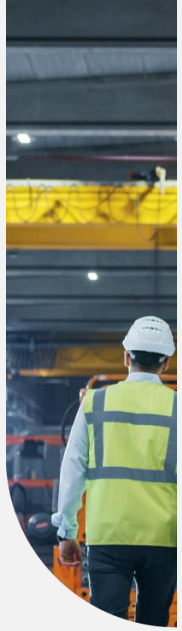


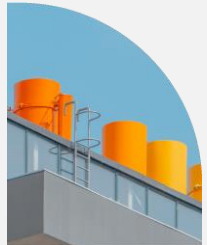
FORTINET

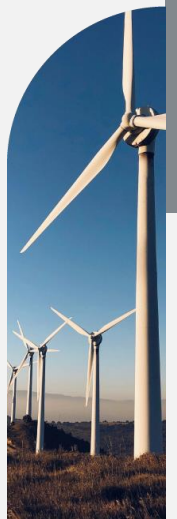
OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Defense-in-Depth Security for Manufacturing

Carlos Sanchez

Director, Operational Technology





Agenda

What you will learn

1

OT Increasingly Connected

Digital Transformation and the pandemic are driving increased connectivity from OT to IT.

2

Defense in Depth for Manufacturing

The Fortinet Security Fabric enables asset owners to enhance security posture spanning IT and OT integration.

3

Rich OT Capabilities

OT-specific features in almost every Fortinet product family.

Digital Innovation is Also Causing Increased Risk

Cyber threats take advantage of the disruption

Sophisticated Threats

Breach and ransomware incidents continue to increase

Digital Attack Surface

As the perimeter expands, billions of “Security Edges” are formed

Ecosystem Complexity

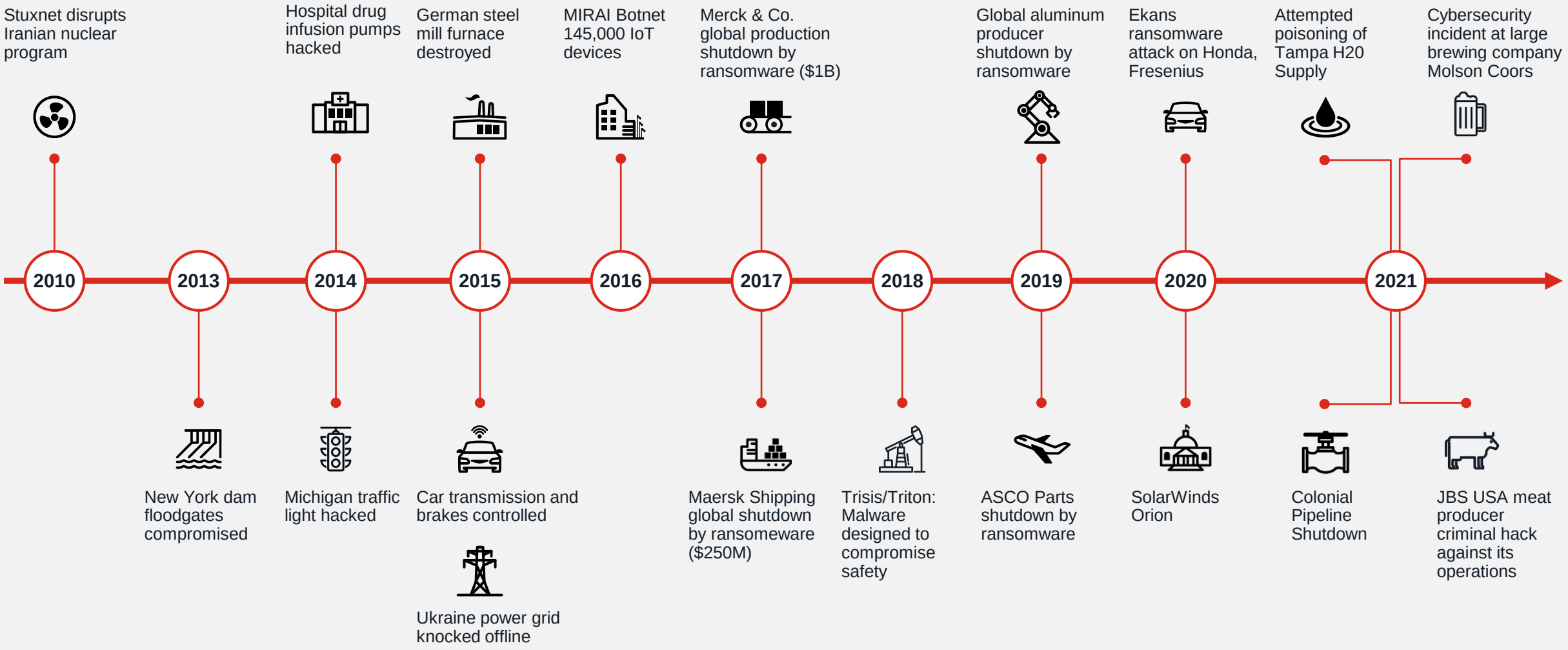
Too many vendors and too many alerts, **not** enough skilled people

Compliance

Global, country, province, industry, and government regulation

OT Infrastructure Attacks

The risk is real



How Can Manufacturers Mitigate Cyber Risk?

Visibility Across the Digital Attack Surface

New “Edges” expand the digital attack surface. Enable visibility over all vectors with a platform of detection.

Protect Against Sophisticated Threats

Breaches and ransomware continue to increase. Protect across all devices, networks, and applications.

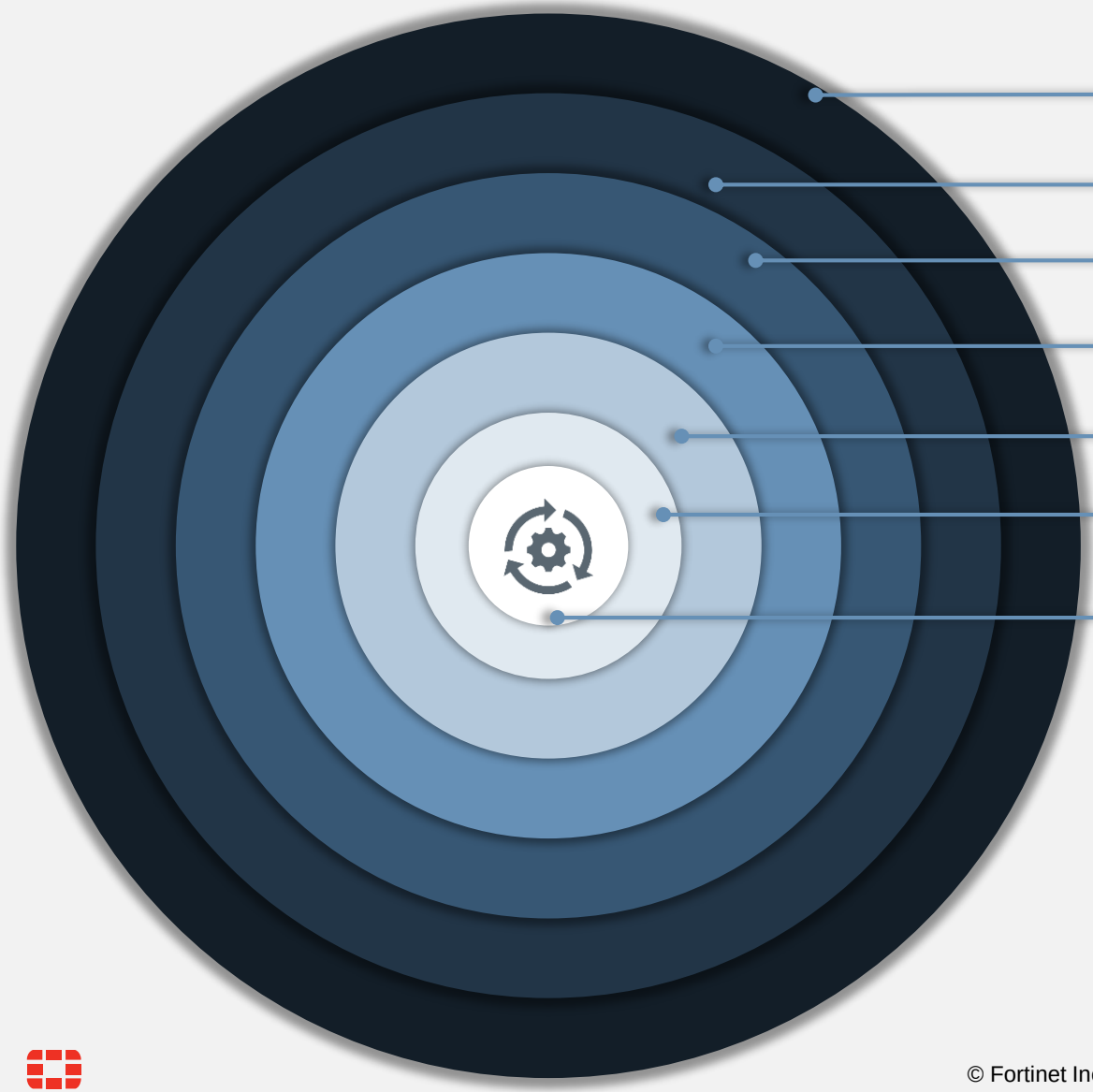
Adopt an Intelligent and Structured Security Architecture

Complexity is the enemy of an effective security posture. Too many vendors, too many alerts, not enough skilled people. Automatically prevent, detect, and respond to cyber threats.

Simplify Compliance

Global, Country, Province, Industry and Government Regulation. Secure network and data from end-to-end and make reporting easier.

Defense in Depth Approach in Smart Manufacturing



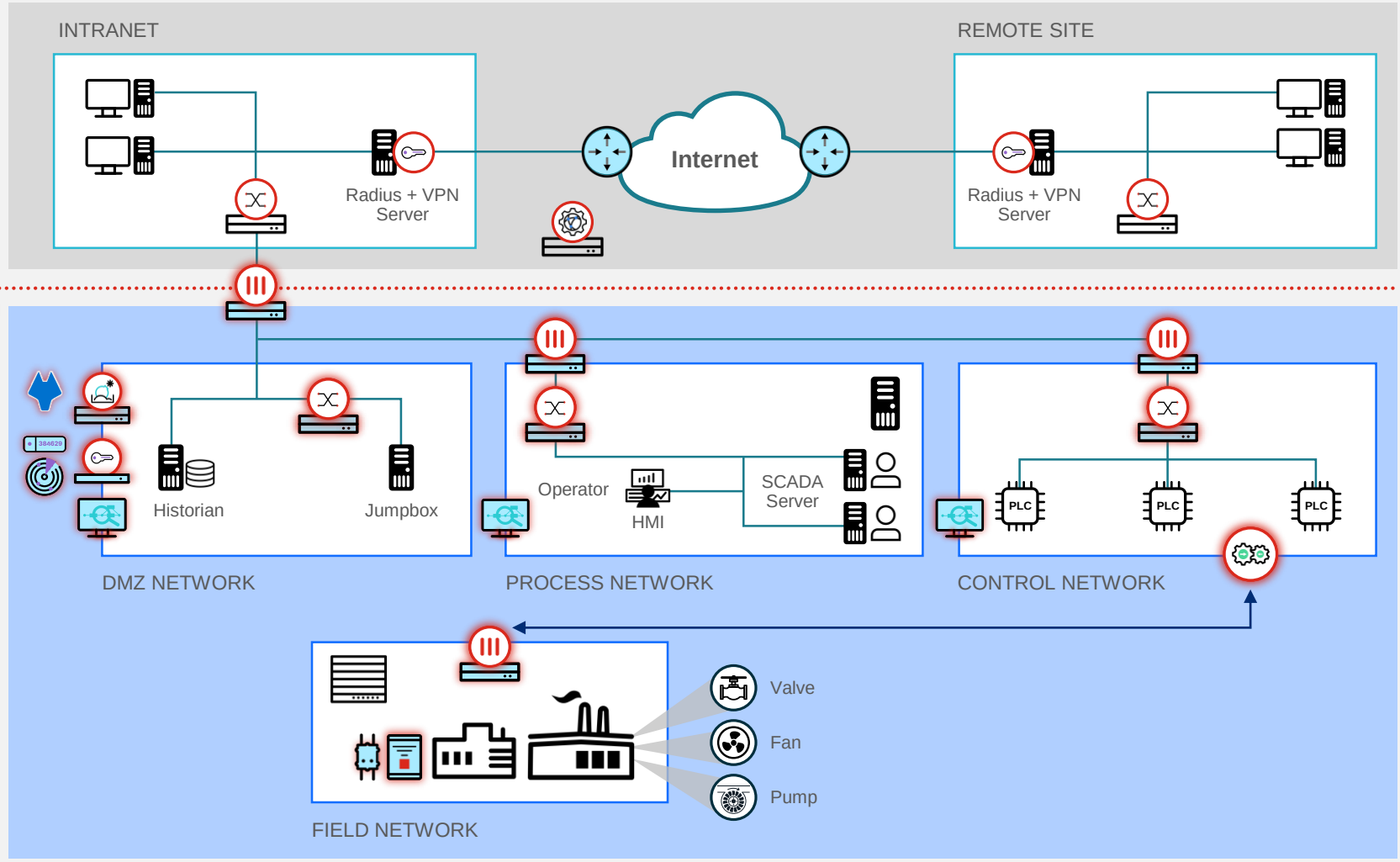
- Policies Layer
- Physical Layer
- Perimeter Layer
- Internal Network Layer
- Host Layer
- Application Layer
- Data Layer

MITRE ATT&CK for ICS
Initial Access
Execution
Persistence
Evasion
Discovery
Lateral Movement
Collection
Command and Control
Inhibit Response Function
Impair Process Control
Impact

Addressing Critical Use Cases Integrating OT and IT

Information Technology (IT)

Operational Technology (OT)



- Zones and Conduits
- Secure Remote Connectivity
- Deep OT Visibility
- Role-based Access Control
- Securing Critical End Point
- Centralize Security Management
- Advanced Persistent Threat

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

Segmentation

with FortiGate, FortiSwitch and FortiAP

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- 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

Routed NGFW

Transparent NGFW

Secure Switch

Switch

Access Point

OT Specific Capabilities

- Multiple form factors:
  - Ruggedized: FW, Switch, AP
  - Traditional form factors
  - Virtualized
- Managed online/offline via FortiManager
- Integrations with leading OT visibility and other technology vendors
- DIN rail, DC powered versions
- Transparent mode, failover bypass
- *The only* ruggedized SD-WAN NGFW
- Centralized switch management, NAC integration

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

Secure Remote Access

with FortiAuthenticator, FortiClient, and FortiToken

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- **Secure Remote Access**
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- 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

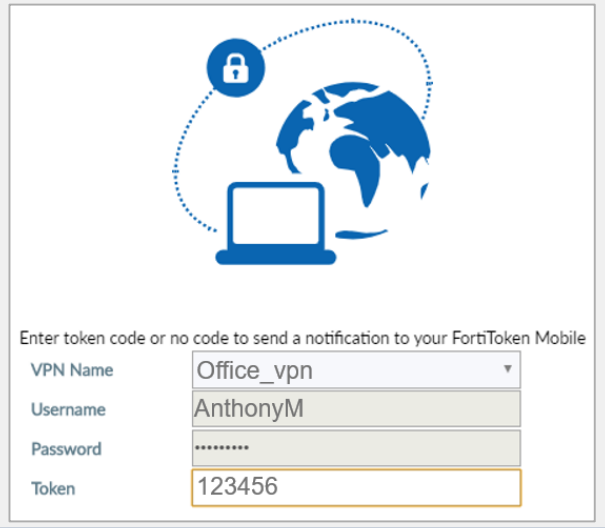
Fortinet Security Fabric

Cloud Security — Cloud NGFW

- **Single Sign-On**
- **VPN**
- **Multi-factor Authentication**

OT Specific Capabilities

- FortiClient provides VPN client with MFA support
- FortiAuthenticator authenticates users with MFA, including PKI and OTP
  - Local user database or integration with 3rd party directories
- FortiToken provides OTP
  - Physical and mobile tokens
  - Self-provisioning

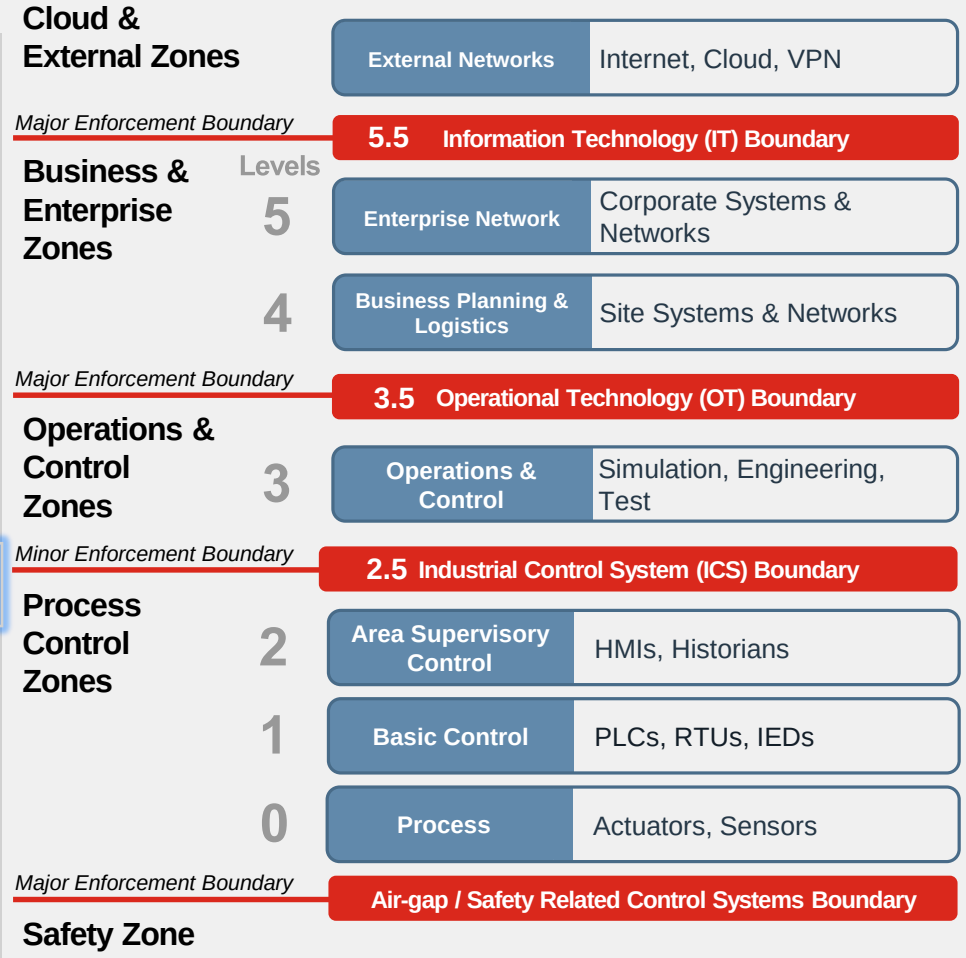


DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

Application Control

with OT Application Control on the FortiGate

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



Fortinet Security Fabric

Application Control

OT Specific Capabilities

- Most contemporary HMIs and Historians are based on HTTP
- Different protocols and applications used in OT networks.
- ~1,800 OT signatures, 3,900+ total (+IT)
- 55 ICS protocols supported protocols and increasing
- Track changes in applications used in the network
- Granular application monitoring and control options

OT Protocols and Applications

- ADDP
- BACnet
- CIP
- CN.IP
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- HART
- ICCP
- LONTalk
- MMS
- Modbus
- OPC
- OpenADR
- Profinet
- R.GOOSE
- S7
- SafetyNET
- Synchrophasor
- TriStation
- …

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

Endpoint Protection

with FortiEDR

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- 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

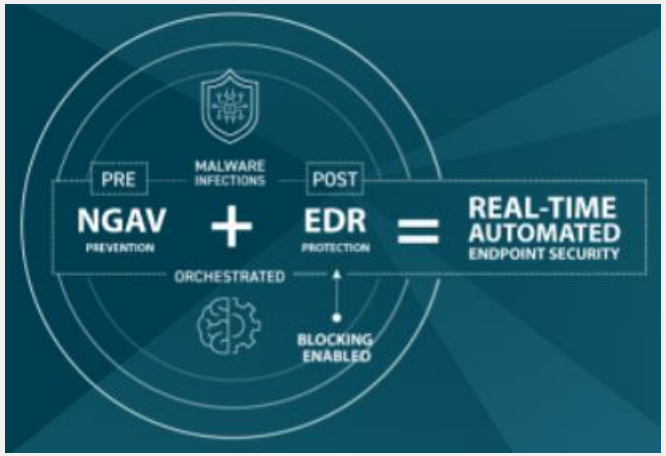
Safety Zone

Fortinet Security Fabric

Endpoint Detection & Response

OT Specific Capabilities

- Compatible with legacy operating systems all the way back to Windows XP, Service Pack 3
- Can be deployed on-premise / air gapped.
- Extremely lightweight agent.
- Alerts on suspicious behavior without disruption
- Allow/deny applications & communication paths
- Protocol agnostic.
- Blocks unauthorized USB sticks.
- Application action control capabilities



DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

NOC / SOC

with FortiManager, FortiSIEM and FortiAnalyzer

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- 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

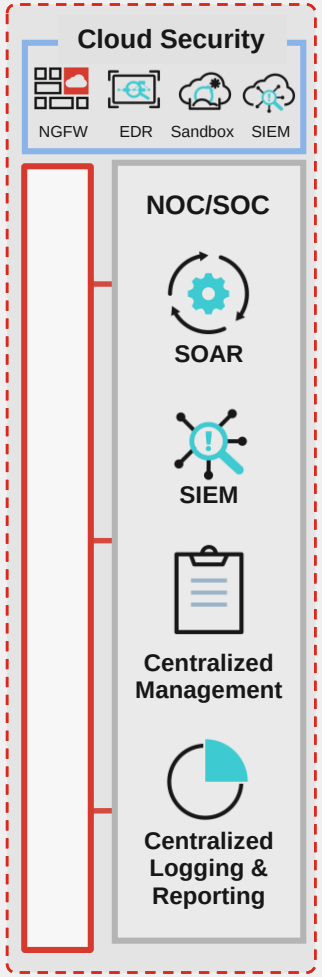
2	Area Supervisory Control	HMIs, Historians
1	Basic Control	PLCs, RTUs, IEDs
0	Process	Actuators, Sensors

Major Enforcement Boundary

Air-gap / Safety Related Control Systems Boundary

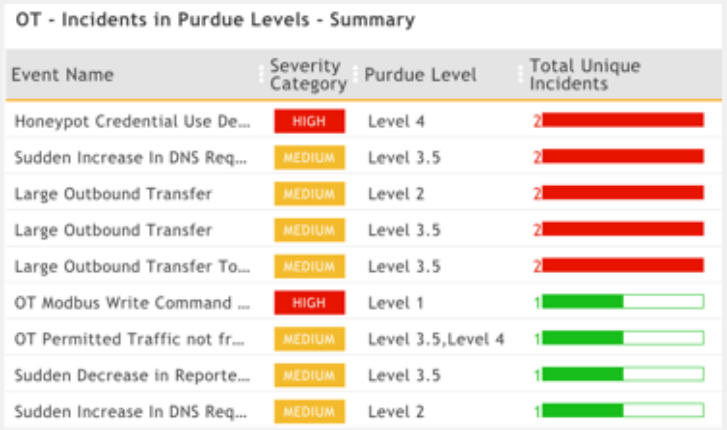
Safety Zone

Fortinet Security Fabric



OT Specific Capabilities

- FortiManager supports offline management of FortiGates, FortiSwitches and FortiAPs
- SW updates and licensing in airgap networks
- FortiAnalyzer has monitoring and reporting tools tailored for Fortinet devices
- FortiSIEM can be deployed on premise, hydbrid or cloud, including OT specific tools and integrations.



OT - Incidents in Purdue Levels - Summary

Event Name	Severity Category	Purdue Level	Total Unique Incidents
Honeypot Credential Use De...	HIGH	Level 4	2
Sudden Increase In DNS Req...	MEDIUM	Level 3.5	2
Large Outbound Transfer	MEDIUM	Level 2	2
Large Outbound Transfer	MEDIUM	Level 3.5	2
Large Outbound Transfer To...	MEDIUM	Level 3.5	2
OT Modbus Write Command ...	HIGH	Level 1	1
OT Permitted Traffic not fr...	MEDIUM	Level 3.5,Level 4	1
Sudden Decrease in Reporte...	MEDIUM	Level 3.5	1
Sudden Increase In DNS Req...	MEDIUM	Level 2	1

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

Specialized OT Teams and Solutions

Specialized Hardware

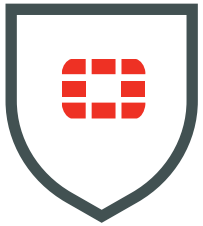
FortiGate Rugged 60F

FortiSwitch Rugged

FortiAP IPS-rated

- Industrial Grade Firewalls, Switches and APs
- Most deployed IT/OT NextGen Firewall Worldwide
- OT-specific EDR, Sandbox, and Deception capabilities

Specialized Threat Information



- DPI with Industrial Protocol Breadth
- OT Application Control Depth
- OT Vulnerabilities Shielding
- More signatures than any other cybersecurity vendor

Specialized Talent

- Referenced Solutions
- Experienced OT Professionals
- OT Specialized Integrators
- 1000+ Professional Services

Ecosystem

- Expand the platform through integration
- 400+ security fabric ecosystem integration
- Tight integrations with leading OT security partners

Operational Technology Ecosystem

Best-in-class integrated solutions for comprehensive protection

OT Technology Partners

Visibility and Threat Intelligence

Dragos, Nozomi Networks, Claroty, ordr, network perception, CyberX, SCADAfence, Industrial Defender, tenable

Operations, Orchestration Automation

OTORIO, splunk>, tdi, rubrik, BACKBOX, SKYBOX Security, servicenow

Other

SIEMENS RUGGEDCOM, FORESCOUT, radiflow, OWL Cyber Defense, DARKTRACE, RAD

Solution Vendors and Systems Integrators

Control Vendors

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

Global System Integration

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

Other(s)

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

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Fortinet Customer Success

Food & Beverage/Manufacturing

Opportunity profile

SITUATION

- Geographically distributed environment
- 300 breweries globally
- 6 Azure locations globally
- Needed visibility across environement

PROBLEM

- Internal Audit showed that they did not segment their IT and OT networks
- Identified Threats that did affect their environment
- Did not have Nextgen Firewalls in their network

CUSTOMER NEEDS

- Protect all breweries from cyber attacks
- Segment their IT and OT networks
- A non-intrusive tool that discovers the OT assets, quickly
- Company that understands OT and IT/OT convergence

SOLUTION

- 2 FortiGate 100Fs each brewery 300 globally
- Virtual VMs 04 and 08
- 2 FortiManagers

The Next Step

Fortinet Can Help

1

Align with the Standards

- Effective Implementation of the NIST Cybersecurity Framework with Fortinet
- Effective ICS Cybersecurity: Using the IEC 62443 Standard

2

Defense in Depth for Manufacturing

Visit us at www.Fortinet.com/Manufacturing

3

Explore the Possibilities

Take our interactive, virtual tour to see for yourself.

Q&A

For more information, visit
Fortinet.com/manufacturing

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021