



Protecting Operational Technology using the Fortinet Security Fabric

Juraj Rumanovský, Systems Engineer

Safe and Secure OT Solutions for Manufacturing



Safe and Secure OT Solutions for Energy & Utilities



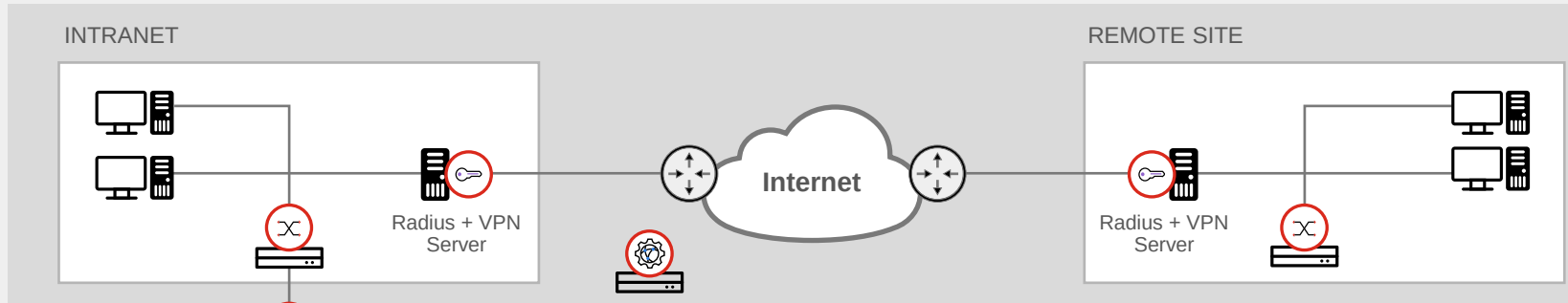


Safe and Secure OT Solutions Transportation Systems

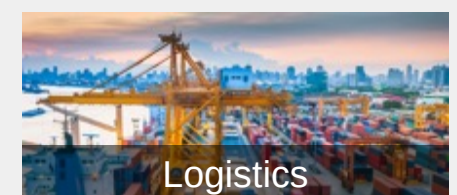
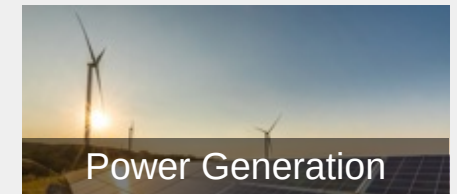
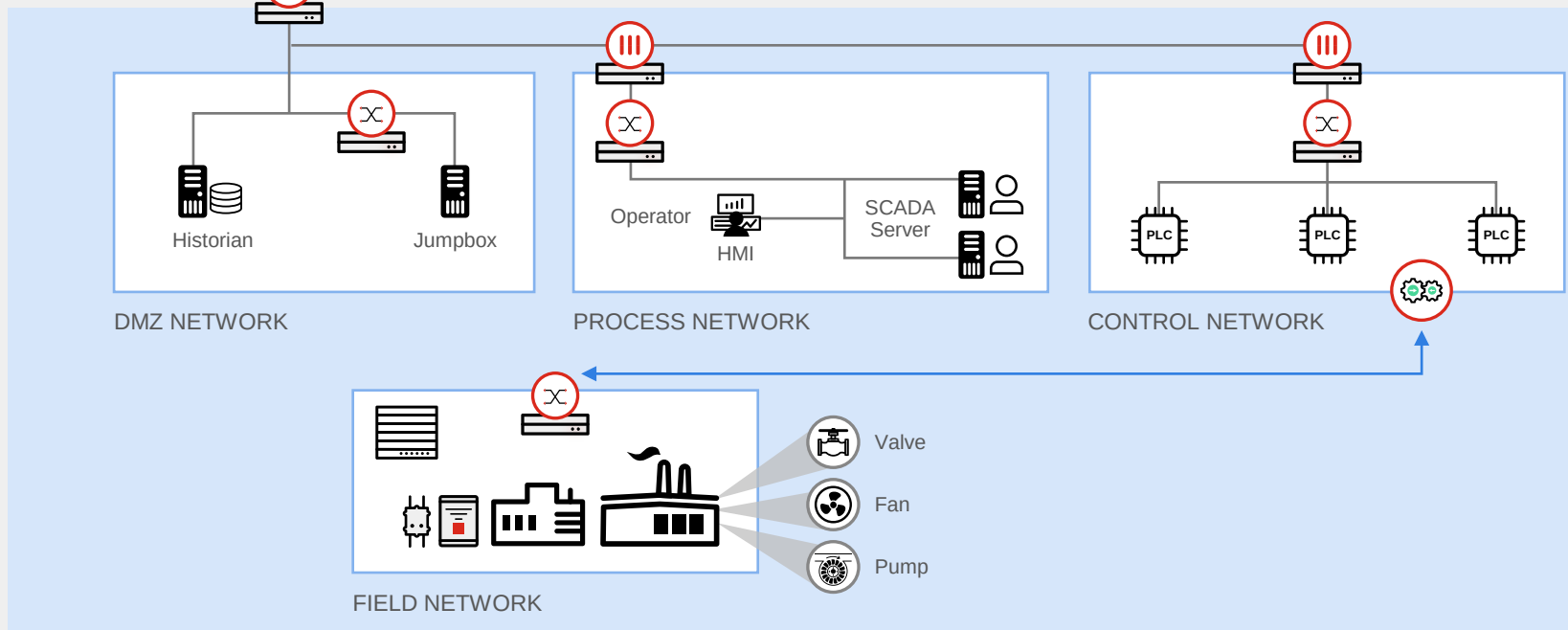


What and where are IT and OT networks?

Information
Technology (IT)



Operational
Technology (OT)



Securing Operational Technology Challenges



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



The attack surface for cyber-physical assets is expanding as a dependence on air-gap protection diminishes with Digital Transformation initiatives driving IT-OT network convergence.



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



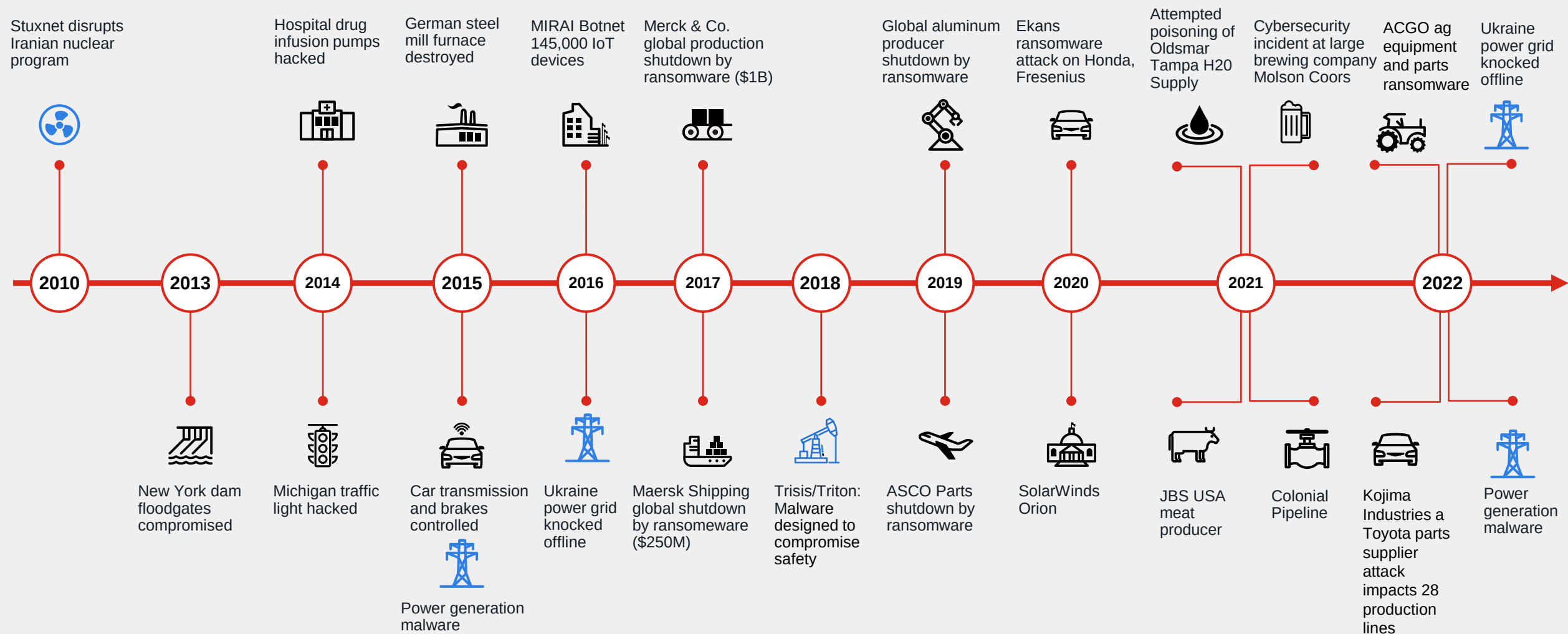
Remote access requirements for third-parties and employees causing additional risks.



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



OT Risk Is Proportional to OT Connectivity

Yet inversely proportional to the integration of IT/OT security management

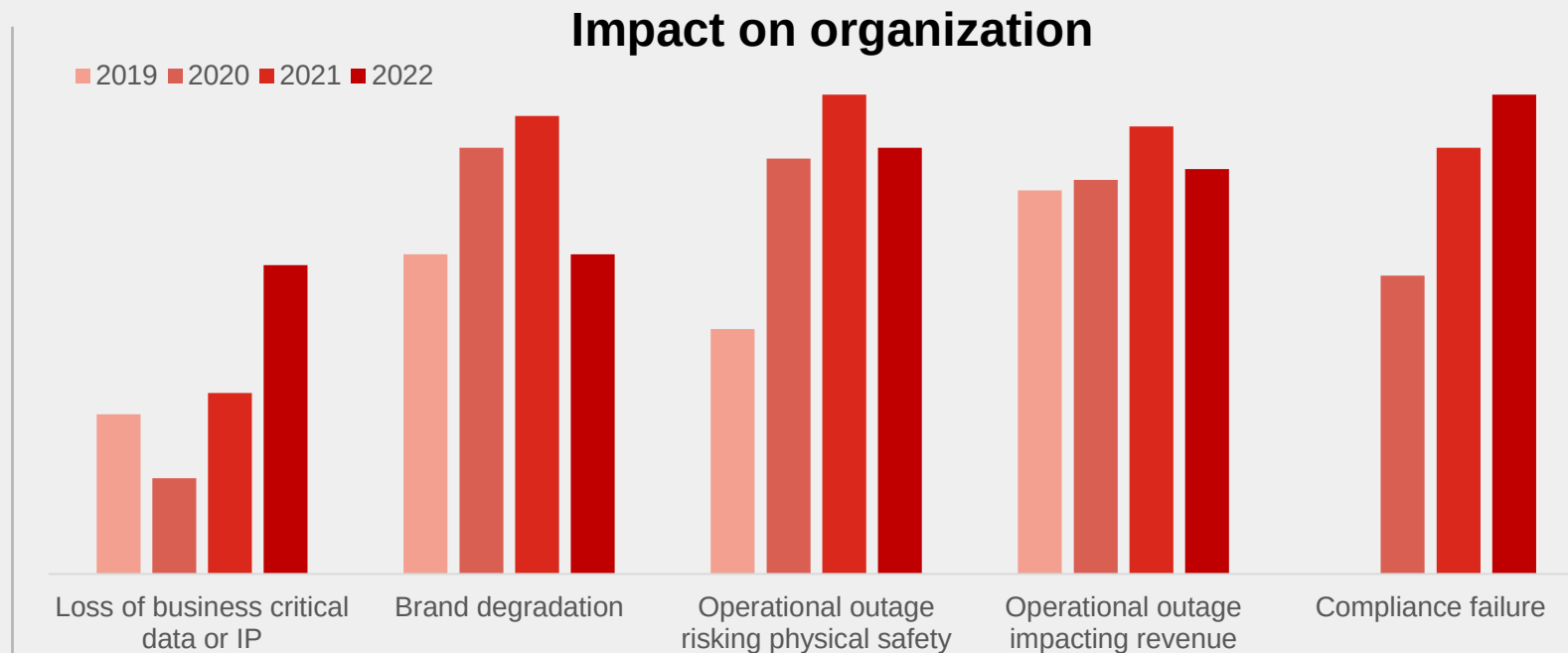


9 out of 10

OT organizations experienced at least one intrusion in the past year and **78% had 3 or more intrusions**, which is up from the results in 2021.

Top-tier organizations are...

...likely to have centralized visibility, use **network access control** and have **security tracking and reporting** in place.



32% more likely to have their SOC monitor and track OT security.

Data is from Fortinet's **2022 State of Operational Technology and Cybersecurity Report**



Source: [Fortinet's 2022 State of Operational Technology and Cybersecurity Report](#)





STAMFORD, Conn., July 21, 2021

Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Organizations Can Reduce Risk by Implementing a Security Control Framework



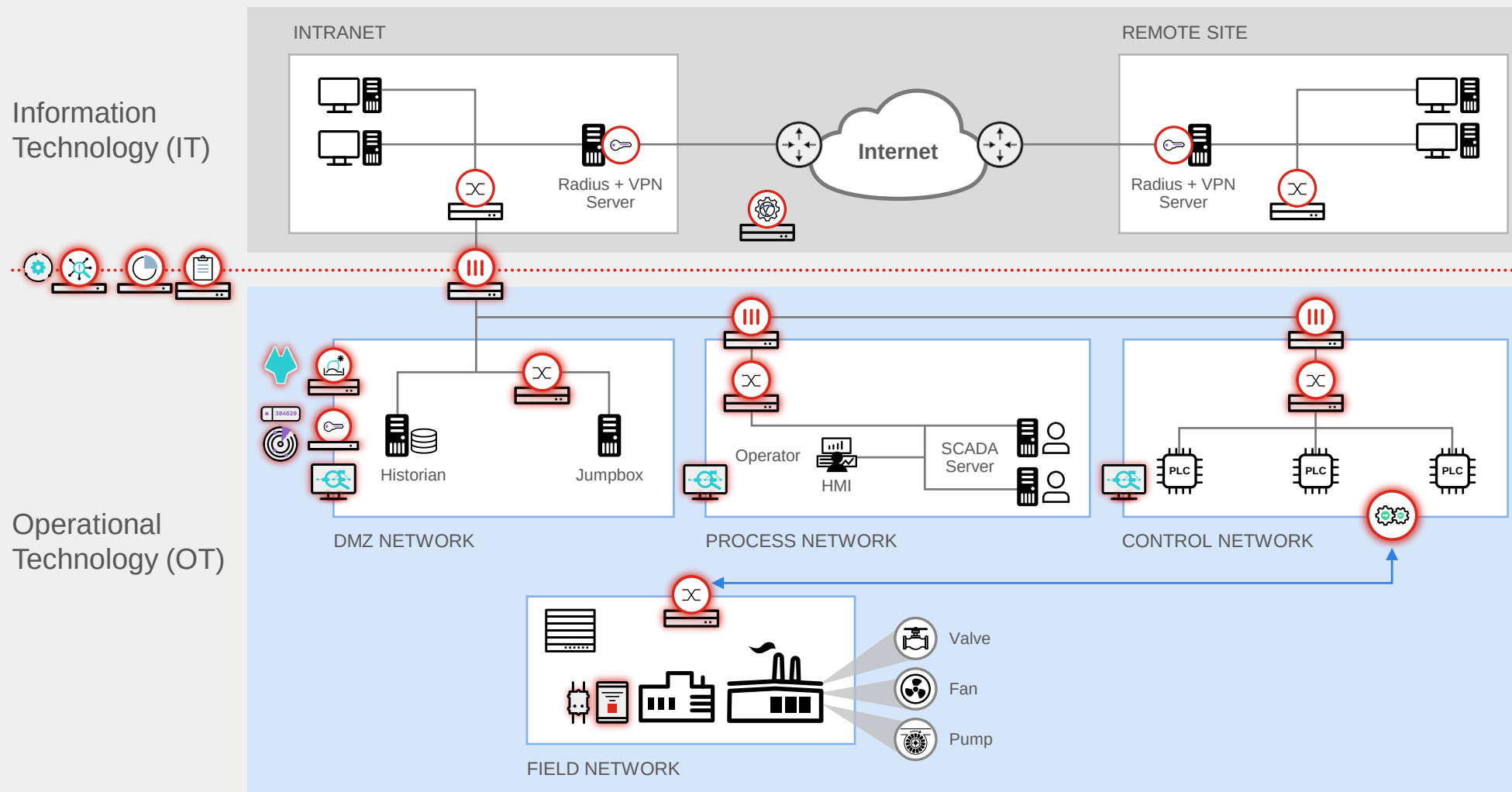


What controls are essential to secure OT environments?

Zones and Conduits	Segmentation protects OT from mistakes and bad actors.	Are your OT assets segmented from the IT side? How flat is your OT network in reality?
Secure Remote Connectivity	Enable secure access for employees and third-parties who connect to your OT environment.	Who requires access to your OT network? How do you enable that securely today?
Deep OT Visibility	You can't protect what you can't see.	How well do you understand what's in your industrial control system?
Role-based Access Control	Limit access to only those who need it.	Do you know who can access what in your OT environment? When was the last time you checked?
Endpoint Security	Apply endpoint security protection to the servers at and near the secure perimeter.	Do you have older servers in your OT environment that are no longer supported?
NOC / SOC	Synergistic benefits of managing everything in one place.	How much money could you save by managing the network security of your OT and IT in the same place?
Advanced Persistent Threat	Advanced Persistent Threats (APT) require advanced solutions.	Have you considered leveraging sandboxing, deception, or AI to up-level your OT security strategy?



Addressing Critical Controls Integrating OT and IT



Zones and Conduits

Secure Remote Connectivity

Deep OT Visibility

Role-based Access Control

Endpoint Security

NOC / SOC

Advanced Persistent Threat

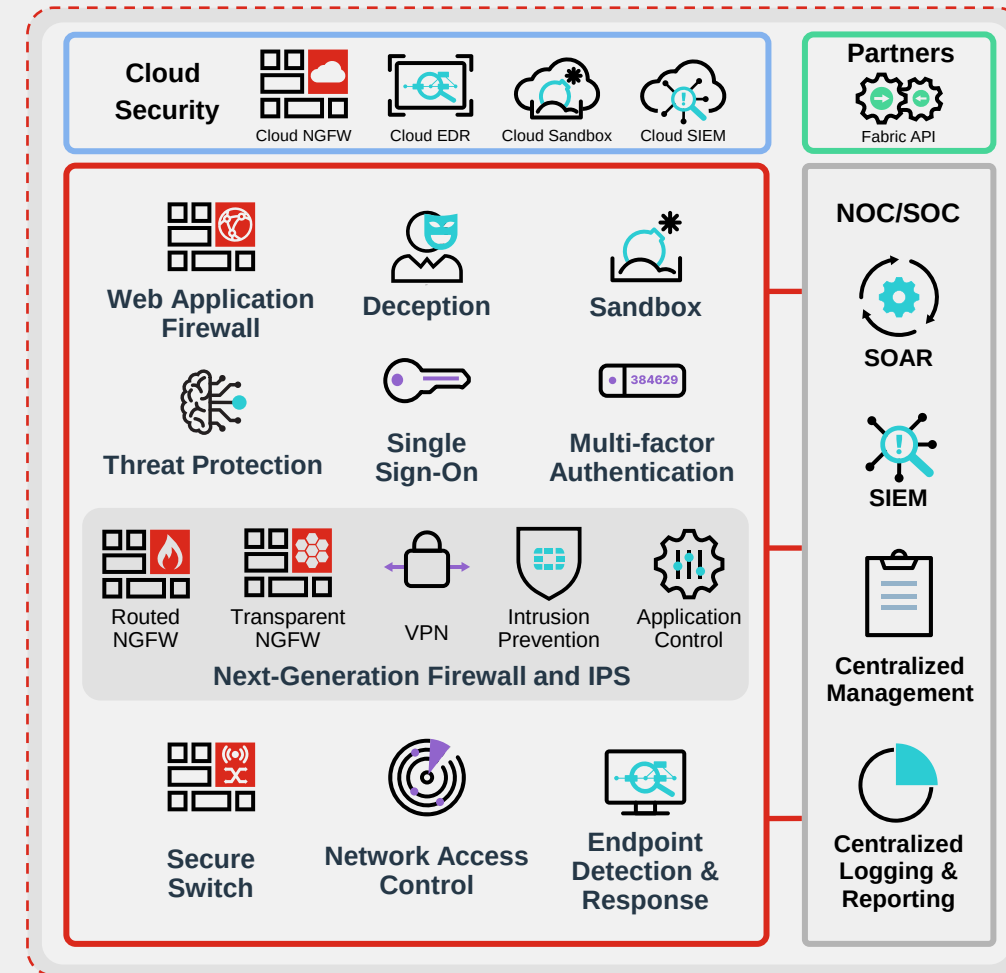
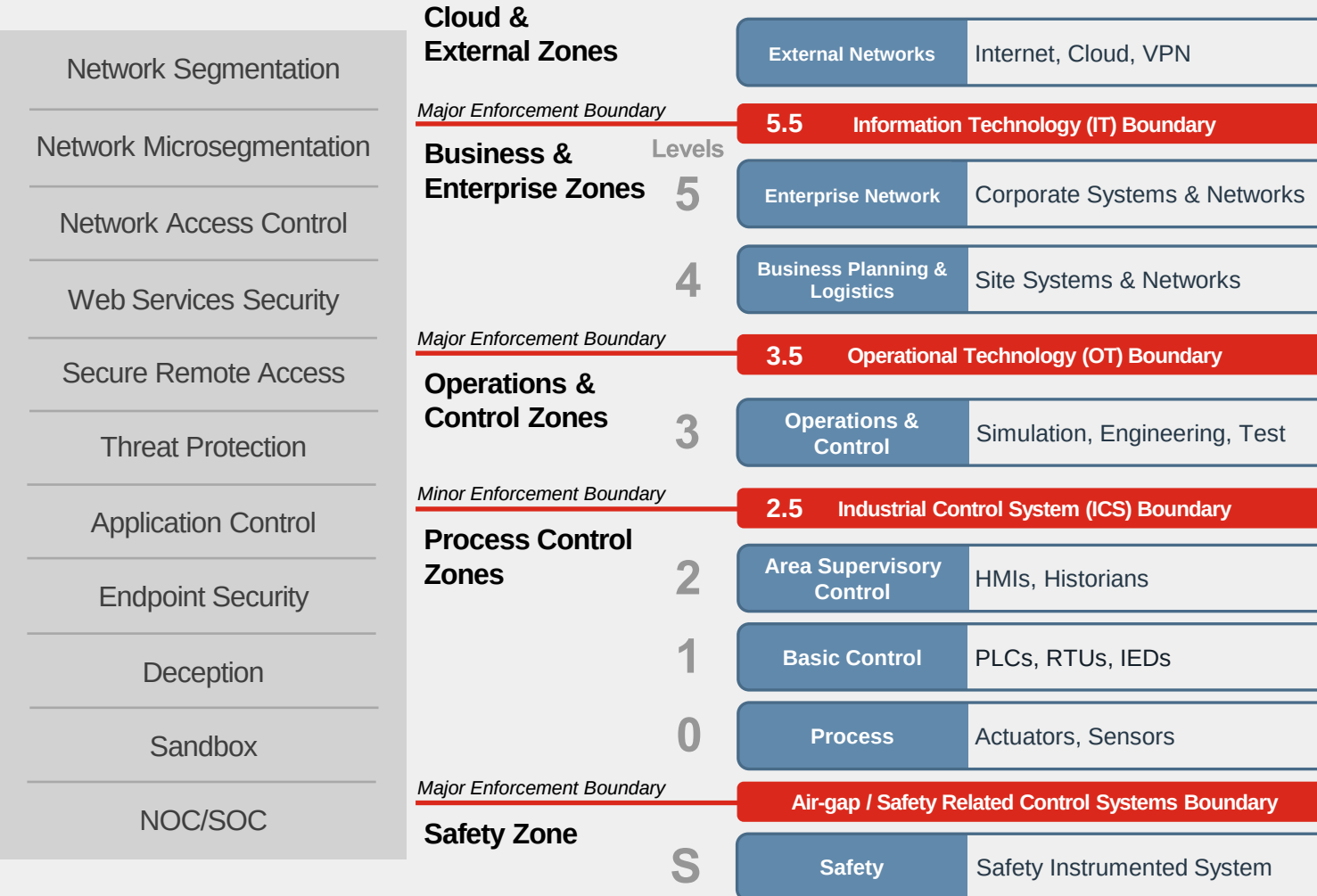


Securing Operational Technology

with the Fortinet Security Fabric



Fortinet Security Fabric



Boundary: Demilitarized Zone (DMZ), Security Conduit

Zones: Security Zones

IPS: Intrusion Prevention System

SIEM: Security Information and Event Management

SOAR: Security Orchestration, Automation and Response



Fortinet Security Fabric and Compliance

Single pane of glass, integrated across multiple products

NIS D Pillars map to NIST CSF, CIS Top 20

Identify (& Visibility) Critical Assets and System



SIEM



NAC



NGFW

Secure Conditional Access to Networks & Assets



NAC



MFA



Client



Tokens

Segmentation, Protection & Response



SOAR



EDR



Switch



NGFW



WIFI



Extender

Events, Alerts and Incident Detection



Analyzer



Sandbox



SIEM



Deception

Risk Management – Proactive Controls



Analyzer



Single Pane Management



Threat Intelligence



Interoperability



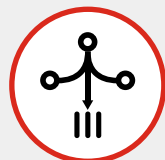
Fortinet Solution Offering for ICS/OT

FortiGate, FortiSwitch, FortiAP Rugged



Ruggedized Design

Fan-less and use of robust components ensure reliable operation in harsh industrial environments.



Consolidated Security Architecture

FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products.



Ease of Management

Allows rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

FortiGate Rugged Series



FGR-60F 3G/4G

SPU SoC Powered, high performance security and VPN gateway



FGR-60F

SPU SoC Powered, high performance security and VPN gateway



FGR-35D

Security appliance with IP67 rating for outdoor environment



FGR-30D

Ruggedized compact security appliance with DIN mounting kit

FortiGate Features

- Security (IPS, FW, OT traffic monitor)
- Encryption (GRE, VXLAN, IPSEC)
- Connectivity (Proxy, VLANs, IPv6.)
- Advance features (SD-WAN)
- Central authentication (LDAP, RADIUS, etc.)
- DLP
- Wi-Fi
- Antivirus
- DNS Filter
- Web Filtering
- IPSEC VPN
- SSL VPN – Client/Clientless
- SSL Inspection
- Packet capture triggered by IPS
- Virtual Domains (VDOM)
- Transparent or Proxy (Man in the middle)

FortiSwitch, FortiAP Rugged Series



FSR-112D-POE and FSR-124D

Fan-less passive cooling with DIN-rail or wall-mountable. Power over Ethernet capable including PoE+. Redundant power input terminals. Mean time between failure greater than 25 years.



FortiAP Rugged 234F

Internal Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified



FortiAP Rugged 432F

External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified



Fortinet's Specialized OT Solutions and Teams

Specialized Offerings



FortiGate Rugged 60F



FortiSwitch Rugged



FortiAP IP-rated

Industrial-grade firewalls, switches and APs

Most deployed IT/OT next-gen firewall worldwide

OT-specific SIEM, EDR, Sandbox, and Deception capabilities

Specialized Threat Information



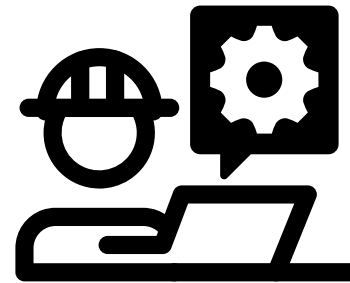
DPI for 70+ OT protocols

Up to payload level visibility and control

Vulnerability shielding for OT assets

More IPS signatures than any other cybersecurity vendor

Specialized Talent



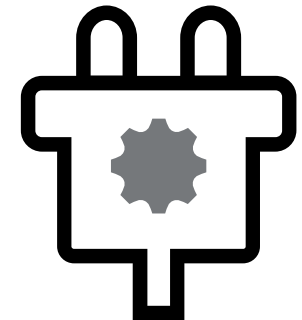
Industry validated and referenced solutions

Experienced OT professionals

Specialized OT integrators

1000+ professional services engineers

Specialized Ecosystem



Extensive solution integration platform

500+ Security Fabric ecosystem integrations

Out-of-the-box integrations with leading OT security solutions



Operational Technology Ecosystem

Best-in-class integrated solutions for comprehensive protection



OT TECHNOLOGY PARTNERS

Visibility and Threat Intelligence



Security Operations Management



Other



SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Industrial Control System Vendors



Global System Integrators



Other



Note: Logos are a representative subset of the Security Fabric Ecosystem



Fortinet OT Customers

Oil & Gas



Electrical & Utilities



Water



Manufacturing



Transportation



FORTINET®