FORTINET®

# Secure Your Operational Technologies with Government Funding

Mike Lauer, National Director of Public Sector Programs

# What is Operational Technology?

- Industrial Control Systems (ICS) are **connected** to an IP based network.
- ICS are **critical** to our community and economy.

Oil and Gas

Power Grids

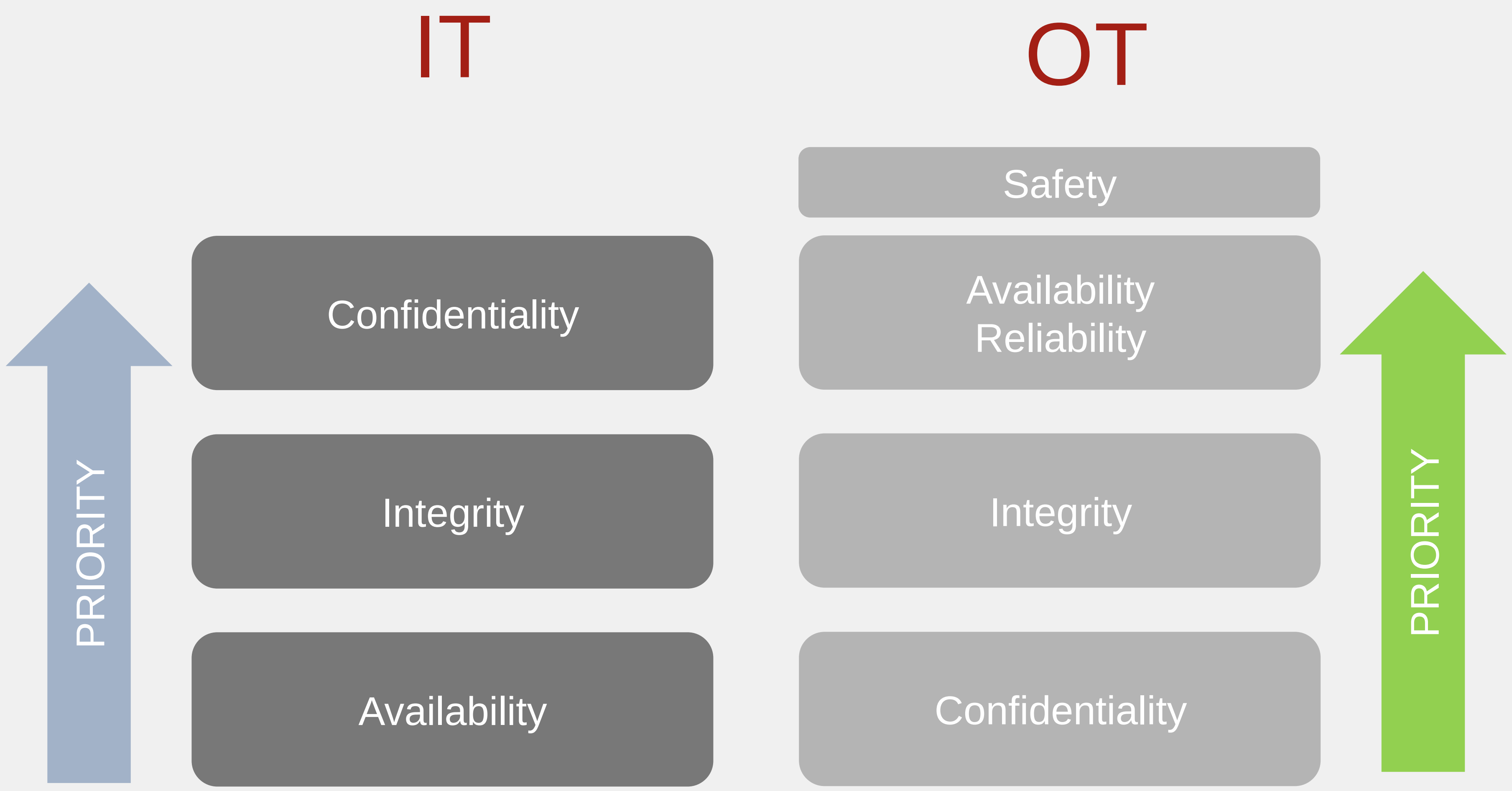
Traffic Control

Water Treatment

Transportation

Manufacturing

# Security Goals



IT

Confidentiality

Integrity

Availability

OT

Safety

Availability
Reliability

Integrity

Confidentiality

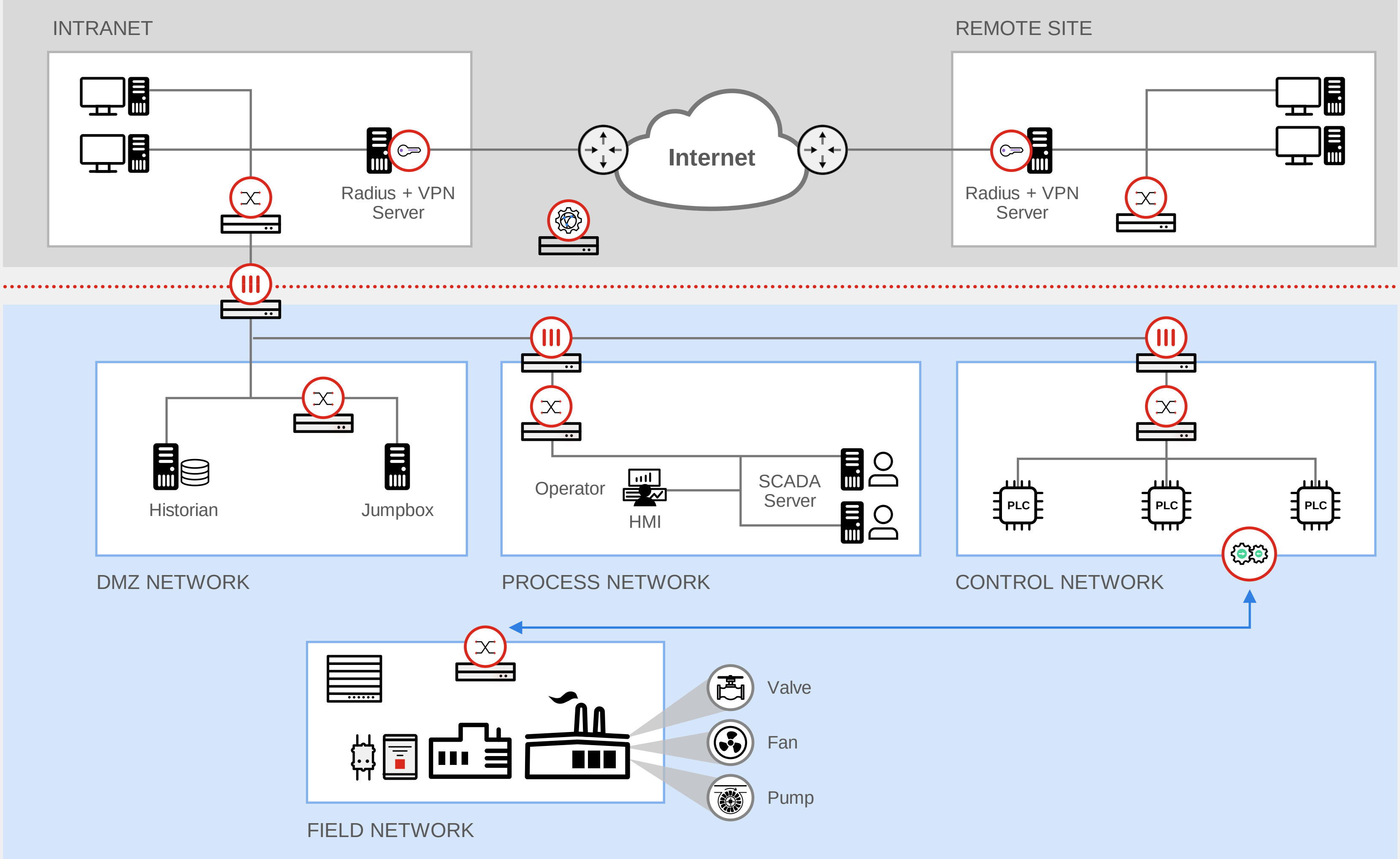
# IT vs OT

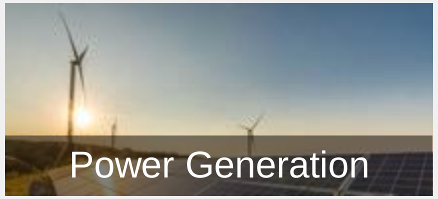
| Category | Information Technology Systems | Industrial Control Systems/OT |
|---|---|---|
| Performance Requirements | • Non-real time (eg. Email, File Servers)<br>• Server-Client response is less time critical<br>• Tightly restricted access control can be implemented to the degree necessary for security | • Real-time (eg. Field Control Commands)<br>• Server-Client response is time critical (milliseconds)<br>• Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction |
| Availability (Reliability) Requirements | • Availability deficiencies can often be tolerated, depending on the system's operational requirements | • High Availability requirements necessitates highly redundant systems |
| Risk Management Requirements | • Manage enterprise data<br>• Major risk impact is delay of business operations, financial loss, business reputation | • Control physical world<br>• Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, asset, or loss of production |
| Communications | • Standard IT communications protocols | • Vendor proprietary and standard SCADA communication protocols |
| Managed Support | • Allow for diversified support styles, supported internally or can be outsourced to one of many providers | • Service support is usually via a single vendor only |
| Component/Application Lifetime | • Lifetime in the order of 3 to 5 years | • Lifetime in the order of 15 to 20 years |
| Major Vendors | • Microsoft, IBM, Oracle, SAP | • ABB, Schneider, GE, Siemens, Honeywell |
| Resources | • 1:1 ratio of staff to desktop PC | • ~1:1000 of staff to devices |

# What and where are IT and OT networks?

Information Technology (IT)

Operational Technology (OT)





# OT Industry Challenges and Trends

# Challenge: Securing Operational Technology

Most industrial control systems lack security by design and are sensitive 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.

Asset owners must comply with industry-specific regulations

# The Industry Agrees…

## IT / OT Convergence

“OT environments that were traditionally separated are no longer completely isolated. They now have direct connections for business, OEMs and other third parties.”

Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework published 17 June 2021

## Long Lifespan

“The automation hardware in a process automation system is often capable of running 20 to 30 years.”

Automation’s Life Cycle Management of Processing Automation Control Systems, published April 2021

## Incidents Underreported

“15% of survey respondents have experienced a security incident last year that crippled operational or mission-critical systems.”

Gartner, Emerging Technologies: Critical Insights for Operational Technology Security published November 10, 2021

## Compromises in IT drive ICS/OT incidents

“Survey participants cite a compromise in IT allowing threats into the ICS/OT control networks as the highest-ranking threat vectors involved in control system incidents.”

SANS *2022* Survey: OT/ICS Cybersecurity, published October 2022

## Mixing legacy and modern tech

“Technical integration of legacy and aging OT technology with modern IT systems is the biggest challenge facing securing OT technology and process.”

SANS 2022 Survey: OT/ICS Cybersecurity, published October 2022

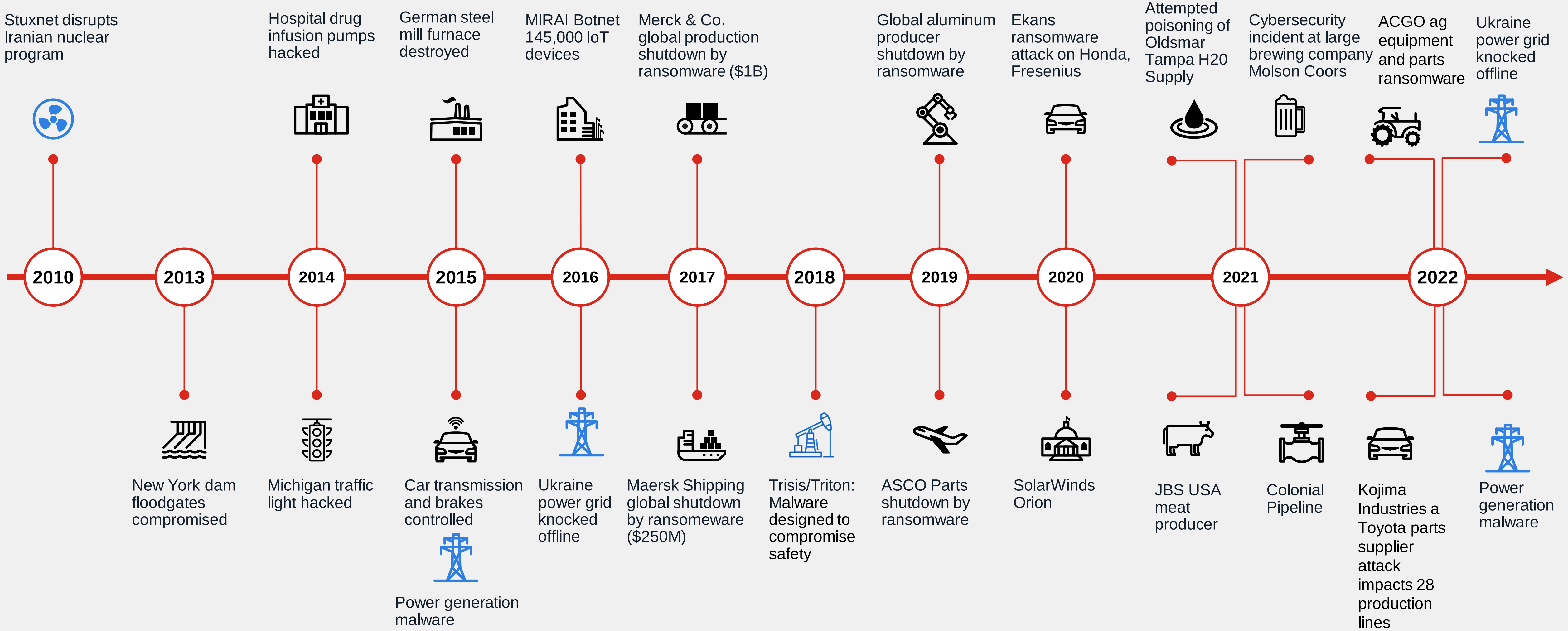
## Ransomware is the highest concern

“Ransomware, extortion, or other financially motivated crimes rank as number one threat vector of concern.”

SANS 2022 Survey: OT/ICS Cybersecurity, published October 2022

# OT Infrastructure Attacks Are Getting Worse

Attacks are increasing in frequency and impact



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
- Power generation malware

2016
- MIRAI Botnet 145,000 IoT devices
- Ukraine power grid knocked offline

2017
- Merck & Co. global production shutdown by ransomware ($1B)
- Maersk Shipping global shutdown by ransomeware ($250M)

2018
- Trisis/Triton: Malware designed to compromise safety

2019
- Global aluminum producer shutdown by ransomware
- ASCO Parts shutdown by ransomware

2020
- Ekans ransomware attack on Honda, Fresenius
- SolarWinds Orion

2021
- Attempted poisoning of Oldsmar Tampa H20 Supply
- Cybersecurity incident at large brewing company Molson Coors
- JBS USA meat producer
- Colonial Pipeline

2022
- ACGO ag equipment and parts ransomware
- Ukraine power grid knocked offline
- Kojima Industries a Toyota parts supplier attack impacts 28 production lines
- Power generation malware

OT targeted attacks

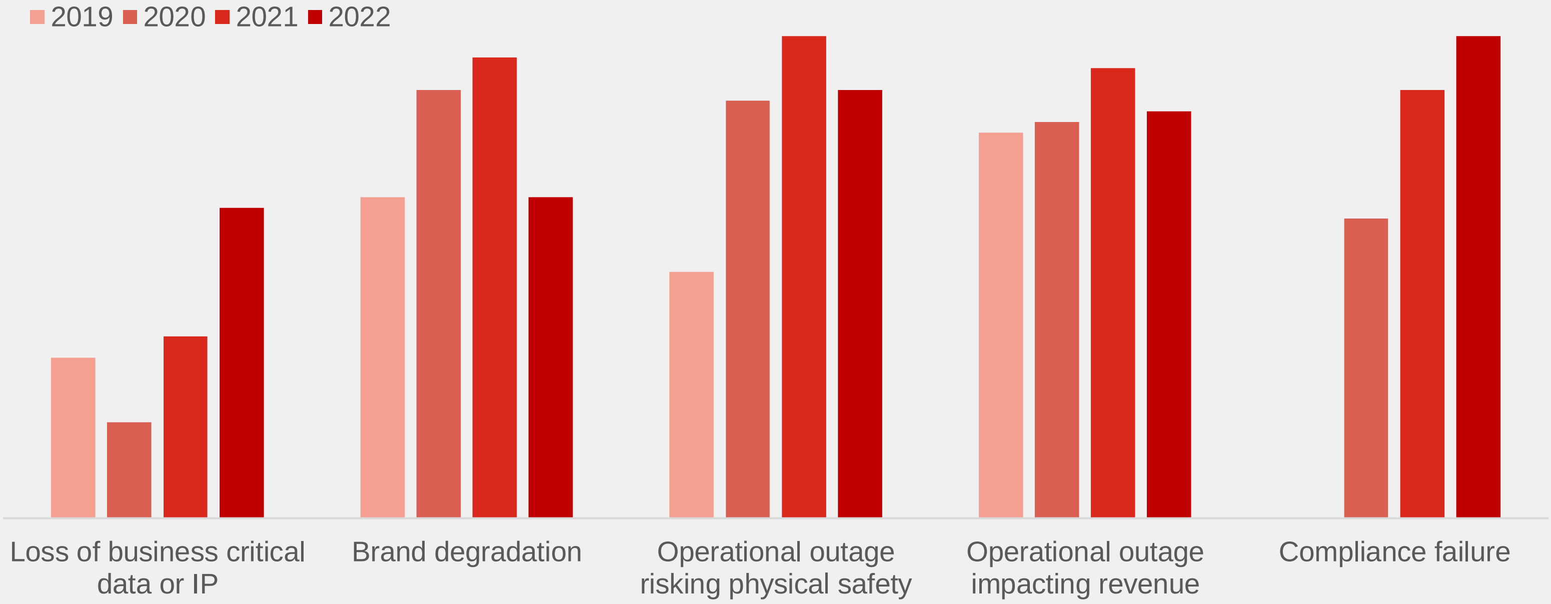
# OT Risk Is Proportional to OT Connectivity

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.

### Impact on organization



## 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

# Best Practices to Secure OT

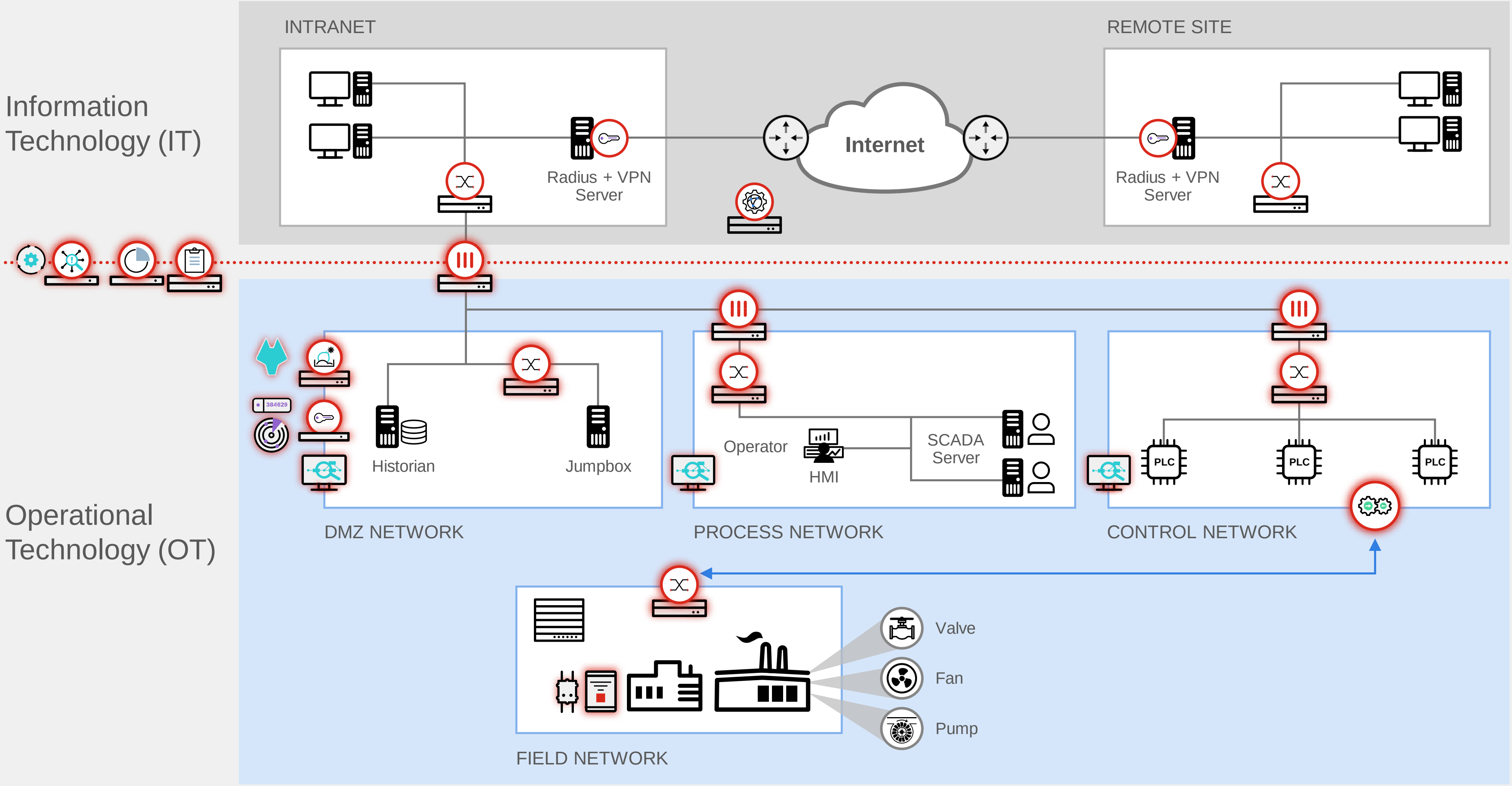
# What controls are essential to secure OT environments?

| | | |
|---|---|---|
| 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

Information Technology (IT)

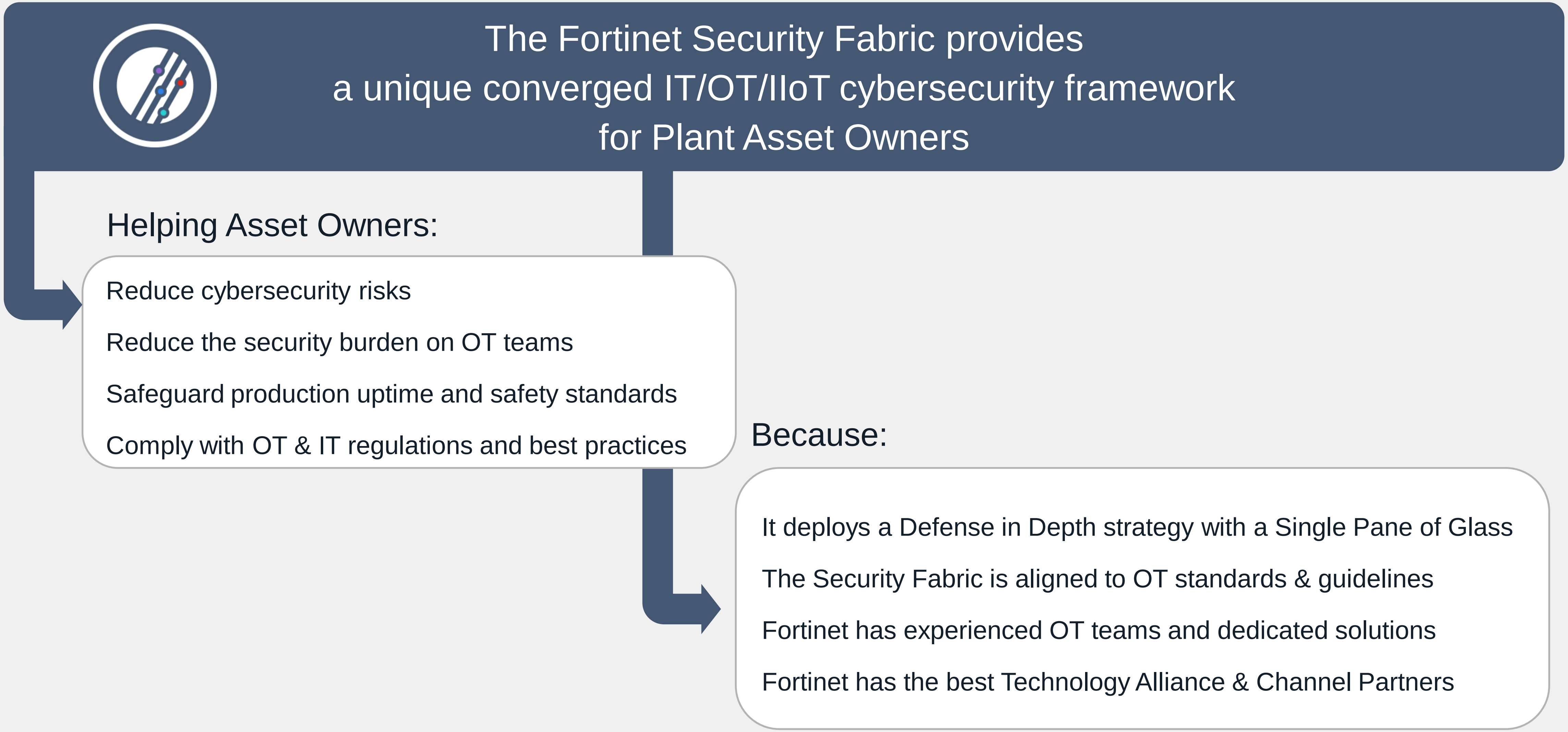
Operational Technology (OT)



- Zones and Conduits
- Secure Remote Connectivity
- Deep OT Visibility
- Role-based Access Control
- Endpoint Security
- NOC / SOC
- Advanced Persistent Threat

# How Fortinet's Products Address OT and IT-OT Convergence

# Fortinet’s Unique Value Proposition for OT Cyber Security



The Fortinet Security Fabric provides
a unique converged IT/OT/IIoT cybersecurity framework
for Plant Asset Owners

Helping Asset Owners:

- Reduce cybersecurity risks
- Reduce the security burden on OT teams
- Safeguard production uptime and safety standards
- Comply with OT & IT regulations and best practices

Because:

- It deploys a Defense in Depth strategy with a Single Pane of Glass
- The Security Fabric is aligned to OT standards & guidelines
- Fortinet has experienced OT teams and dedicated solutions
- Fortinet has the best Technology Alliance & Channel Partners

# Fortinet Security Fabric

## Broad

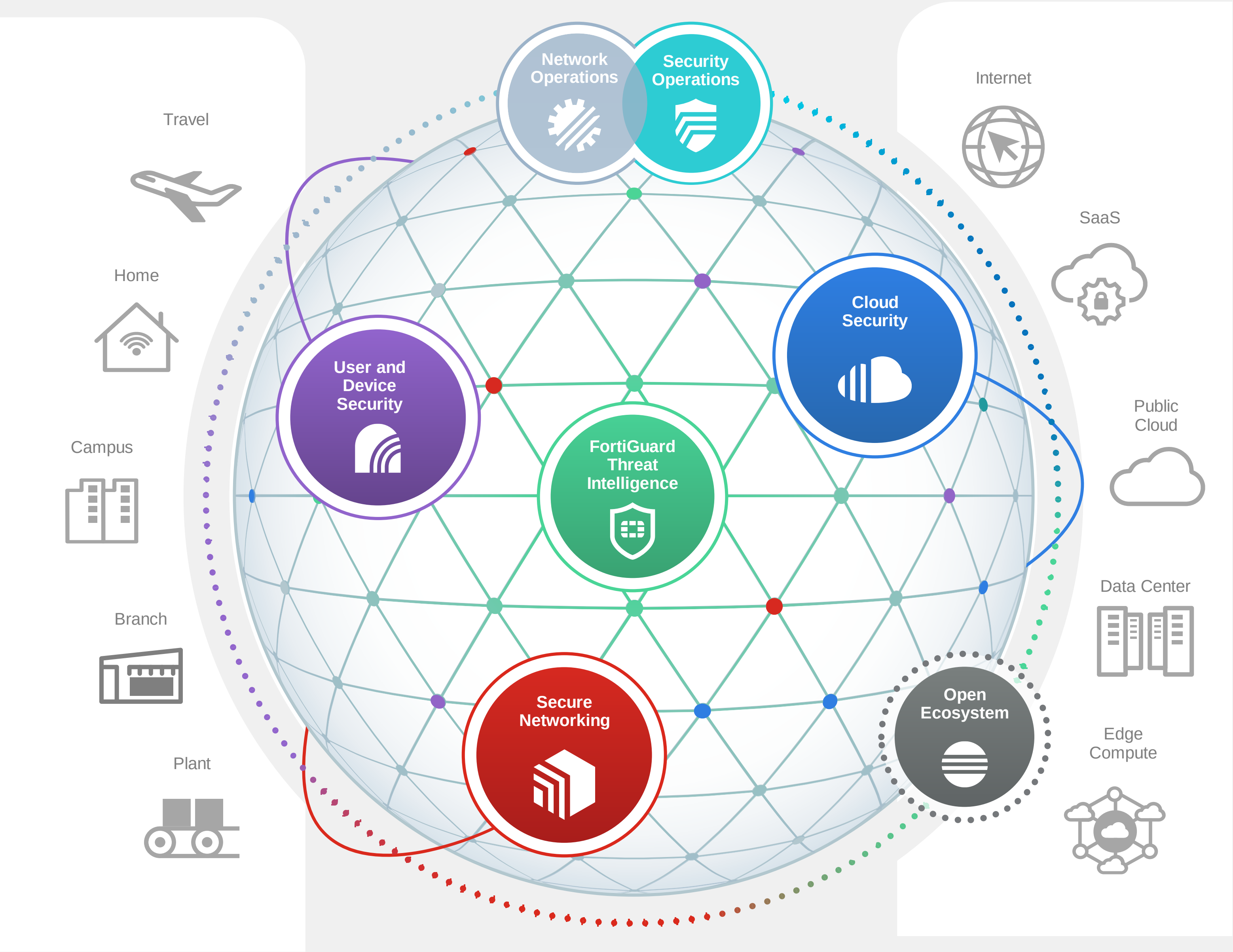
visibility and protection of the entire digital attack surface to better manage risk

## Integrated

solution that reduces management complexity and shares threat intelligence

## Automated

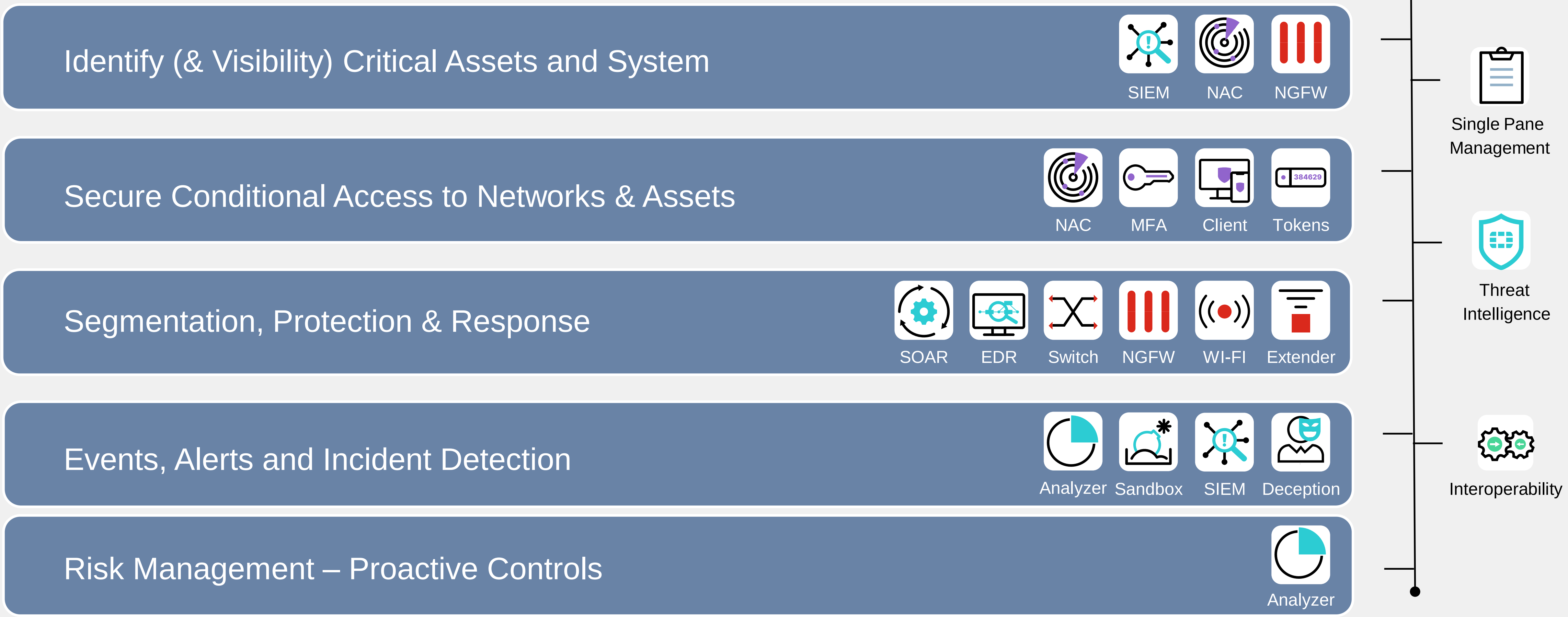
self-healing networks with AI-driven security for fast and efficient operations



# 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

Secure Conditional Access to Networks & Assets

Segmentation, Protection & Response

Events, Alerts and Incident Detection

Risk Management – Proactive Controls

# Fortinet Solution Offering for ICS/OT

## FortiGate and FortiSwitch Rugged with FortiAP Outdoor

COMMON CRITERIA CERTIFIED EAL4+ · ICSA labs · FIPS VALIDATED 140-2 · IEC 61850-3 IEEE 1613

### Ruggedized Design

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

### Consolidated Security Architecture

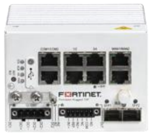
FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products.

### Ease of Management

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

## FortiGate Rugged Series

**FGR-70F 3G/4G**
SoC4-powered, security and VPN gateway with compact, fanless design and embedded 3G/4G/LTE



**FGR-70F**
SoC4-powered, security and VPN gateway with compact, fanless design

**FGR-60F 3G/4G**
SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

**FGR-60F**
SoC4-powered, security and VPN gateway

## 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 Rugged, FortiAP Outdoor Series

**FSR-112D-POE and FSR-424F**
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 Outdoor 234F**
Internal Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

**FortiAP Outdoor 432F**
External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

# Operational Technology Ecosystem

Best-in-class integrated solutions for comprehensive protection

FORTINET FABRIC-READY

## OT TECHNOLOGY PARTNERS

### Visibility and Threat Intelligence

DRAGOS
NOZOMI NETWORKS
CLAROTY
ordr
np network perception
CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY
SCADAfence
INDUSTRIAL DEFENDER®
tenable

### Security Operations Management

OTORIO
splunk>
tdi technologies
rubrik
BACKBOX
SKYBOX SECURITY
servicenow.

### Other

SIEMENS RUGGEDCOM
FORESCOUT
radiflow
OWL Cyber Defense
DARKTRACE
RAD

## SOLUTION VENDORS AND SYSTEMS INTEGRATORS

### Industrial Control System Vendors

Schneider Electric
ABB
SIEMENS Ingenuity for life
YOKOGAWA
HIRSCHMANN A BELDEN BRAND
EMERSON
Rockwell Automation
GE
SEL SCHWEITZER ENGINEERING LABORATORIES

### Global System Integrators

Hewlett Packard Enterprise
IBM
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
Orange Cyberdefense
HCL
Atos
NTT
accenture

### Other

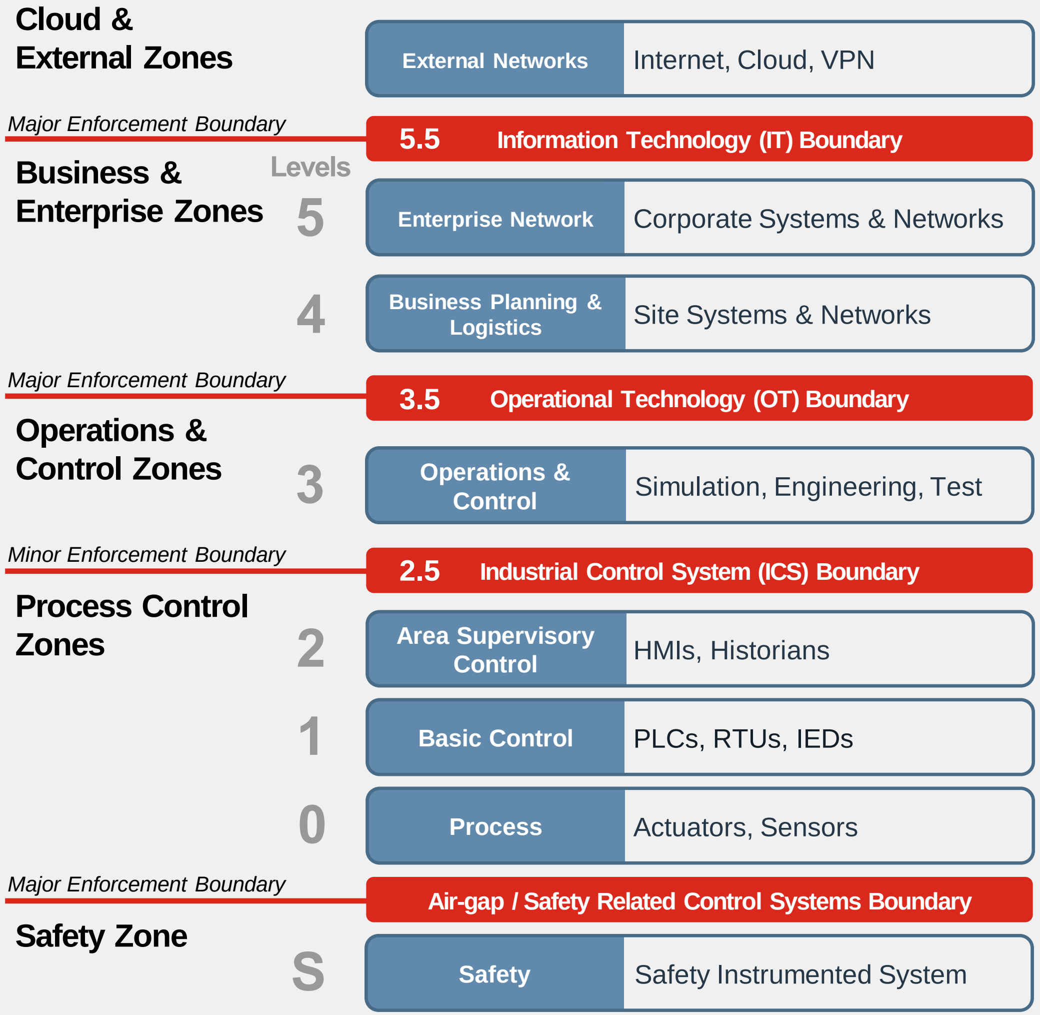
Baker Hughes
T · · Systems ·
Johnson Controls
Eleven Paths A Telefónica COMPANY
World Wide Technology, Inc.

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

# Securing Operational Technology

## with the Fortinet Security Fabric

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Deception
- Sandbox
- NOC/SOC



**Cloud & External Zones**

External Networks – Internet, Cloud, VPN

*Major Enforcement Boundary*

5.5 Information Technology (IT) Boundary

**Business & Enterprise Zones**

Levels

5 Enterprise Network – Corporate Systems & Networks

4 Business Planning & Logistics – Site Systems & Networks

*Major Enforcement Boundary*

3.5 Operational Technology (OT) Boundary

**Operations & Control Zones**

3 Operations & Control – Simulation, Engineering, Test

*Minor Enforcement Boundary*

2.5 Industrial Control System (ICS) Boundary

**Process Control Zones**

2 Area Supervisory Control – HMIs, Historians

1 Basic Control – PLCs, RTUs, IEDs

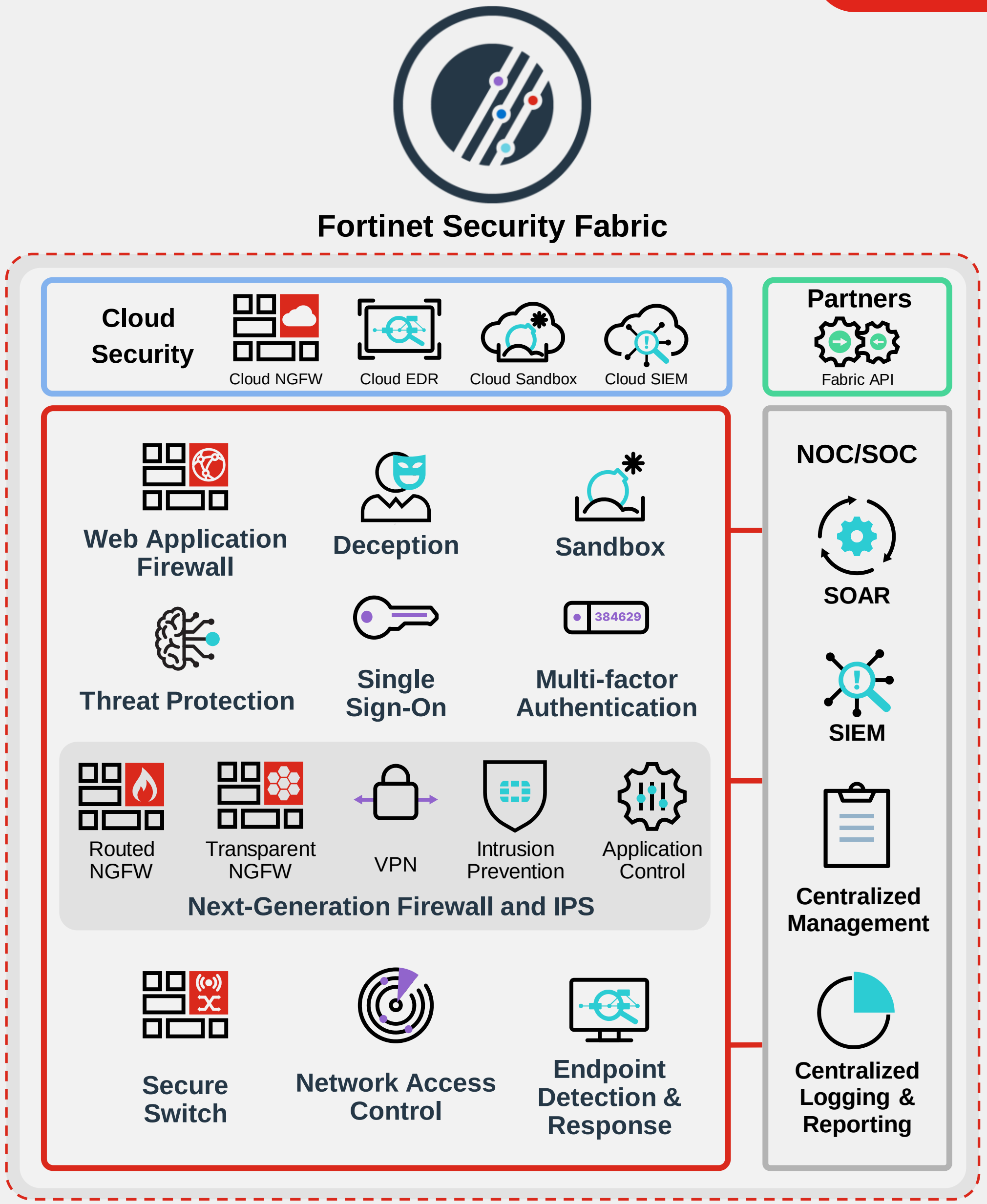
0 Process – Actuators, Sensors

*Major Enforcement Boundary*

Air-gap / Safety Related Control Systems Boundary

**Safety Zone**

S Safety – Safety Instrumented System



**Fortinet Security Fabric**

Cloud Security: Cloud NGFW, Cloud EDR, Cloud Sandbox, Cloud SIEM

Partners: Fabric API

Web Application Firewall, Deception, Sandbox

Threat Protection, Single Sign-On, Multi-factor Authentication

Next-Generation Firewall and IPS: Routed NGFW, Transparent NGFW, VPN, Intrusion Prevention, Application Control

Secure Switch, Network Access Control, Endpoint Detection & Response

NOC/SOC: SOAR, SIEM, Centralized Management, Centralized Logging & Reporting

*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*

# Funding to address Securing OT

# State and Local Cybersecurity Grant Program (SLCGP)

Administered by the **Department of Homeland Security (DHS)** and the **Federal Emergency Management Agency (FEMA)**, grant funds will be used to improve the nation’s cybersecurity posture and protect critical infrastructure from malware, ransomware, and other threats.

States may choose to subgrant funds directly to eligible local entities to purchase necessary cybersecurity solutions and other eligible expenses, or they may purchase cybersecurity solutions and other eligible expenses at the state level on behalf of all local governments.

## Funding Amount

$1 billion to 56 U. S. states and territories from FY22 through FY25.

## Deadlines

States applied for FY22 funds last November. States will apply for the FY23 funds in mid-summer. Local deadlines will vary by state.

## Eligibility

States, counties, municipalities, the District of Columbia, tribal governments, and five US territories are eligible.

# Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program

Administered by the **Department of Energy** with assistance from the **Office of Cybersecurity, Energy Security, and Emergency Response**. Funding is available to provide grants and technical assistance to, and enter into cooperative agreements with, eligible entities to protect against, detect, respond to, and recover from cybersecurity threats.

Priority will be given to utility providers with limited resources or critical assets.

## Funding Amount

$250 million from 2023- 2026.

## Deadlines

The initial application process is expected to open in 2023. The Request for Proposal (RFP) was due in December 2022.

## Eligibility

Rural electric cooperatives, publicly-owned electric utilities, and small investor-owned utilities.

# American Rescue Plan (ARP) Coronavirus State and Local Fiscal Recovery Funds

Provides funds to units of government for uses related to COVID-19 response and mitigation, and to offset government revenue losses related to the public health emergency.

Per the Final Ruling from the Treasury released in January 2022, funds may be used for:

- The modernization of cybersecurity, including hardware, software, and the protection of critical infrastructure.
- To maintain vital government services.
- And finally, to address long-term investments such as water, sewer, and broadband infrastructure.

**Funding Amount**

$350 billion across state and local governments.

**Deadline**

December 31, 2024.

**Eligibility**

States, counties, municipalities, the District of Columbia, tribal governments, and five US territories are eligible.

# Homeland Security Grant Programs

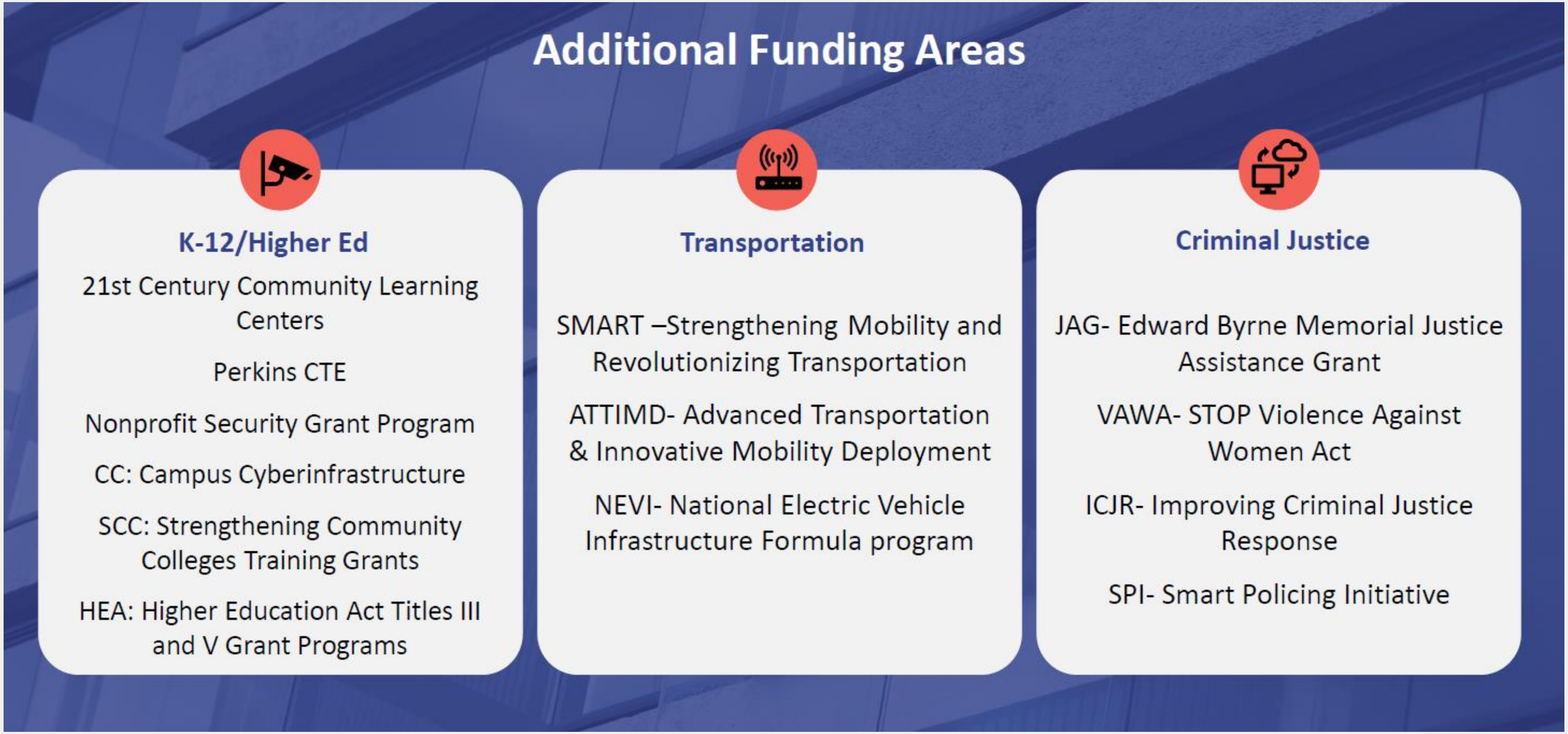
Provides funding for the execution of the Prevention, Protection, Mitigation, Response, and Recovery mission areas and the realization of a secure and resilient Nation.

National priority areas include:

- Enhancing the protection of soft targets/crowded places
- Enhancing information and intelligence sharing and analysis
- Combating domestic violent extremism
- Enhancing cybersecurity
- Enhancing community preparedness and resilience
- Enhancing election security

**Programs Include:**

- State Homeland Security Program (SHSP)
- Tribal Homeland Security Program (THSGP)
- Urban Areas Security Initiative (UASI)
- Operation Stonegarden Grant Program (OPSG)
- Nonprofit Security Grant Program (NSGP)
- Transit Security Grant Program (TSGP)
- Port Security Grant Program (PSGP)



## Additional Funding Areas

### K-12/Higher Ed

21st Century Community Learning Centers

Perkins CTE

Nonprofit Security Grant Program

CC: Campus Cyberinfrastructure

SCC: Strengthening Community Colleges Training Grants

HEA: Higher Education Act Titles III and V Grant Programs

### Transportation

SMART –Strengthening Mobility and Revolutionizing Transportation

ATTIMD- Advanced Transportation & Innovative Mobility Deployment

NEVI- National Electric Vehicle Infrastructure Formula program

### Criminal Justice

JAG- Edward Byrne Memorial Justice Assistance Grant

VAWA- STOP Violence Against Women Act

ICJR- Improving Criminal Justice Response

SPI- Smart Policing Initiative

# Fortinet Grant Support Program

*Fortinet and our partners are now offering a comprehensive grant support program. This FREE program provides public sector agencies with grant information, customized research, and consultation services that help develop project ideas, identify available grant funding for technology-rich projects, and even expand initiatives that are already in the works.*

FORTINET

# Evaluate Your Industrial Controls Network Risk with the Fortinet Cyber Threat Assessment Program

## Gauge Current Security, Applications, and Utilization of your Operational Technology (OT) Network

As industrial environments increase connectivity with internet-based corporate networks and adopt Internet of Things (IoT) or industrial IoT (IIoT) technologies, security becomes a critical priority for operational technology (OT). Accurate detection of today's advanced threats and full visibility of the users, data, devices and applications used in OT is a must. If you are concerned about ensuring safe, available and secure operations while protecting the legacy and modern industrial equipment, an OT assessment is a recommended next step.

Validate your OT network's security effectiveness, application flows, and utilization by enlisting expert guidance. A Fortinet expert will use a FortiGate to monitor key indicators within your OT network. After several days of gathering information, you will receive an OT Assessment Report which is divided into three primary sections:

- **Security and Threat Prevention –** How effective is your current network security solution? Learn more about application vulnerabilities are attacking your network, which malware/botnets were detected and even pinpoint "at risk" devices within your network. Make sure your existing security solution isn't letting anything slip through the cracks by leveraging FortiGuard Labs' award-winning content security.
- **OT/IT Application Usage –** What steps are you taking to monitor traffic flows in your network? Improve your visibility to traffic and most used applications within your OT environment. Monitor traffic patterns to identify network anomalies whether accessing on-site or via remote access.
- **Network Utilization and Performance –** How should your network security solution be optimized for performance?Find out more about your throughput, session and bandwidth requirements during peak hours. Ensure your security solution is sized and optimized properly based on your actual usage.

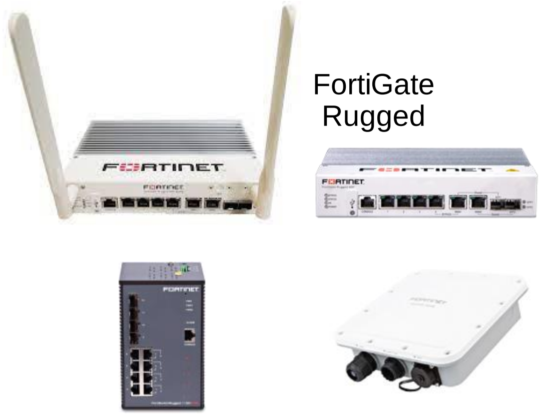
| # | Risk | Threat Name | Type | Victims | Sources | Count |
|---|---|---|---|---|---|---|
| 1 | 5 | Honeywell OPOS Multiple ActiveX Open Method Buffer Overflow | Buffer Errors | 2 | 1 | 5 |
| 2 | 5 | Unitronics VisiLogic OPLC TeeCommander Memory Corruption | Buffer Errors | 1 | 1 | 2 |
| 3 | 3 | Schneider Electric GP-Pro EX ParseAPI Heap Buffer Overflow | Buffer Errors | 3 | 1 | 112 |
| 4 | 2 | Siemens SIMATIC WinCC Flexible Runtime Stack Buffer Overflow | Buffer Errors | 1 | 1 | 38 |
| 5 | 2 | Trihedral VTScada WAP Directory Traversal | Path Traversal | 3 | 1 | 14 |
| 6 | 1 | Modbus TCP Report Server Info | Permissions/Privileges/Access Control | 1 | 1 | 12 |

12a 1a 2a 3a 4a 5a 6a 7a 8a 9a 10a 11a 12p 1p 2p 3p 4p 5p 6p 7p 8p 9p 10p 11p
Sun
Mon
Tue
Wed
Thu
Fri
Sat

Obtaining an OT Assessment Report will give you a critical and quantified view into your current industrial security posture. Find out if you qualify

# Fortinet’s Specialized OT Solutions and Teams

## Specialized Offerings



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

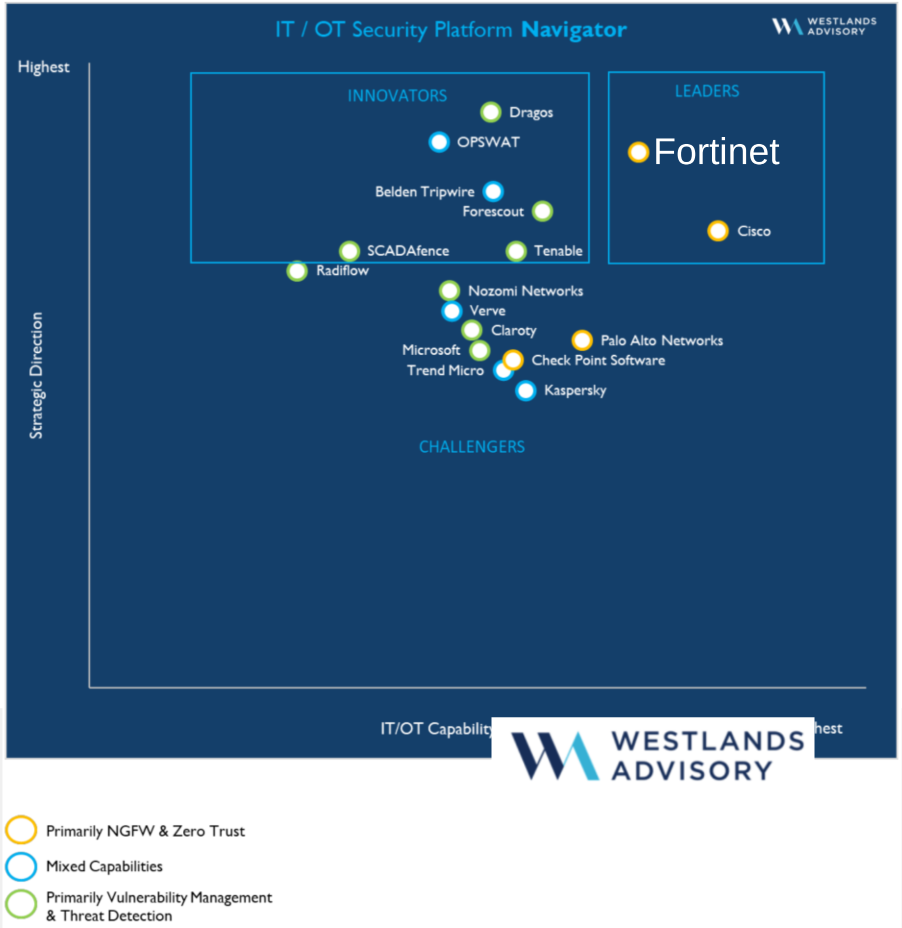
500+ Security Fabric ecosystem integrations

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

# Fortinet Is a Leader in the IT/OT Security Platform Navigator 2022

Broad, Integrated and Automated Security Fabric enables secure digital acceleration for asset owners and original equipment manufacturers

IT/OT Security Platform Navigator 2022



FORTINET®