Hackeři a škodlivý kód v síti průmyslového řízení: OT Security Fabric je připraven je zastavit

Jan Václavík

Systems Enigneering Team Lead, Fortinet

jvaclavik@fortinet.com

Cíle modernizace OT (Operational Technology)

Zlepšit bezpečnost

Optimalizovat efektivitu výroby

Umožnit rozhodování v reálném čase

Zabezpečení sítí Operation Technology




Většina průmyslových řídicích systémů **nemá bezpečnost zabudovanou již v návrhu** a je **citlivá na jakékoli změny**.

Rostoucí adopce nových technologií, jako jsou **5G, IIoT a cloud**.

Rozšiřování attack surface (útočná plocha); závislost na ochraně pomocí air-gap se zmenšuje.

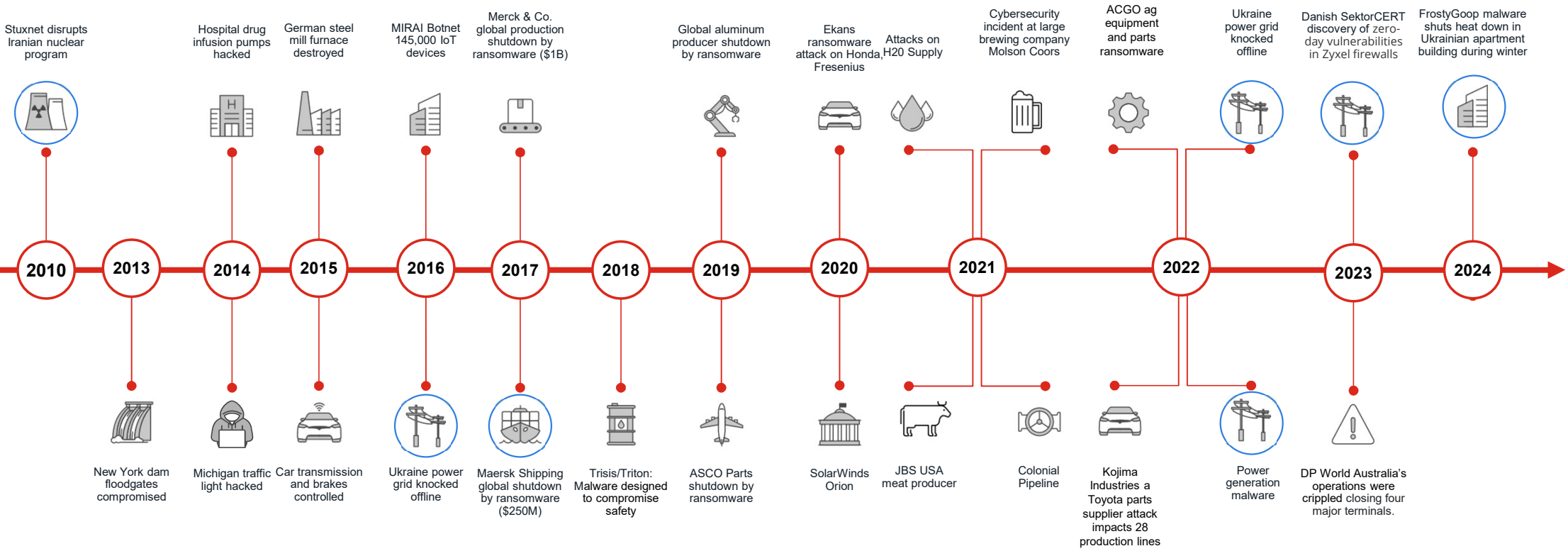
Požadavky na vzdálený přístup pro třetí strany a zaměstnance vytvářejí další bezpečnostní rizika.

Iniciativy digitální transformace (Industry 4.0) podporují konvergenci IT a OT sítí.

Závislost na OEM dodavatelích a systémových integrátorech (SI) vystavuje kritické systémy dalším rizikům.

Útoky na OT infrastrukturu se stupňují

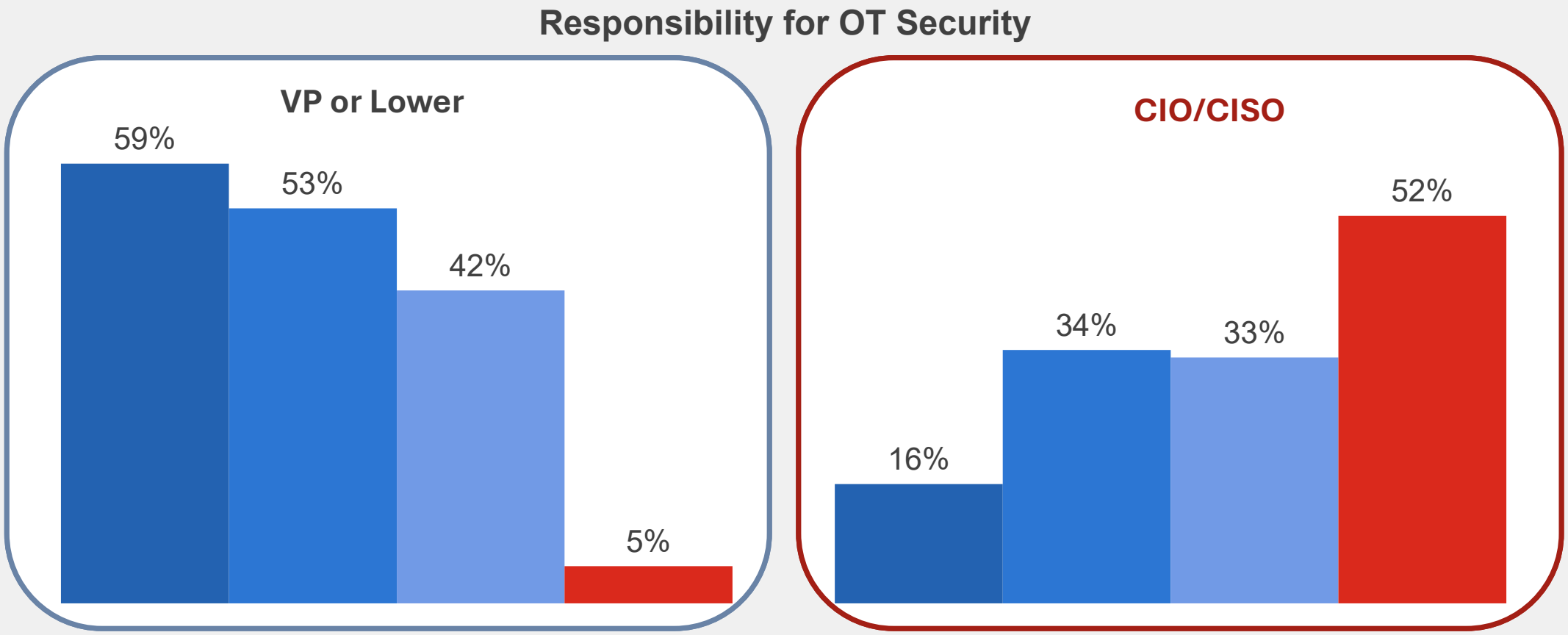
Attacks are increasing in frequency and impact



OT targeted attacks

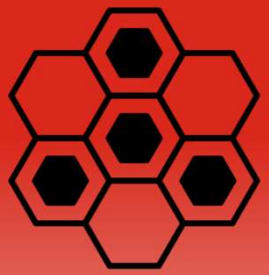
OT bezpečnost: důležitější než kdykoli předtím

CISOs a vrcholoví manažeři přebírají odpovědnost za kybernetickou bezpečnost OT.



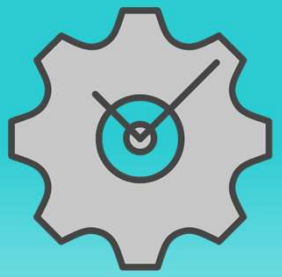
*The Fortinet 2025 State of Operational Technology and Cybersecurity Report

Doporučené osvědčené postupy pro ochranu OT

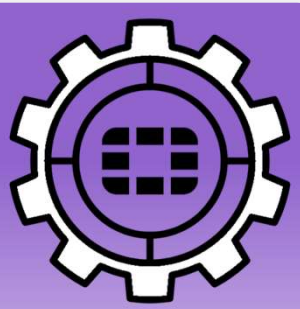


Segmentation

Visibility & Compensating Controls



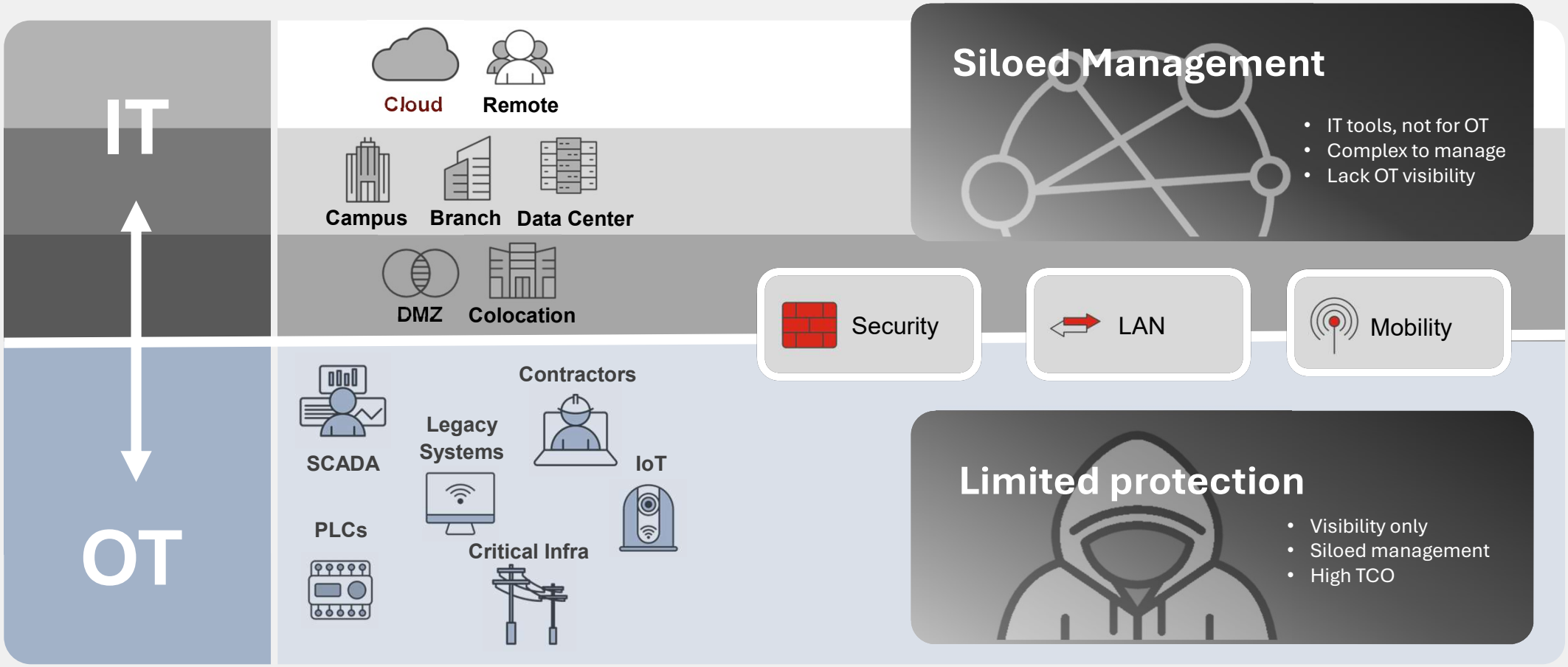
SOC & Incident Response



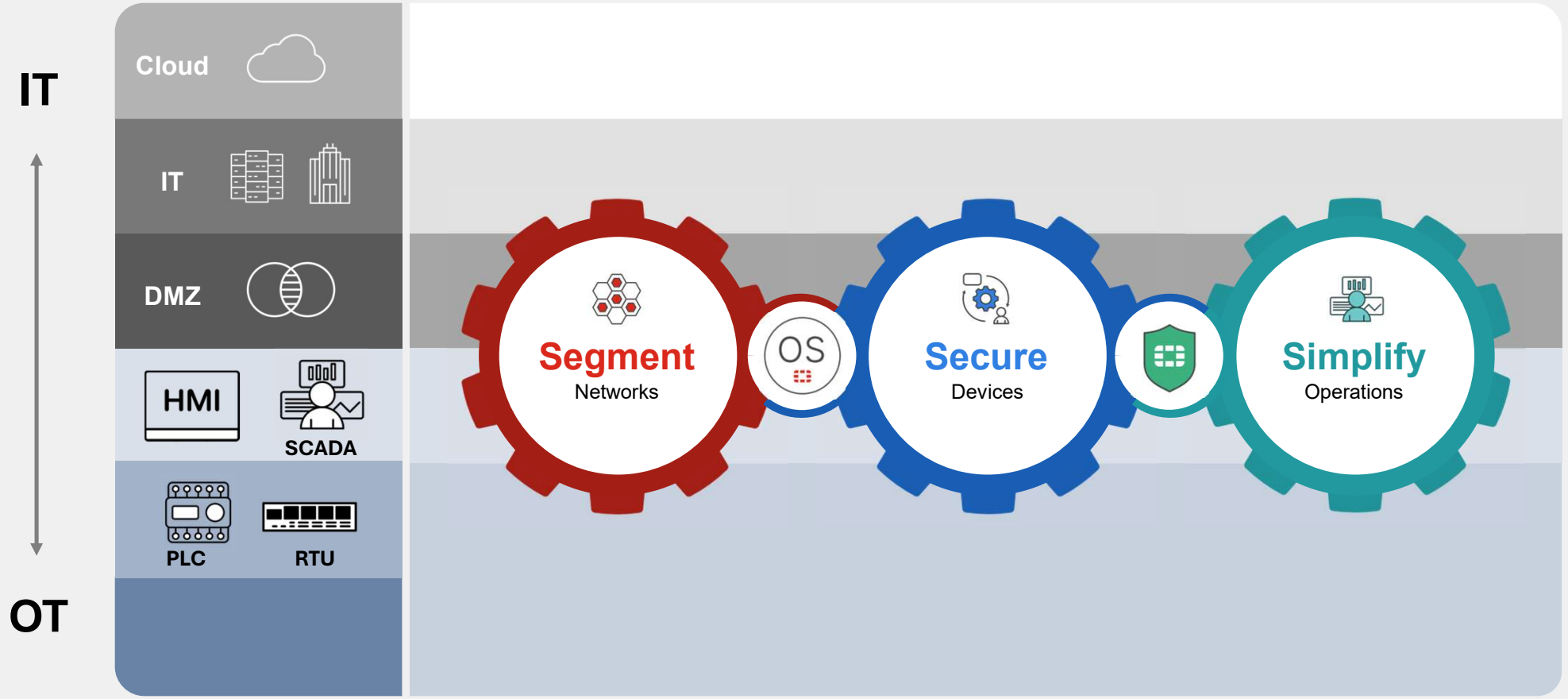
Platform Approach

OT threat intelligence

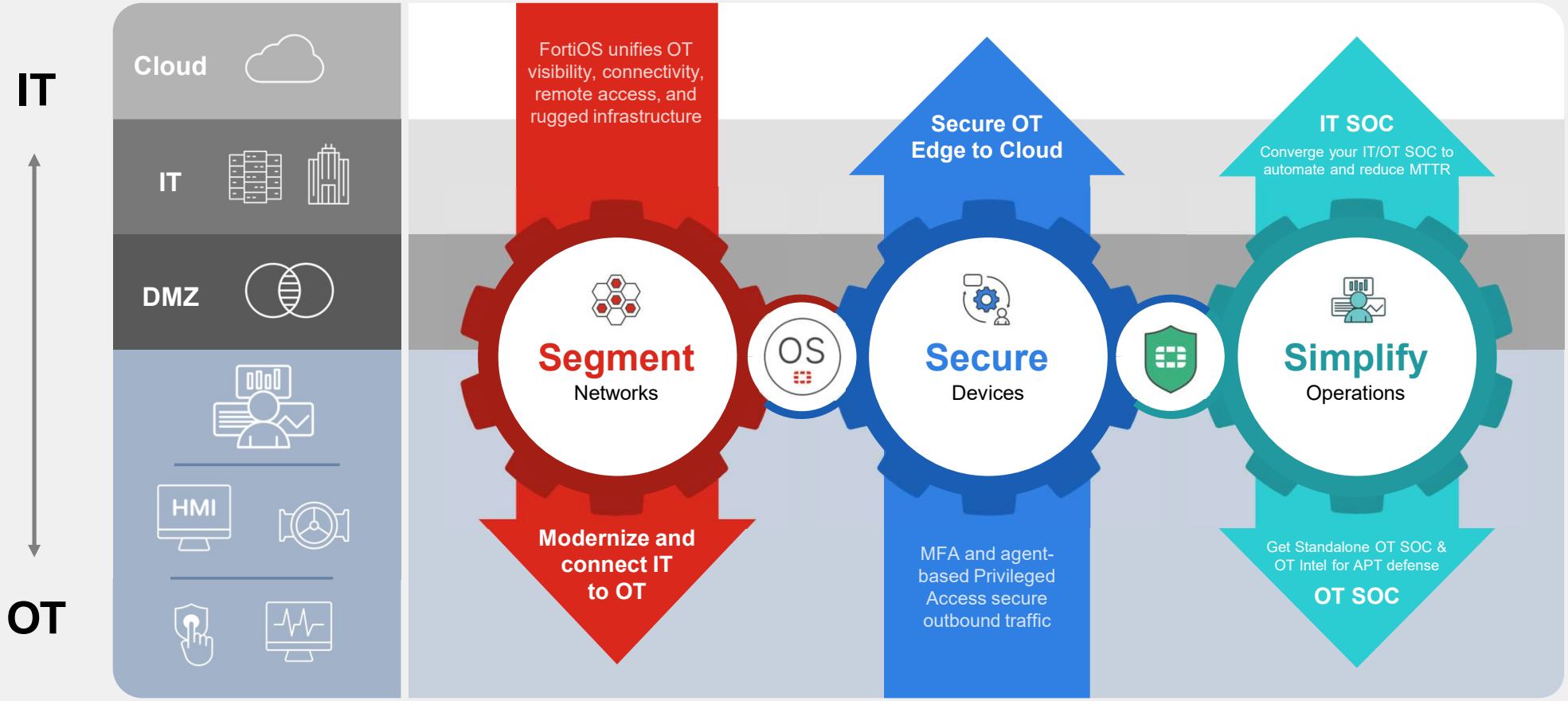
Běžné výzvy při zabezpečení OT



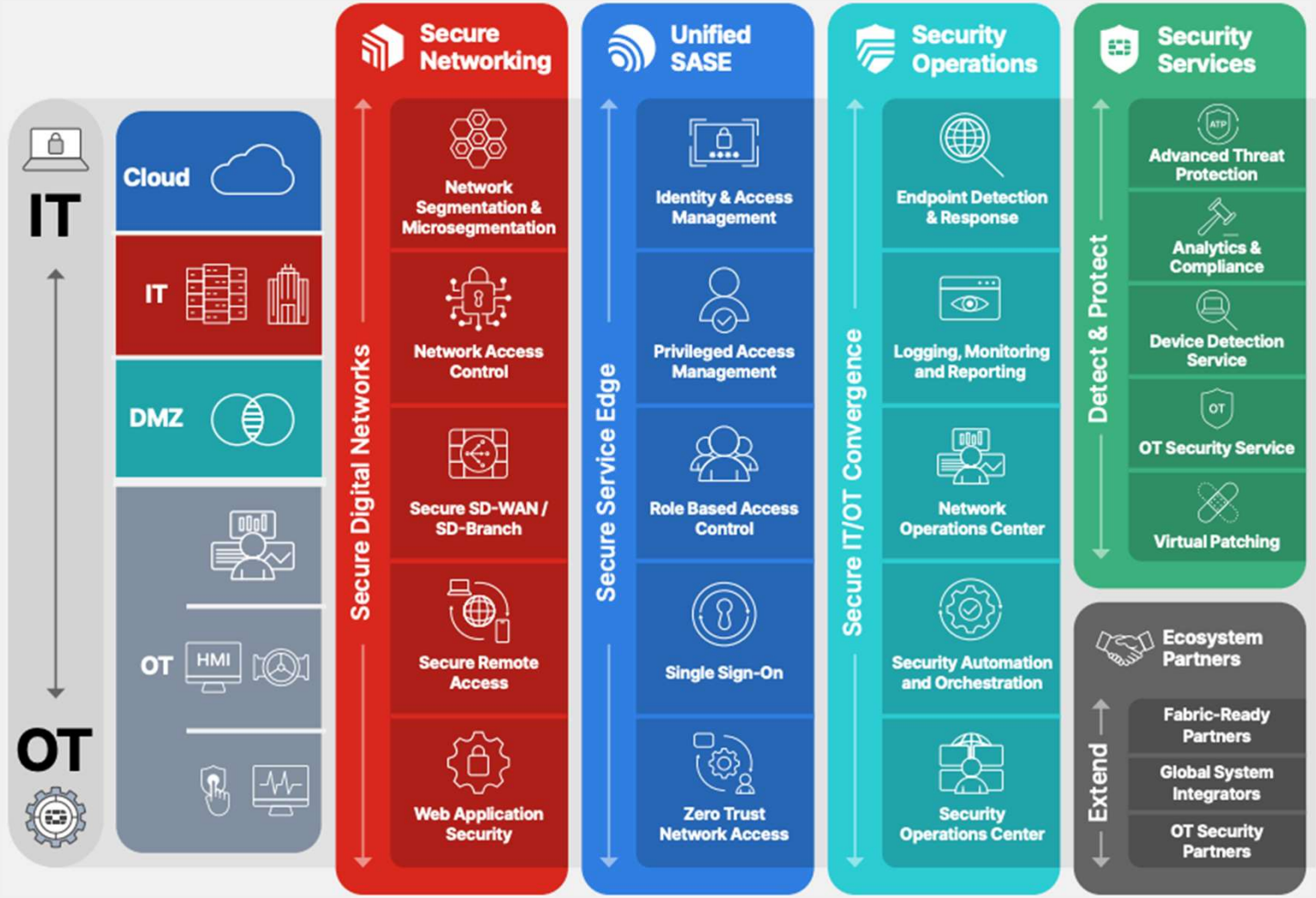
Fortinet OT Security Platform: Komplexní zabezpečení OT



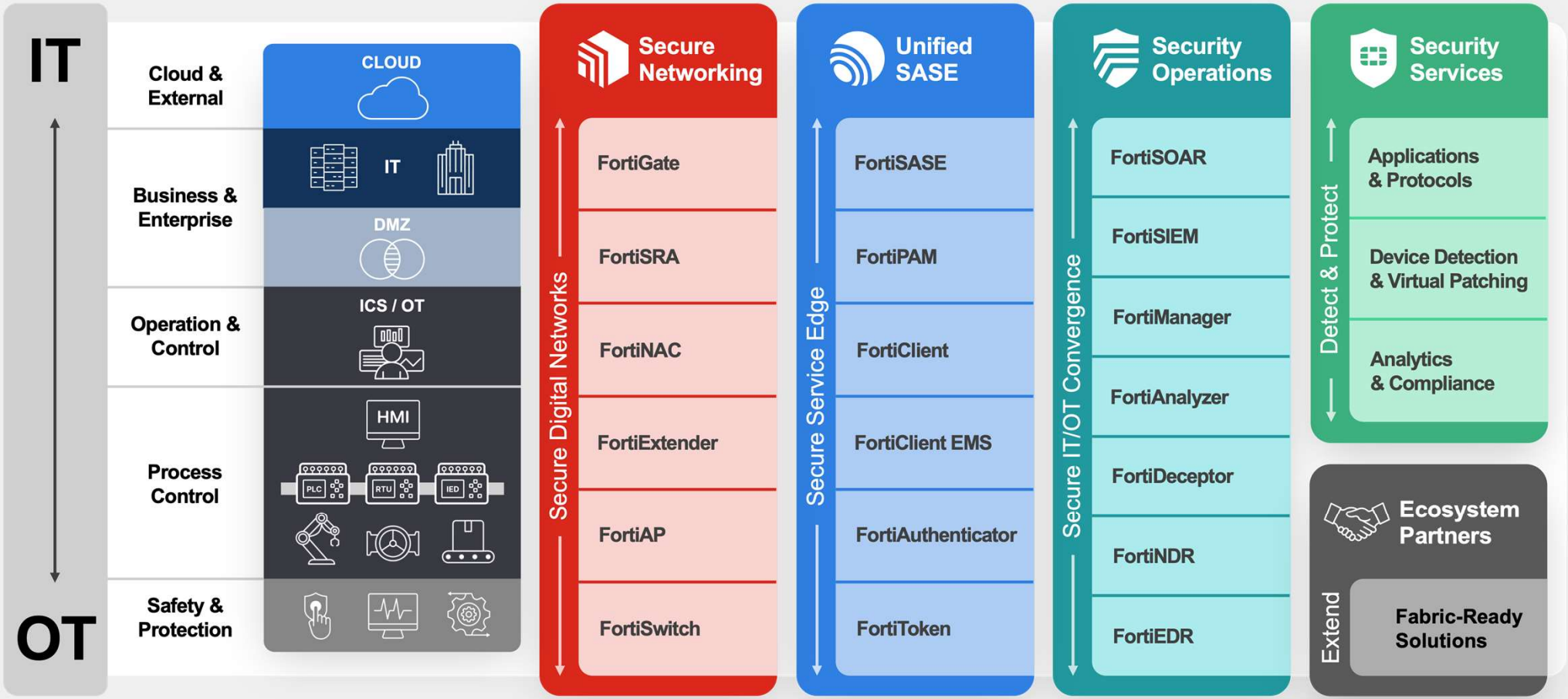
Fortinet OT Security Platform: Komplexní zabezpečení OT



OT Security Platform



OT Security Platform

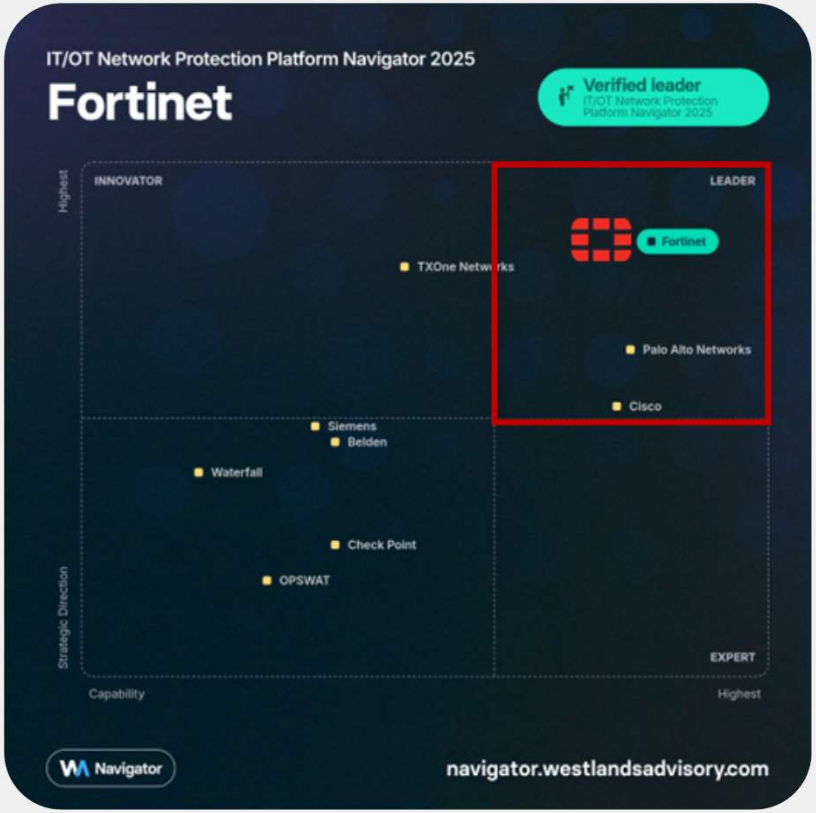


Proč řešit zabezpečení OT sítí pomocí Fortinet Security Fabric?

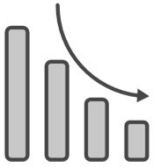
3× lídr v oblasti OT platforem Westlands Advisory IT/OT Cybersecurity Platform Navigator

Významné přednosti: Integrace napříč **Fortinet OT Security Platform** **Inovace** při zabezpečení složitých prostředí

Fortinet je široce uznáván průmyslovými podniky, provozovateli kritické infrastruktury a zainteresovanými stranami v oblasti kybernetické bezpečnosti OT jako přední poskytovatel platforem pro OT bezpečnost.



Fortinet a OT Security

	Komplexní OT platforma	Vhled do OT protokolů	Konvergence mezi OT a IT světem
Customer Benefit			
How Fortinet Delivers	Nejširší OT platforma s integrovanou bezpečnou sítí, principem zero trust a SecOps navržená pro OT.	Nejvíce OT signatur pro ochranu neopravených OT zařízení, unikátní automatizované virtuální záplatování.	Společný FortiOS pro IT a OT umožňující plynulé, efektivní a bezpečné provozování sítí.
Impact			
Proven Results	 **93%** Reduction in threats	 **2x** More OT signatures	 **86%** Reduction in TCO

FortiGuard OT Security Service

+3,500	+1,600	~800	+2,100
Protocol Rules	OT App Detection Rules	IPS Rules	OT Virtual Patch Rules

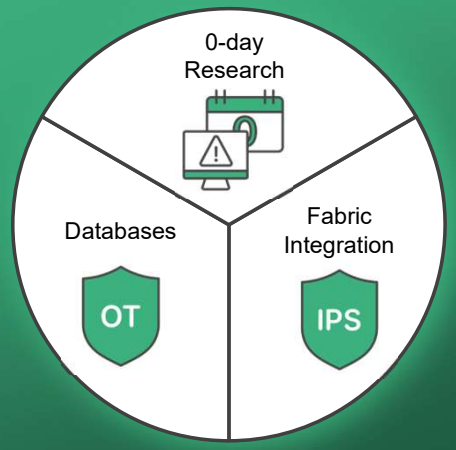
OT Protocols

Allen Bradley DF-1
DNP3
Ether-S-Bus
EtherCAT
EtherNet-IP/CIP
FL-NET
GE EGD
IEC 60870-5-104
IEC 61850
IEC Synchrophasor
KNXnet/IP
LonTalk
Mitsubishi MELSEC
MMS
Modbus RTU
Modbus TCP/IP
OCPP
OPC
OPC UA
Profinet CBA
Profinet IO
Rockwell FactoryTalk
SafetyNET
SECS-II/GEM
SEL Fast Nessage
Schnedier UMAS
Siemens S7
Siemens S7 Plus
Siemens SIMATIC CAMP
TRDP
Triconex TSAA
Triconex TriStation
WITSML

…and many, many more

AI-Powered Security

FortiGuard Labs Threat Intelligence

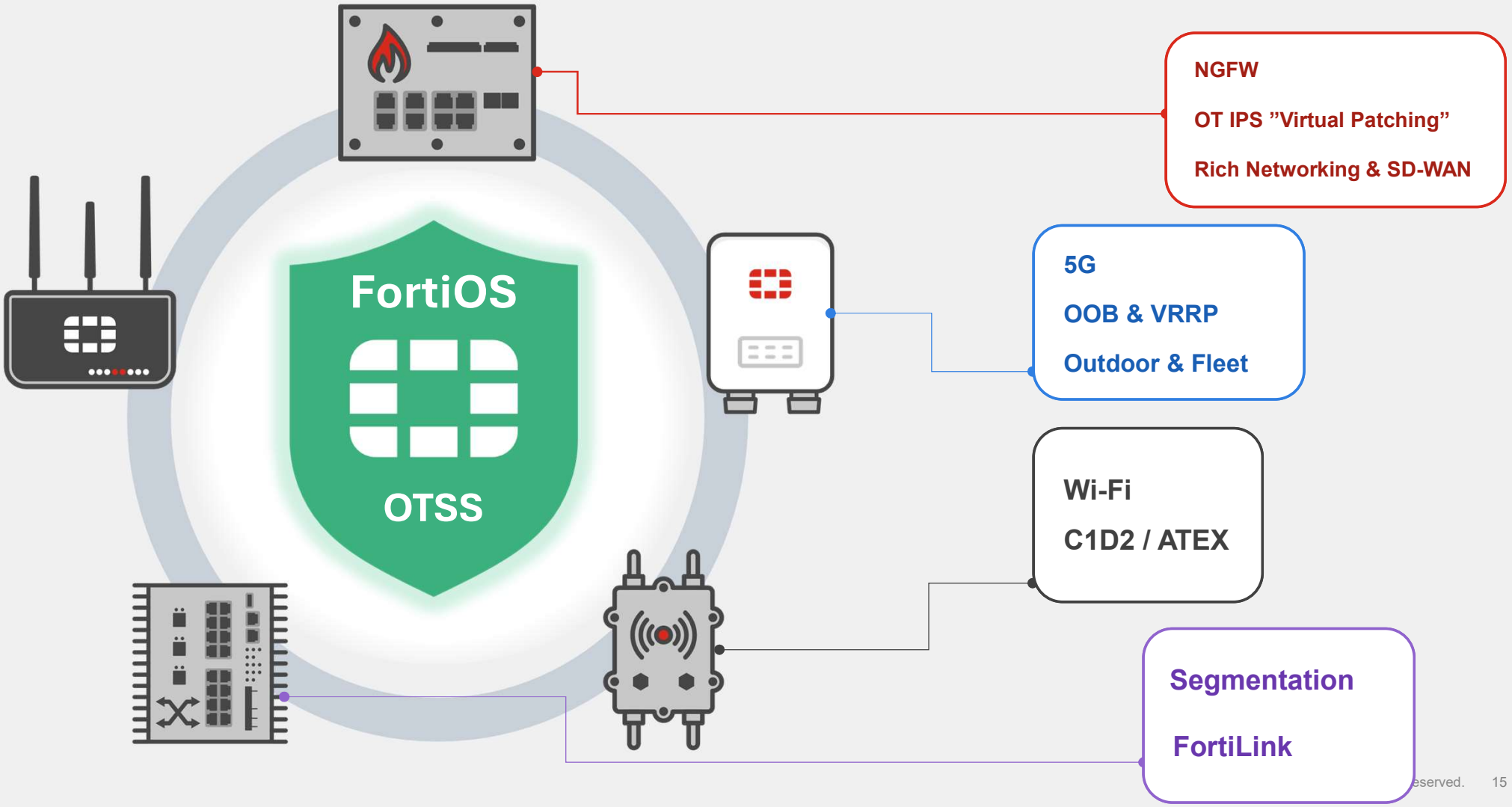


OT Vulnerabilities

ABB
ETIC
Advantech
Fuji
AVEVA
GE
B&R Automation
Iconics
Contec
Inductive Automation
Delta IA
InHand Networks
DUT CCE
KeySight
Eaton
Korenix
Moxa
Ricon
mySCADA
Rockwell
OAS
Schneider
Omron
SEL
Osprey
Siemens
Pepperl+Fuchs
Sierra Wireless
PnP SCADA
WECON
PTC
Wibu Systems

Integrations | OS | NGFW | SD-WAN | NDR | Deception | Sandbox | NAC

Plně odolné pro jakékoli nasazení



FortiGate Rugged Series

SP4 SP5

FortiGate Rugged 70F Series

FortiGate Rugged 60F Series

FortiGate Rugged 70G-5G Dual

FortiGate Rugged 50G-5G

Rugged Design

Wide Input Voltage

5G

5G Variants

Digital I/O

IEC 61850-3
IEEE 1613

EN 50155

Industrial Certifications

OS

FortiOS

SP5

ASIC

Rugged Appliance

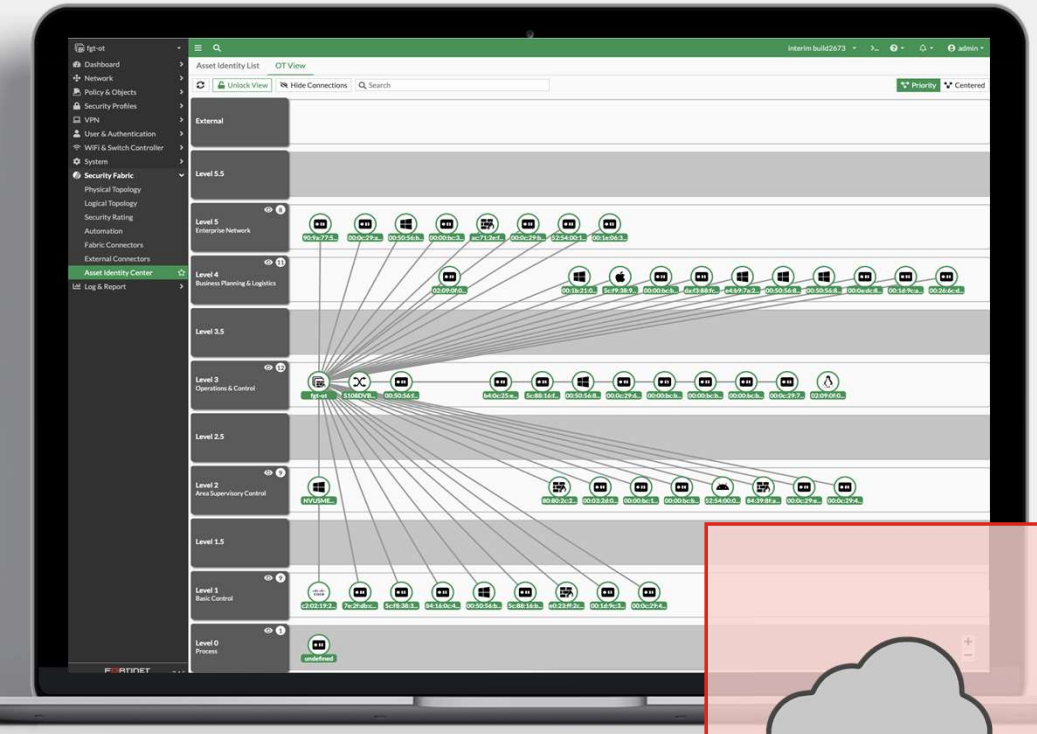
Standard Appliance

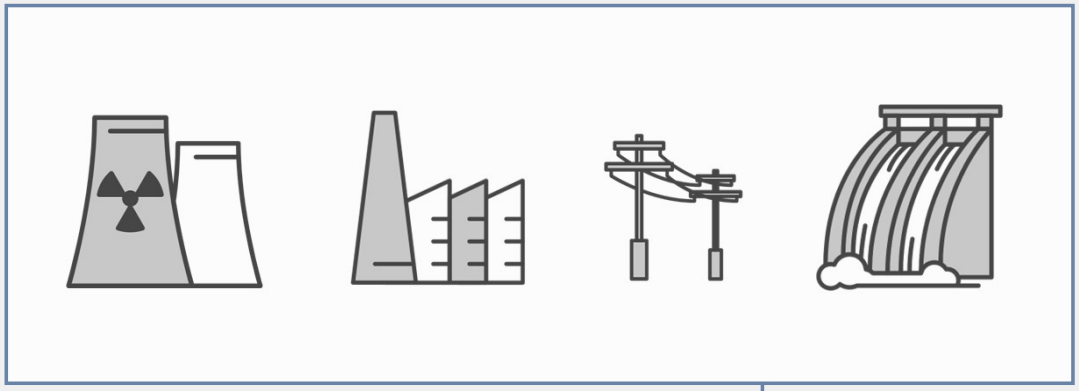
Virtual Machine

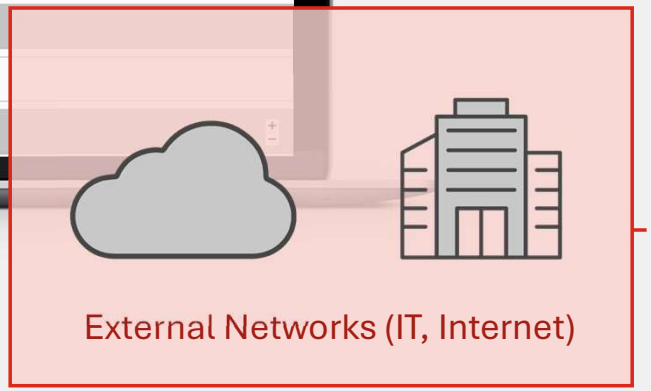
Container Software

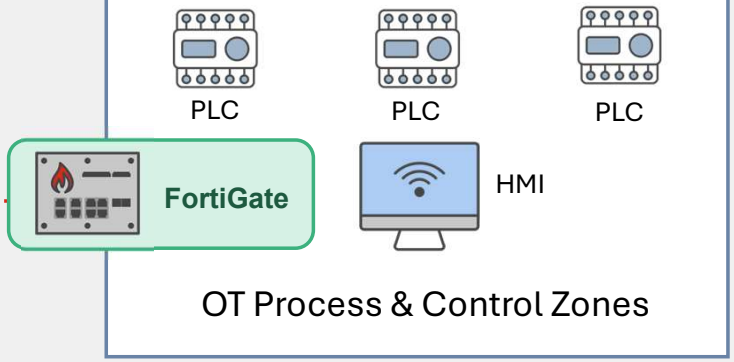
Virtual Patching: Ochrana starších OT zařízení před zneužitím

S aktivovanou funkcí FortiGate automaticky nasazuje OT IPS pravidla k ochraně zranitelných starších zařízení (PLC, HMI atd.) vystavených externím sítím.









Není to jen o NGFW pro OT

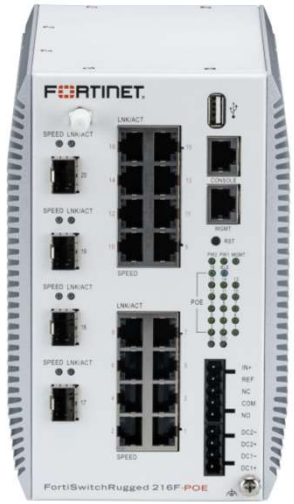
Industrial Switching

FortiLink

BLE

FortiSwitch Rugged 108F

FortiSwitch Rugged 112F-PoE



FortiSwitch Rugged 216F-PoE

FortiSwitch Rugged 424F-PoE

Rugged Design
DIN-rail, Rackmount

802.3 PoE

Redundancy
MRP/PRP/HSR

Segmentace OT sítí pomocí FortiLink

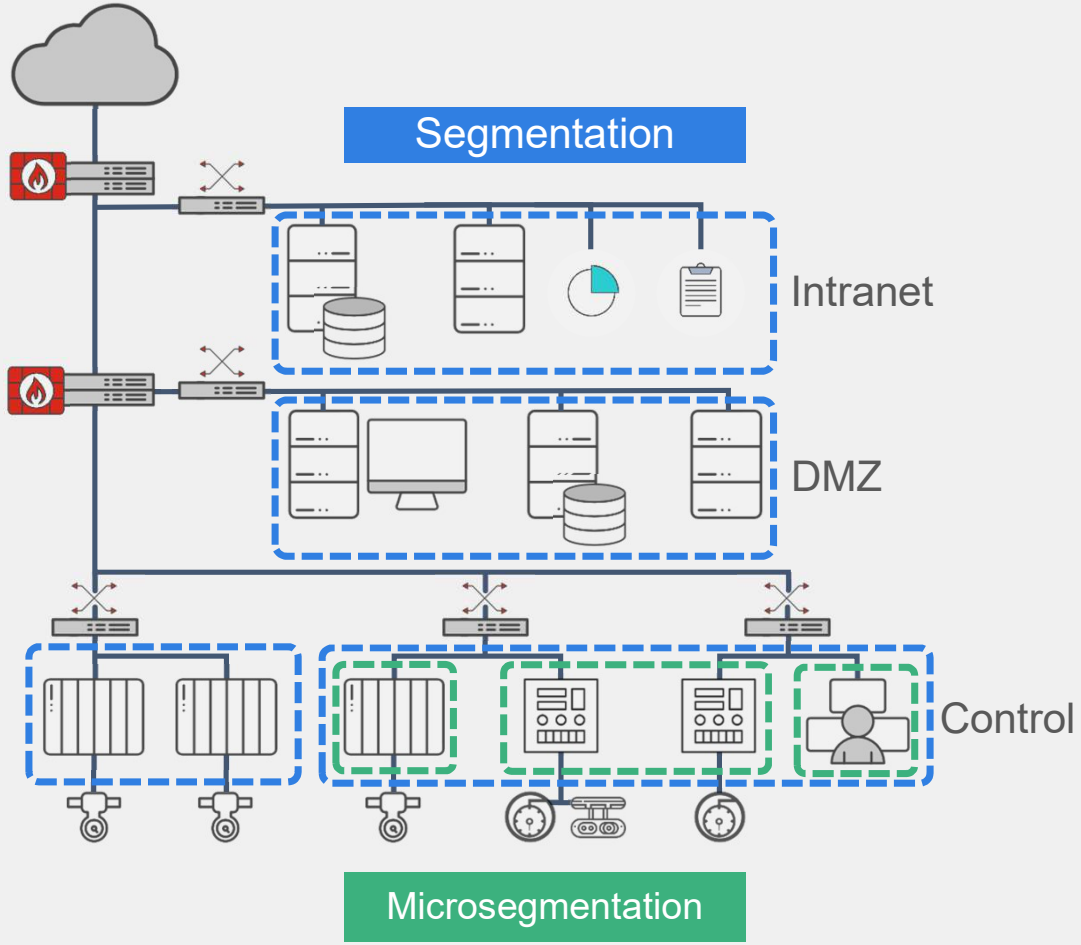
Rozdělení OT systémů do zón

Řízení OT provozu

Implementuje klíčové OT koncepty

Lepší bezpčenost než s klasickou segmentací

Integruje NGFW a LAN



FortiExtender Rugged

Průmyslové 5G routery & Wireless WAN

VXLAN Extension

BLE

Digital I/O Port

5G

Wireless WAN & P5G

Outdoor & Fleet Support

IEC 61850-3
IEEE 1613

EN 50155

Industrial Certifications

Wi-Fi 6

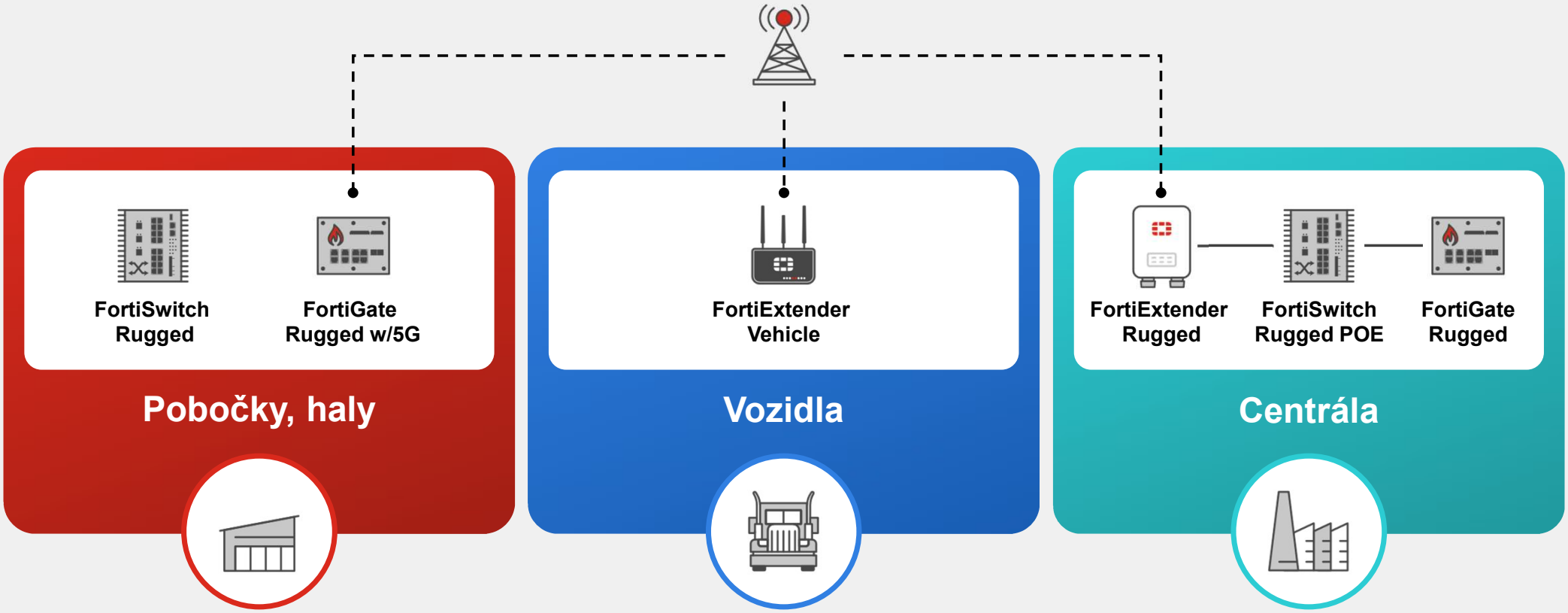
IP64 & IP67 Form Factors

eSIM, Dual Physical SIM & Dual Radio support

VRRP & Out of Band Management

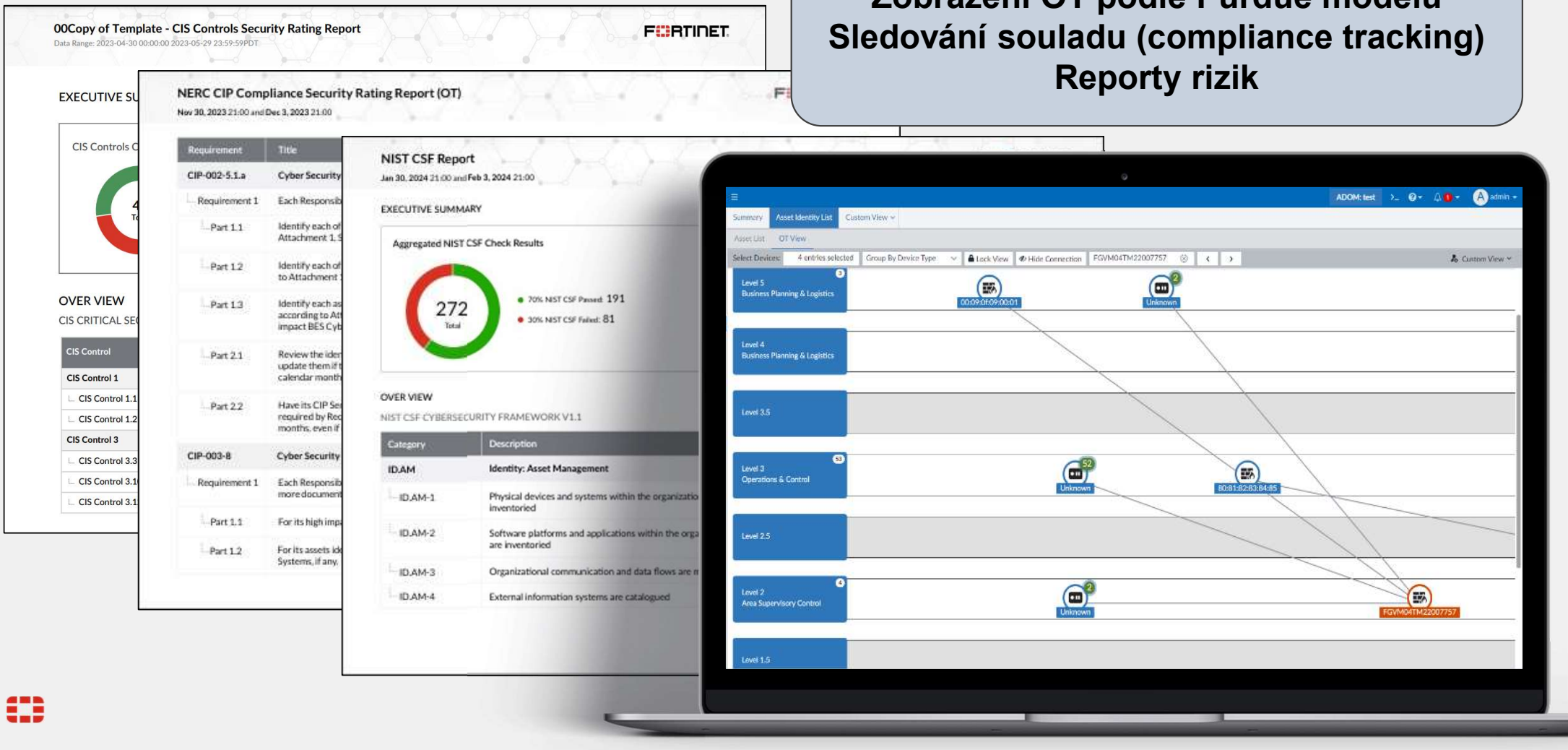
Vylepšená segmentace a bezpečné připojení

Umožnit bezpečnou transformaci napříč celou organizací



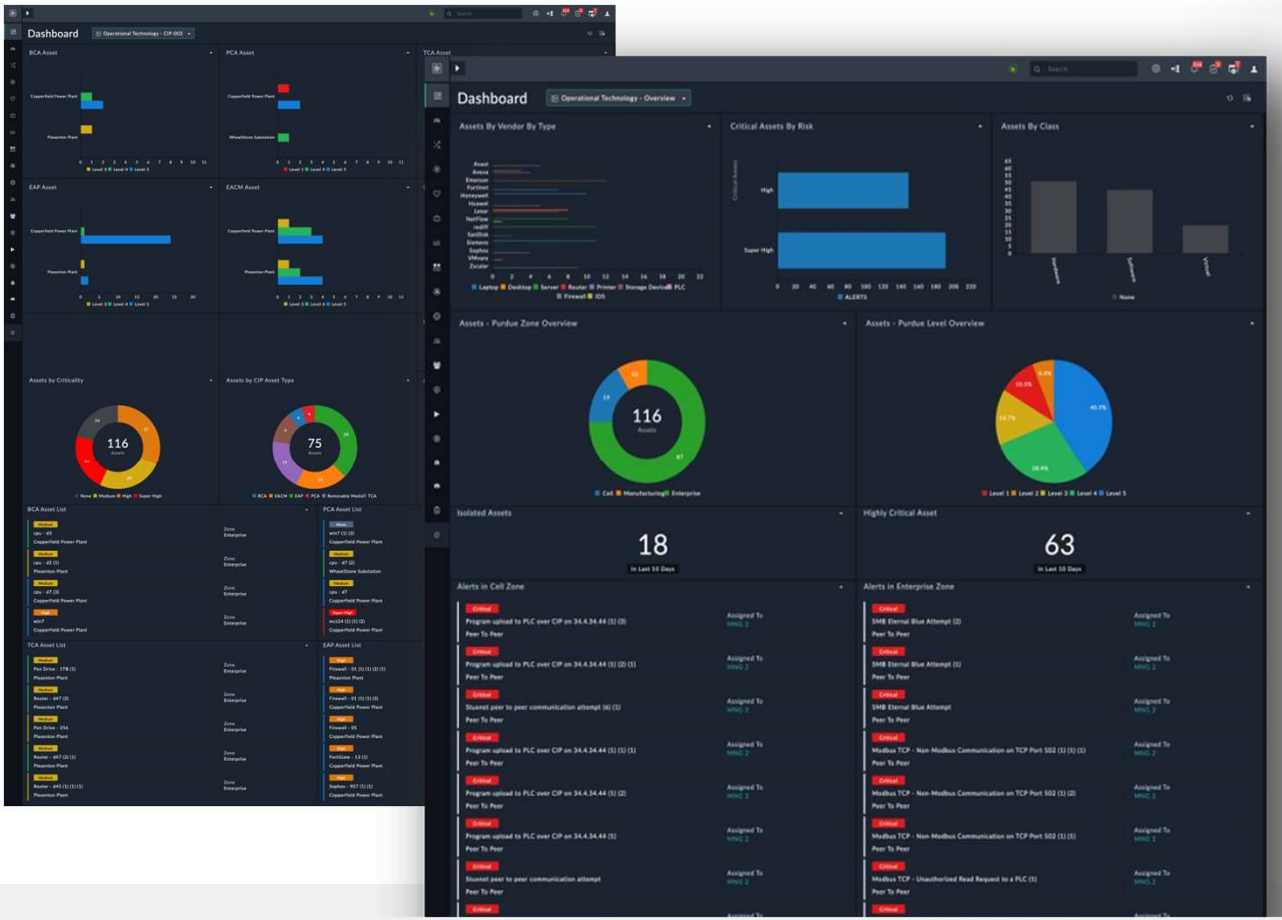
FortiAnalyzer: Dashboard a reporty zaměřené na OT

Zobrazení OT podle Purdue modelu
Sledování souladu (compliance tracking)
Reporty rizik

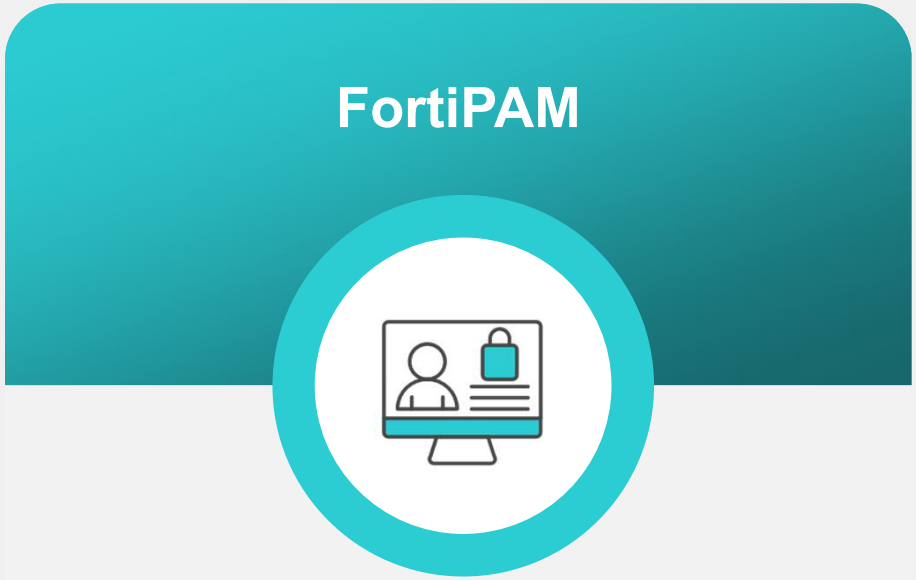


FortiSOAR OT/IT

- **FortiSOAR přidal OT/IT přehledové dashboardy pro vizualizaci aktiv a upozornění napříč úrovněmi Purdue. Například:**
- Metriky založené na **Purdue modelu** a rozložení aktiv
- Metriky **důležitých zranitelností**
- Metriky **OT rizik**
- Metriky **běžných technik útoků**
- Metriky **nejvýznamnějších upozornění**
- Metriky **MTTD/MTTR** (Mean Time to Detect / Mean Time to Respond)



Bezpečný vzdálený přístup do OT sítí



Control Remote Access

- Zajistit přístup pouze oprávněným uživatelům podle principu nejmenších práv

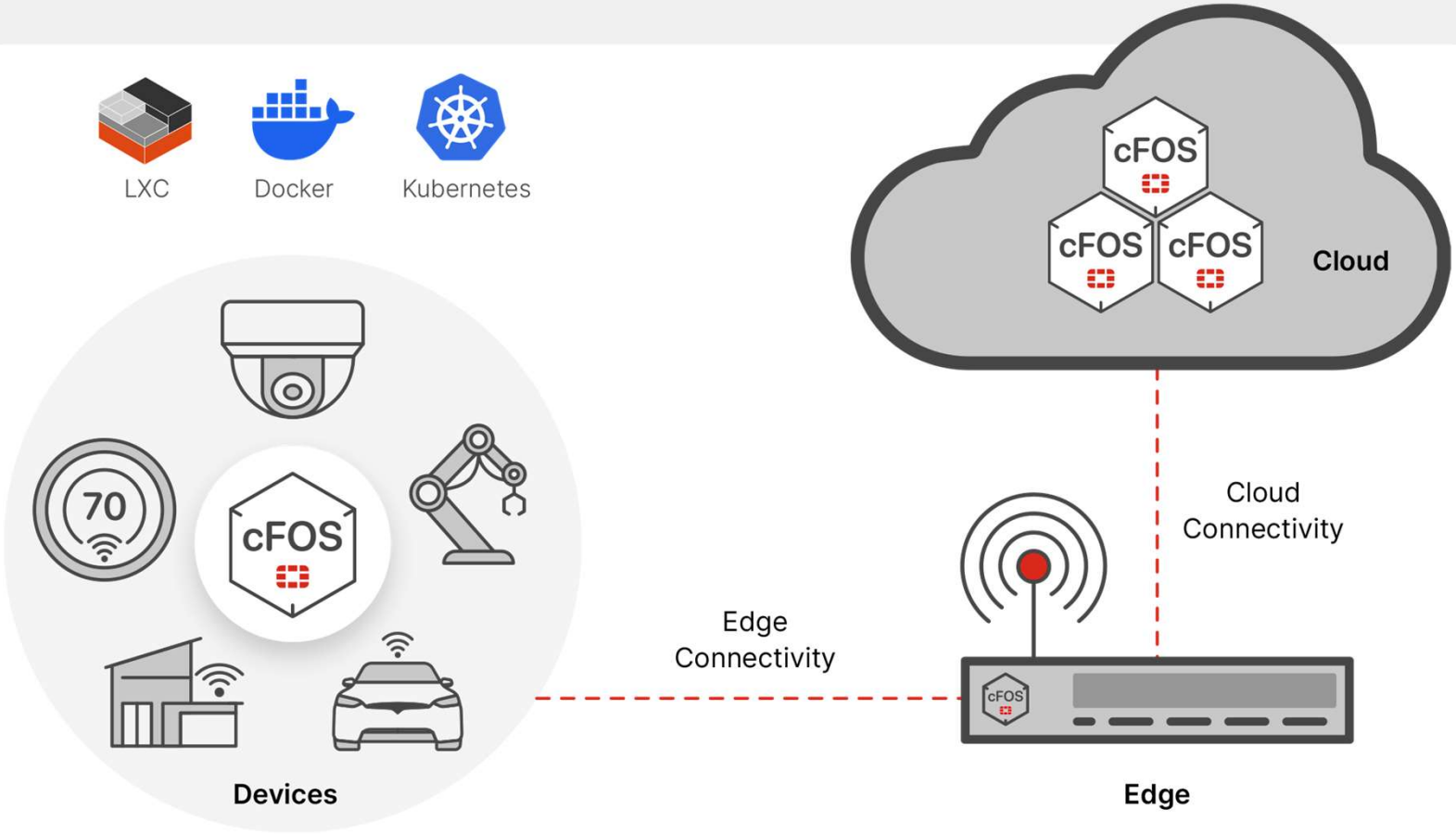
Manage Secrets

- Bezpečně ukládat přihlašovací údaje a automaticky vytvářet a měnit hesla

Monitor Sessions

- Audit po ukončení relace a možnost okamžitě ukončit relace v reálném čase

Container FortiOS



Partnerství v OT segmentu

FORTINET FABRIC-READY

OT TECHNOLOGY PARTNERS

Technology Alliance Partners

NOZOMI NETWORKS
ARMIS
DRAGOS
CLAROTY
PENGUIN SOLUTIONS
HIGHWAY 9 NETWORKS
servicenow
RUGGEDCOM A Siemens Business
SEL SCHWEITZER ENGINEERING LABORATORIES
rubrik
INDUSTRIAL DEFENDER
WELOTEC
OWL Cyber Defense
Radiflow
RAD
DARKTRACE
tenable

Control Vendors

GE
ABB
Johnson Controls
EMERSON
Rockwell Automation
Schneider Electric
YOKOGAWA
Honeywell
SIEMENS
SEL SCHWEITZER ENGINEERING LABORATORIES
Weidmüller

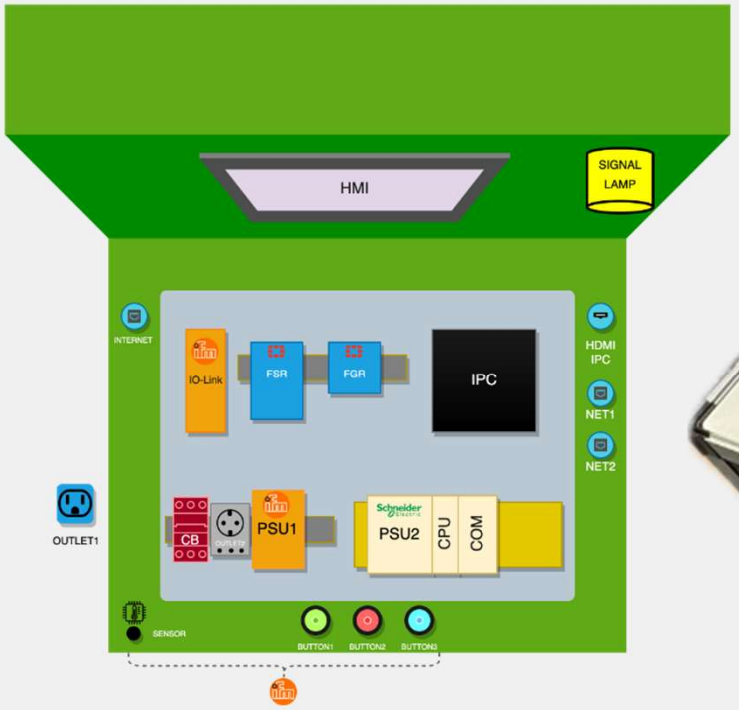
GSI/Service Provider/Channel

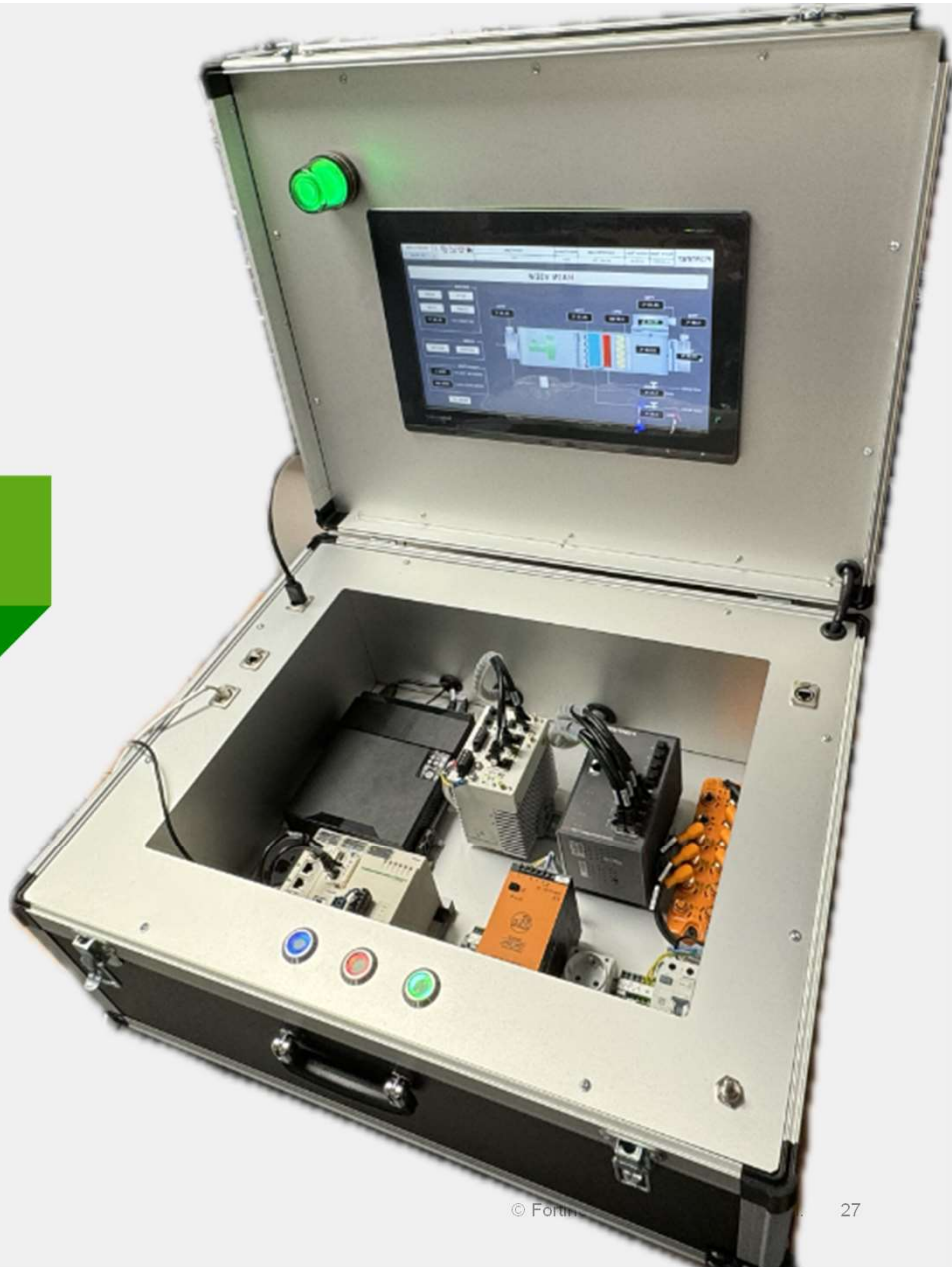
Hewlett Packard Enterprise
Atos
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
REVISYS
Orange Cyberdefense
NTT
OPTIV
T-Systems
accenture
Cognizant
HCL
wipro
IBM
World Wide Technology, Inc.
RED TRIDENT INC
Eleven Paths A Telefónica COMPANY

Pozvánka na náš stánek

OT demo case

- Simulace řízení vytápění a chlazení budovy
- Demonstrace práce s incidenty k OT prostředí






FORTINET