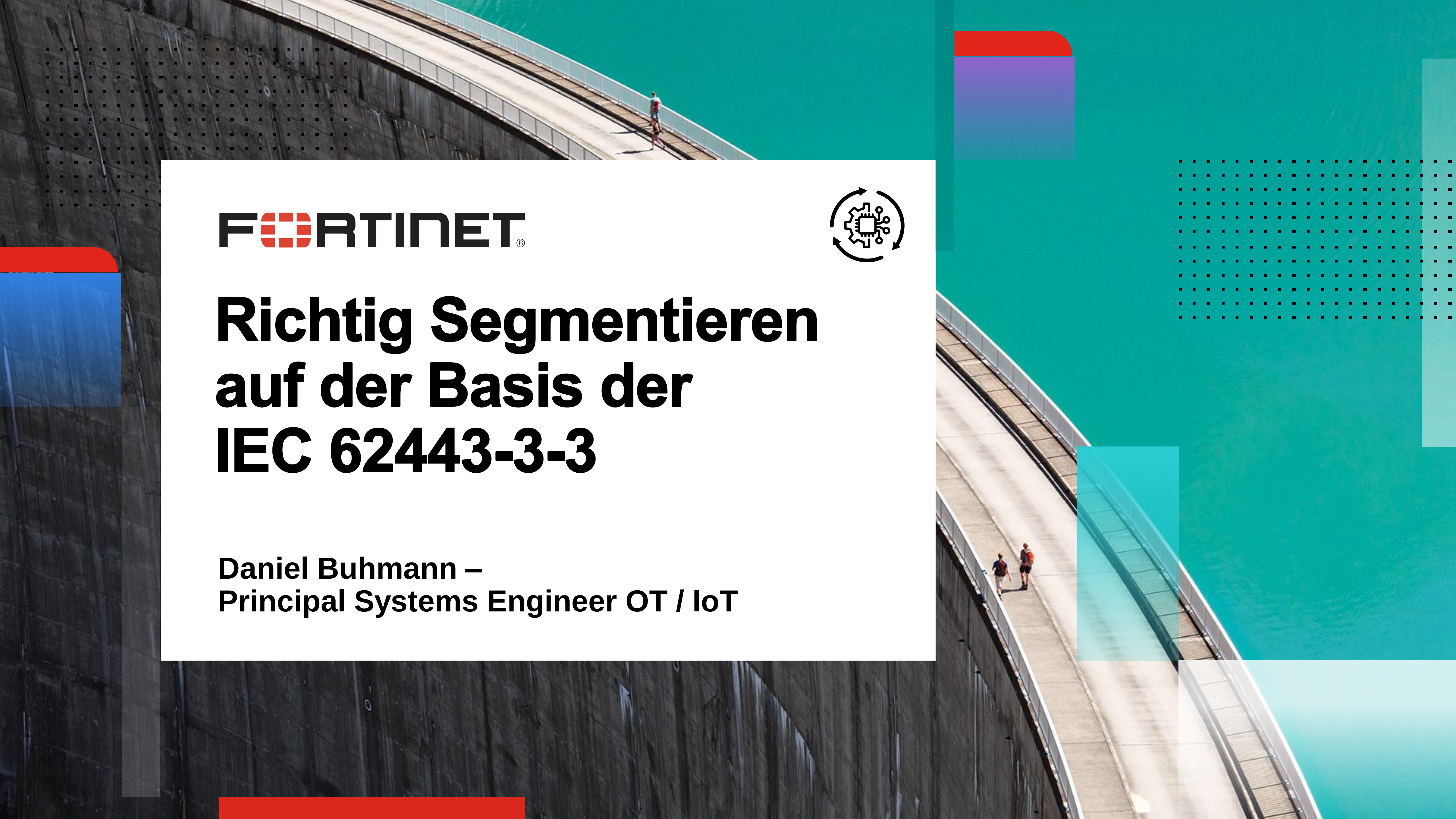


Richtig Segmentieren auf der Basis der IEC 62443-3-3

Daniel Buhmann –
Principal Systems Engineer OT / IoT

About me

Daniel Buhmann

- Principal Systems Engineer /
  OT Subject Matter Expert at Fortinet
- ICS Security since 2005
  - Risk & Vulnerability Assessments
  - Solution planning and implementation
  - Security Consultant
  - Trainer & Presenter

Fortinet makes possible a digital world you can always trust

Fortinet’s mission is to secure people, devices, and data everywhere.

Security Fabric Strategies for OT

Preserve business continuity and compliance in the face of changing technology and digitalization

Threat Detection and Protection

Threat and Vulnerability Management

Compliance

Accelerated Digitalization

OT Focus

- Network segmentation and micro-segmentation
- Broad coverage for OT protocols and applications
- Virtual patching for legacy ICS and OT systems
- ICS and OT specific dashboards
- Simplified user interfaces

Security Fabric Strategies for OT

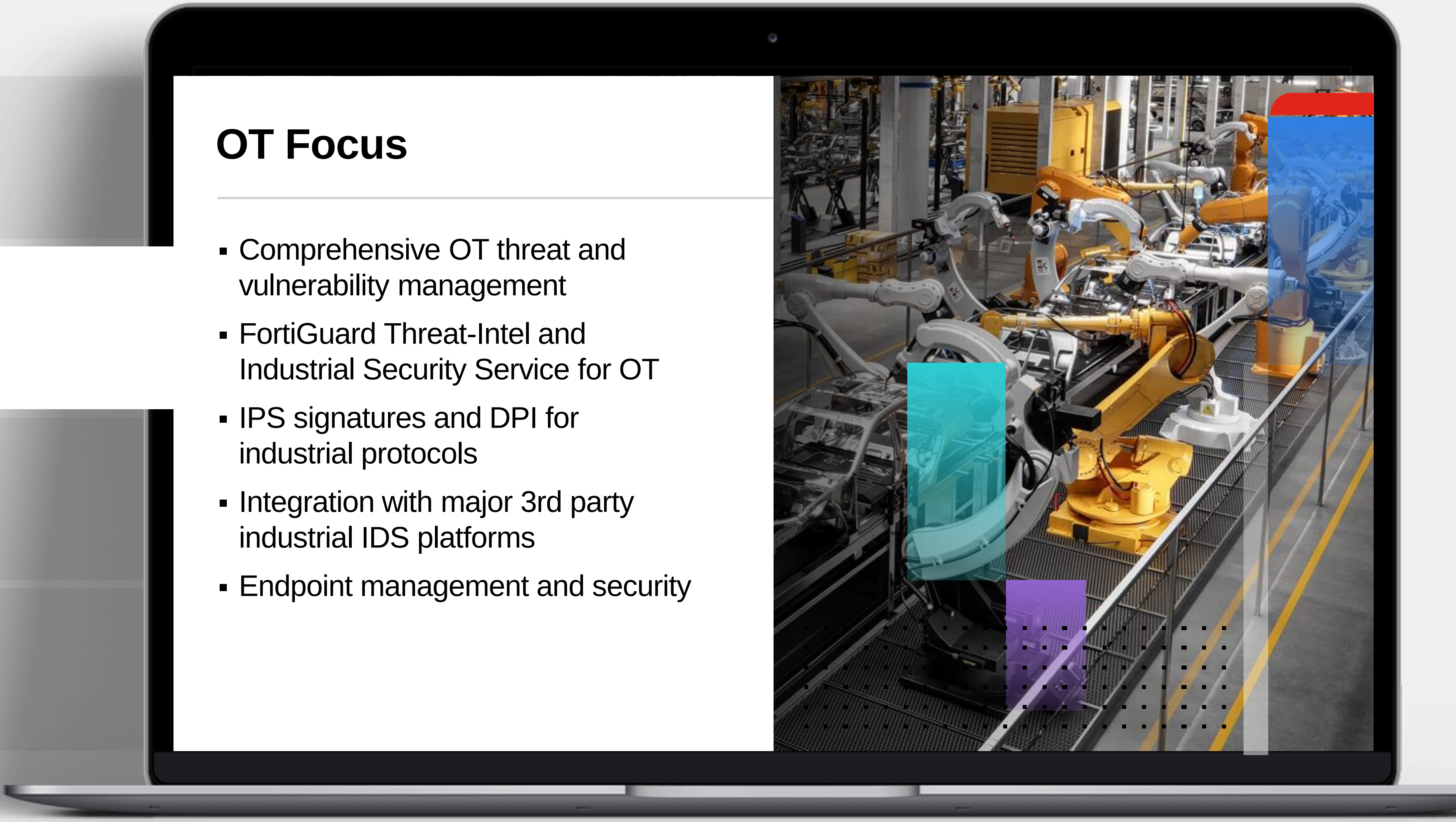
Preserve business continuity and compliance in the face of changing technology and digitalization

Threat Detection and Protection

Threat and Vulnerability Management

Compliance

Accelerated Digitalization



OT Focus

- Comprehensive OT threat and vulnerability management
- FortiGuard Threat-Intel and Industrial Security Service for OT
- IPS signatures and DPI for industrial protocols
- Integration with major 3rd party industrial IDS platforms
- Endpoint management and security

Security Fabric Strategies for OT

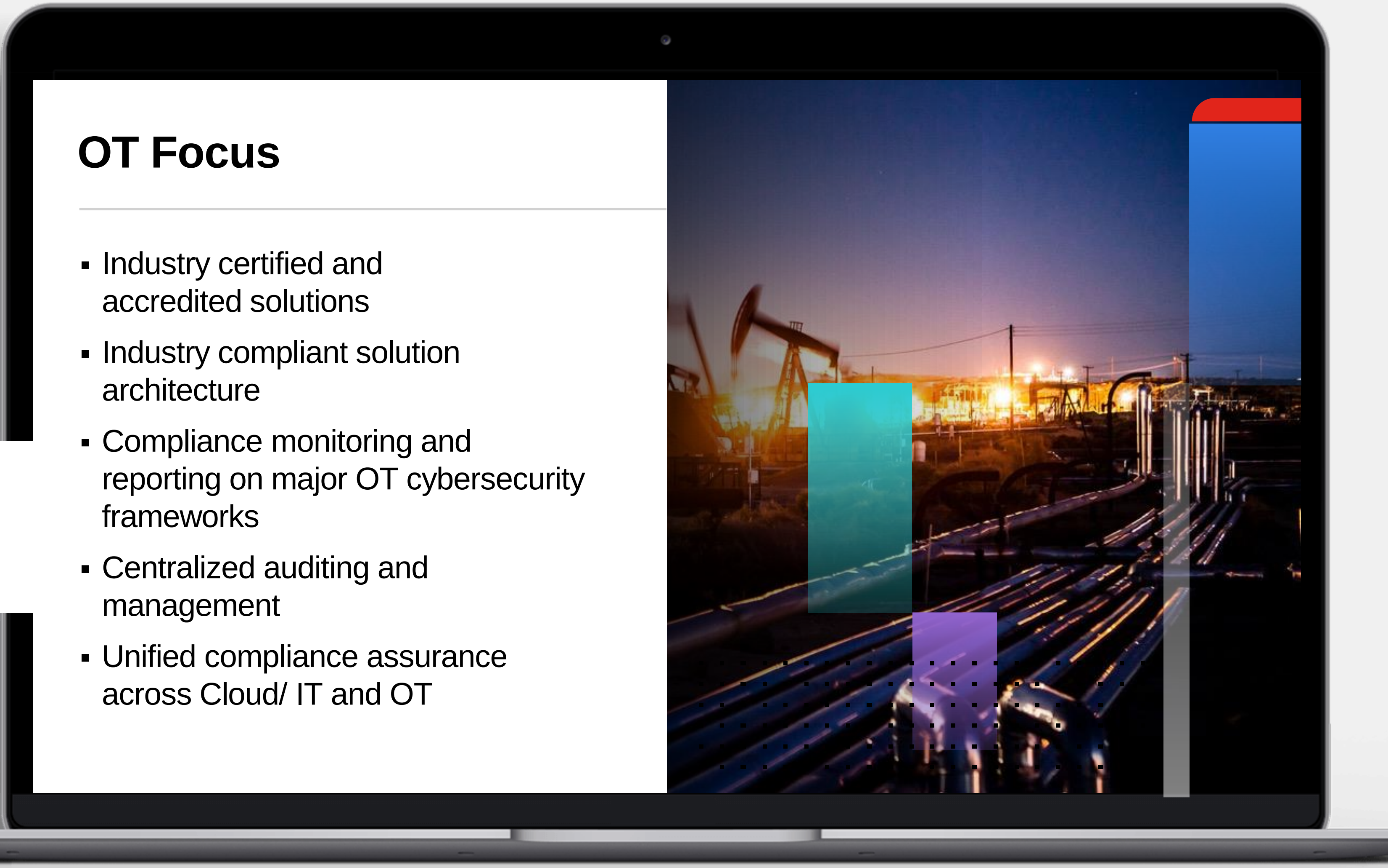
Preserve business continuity and compliance in the face of changing technology and digitalization

Threat Detection and Protection

Threat and Vulnerability Management

Compliance

Accelerated Digitalization



OT Focus

- Industry certified and accredited solutions
- Industry compliant solution architecture
- Compliance monitoring and reporting on major OT cybersecurity frameworks
- Centralized auditing and management
- Unified compliance assurance across Cloud/ IT and OT

Security Fabric Strategies for OT

Preserve business continuity and compliance in the face of changing technology and digitalization

Threat Detection and Protection

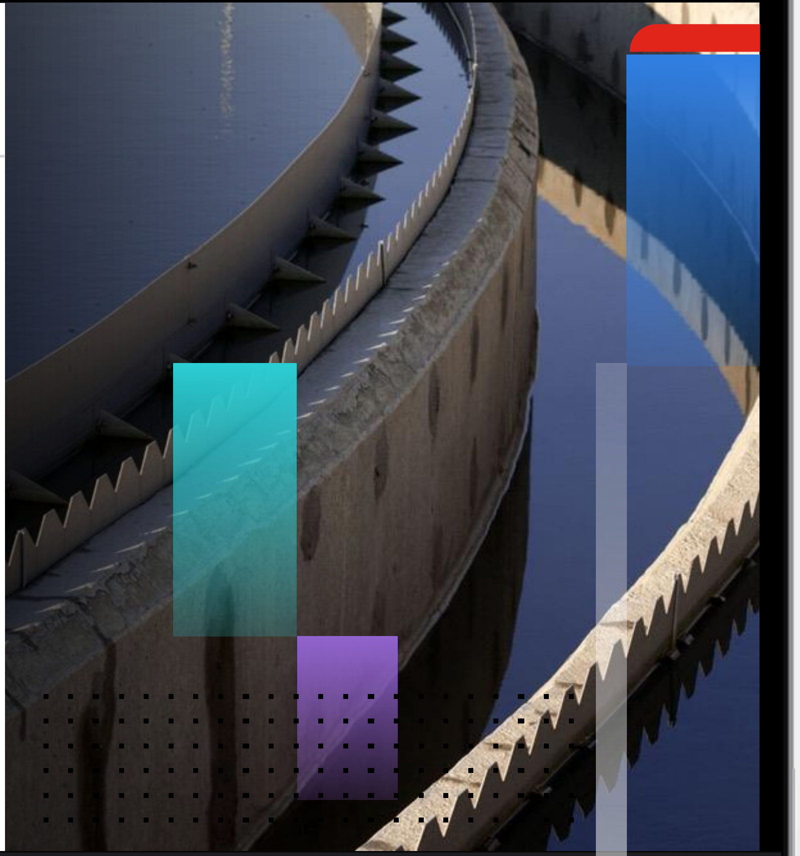
Threat and Vulnerability Management

Compliance

Accelerated Digitalization

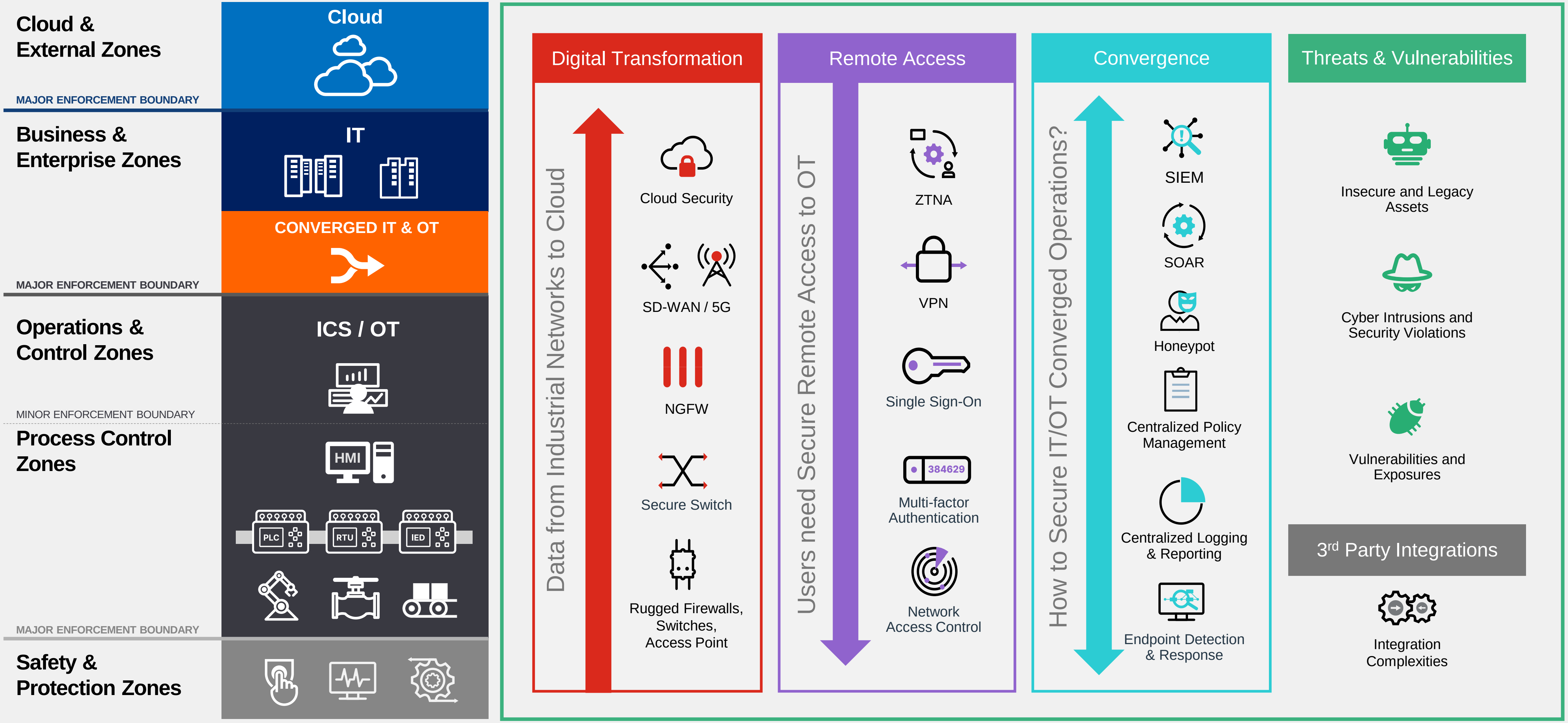
OT Focus

- Specialized solutions for OT
- Secure by design solution architecture
- Security automation and orchestration
- Partnerships and alliances with industrial automation and control system vendors
- Open Fabric integration platform for 3rd parties



OT Security Needs

Common Challenges



Cloud & External Zones

MAJOR ENFORCEMENT BOUNDARY

Business & Enterprise Zones

MAJOR ENFORCEMENT BOUNDARY

Operations & Control Zones

MINOR ENFORCEMENT BOUNDARY

Process Control Zones

MAJOR ENFORCEMENT BOUNDARY

Safety & Protection Zones

Cloud

IT

CONVERGED IT & OT

ICS / OT

Digital Transformation

Data from Industrial Networks to Cloud

- Cloud Security
- SD-WAN / 5G
- NGFW
- Secure Switch
- Rugged Firewalls, Switches, Access Point

Remote Access

Users need Secure Remote Access to OT

- ZTNA
- VPN
- Single Sign-On
- Multi-factor Authentication
- Network Access Control

Convergence

How to Secure IT/OT Converged Operations?

- SIEM
- SOAR
- Honeypot
- Centralized Policy Management
- Centralized Logging & Reporting
- Endpoint Detection & Response

Threats & Vulnerabilities

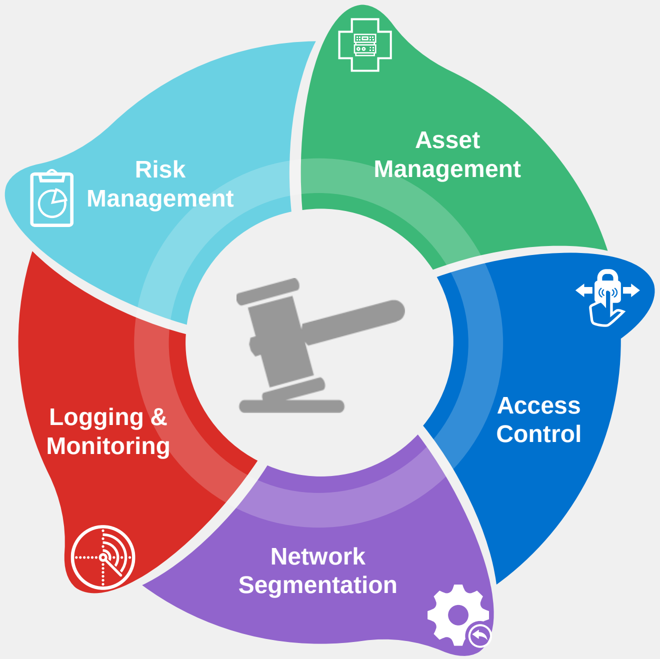
- Insecure and Legacy Assets
- Cyber Intrusions and Security Violations
- Vulnerabilities and Exposures

3rd Party Integrations

- Integration Complexities

Alignment with OT standards & guidelines

Meet compliance requirements with Fortinet Security Fabric



NIS D Pillars
Maps to **NIST CSF**
& IEC 62443

Asset Management	SIEM, NAC, NGFW, API
Access Control to Networks & Assets	NGFW, NAC, FAC, Client, Tokens, Proxy
Segmentation, Protection & Response	NGFW, Switch, WIFI, EDR, Tokens, Proxy
Events, Alerts and Incident Detection	SOAR, SIEM, Analyzer
Risk Management	Manager, SIEM, Analyzer, Tester

Single Pane Management

Threat Intelligence

Interoperability

Restricted Data Flow [FR5]

- *„[…] asset owners need to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information.“*
- Network Segmentation
  - IT and OT
  - Edge computing and cloud analytics
- Primary most common activity
  - Segment off non-control system networks
- Reduce exposure of ICS network (ingress) and spread from ICS network (egress)

Network Segmentation

Restricted Data Flow

As IT and OT converge, the air gap is no longer the first line of defense in restricting data flow. How can Fortinet address the segmentation required for reducing exposure and the spread within an ICS environment?

FortiGate

FortiSwitch

FortiAP

FortiNAC

Industrial Security Approach

Fortinet Security Fabric

Innovate

Industry-leading Accelerated Security

Automate

- **Automated Rules**
- **Federated Upgrades**

Simplify

- **Adaptable Policy**
- **Expanded Coverage**

OS

FortiOS

Appliance

Private Cloud

Public Cloud

Visibility

- Device Profiling
- Device Fingerprint
- IIOT Device Identification
- User Detection & Identification

Control

- ZTNA
- Traffic Steering
- Traffic Shaping

Intelligence

- Event Logging
- Event Correlation
- Automated Response

APT

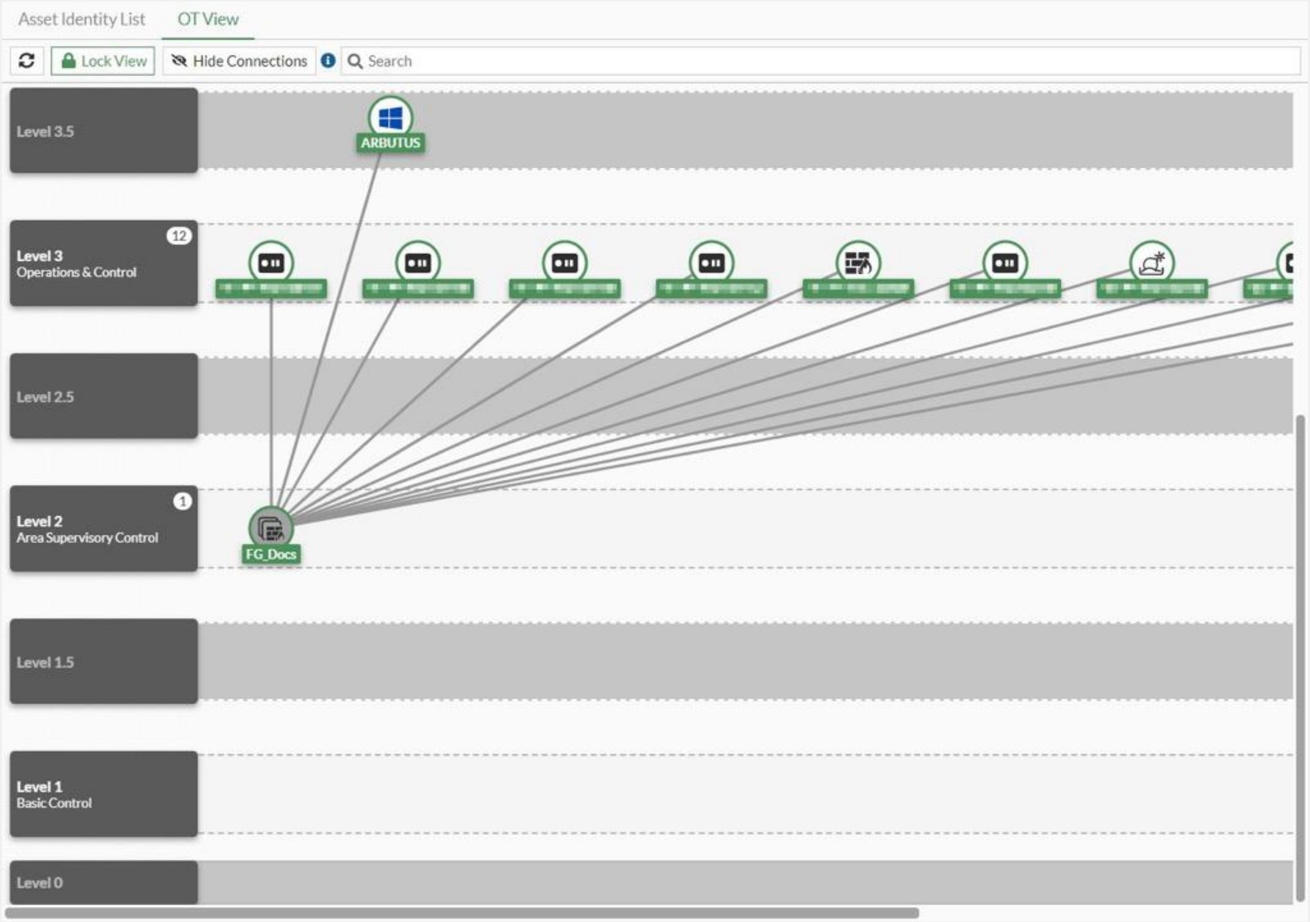
- FortiGuard Labs
- Artificial Intelligence
- Deception Technology
- Sandboxing

Consolidation

Integration

Asset Identity Center – OT View

> “Visualize network assets in Purdue Level based network topology and understand whether the security zones and conduits are implemented correctly and operating as intended.



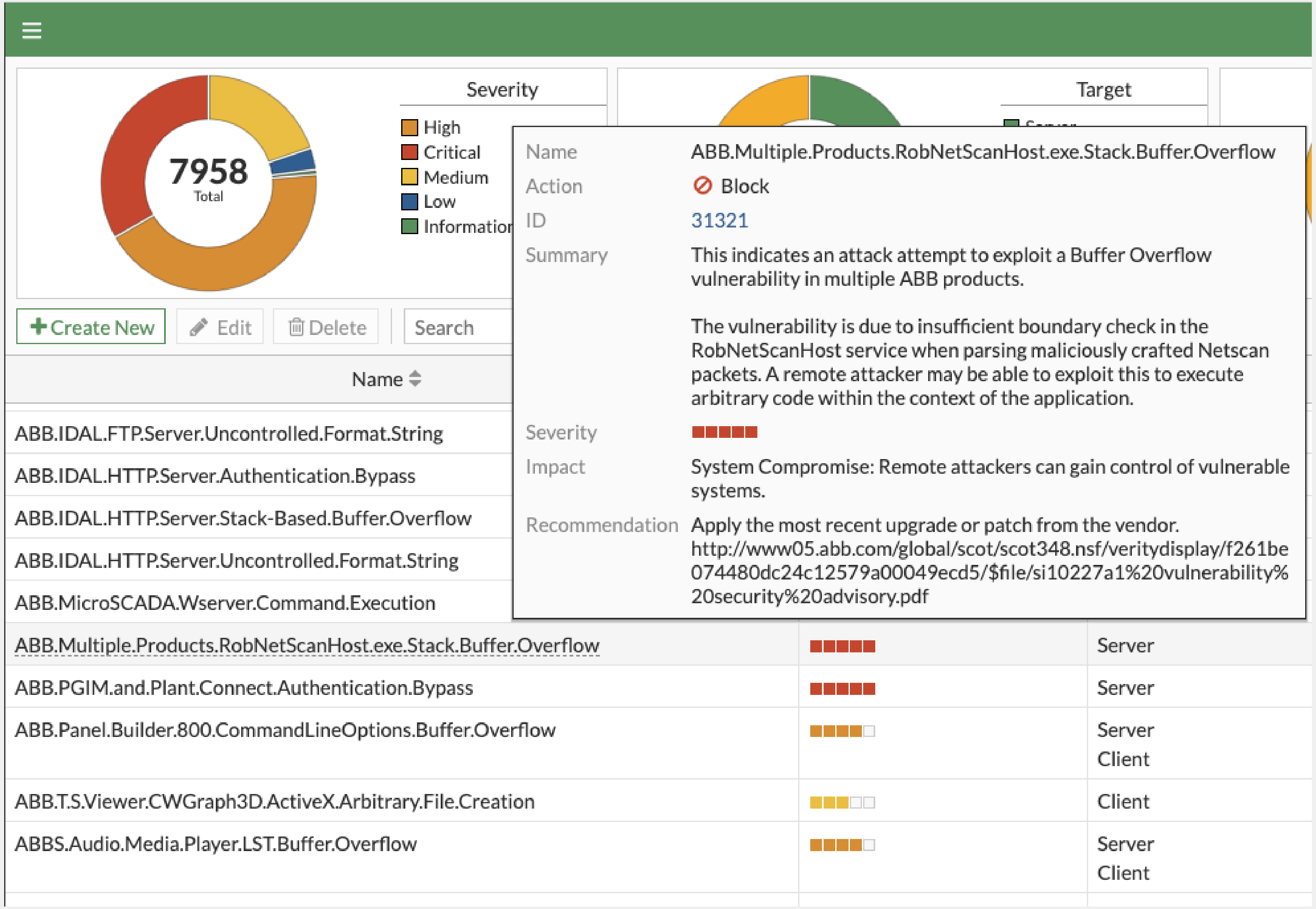
Virtual Patching

Protect Against:

- Known vulnerabilities and zero-day exploits
- Protocol abnormalities

Supports:

- IP exemptions
- Custom logging
- Source quarantine
- Signatures
- Packet



Name: ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow

Action: ⊘ Block

ID: 31321

Summary: This indicates an attack attempt to exploit a Buffer Overflow vulnerability in multiple ABB products.

The vulnerability is due to insufficient boundary check in the RobNetScanHost service when parsing maliciously crafted Netscan packets. A remote attacker may be able to exploit this to execute arbitrary code within the context of the application.

Severity: ■■■■■

Impact: System Compromise: Remote attackers can gain control of vulnerable systems.

Recommendation: Apply the most recent upgrade or patch from the vendor. http://www05.abb.com/global/scot/scot348.nsf/veritydisplay/f261be074480dc24c12579a00049ecd5/$file/si10227a1%20vulnerability%20security%20advisory.pdf

Name		
ABB.IDAL.FTP.Server.Uncontrolled.Format.String		
ABB.IDAL.HTTP.Server.Authentication.Bypass		
ABB.IDAL.HTTP.Server.Stack-Based.Buffer.Overflow		
ABB.IDAL.HTTP.Server.Uncontrolled.Format.String		
ABB.MicroSCADA.Wserver.Command.Execution		
ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow	■■■■■	Server
ABB.PGIM.and.Plant.Connect.Authentication.Bypass	■■■■■	Server
ABB.Panel.Builder.800.CommandLineOptions.Buffer.Overflow	■■■■□	Server Client
ABB.T.S.Viewer.CWGraph3D.ActiveX.Arbitrary.File.Creation	■■■□□	Client
ABBS.Audio.Media.Player.LST.Buffer.Overflow	■■■■□	Server Client

AUG 2023

OT Intrusion Prevention

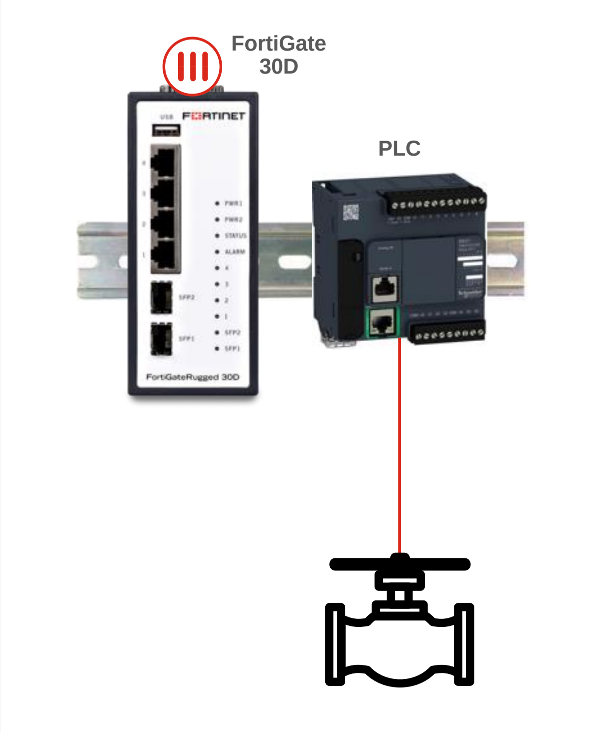
Vulnerability Protection for OT Environments

Top Vendors (since Jan 2022)			
Delta	29	Siemens	8
Schneider	19	WECON	6
Advantech	15	IA	5
Rockwell	9	Sierra Wireless	5
Moxa	8	*Other*	46

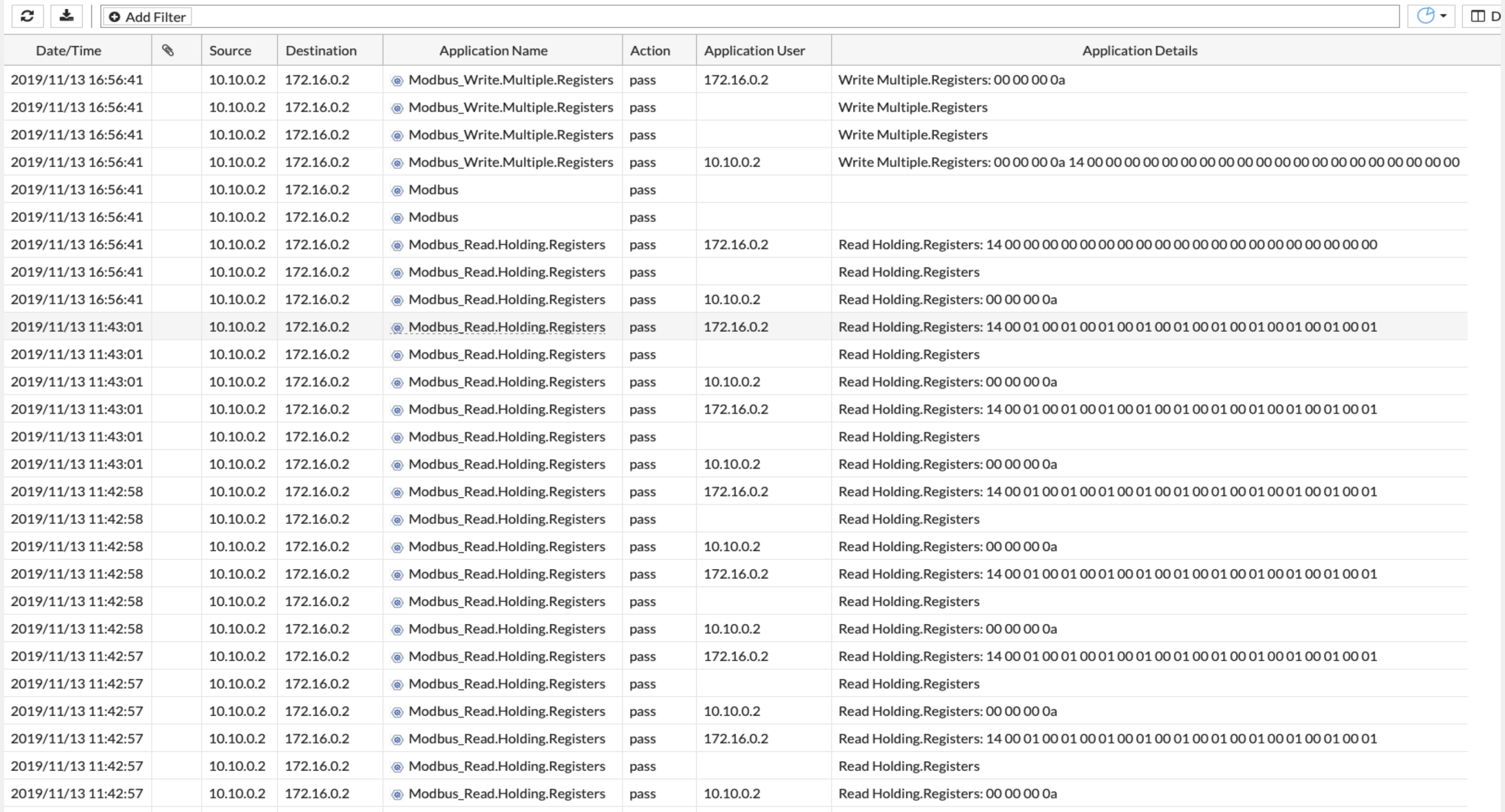
Entire list: https://www.fortiguard.com/encyclopedia?type=isips
Request a signature: https://www.fortiguard.com/faq/ips-contact

Protocol Specific Visibility

Passive deep packet inspection and logging



- Dynamic identification
- Passive visibility



Date/Time	📎	Source	Destination	Application Name	Action	Application User	Application Details
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Write.Multiple.Registers	pass	172.16.0.2	Write Multiple.Registers: 00 00 00 0a
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Write.Multiple.Registers	pass		Write Multiple.Registers
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Write.Multiple.Registers	pass		Write Multiple.Registers
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Write.Multiple.Registers	pass	10.10.0.2	Write Multiple.Registers: 00 00 00 0a 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus	pass		
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus	pass		
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 16:56:41		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:43:01		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:42:58		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	172.16.0.2	Read Holding.Registers: 14 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass		Read Holding.Registers
2019/11/13 11:42:57		10.10.0.2	172.16.0.2	Modbus_Read.Holding.Registers	pass	10.10.0.2	Read Holding.Registers: 00 00 00 0a

Fortinet Secure LAN Edge Delivered by FortiLink

Security-Driven Networking in Action

INTEGRATED SECURITY

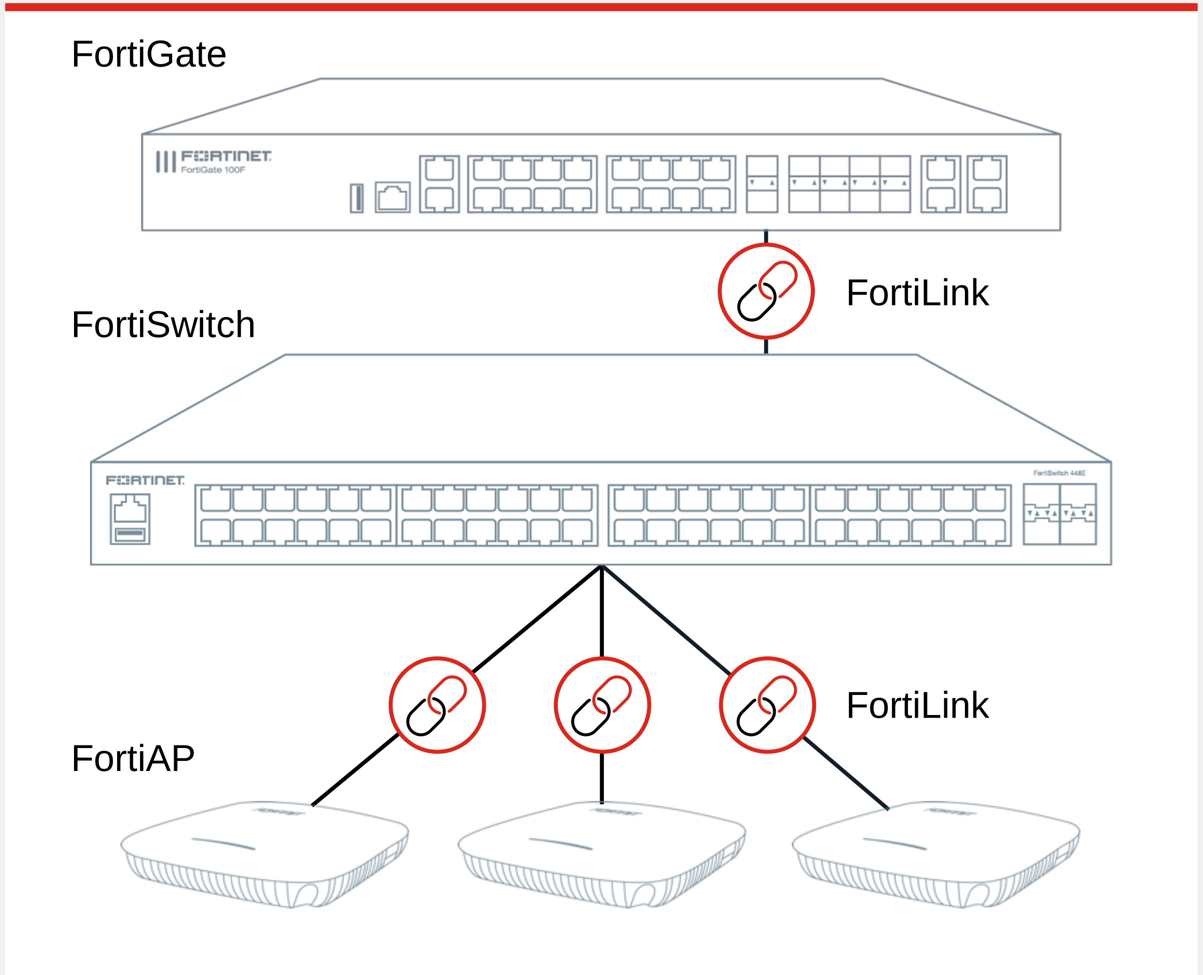
- Extends NGFW features to the LAN
- Base NAC features included
- Giant step beyond centralized management

SIMPLICITY

- Agile deployment and management
- Flexible architecture, scales as needs change

LOWER TOTAL COST OF OWNERSHIP

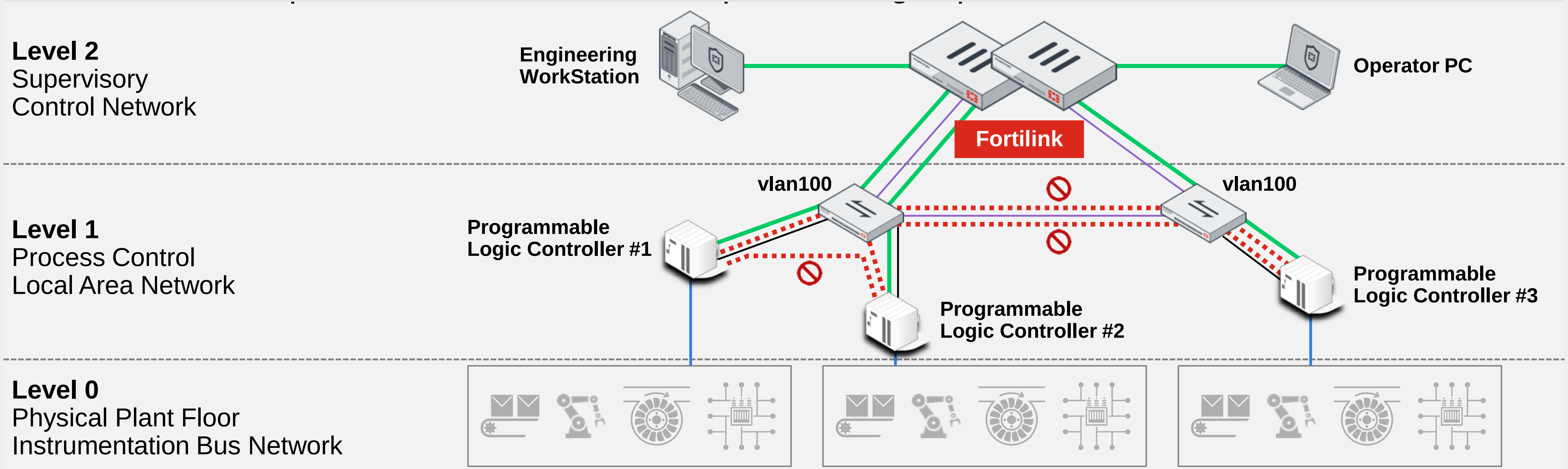
- Included with FortiOS
- No licenses required



MicroSegmentation Access VLAN – Isolate the Hosts

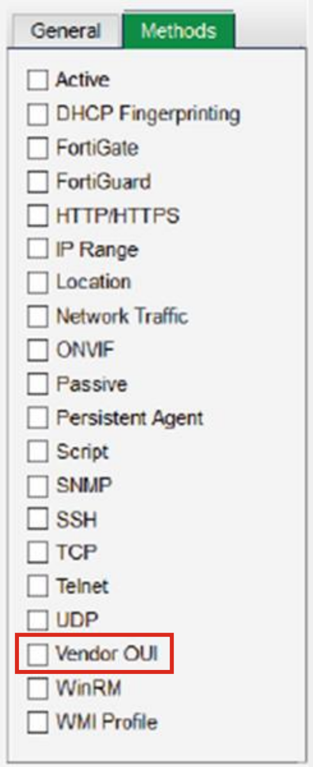
Enabling VLAN in OT with bolt-on NGFW Security

- Provide extra security to the Process Layer: block intra-vlan traffic
  - Hosts are not able to see each other
  - Host can only communicate with the Fortigate
  - The FortiGate implements the allowed access per host or group of hosts



Context MicroSegmentation—FortiNAC

Visibility and control: Device profiling and automatic VLAN assignment



General | Methods

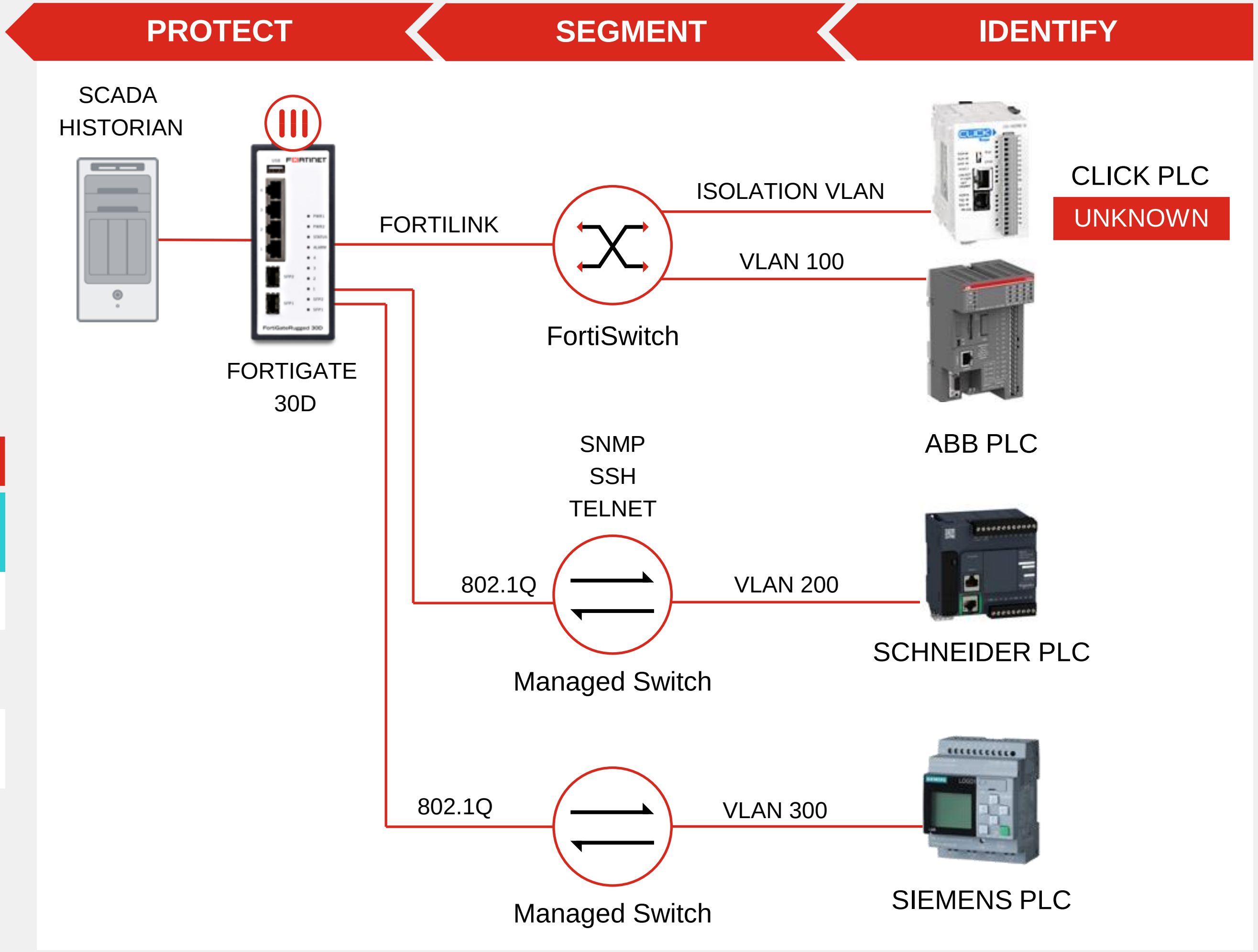
- □ Active
- □ DHCP Fingerprinting
- □ FortiGate
- □ FortiGuard
- □ HTTP/HTTPS
- □ IP Range
- □ Location
- □ Network Traffic
- □ ONVIF
- □ Passive
- □ Persistent Agent
- □ Script
- □ SNMP
- □ SSH
- □ TCP
- □ Telnet
- □ UDP
- □ Vendor OUI
- □ WinRM
- □ WMI Profile

170 Vendors Supported
20 Profiling Methods

APP ID – Protocol (MODBUS)

IPS – Vendor Specific

PROTECT	SEGMENT	IDENTIFY
IPV4 POLICY IN FORTIGATE	SWITCH VLAN	NAC PROFILING CRITERIA
BLOCK	ISOLATION	VENDOR OUI
ALLOW ACCESS TO HISTORIAN	100 - ABB	VENDOR OUI
ALLOW ACCESS TO HISTORIAN	200 - SCHNEIDER	VENDOR OUI
ALLOW ACCESS TO HISTORIAN	300 - SIEMENS	VENDOR OUI



Purdue Level 1 – Process Control

OT Aware Security Fabric

Secure Networking

- Network Segmentation
- Network Microsegmentation
- Secure SD-WAN / SD-Branch
- Web Application Security

Zero Trust Access

- Network Access Control
- Role Based Access Control
- Secure Remote Access

Network Operations

- Logging, Monitoring and Reporting
- Network Operations Center

Security Operations

- Security Automation and Orchestration
- Security Operations Center

Threat Intel & Response

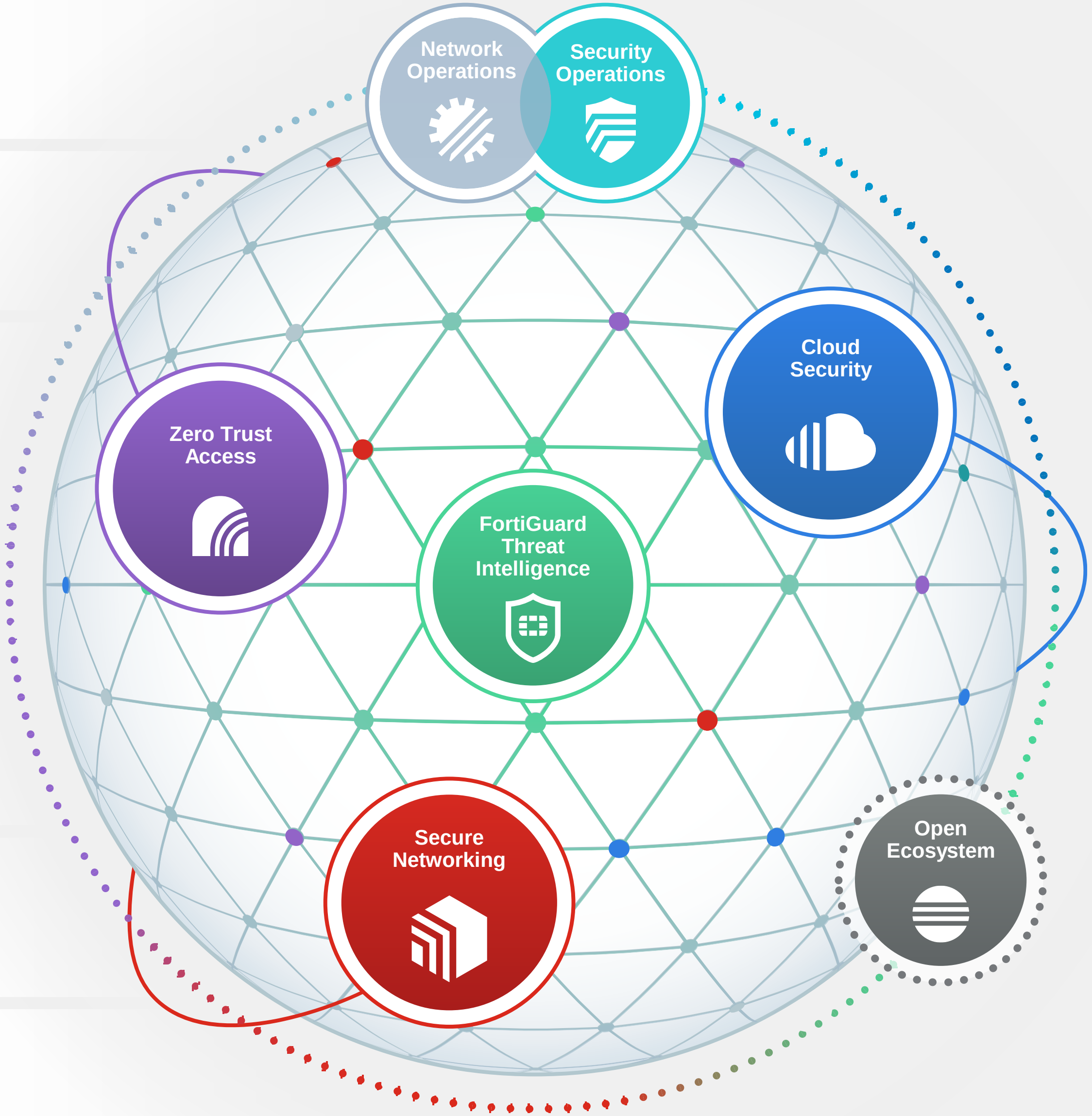
- Endpoint Detection & Response
- Advanced Threat Protection
- Industrial Security Service
- IoT Detection Service

Open Ecosystem

- ICS/OT Security Partners
- Fabric-Ready Partners

Specialized Industrial Solutions

- Rugged Hardware Appliances
- Virtual Machine Appliances
- 3G/4G/5G Wireless Appliances



Appliance

Virtual

Hosted

Cloud

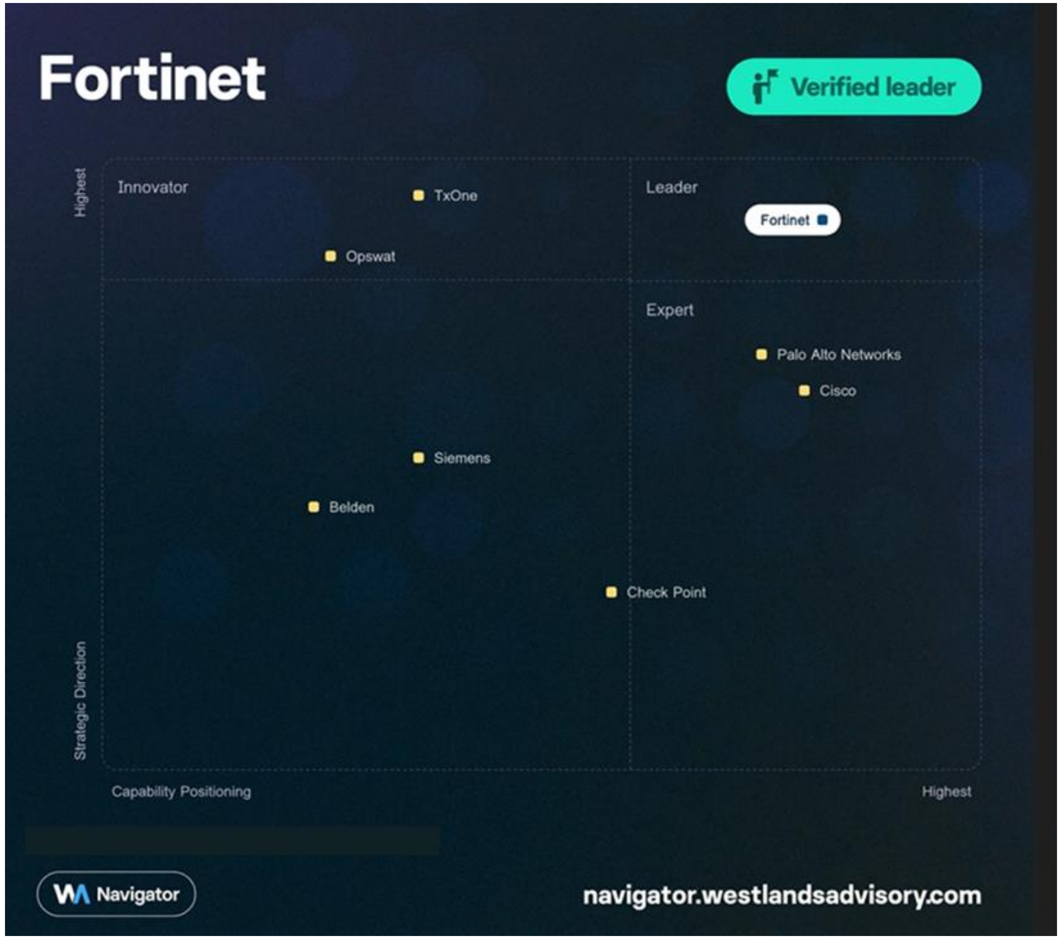
Agent

Container

Fortinet: the lone Leader in the 2023 Network Protection Navigator

Broad, Integrated and Automated OT Aware Security Fabric enables secure digital acceleration for asset owners and IT/OT convergence of security operations

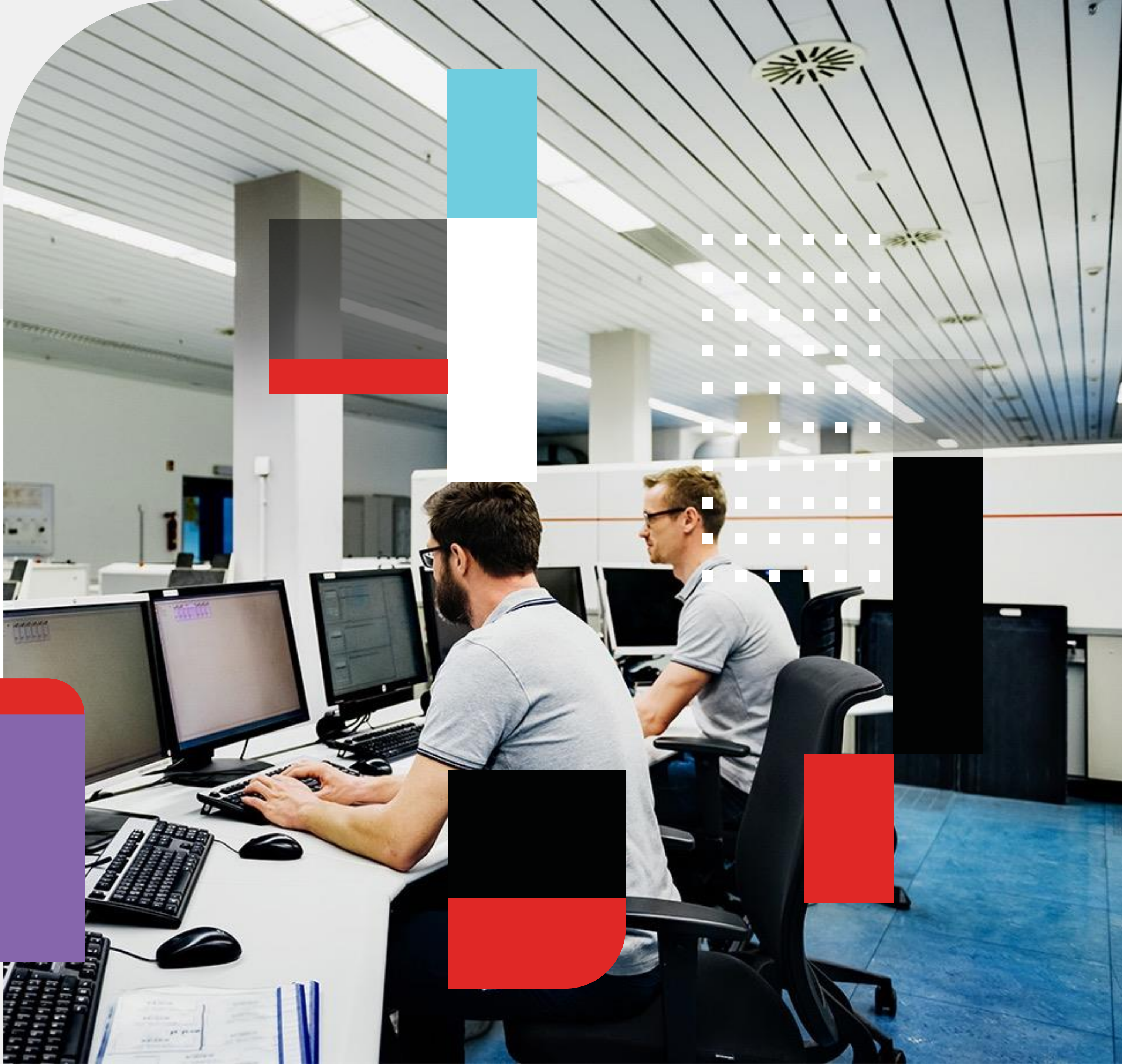
IT/OT Network Security Platform
Navigator 2023



Q&A

THANK YOU

More information
at Fortinet.com/OT



FORTINET®

Daniel Buhmann
Principal Systems Engineer OT / IoT

☎ +49 151 184 837 52
dbuhmann@fortinet.com
https://www.linkedin.com/in/danielbuhmann/

https://ready.fortinet.com/ot