SECURITY SUMMIT
Academy

Atelier

Perché fabbrica connessa deve far rima con Cyber Security?

Alessio L.R. Pennasilico, Comitato Tecnico Scientifico Clusit
Carlo Forneris, Principal System Engineer Fortinet
Giulia Procoli, Systems Engineer Fortinet

10 settembre 2020, ore 15:00 - StreamingEdition

#securitysummit #academy #streamingedition

Alessio L.R. Pennasilico aka -=mayhem=-

Practice Leader Information & Cyber Security Advisory Team @ P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Presidente dell'Associazione Informatici Professionisti AIP Associazione Informatici Professionisti ITCS Italian Computer Society

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

SCADA, OT, IoT, Industry 4.0 ed ICT

Il mondo dell'automazione industriale negli ultimi 30 anni
è stato oggetto di una rivoluzione

Da *automatizzato* è diventato *informatizzato*

OT: Un mondo sempre più IT

Dal cavo seriale al cavo ethernet e WiFi

Da protocolli proprietari a protocolli standard

Da hardware dedicato a hardware General Purpose

Da Sistemi operativi proprietari a sistemi General Purpose

Da reti isolate a reti integrate

Con quali ulteriori opportunità, garanzie e rischi?

Opportunità e rischi

Risparmio, risparmio, risparmio e standardizzazione

Ma chi c’è dall’altra parte del cavo?

Qualcuno potrebbe manipolare le informazioni?

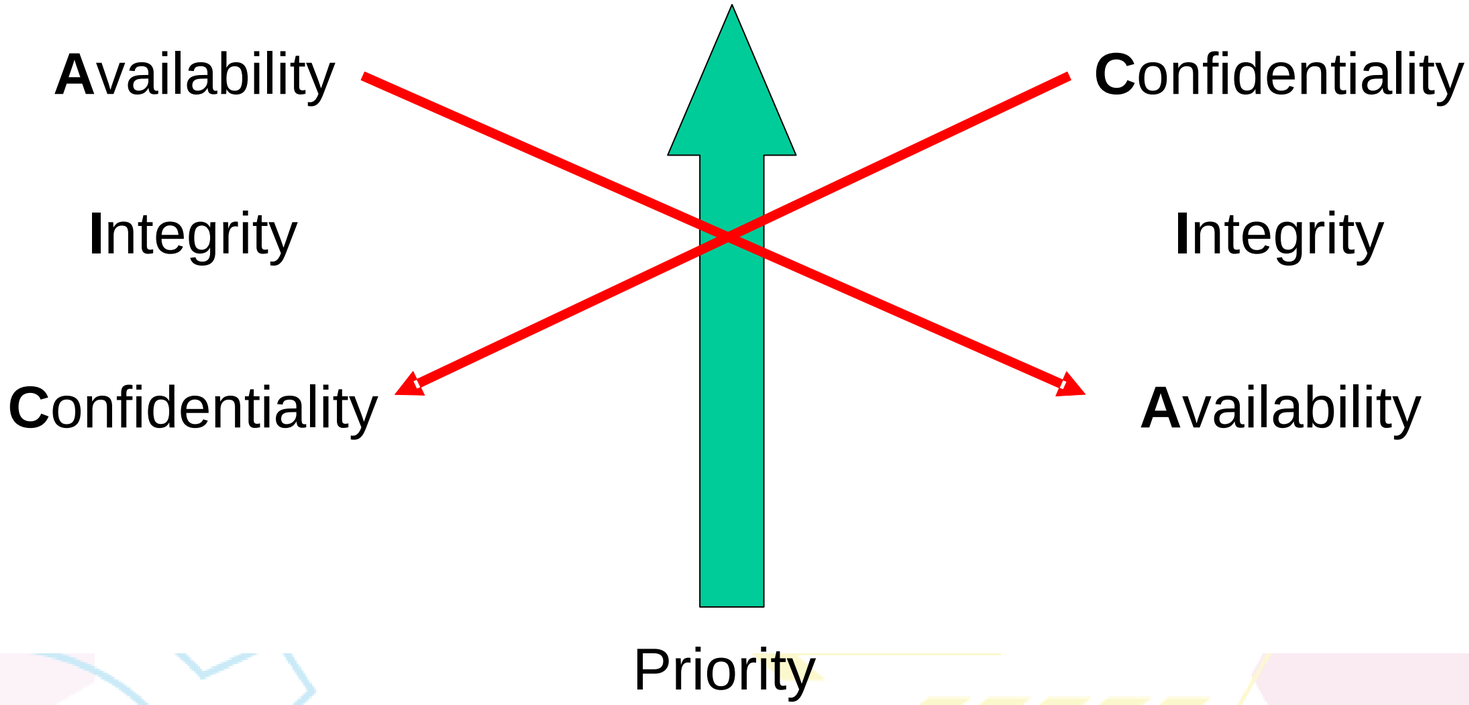
Interagire con i dispositivi?

RID vs DIR

Quali sono le priorità di un CIO? Di un CISO?
Quali quelle di un Direttore della Produzione?

Quali secondo ISO 27001?
Quali secondo IEC 62443?

IEC 62443 vs ISO 27001



Attenzione ai requisiti normativi

Dall'adeguamento alla Direttiva NIS (D.Lgs. 65/18)

All'inclusione nel perimetro cibernetico nazionale

A requisiti di Data Protection

Potrebbe non essere sempre evidente ogni requisito se non è stata eseguita una analisi formale del contesto

Come cambiano in ambito OT alcuni processi IT Security

System & Network Architecture

EndPoint Protection

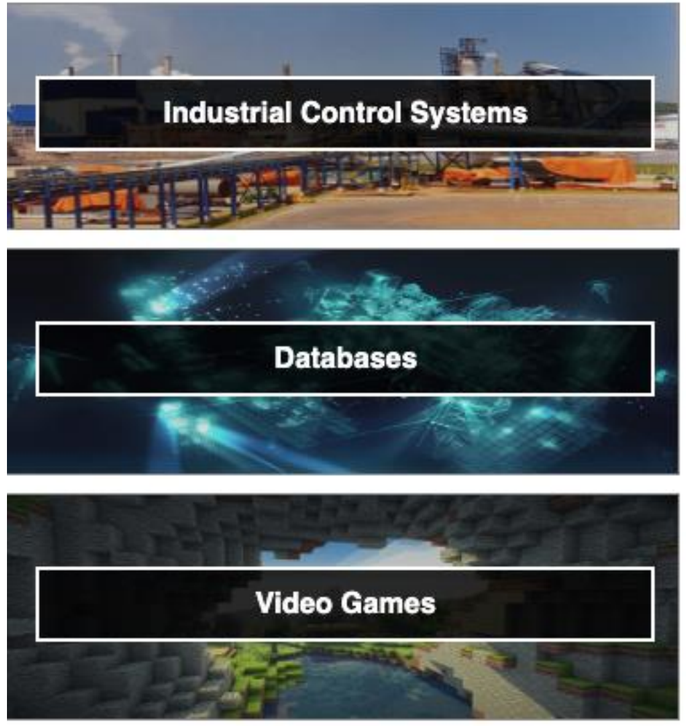
Patch Management

Vulnerability Management

Accessi per manutenzione

Rischi: come Shodan evidenzi le infrastrutture non gestite correttamente

Featured Categories



Top Voted

12,103
Webcam
best ip cam search I have found yet.
webcam surveillance cams 2010-03-15

5,046
Cams
admin admin
cam webcam 2012-02-06

2,604
Netcam
Netcam
netcam 2012-01-13

2,000
default password
Finds results with "default password" in the ba...
router default password 2010-01-14

Recently Shared

1
iomega
2020-09-08

4
sex
2020-09-08

1
Lots of DVR's
2020-09-08

2
SCADA PlantVisor Guest allowed
Guest without pass allowed
2020-09-06

Minacce ed Incidenti specifici per il mondo SCADA/OT: sono in continuo aumento

…

Stuxnet (2010)

Duqu, Flame, and Gauss (2011)

Shamoon (2012)

Target, Havex (2013)

Black Energy (2014)

Ukraine Power Grid (2015)

Kemuri, Ukraine Power Grid (2016)

CrashOverRide (2017)

…

Conclusioni

E’ necessario

creare una consapevolezza condivisa tra i team IT, OT e Security

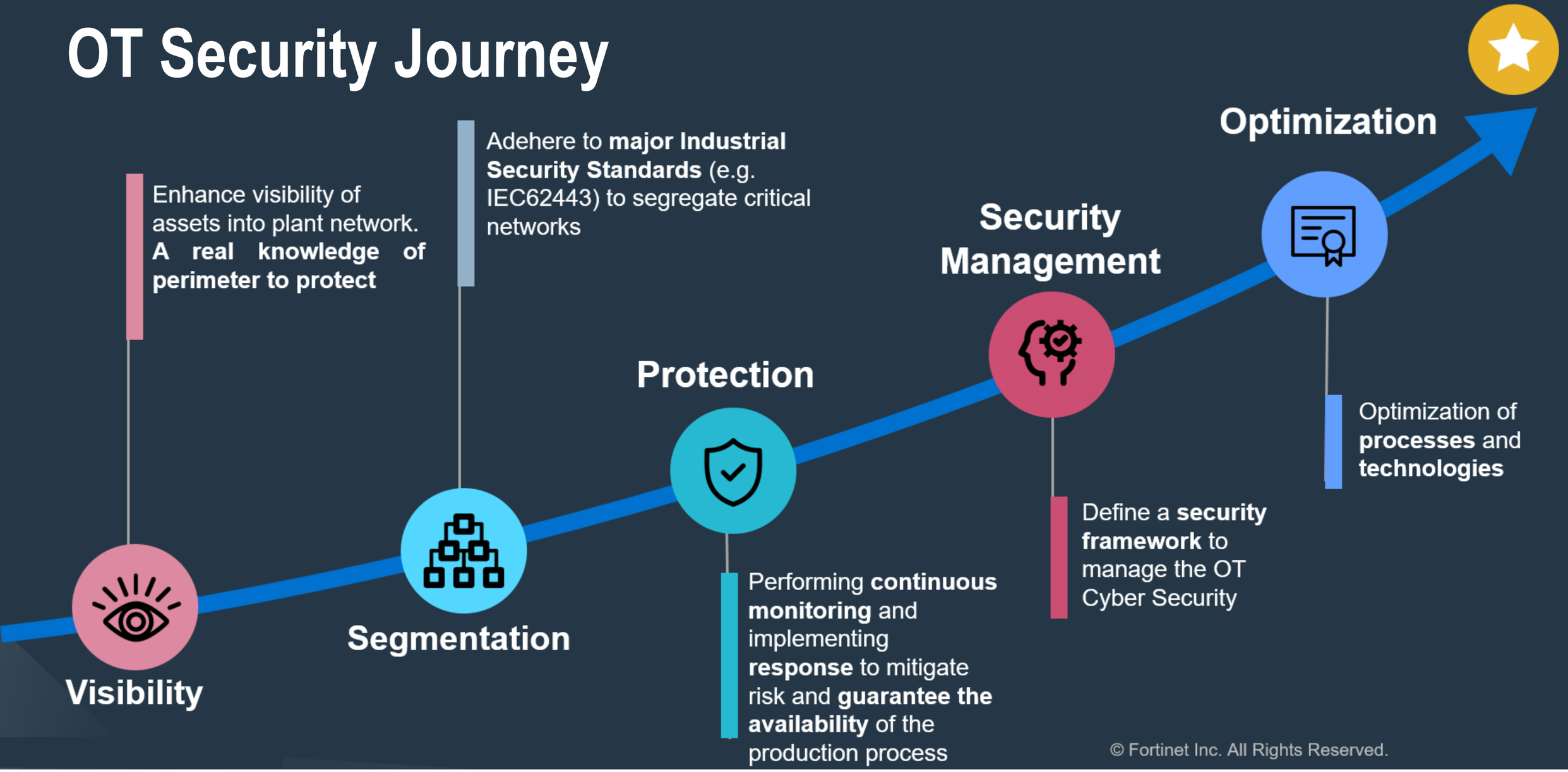
creare l’organizzazione, i processi
ed adottare le architetture e le tecnologie
adeguati al contesto

Carlo FORNERIS

FORTINET PRINCIPAL SYSTEMS ENGINEER

OT SPECIALIST

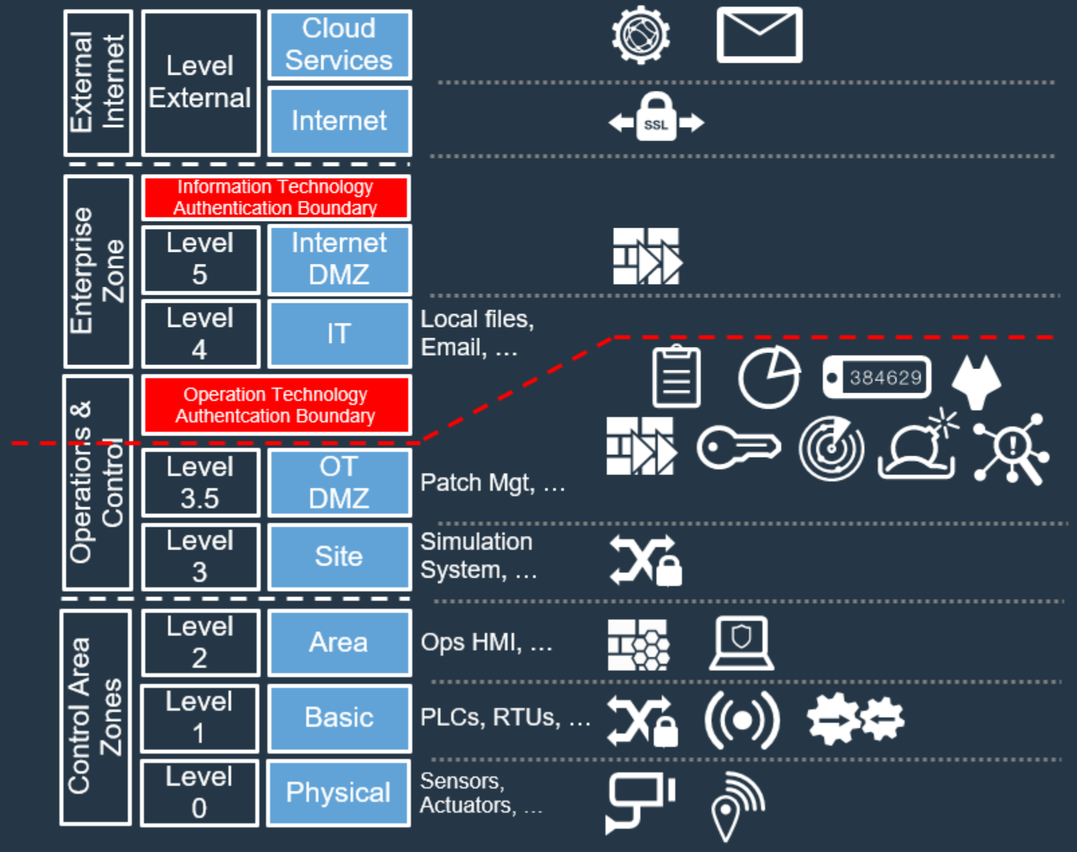
OT Security Journey



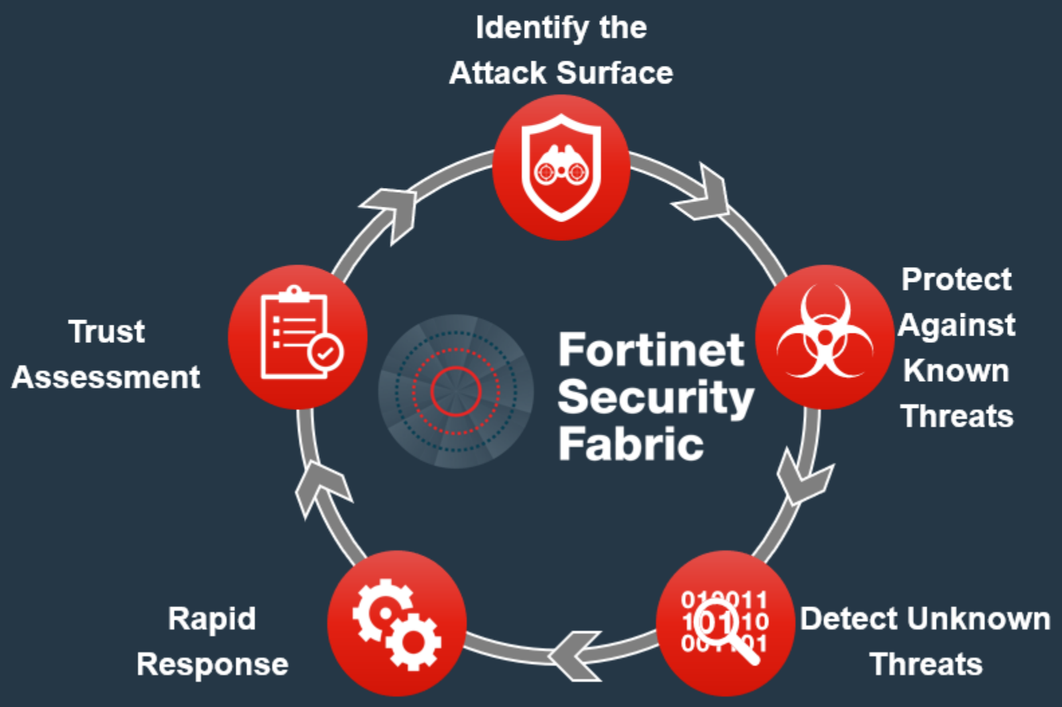
Security Framework aligned to OT Standards & Guidelines

Purdue/IEC62443 Ref. model

Fortinet Security Fabric



NIST Cyber Security Framework



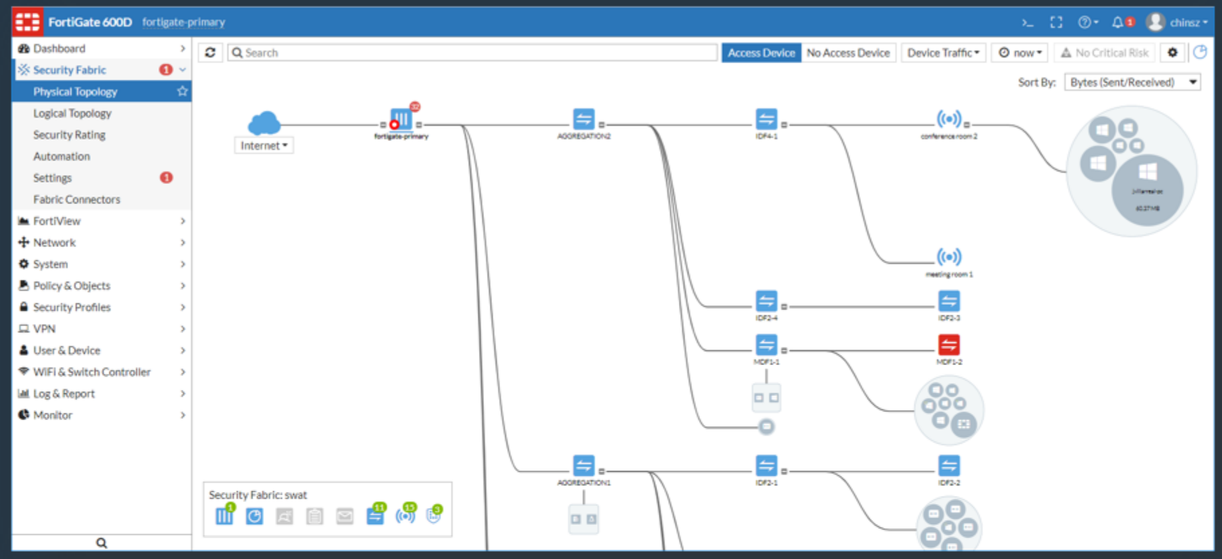
Network Segmentation

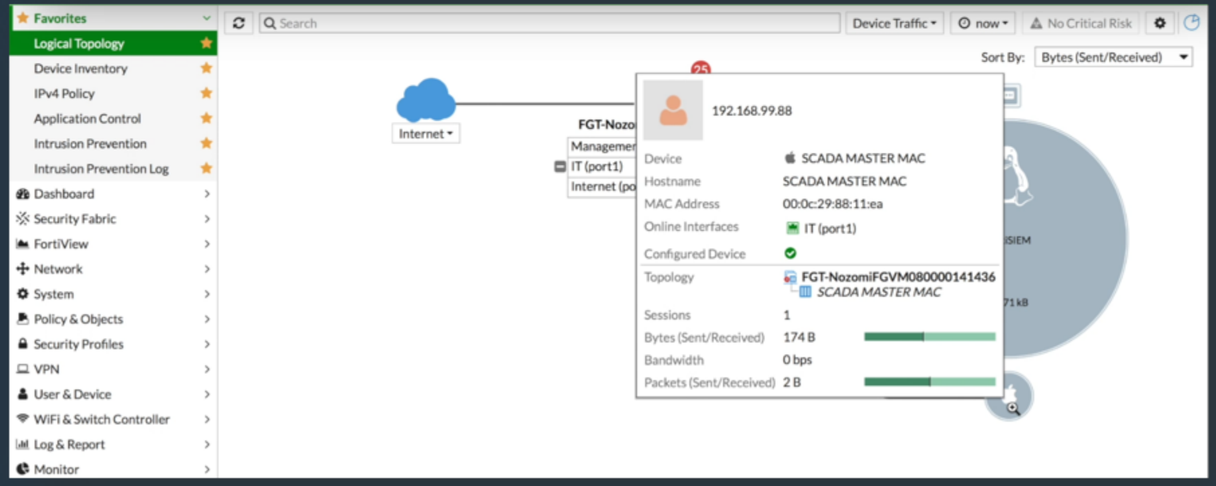
Challenge

- No visibility on OT
- OT network is FLAT

Customer needs

- Define functional segments or “zones”
- Allow access to “zones” only by authorized users
- Allow access to “zones” only by authorized applications
- Adhere to the ISA / IEC-62443 standard





Virtual Patching

Challenge

- PLC based on outdated OS
- PLC exposing known Vulnerabilities
- No chance to patch OS

Customer needs

- Protect PLC from Known Vulnerability
- Protect PLC from Known Malware
- Protect PLC from Unknown Malware*

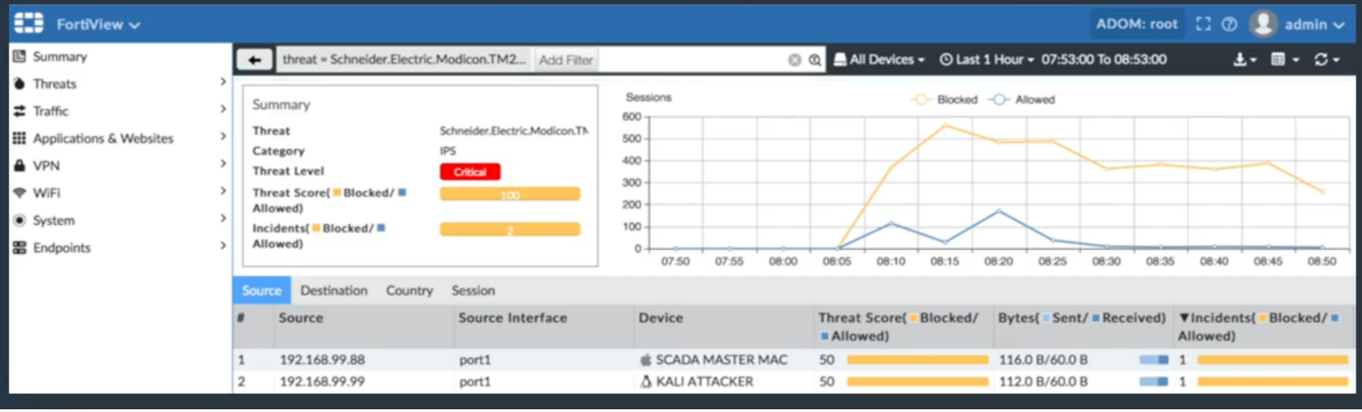
Some of the Supported Protocols

- ✓ 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

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



* Optional

Third Party Remote Access

Challenge

- Third party IT vendor have full access
- No control on the PCs of IT vendor
- No visibility on “third party” access

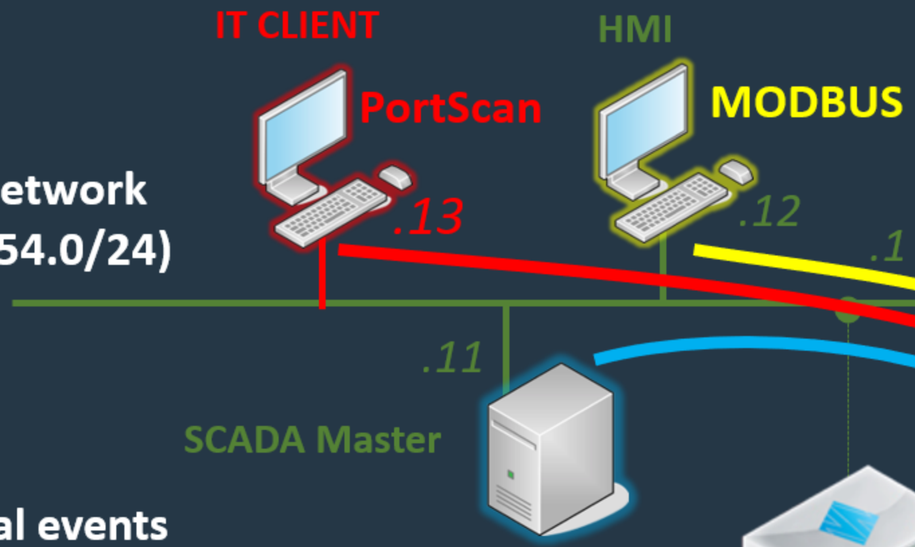
Customer needs

- Define a single point of access
- Increase the reliability of zones’ access

Nozomi Networks: Fortinet Fabric Ready for ICS

- Leverages Security Fabric APIs to deliver pre-integrated, end-to-end security offerings
- Integrated products improve threat awareness & intelligence, broaden & coordinate threat response and policy enforcement
- Faster time-to-deployment & reduced costs due to pre-validation of solutions
- Learning approach on OT traffic to create a baseline.
- Identify more that 150 Scada protocols traffic
- Able to receive commands from Nozomi to apply realtime policy enforcement
- Fabric Connector ready to accept Nozomi bi-directional communication.
- Visibility of action applied

Fortinet-Nozomi automation



Fortigate Policy rule

Seq.#	Name	Source	Destination	Schedule	Service	Action
Process Network (port2) - Control Network (port2) (1 - 3)						
1		n2os_fortigate 192.168.254.12	n2os_fortigate 192.168.253.11	always	n2os_tcp_502	DENY
2		n2os_fortigate 192.168.254.13	all	always	ALL	DENY
3	Accepted Protocols	all	all	always	Modbus SSH	ACCEPT

Authorized Traffic

Dynamic Policy
Block Traffic

Nozomi normal events

Host	Name	Label	Type	Value	Last value	Protocol
192.168.253.11	ir7	Reservoir Water Level	analog	47.000	47.000	modbus
192.168.253.11	ir8	Lake Water Level	analog	1002	1002	modbus

Nozomi SCADA-Guardian Incidents

Incidents & Alerts

Page 1 of 1, 2 entries — Group by incident — Auto — Count by field... — 13 selected

Actions	Time	ID	Type ID	Name	Description
	12:47:19.694	26f3de86	INCIDENT:NEW-NODE	New Node	New node 192.168.254.13 appeared on the network
	12:47:19.694	df9685ed	INCIDENT:PORT-SCAN	Port Scan	Port Scan made by 192.168.254.13 on subnet 192.168.253.0/24 within tcp
	12:50:37.085	9e159be5	INCIDENT:NEW-COMMUNICATIONS	New Commur	Known nodes 192.168.254.12 and 192.168.253.128 have started new communication

Giulia PROCOLI

FORTINET SYSTEMS ENGINEER

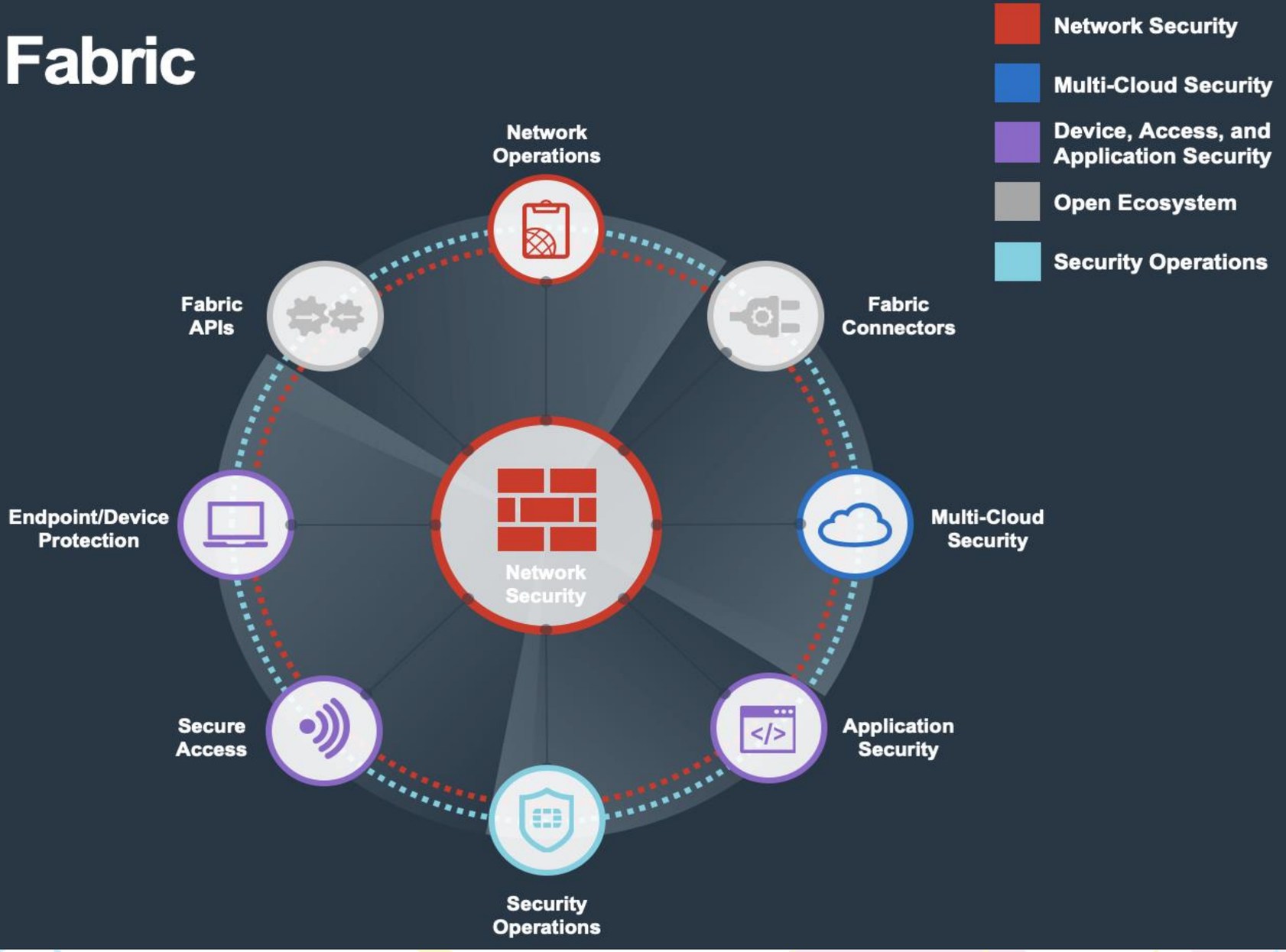
OT SPECIALIST

Fortinet Security Fabric

BROAD
Visibility of the entire digital attack surface

INTEGRATED
AI-driven breach prevention across devices, networks, and applications

AUTOMATED
Operations, orchestration, and response



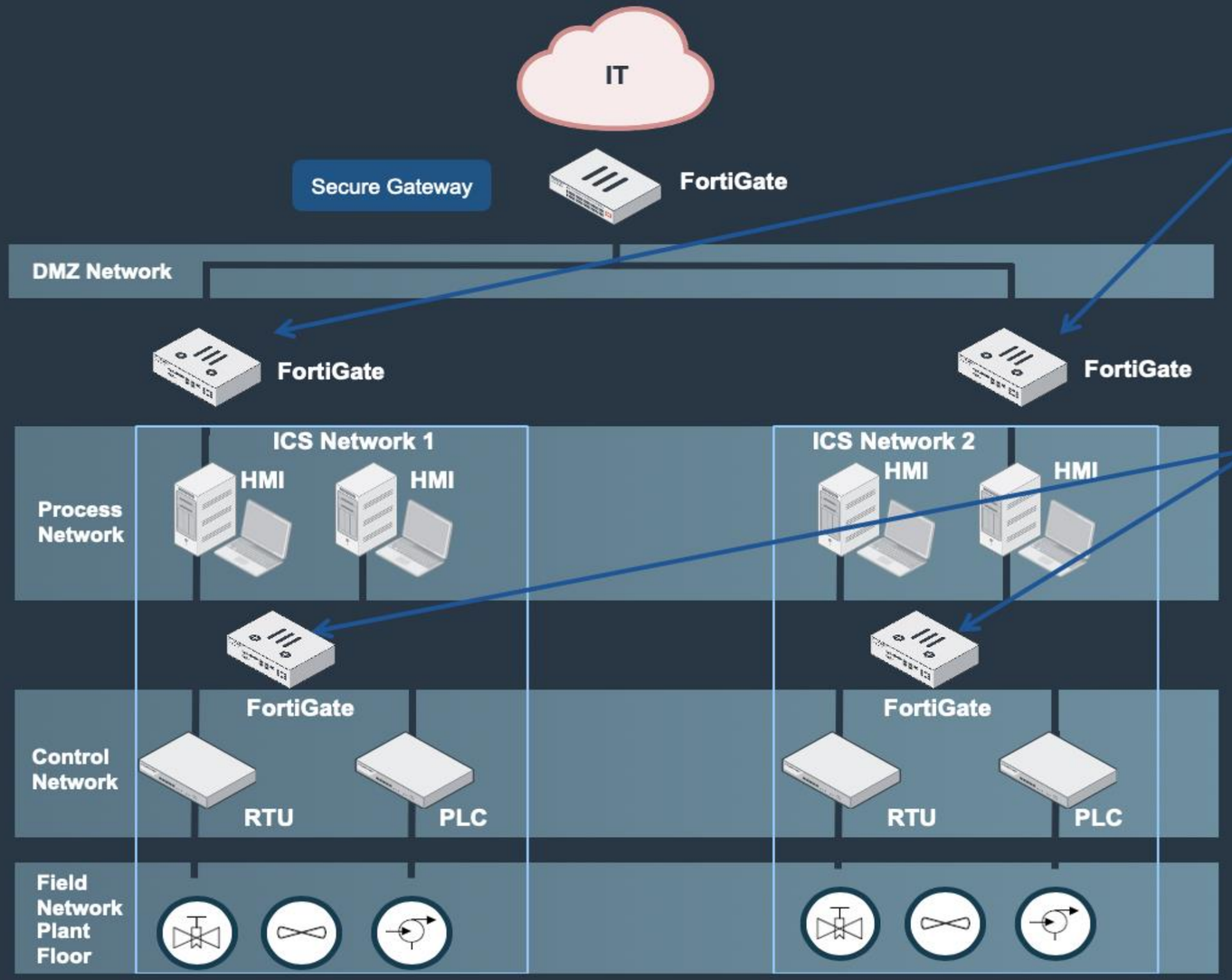
Fortinet's Approach to Securing Manufacturing

Enterprise Zone

DMZ

Operations and Control

Control Area Zone(s)



Segmentation of different ICS Networks

Granular Segmentation within the ICS Network

IEC 61850

EMI

Thermal

Vibration

Industrial Grade & Compliance Ready

Unified Secure Access

Security Fabric | NETWORKING

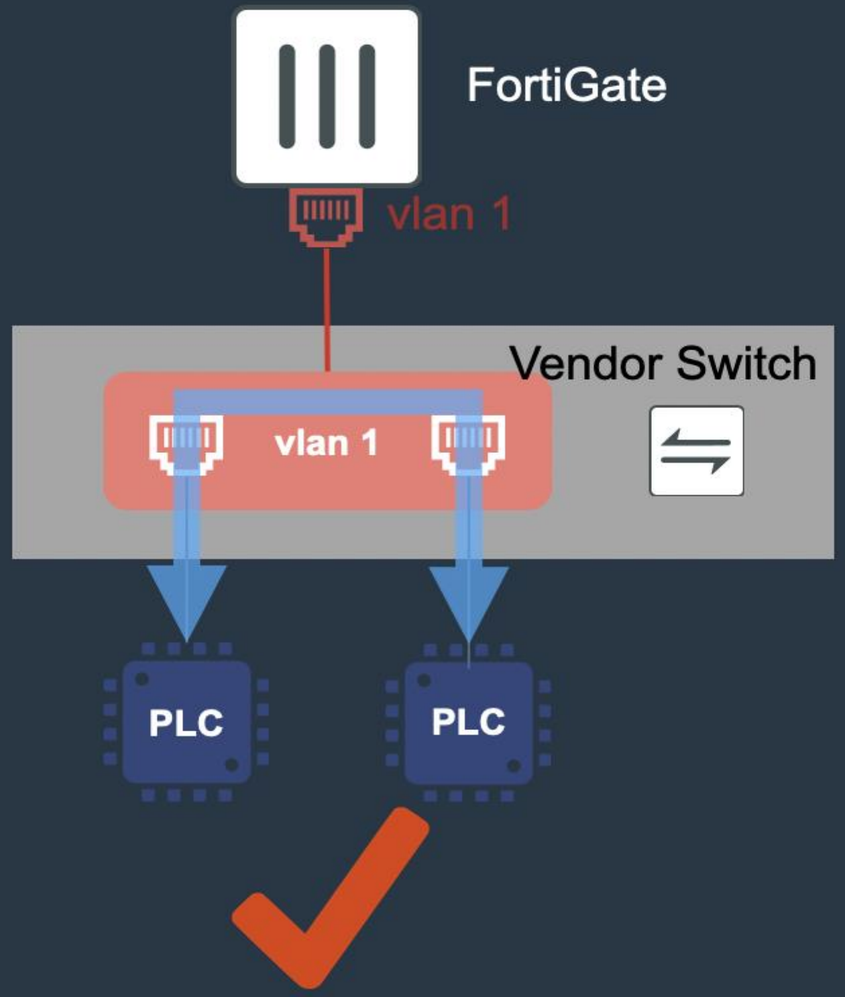
Shared Services

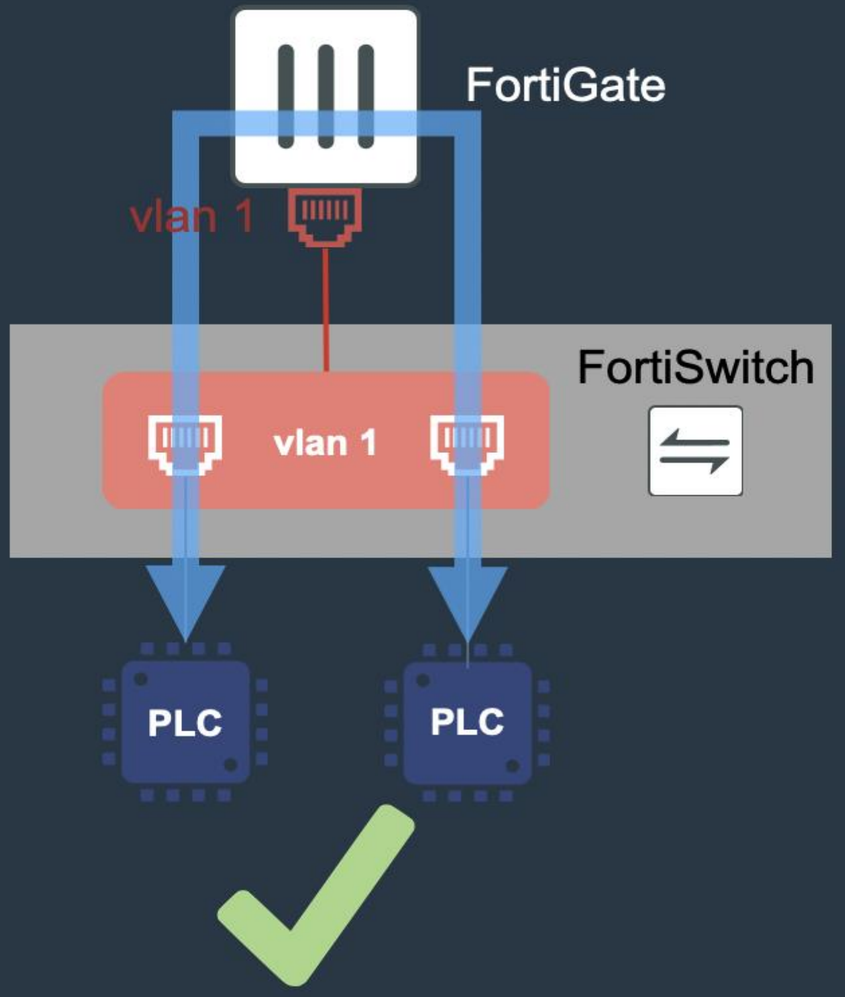
- ☑ Configuration
- ☑ User/Device Identification and Control
- ☑ Content Inspection and Protection
- ☑ Visibility
- ☑ Logs & Reports

INTEGRATED SWITCH MANAGEMENT

Integrated Connectivity Management with Security

Micro Segmentation

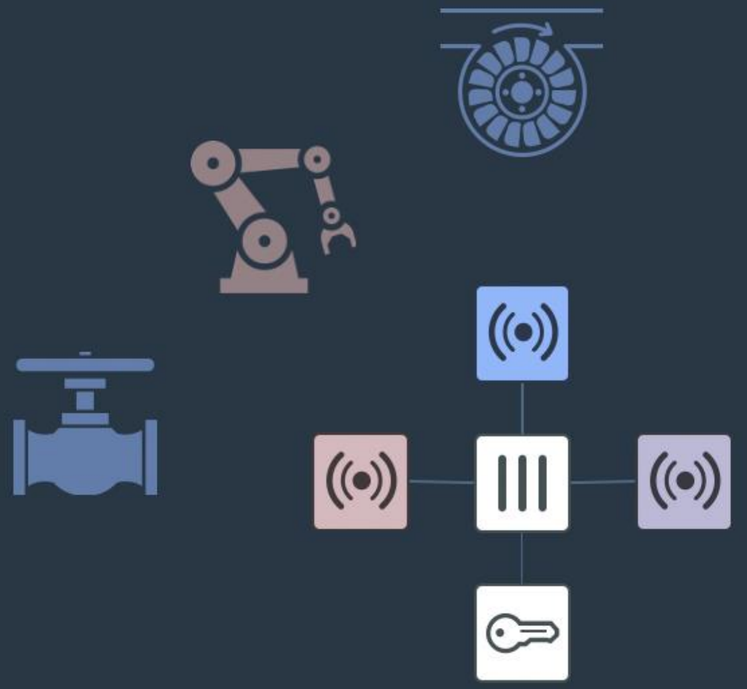




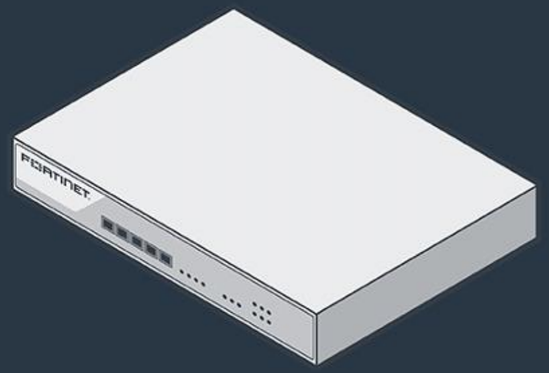
Secure Access and Wireless

OT & Industrial IoT Segmentation

- Single SSID
- Multiple PSKs (MPSK)
- Per device type segmentation
- Radius Authentication (FortiAuthenticator)
  - MAC Authentication
  - Dynamic Group/VLAN Allocation
- Per VLAN interface and/or Identity Based policies



Security of IoT - FortiNAC
Network Access Control



- Identify and profile all endpoints, IoT devices, users, & applications
- Segmentation based on endpoint characteristics and behavior
- Continuous risk assessment and automated responses for dynamic network control across 3rd party devices

Watching Every Node on the Network

Breach Protection Strategy

Lockheed Martin Cyber Kill-Chain Model

Reconnaissance: FortiDeceptor

- Create Decoys and Lures to entice attackers
- Increase cost & time of attacker
- Proactive early warning of reconnaisance activities, attempts to penetrate
- Reports IP/Geo of attackers, IPS attacks used,
  expose external/internal attackers
- Cut down time of breach detection

Delivery & Exploit Decoys

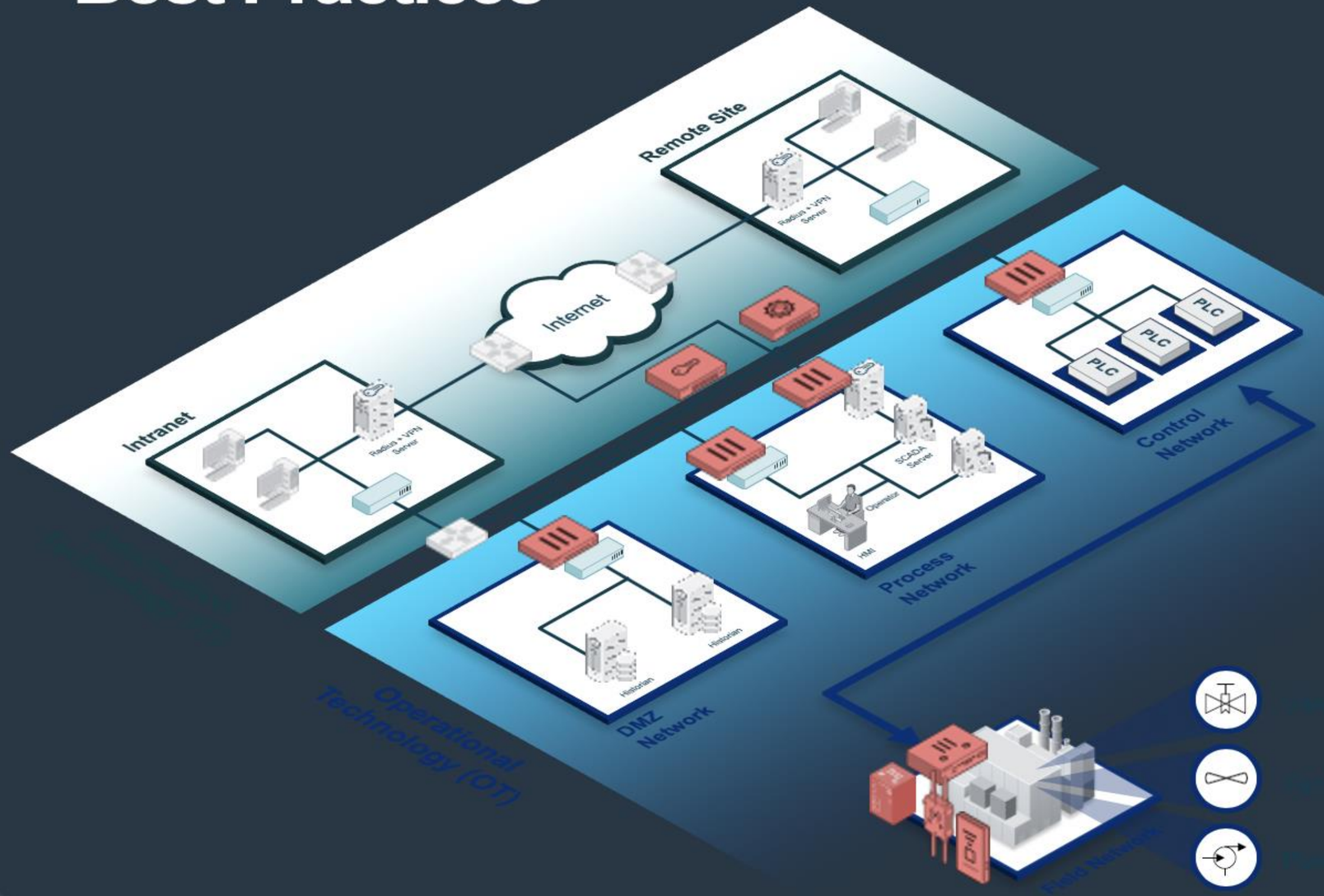
- Exposing Attacks on Decoys
- Intrusions To & From Decoys
- Malware Planted on Decoy
- Web Sites Visited
- Normal Users Should Not Be Aware of Decoys Existence
- Real time Tracking & Display by Anti-Exploit Engine
- Group by Timeline & Campaign

Action on Objectives: Exfiltrate

- Randomized Decoy Content (File & SQL server)
- Understand Attackers Objective (e.g. Exfiltrate Data, jump host, Network Scan)
- Auto Quarantine of Attackers (FortiGates)
- Send alerts to any SIEM

TIME

Best Practices



- Segmentation and Encrypted Communication (FortiGate)
- Enable Secure Wired and Wireless Access (FortiAP, FortiSwitch)
- Role Based Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)
- Vulnerability and Patch Management (FortiWeb, FortiClient and FortiGate)

IPS & Application Control for Industrial Systems

Some of the Supported Protocols

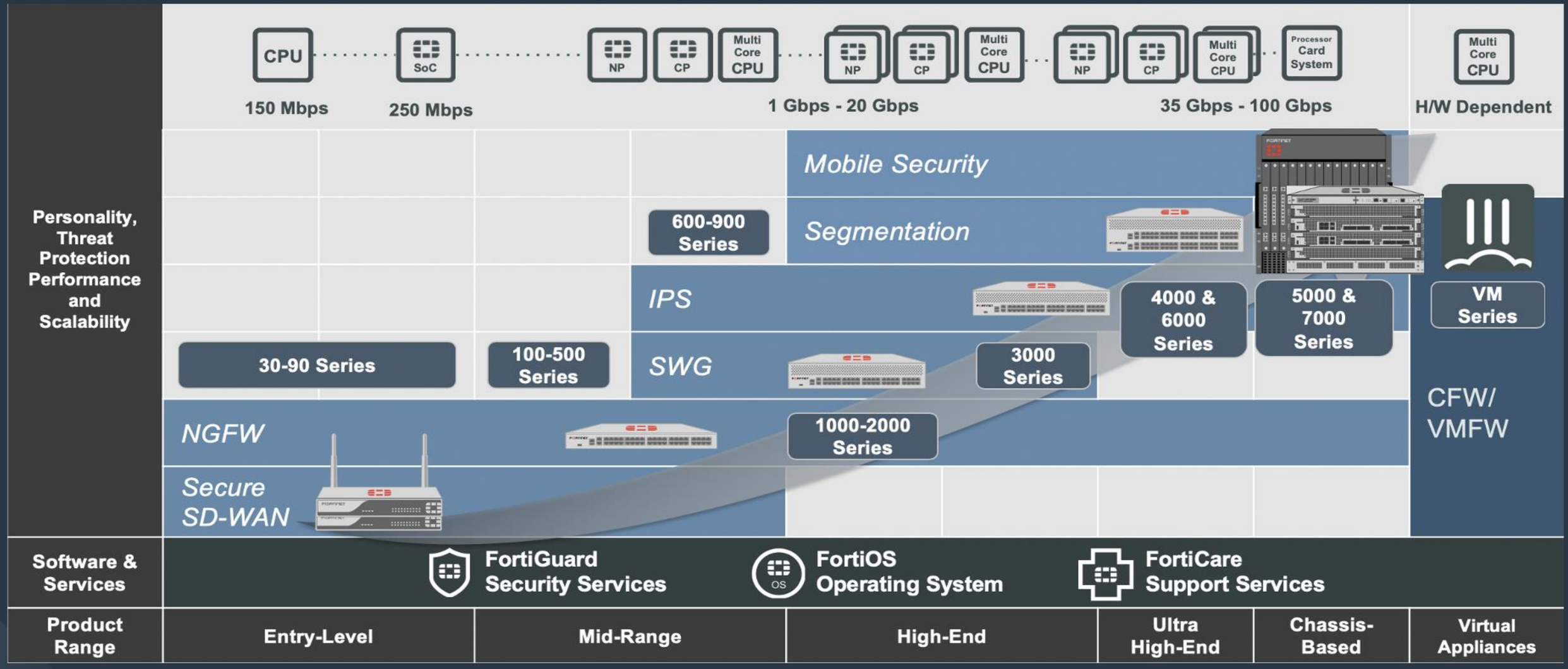
- ✓ BACnet
- ✓ DNP3
- ✓ Elcom
- ✓ EtherCAT
- ✓ EtherNet/IP
- ✓ HART
- ✓ IEC 60870-6 (TASE 2) /ICCP
- ✓ IEC 60870-5-104
- ✓ IEC 61850
- ✓ LONTalk
- ✓ MMS
- ✓ Modbus
- ✓ OPC
- ✓ Profinet
- ✓ S7
- ✓ SafetyNET
- ✓ Synchrophasor

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

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

All FortiGate Products align to OT Environments



Q&A