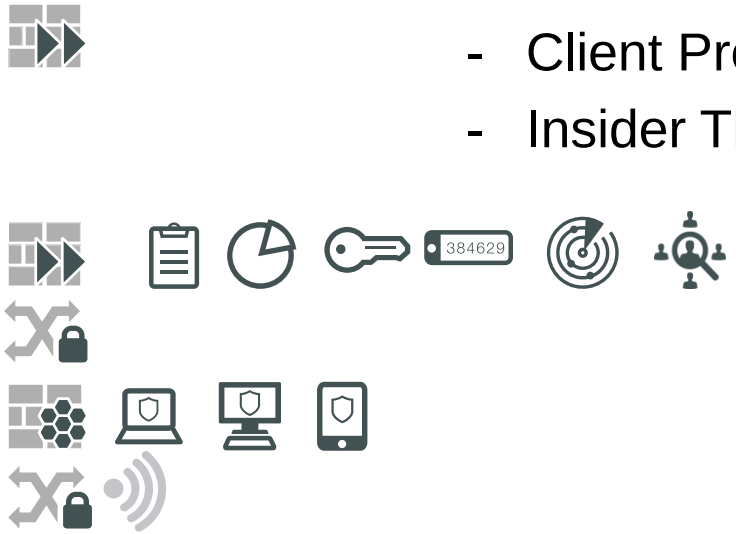


Step 3. Internal segmentation

- OT Segmentation Firewall w/ OT-specific protections
- Industrial Switching & Wireless

Customer Journey for Securing OT Infrastructure

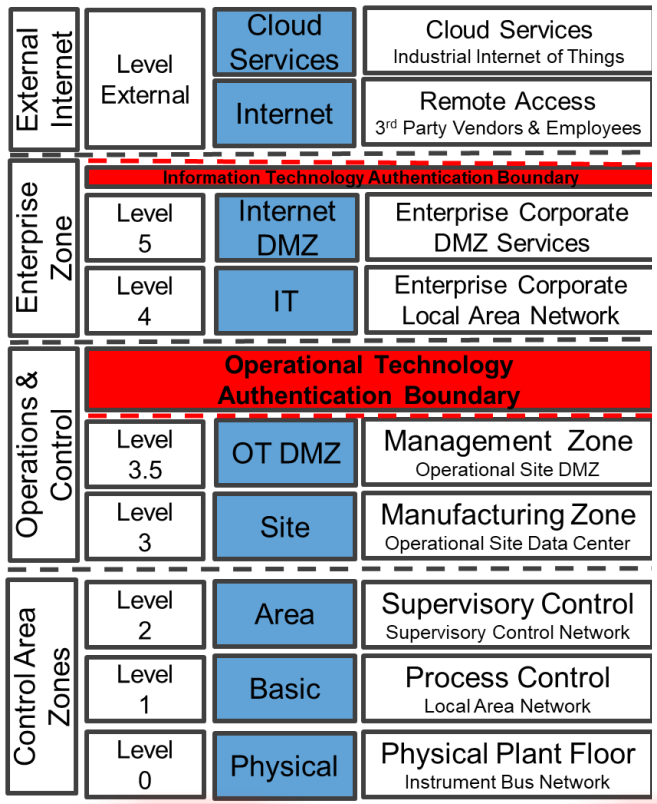


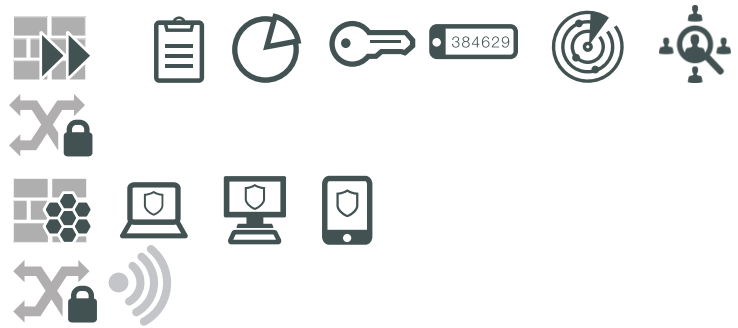


Step 4. Access Control Internal segmentation

- User Authentication (with MFA)
- Device Authentication with NAC
- Client Protection
- Insider Threat Detection (EUBA)

Customer Journey for Securing OT Infrastructure

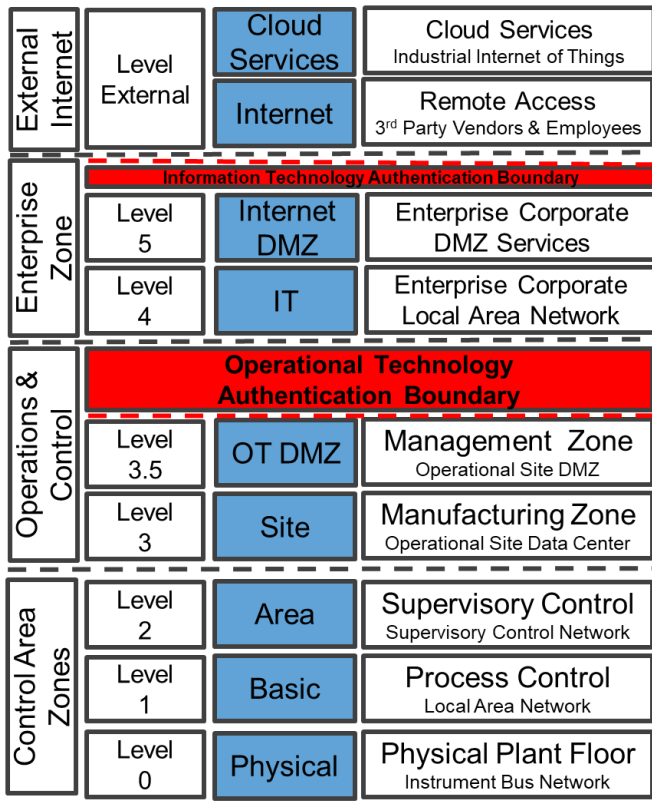


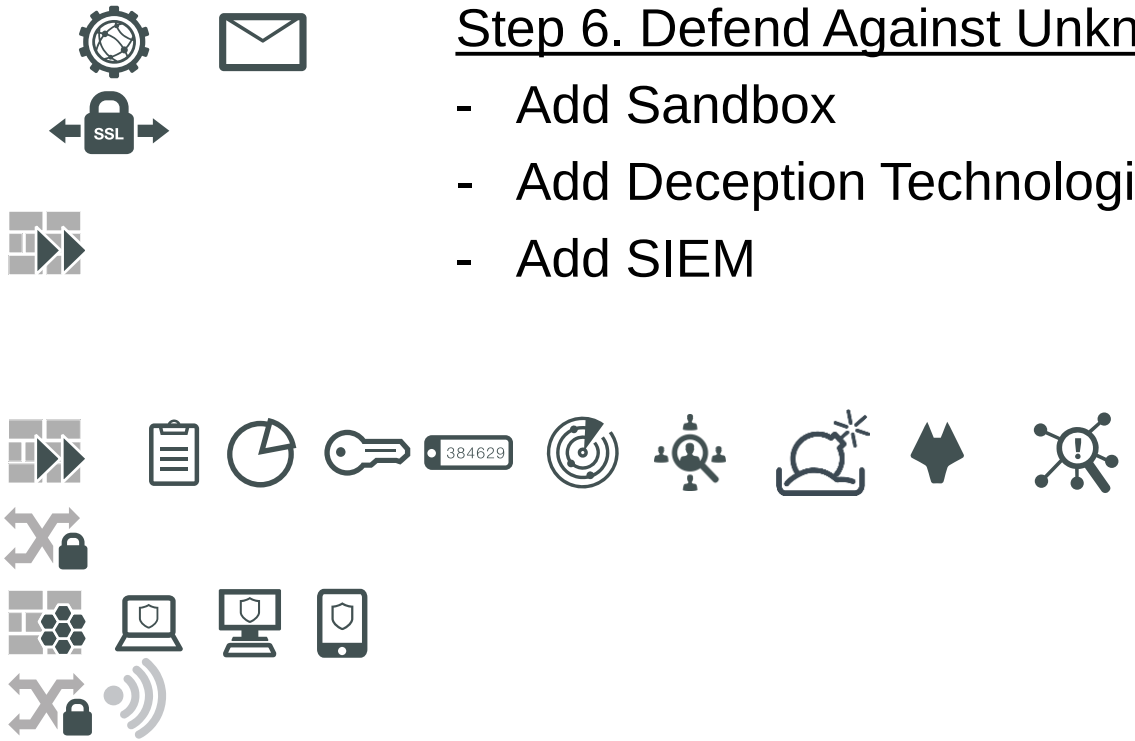


Step 5. Cloud Security

- Add Cloud WAF
- Secure Cloud-based Apps
- Secure remote access

Customer Journey for Securing OT Infrastructure

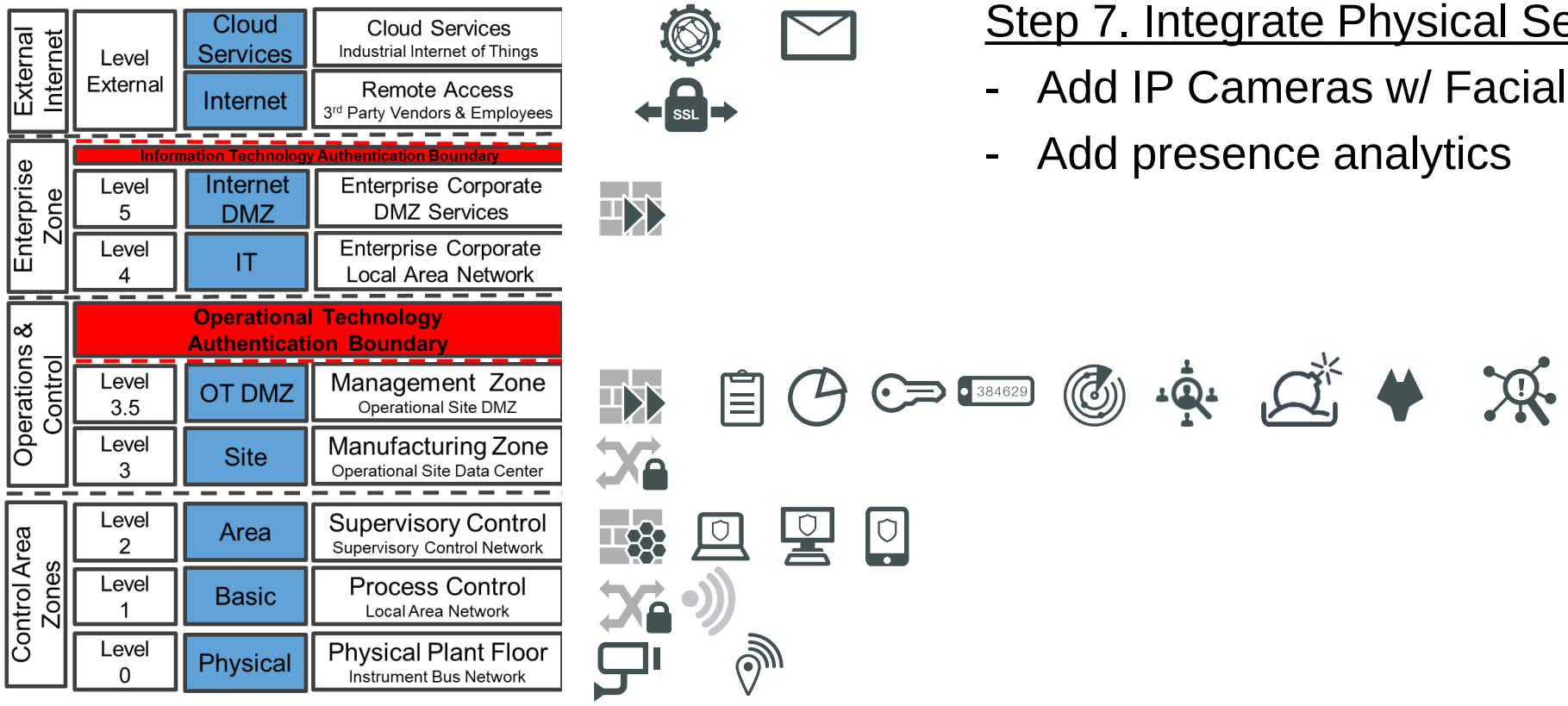




Step 6. Defend Against Unknowns

- Add Sandbox
- Add Deception Technologies
- Add SIEM

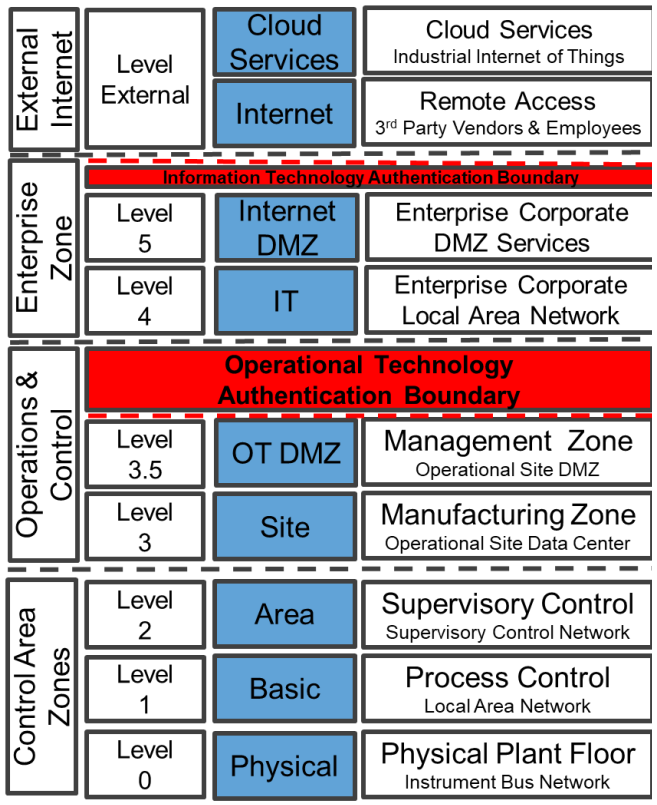
Customer Journey for Securing OT Infrastructure



Step 7. Integrate Physical Security

- Add IP Cameras w/ Facial Recognition
- Add presence analytics

Customer Journey for Securing OT Infrastructure



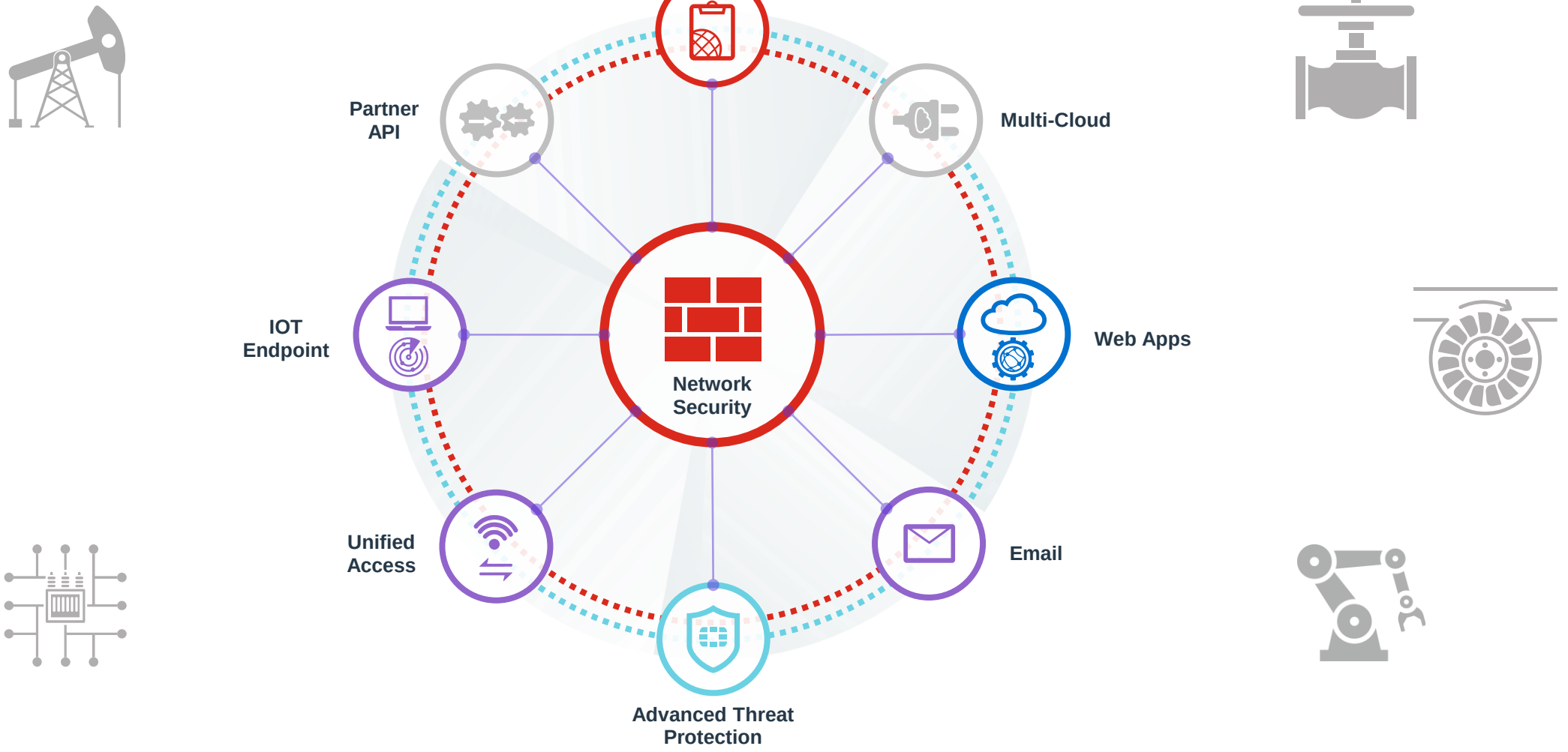
Step 8. Contextual Awareness

- Add DPI vendors with OT capabilities

Fortinet in OT

A Longstanding Leader

Fortinet Security Fabric for Protecting ICS/SCADA



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

We are here to help

Operational Technology and Critical Infrastructure Expertise

Michelle Balderson

Director, Operational Technology and Critical Infrastructure

More than 25 years of experience bringing focus to people, process and technology to help solve business challenges.

Rick Peters

Director, Operational Technology Global Enablement | Electrical Engineer

More than 35 years of cybersecurity and global partnering experience working across foreign, domestic, and commercial industry sectors.

Kunle Adetero

Consulting System Engineer
Operational Technology & Critical Infrastructure
System Engineering

More than 25 years of Experience in cybersecurity, solutions design and deployment, working across multiple foreign, domestic, and commercial industry sectors.

Chris Blauvelt

System Engineer
Operational Technology & Critical Infrastructure
System Engineering

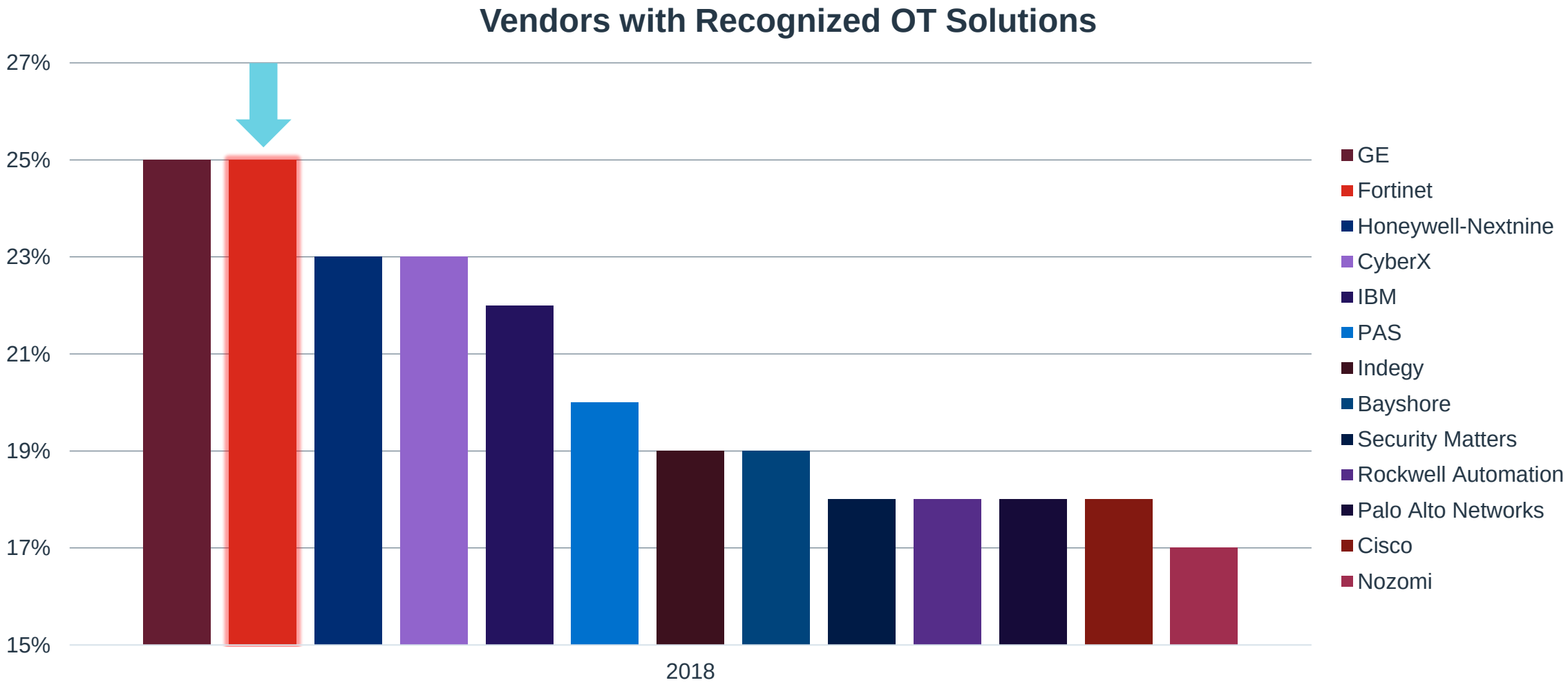
More than 10 years of experience, developing, building, and maintaining electrical power automation and control systems

Carlos Sanchez

System Engineer
Operational Technology & Critical Infrastructure
System Engineering

More than 30 years experience designing and deploying secure critical infrastructure for OT companies worldwide.

Fortinet Known as a Leader in OT



Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Thank you!


FORTINET

SECURITY STRATEGY FOR OT

- Visibility
- Control
- Situational Awareness

VISIBILITY

- Defining the attack surface
- Active device and traffic profiling
- Traffic visibility to ensure actionable intelligence
- Being selective on allowed traffic, ports, protocols and services
- Secure gateway acts as your traffic cop

CONTROL

- Multifactor authentication to determine permissions and access
- Network segmentation and micro segmentation for layered and leveled approach, Zones of Control
- Quarantine and sandboxing to prevent threat before it acts

BEHAVIOR ANALYTICS

- Central security tool for logging, reporting and analytics
- Analyzer tools evaluating activity collected across system
- Security information and event management (SIEM)
- Continuous trust, threat assessments inside out, outside in

SECURITY TRANFORMATION BEST PRACTICES

- Identify assets, classify, and prioritize value
- Segment the network
- Converge cyber and physical security assets to gain situational awareness
- Analyze traffic for threats and vulnerabilities
- Control Identity and Access Management (IAM)
- Secure both wired and wireless access

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
- ✓ Honeywell
- ✓ Iconics
- ✓ InduSoft
- ✓ IntelliCom
- ✓ Measuresoft
- ✓ Microsys
- ✓ MOXA
- ✓ PcVue
- ✓ Progea
- ✓ QNX
- ✓ RealFlex
- ✓ Rockwell Automation
- ✓ RSLogix
- ✓ Siemens
- ✓ Sunway
- ✓ TeeChart
- ✓ VxWorks
- ✓ WellinTech
- ✓ Yokogawa

Deep Packet Inspection (DPI) Application Control Context Signatures
Modbus, IEC 60870-6 (ICCP) and IEC.60870-5.104
Context Logging to FortiAnalyzer, FortiSIEM, and Syslog

Fortinet Operational Technology & Alliance Partnerships

TECHNOLOGY PARTNERS

NOZOMI NETWORKS

SIEMENS

CLAROTY

RAD

ForeScout

SCADAfence

DRAGOS

Indegy

SOLUTION VENDORS AND SYSTEMS INTEGRATORS

SIEMENS

ABB

Schneider Electric

YOKOGAWA

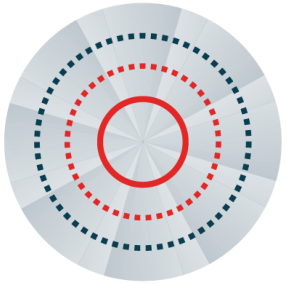
dimension data

World Wide Technology, Inc.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

NTT Communications

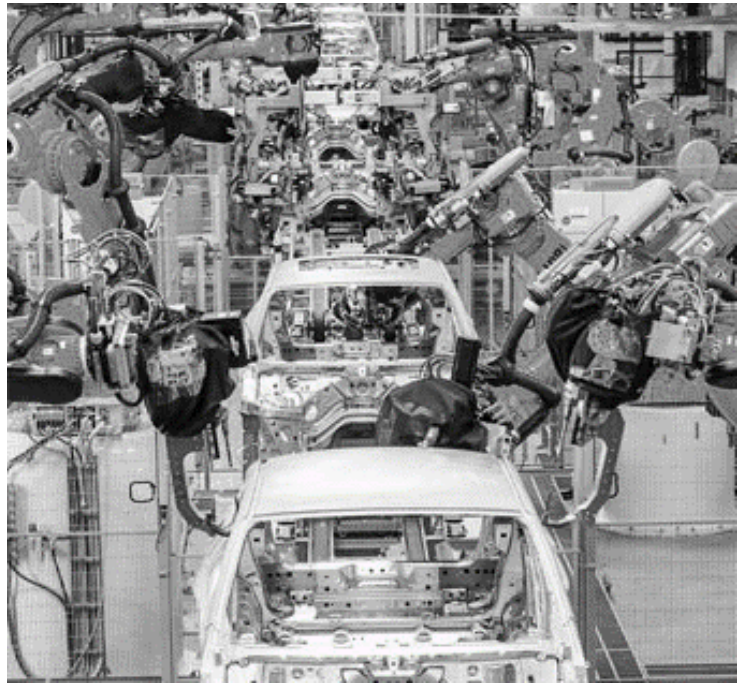
Summary



Fortinet Security Fabric

- OT is Evolving due to variety of pressures
  - OT has similar and different pressures and demands than IT
  - OT is recognizing the need for cybersecurity throughout their OT environment
- Fortinet is a proven Security Vendor with solutions for both IT and OT Environments
  - Extensive Operational Technology and Critical Infrastructure Expertise since 2004
  - Extensive Information Technology Expertise since 2000
  - IT/OT Convergence Expertise, Emerging Market
  - Enterprise Customer Focus
- Fortinet has Established Solutions, Strong Partnerships
  - Operational Technology Framework approach
  - Consulting Approach with Partners, and within Fortinet Processes

OT Customer Success

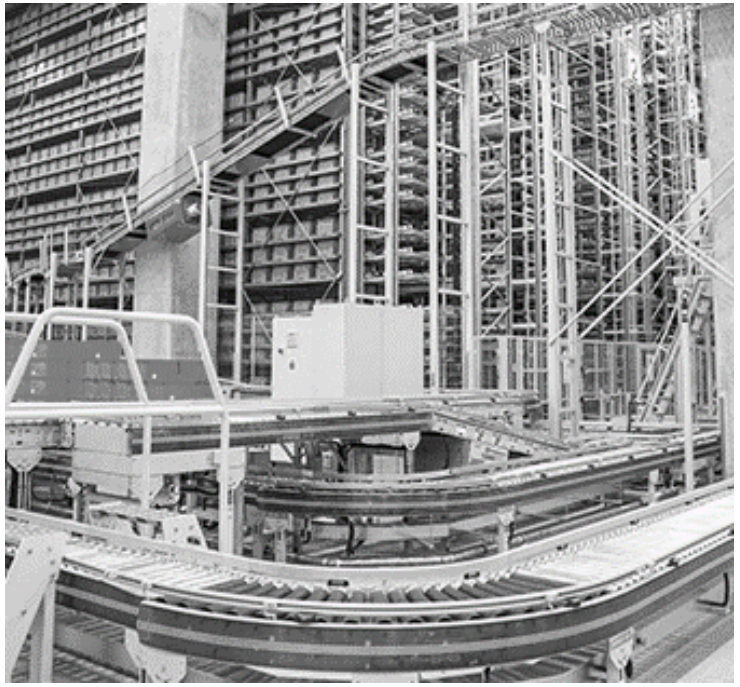


Manufacturing

- Modernization of Security
- Concerns about Security Effectiveness
- Top of the list that keep Executives up at night

Energy & Utilities

- Impact on Operations as a result of a breach
- Concerns about Security Effectiveness
- Top of the list that keep Executives up at night



Transportation & Logistics

- Risk of attacks into IT and OT Infrastructure
- Concerns about Security Effectiveness
- Minimum visibility of network traffic

Importance of IT and OT Convergence for ICS/SCADA Deployment

Industry 4.0 and the Industrial Revolutions of Change

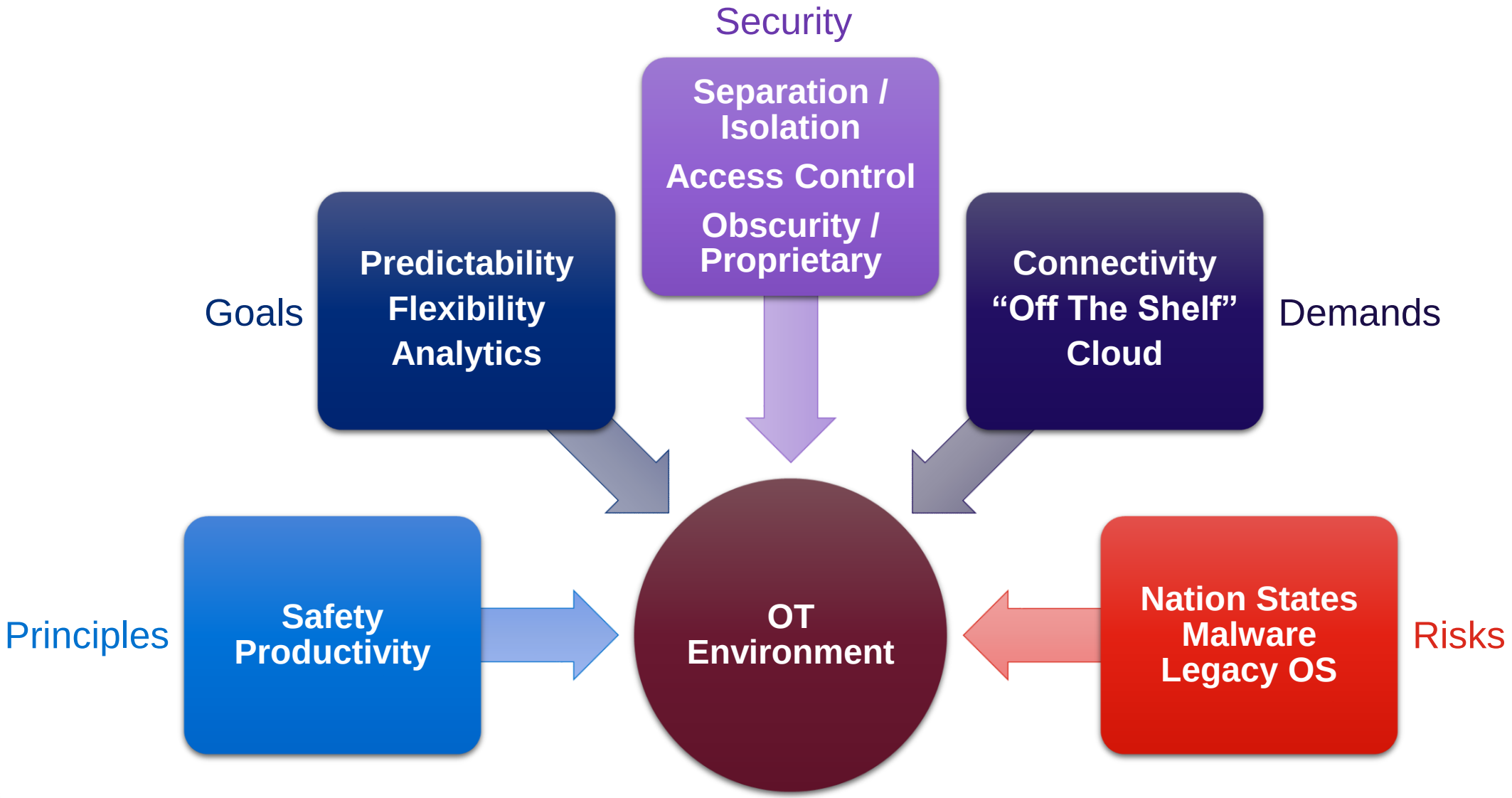
4th	*2010-present* **Fourth Industrial Revolution** Intelligent Automation	• Converging Digital Capabilities • Digital Transformation driving Customer Choice • Personalized Customer Experience
3rd	*1970s-2000s* **Third Industrial Revolution** Electronic Automation	• Computer Driven Automated Processes
2nd	*Beginning of 20th century* **Second Industrial Revolution** Industrialization	• Mass Production Electrically Powered Production Lines
1st	*Late 18th century* **First Industrial Revolution** Power generation	• Stream Powered Processes and Electric Power Generation

Accelerating Rate of Change

- Human Driven Muscle Power processes, Farming and Agriculture

Source: 2019 Manufacturing Trends Report, Microsoft Dynamics 365

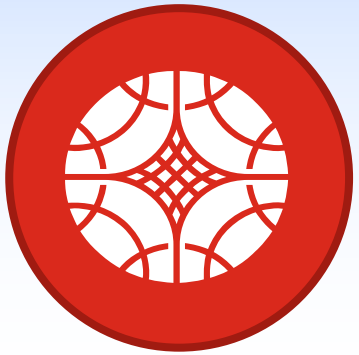
Unique Challenges



Familiar Customer Issues

Attack Surface

Digital Attack surface is rapidly expanding



BROAD

Visibility of the entire digital attack surface

Advanced Threats

Requires rapid Detection and Prevention

INTEGRATED

Protection across all devices, networks, and applications

Vendor Complexity

Complexity slows down Management and Response

AUTOMATED

Operations and response driven by Machine Learning

Safe and Secure OT Solutions for Manufacturing

Safe and Secure OT Solutions for Energy & Utilities

Safe and Secure OT Solutions Transportation Systems

Purdue Model for Control Hierarchy

Enterprise Zone

Level 5: Enterprise

Level 4: Site Business Planning and Logistics

Manufacturing Zone

Level 3: Site Manufacturing Operations and Control

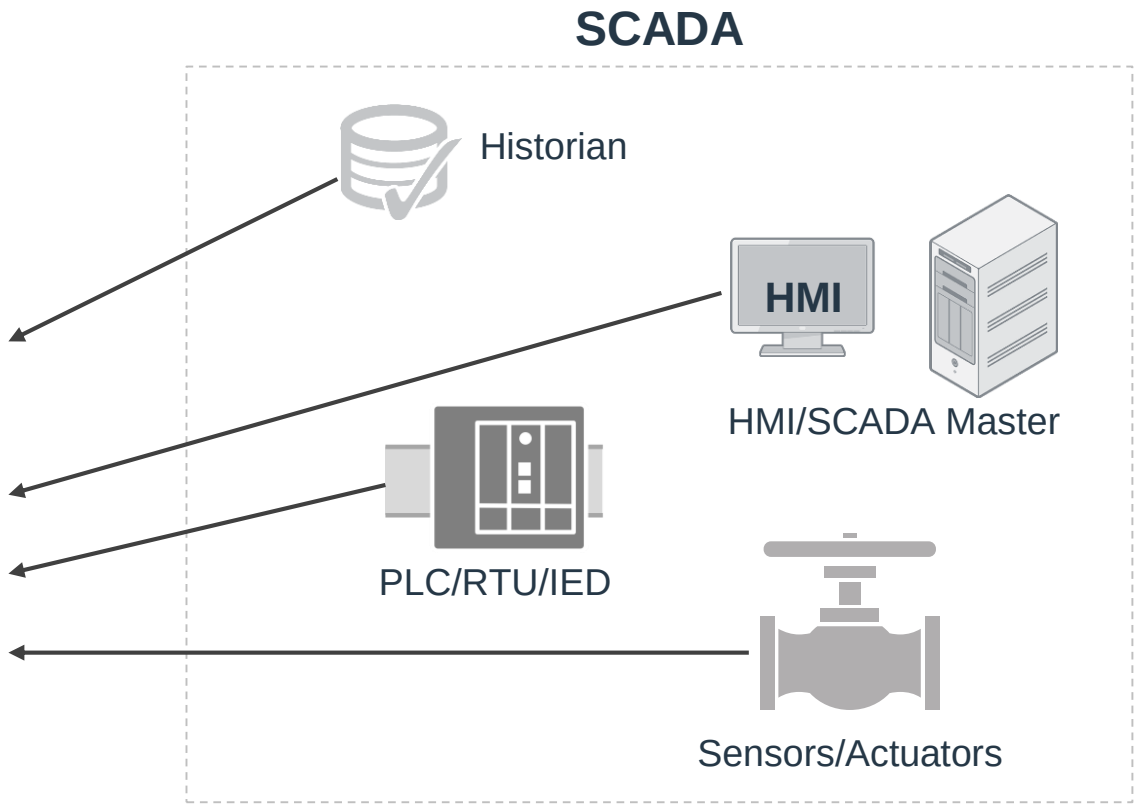
Cell/Area Zone

Level 2: Area Supervisory Control

Level 1: Basic Control

Level 0: Process

Safety Zone



- Logical framework to describe the basic functions and composition of a manufacturing system. Adopted in other models and industries
- Segments devices and equipments into hierarchical functions
- Based on this segmentation of the plant technology, the ISA-99 Committee for Manufacturing and Control Systems Security has identified the levels and logical framework