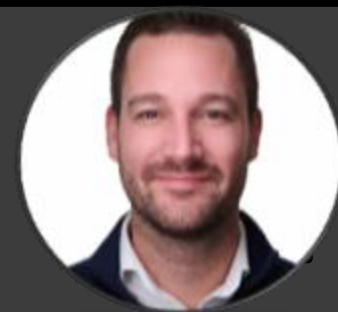


Protecting Operational Technology using the The Platform Journey

Jasper Wubben

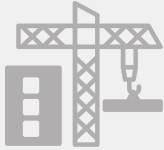
Business Development Manager – Operational Technology (OT)



What is Operational Technology (OT)

Industry 4.0 & Digital Transformation

Mechanization



INDUSTRY 1.0

Mechanization, powered by steam, weaving loom



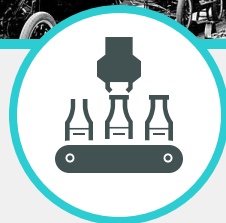
1784

Mass Production



INDUSTRY 2.0

Mass production, assembly line, electrically powered



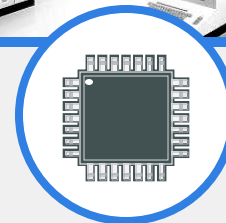
1870

Automation



INDUSTRY 3.0

Automation, Electronics, and computer driven automated Processes



1969

Robotization



INDUSTRY 4.0

Cyber Physical Systems, Internet of Things, Smart Networks for Digital Transformation, **Data Driven Business Decisions.**



TODAY

Mass Customization

≈ 90 years

≈ 100 years

≤ 45 years

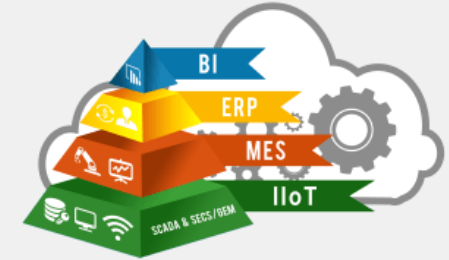
Increased Efficiency

Lower Operational Costs

Real-time Decision Insight



What we need to handle today in OT



- Integration with ERP, CRM.
- Manufacturing uncontrolled Direct Remote Access (Secomea, Tosi, ASEM)
- 4G/5G and Wifi.
- IoT / Industrial IoT connections
- Connection to Public Cloud (IaaS, SaaS)

Supply chain becomes a vector!!!



Challenge: Securing Operational Technology



Challenge: Securing Operational Technology

We All Agree...



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, gives complexity.



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**.



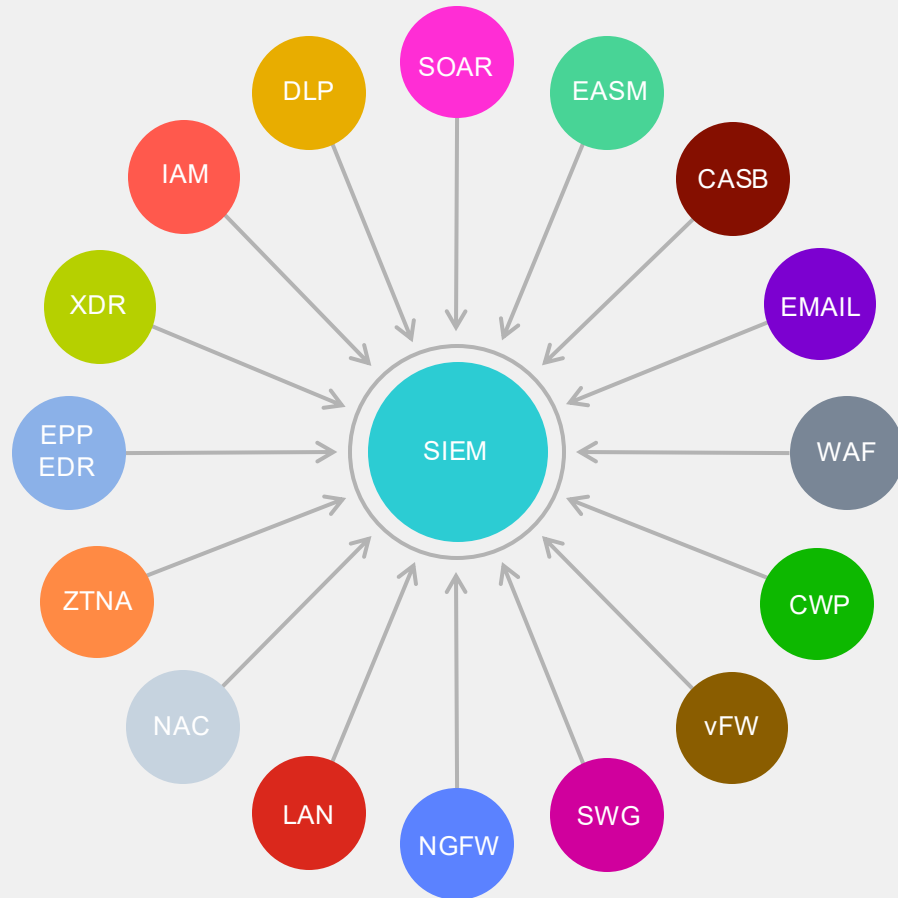
Fortinet Approach: Operational Technology Security Solution



Consolidation of Security Point Product Vendors

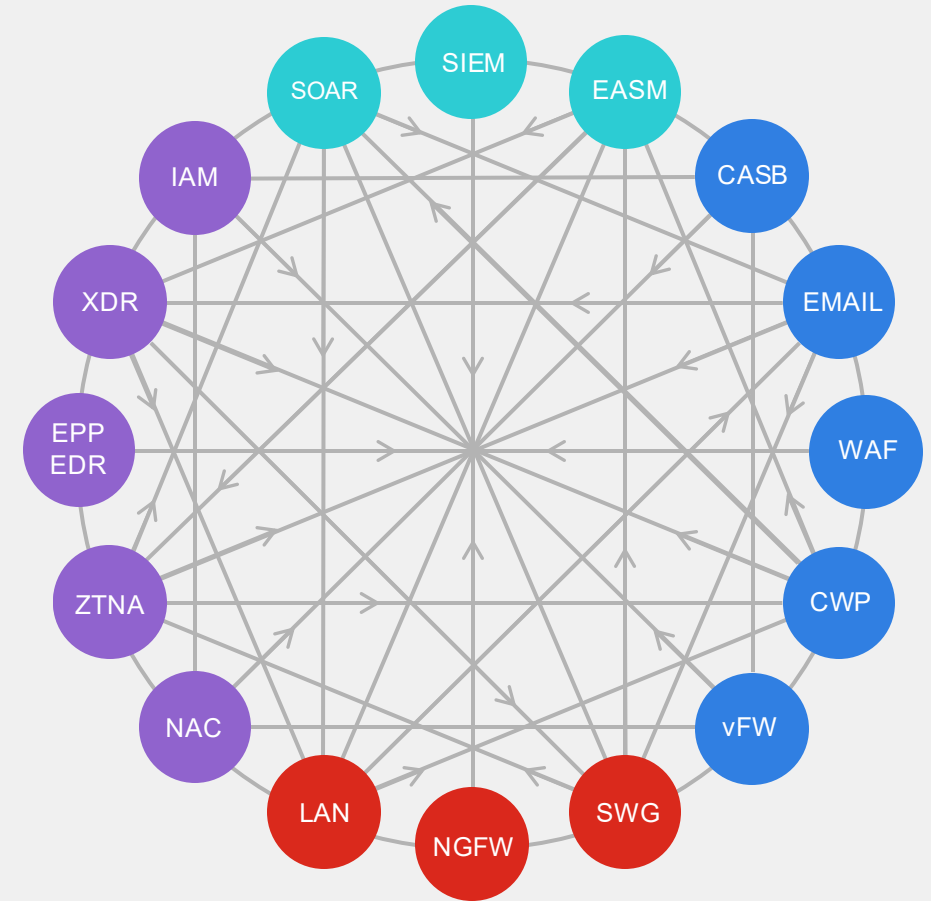
Gartner Cybersecurity Mesh Architecture (CSMA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms



Fortinet Security Fabric

Broad

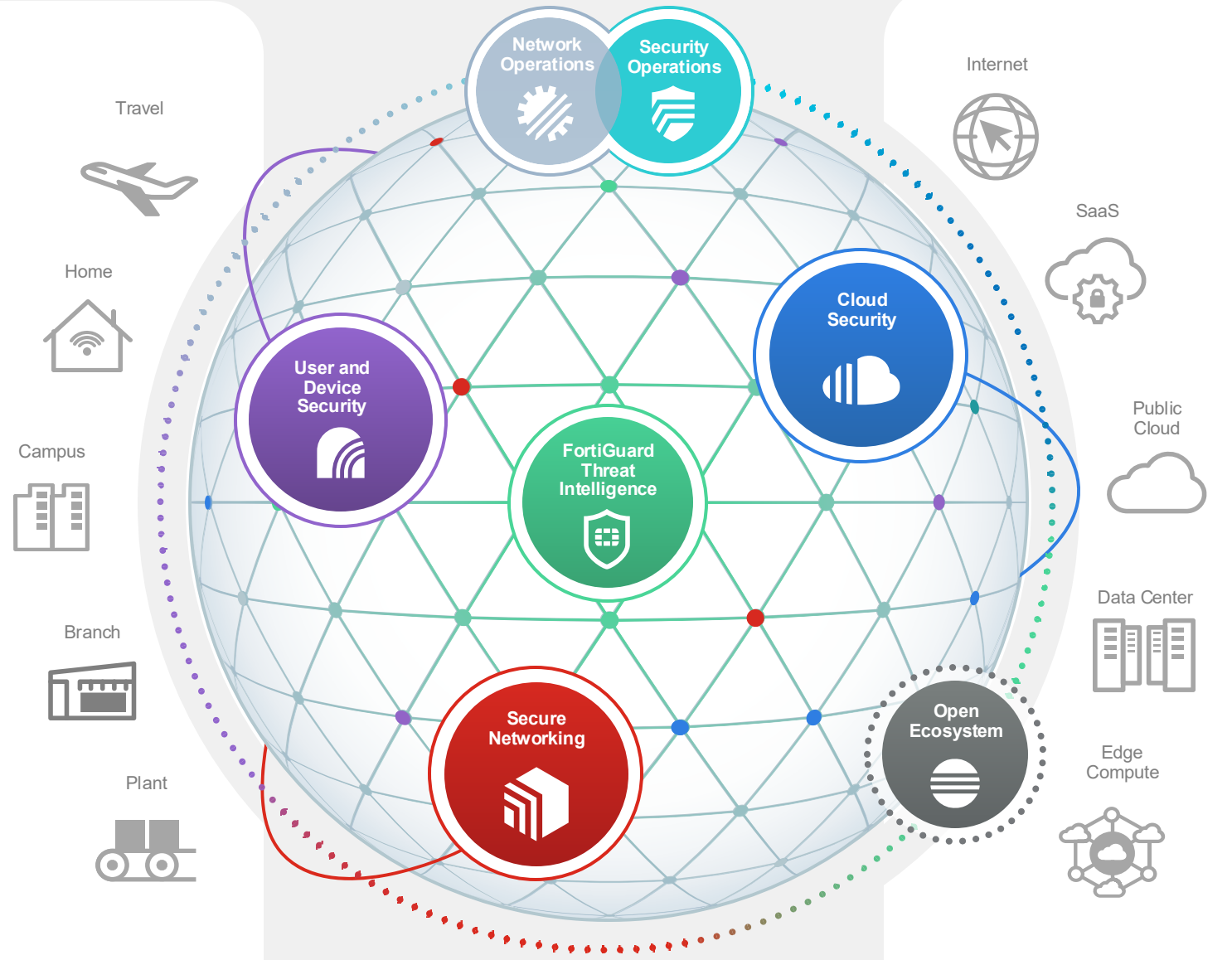
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

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



The only company with the same Operating Systems across ALL Network Security Markets



December 2022 Magic Quadrant for Network Firewalls

September 2025 Magic Quadrant for SD-WAN



March 2025 Magic Quadrant for Wired & Wireless LAN

August 2025 Magic Quadrant for Single-Vendor SASE

April 2024 Magic Quadrant for Security Services Edge


FortiOS Operating System





Best Practice #1: Network Segmentation

Segment the Network into Zones and Implement Security Boundaries



IEC-62443:

Foundational Requirement (FR5) Restricted Dataflow, SR 5.1 Network Segmentation



Segment the Network into Zones and Conduits

Segmentation and Micro segmentation (IA-IEC 62443-3-2)

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

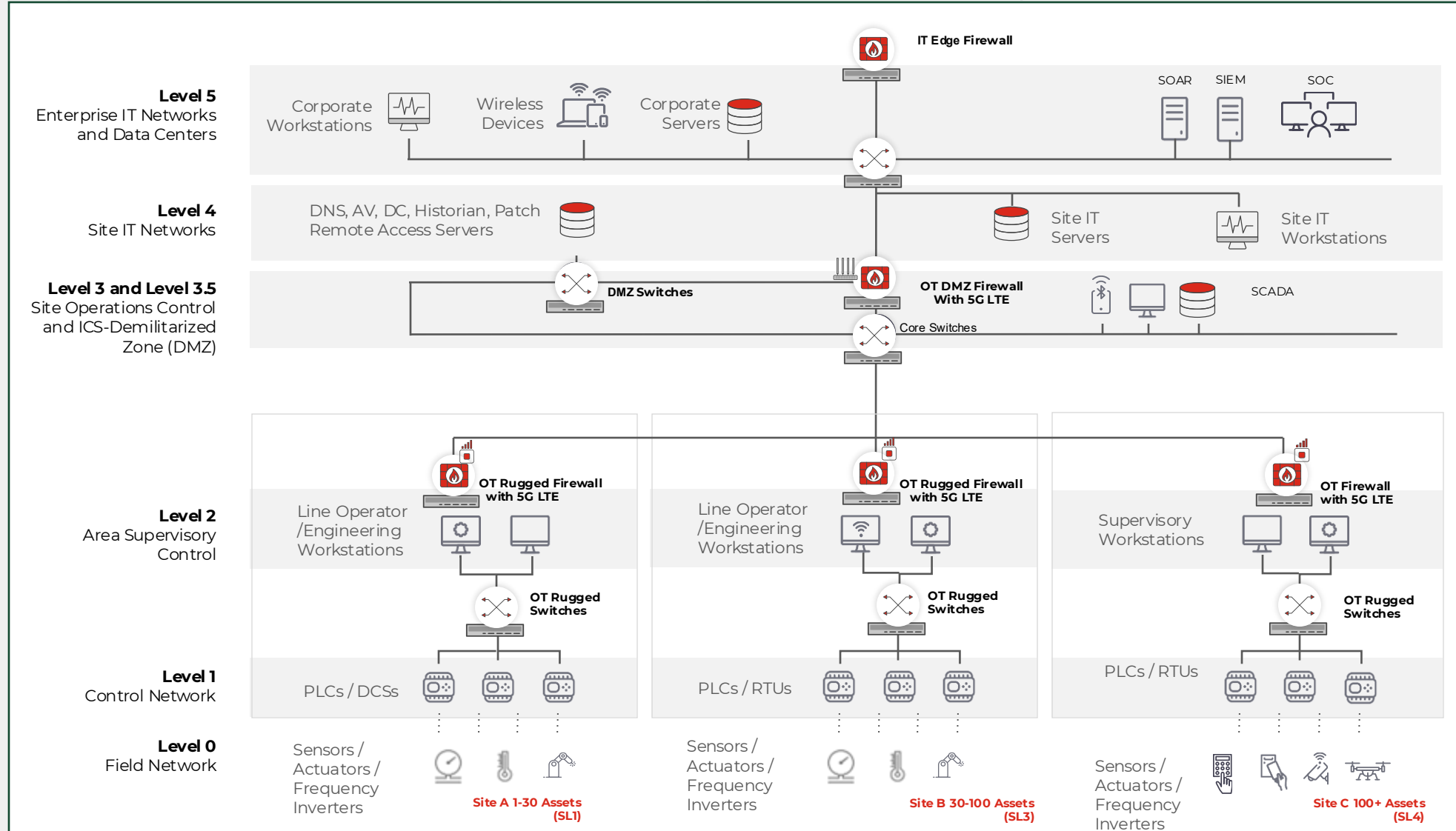
The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer		
FR 5 – SRs and REs					Relevance	Compliance	Solution Description
					IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 5.1 – Network segmentation					Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.1 RE 1 – Physical network segmentation					IACS	None	N: IACS asset owner or manufacturer or integrator need to ensure physical network segmentation for relevant IACS assets.
SR 5.1 RE 2 – Independence from non-control system networks					Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.1 RE 3 – Logical and physical isolation of critical networks					Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks. Applicable for logical segmentation.



Segment the Network into Zones and Conduits

Segmentation and Micro segmentation (IA-IEC 62443-3-2)



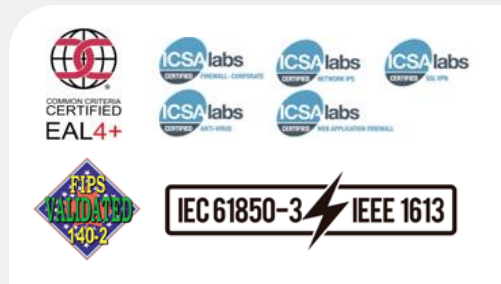
Network Segmentation

Connectivity (5G)
With Secure SDWAN



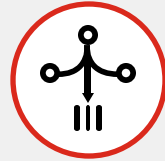
Fortinet Solution Offering for ICS/OT

FortiGate and FortiSwitch Rugged with FortiAP Outdoor



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-50G-5G

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



FGR-70F / FGR-70F-3G4G

SoC4-powered, security and VPN gateway with compact, fanless design



FGR-70G-5G-Dual

Integrated 5G, SD-WAN, Wi-Fi, ZTNA app gateway, and security into one appliance for simplified operations



FGR-60F / FGR-60F-3G4G

SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

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



Rugged FortiSwitches

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 Outdoor 234F/432F

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



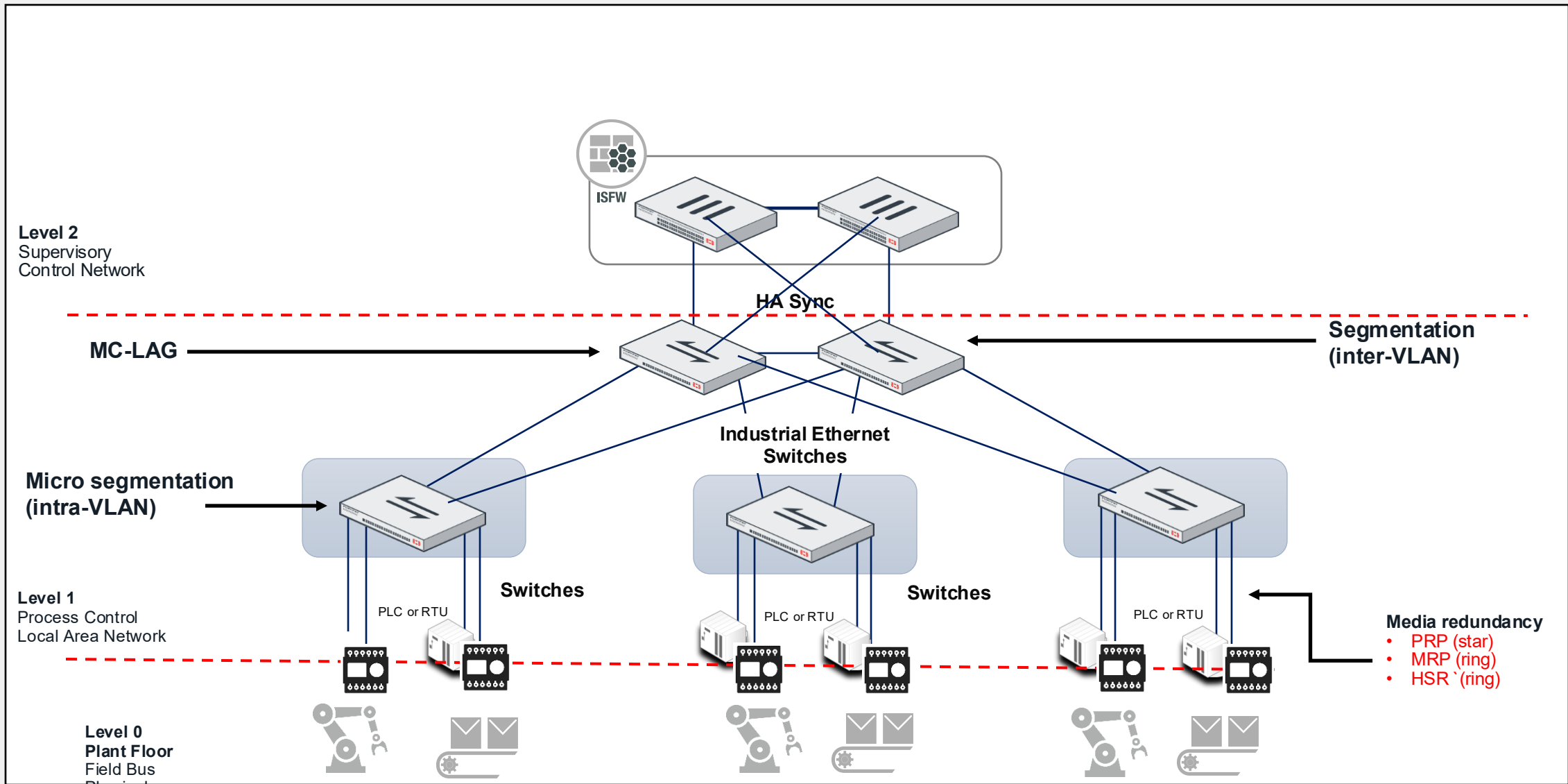
5G Extender

For Secure Connectivity of AGV, Trucks, Mobility.



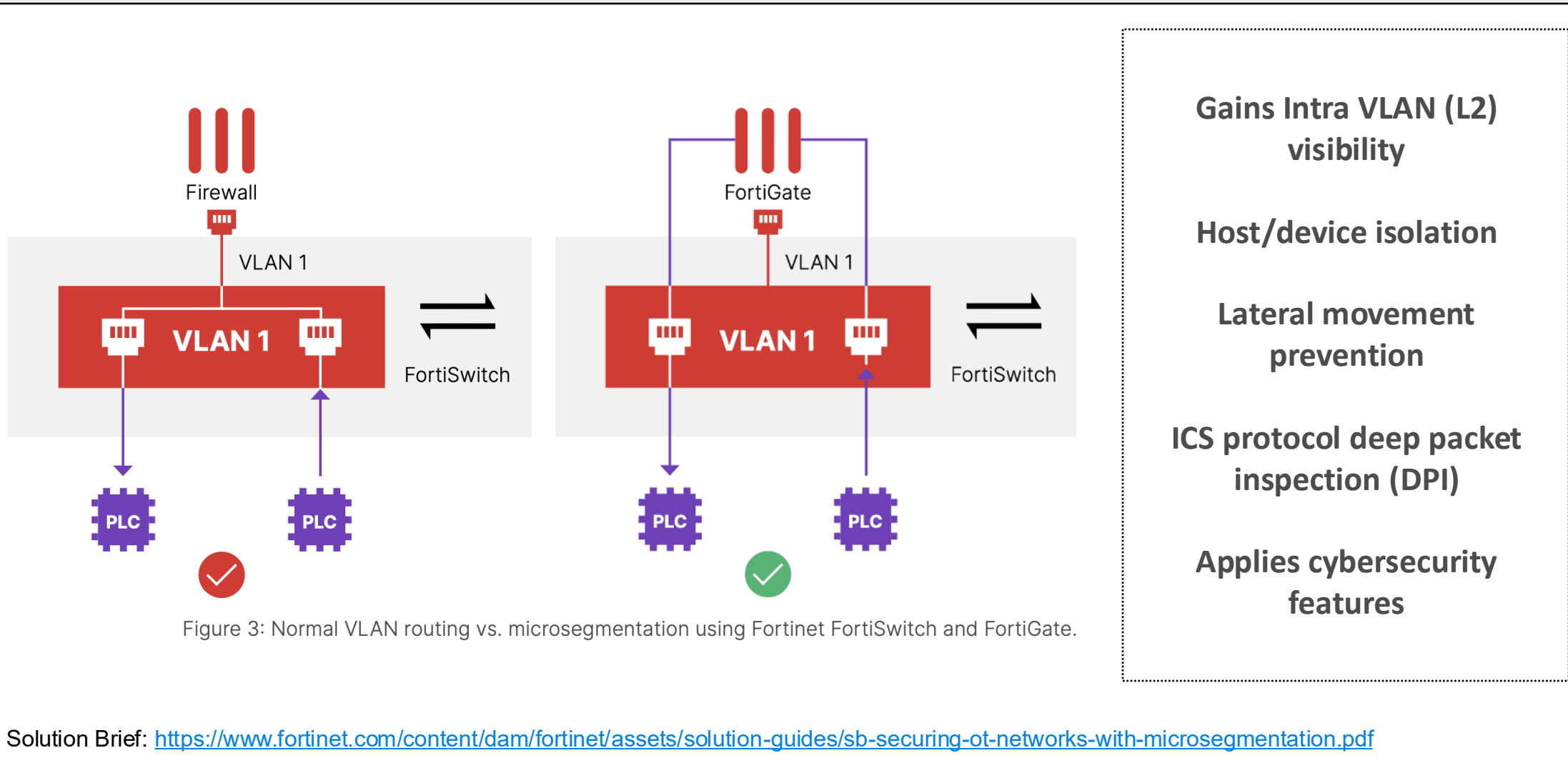
Segment the Network into Zones and Conduits

Segmentation and Micro segmentation (IA-IEC 62443-3-2)



Segment the Network into Zones and Conduits

Segmentation and Micro segmentation (IA-IEC 62443-3-2)





Best Practice #2: Deep OT Visibility and Security Services

Deny by Default, Allow by exception

IEC-62443:

Foundational Requirement (FR5) Restricted Dataflow, SR 5.2.



Deep OT visibility and Security Services

9.4 SR 5.2 – Zone boundary protection

9.4.1 Requirement

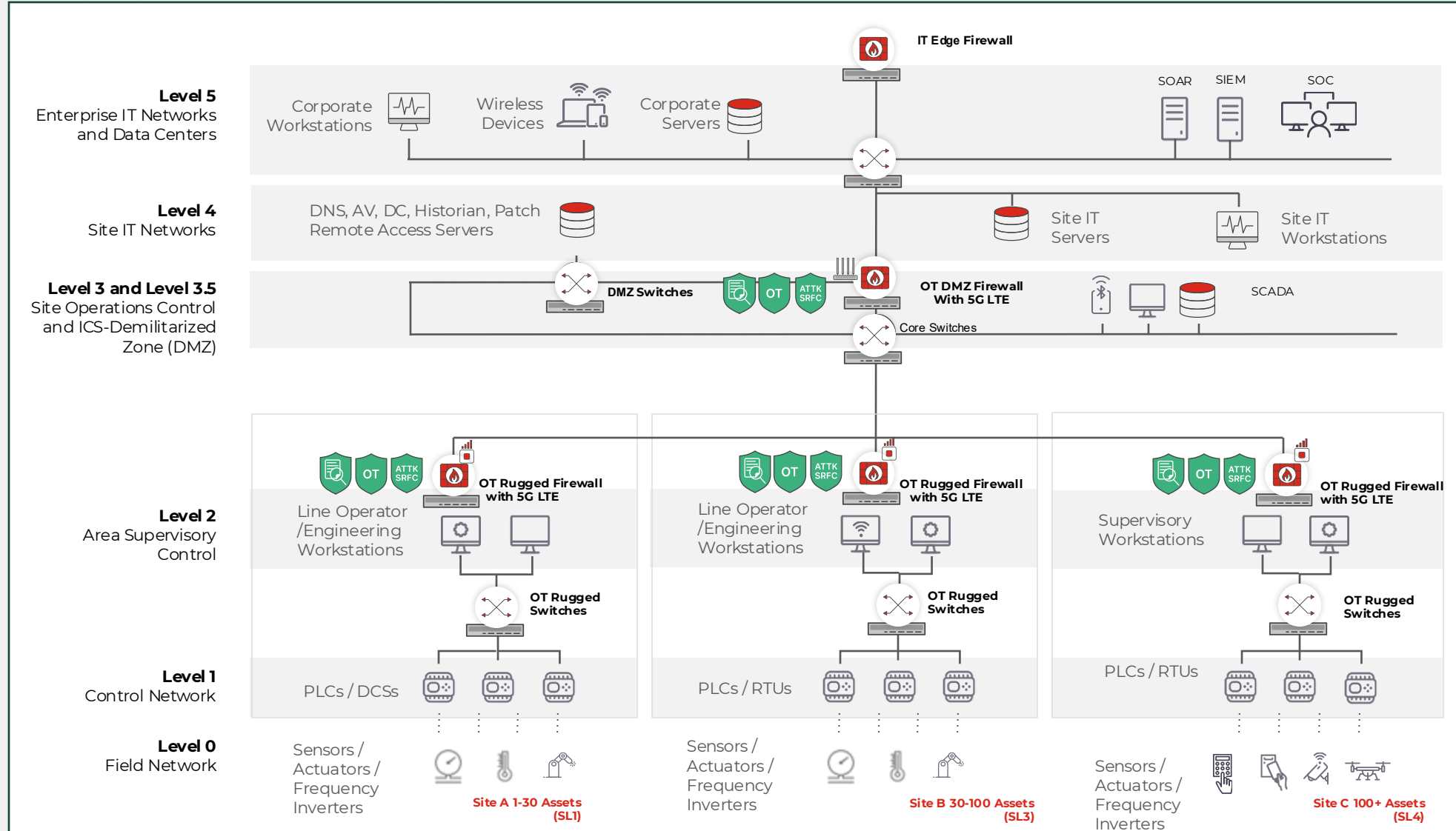
The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer		
FR 5 – SRs and REs					Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 5.2 – Zone boundary protection	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks and centralised logging and monitoring.
SR 5.2 RE 1 – Deny by default, allow by exception		✓	✓	✓	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.2 RE 2 – Island mode			✓	✓	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.
SR 5.2 RE 3 – Fail close			✓	✓	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.
SR 5.3 – General purpose person-to-person communication restrictions	✓	✓	✓	✓	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy.
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications			✓	✓	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy.
SR 5.4 – Application partitioning	✓	✓	✓	✓	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration.



Deep OT Visibility and Security Services

Deny by Default, Allow by exception



Network Segmentation

Connectivity (5G)
With Secure SDWAN

Deep OT Visibility and
Security Services



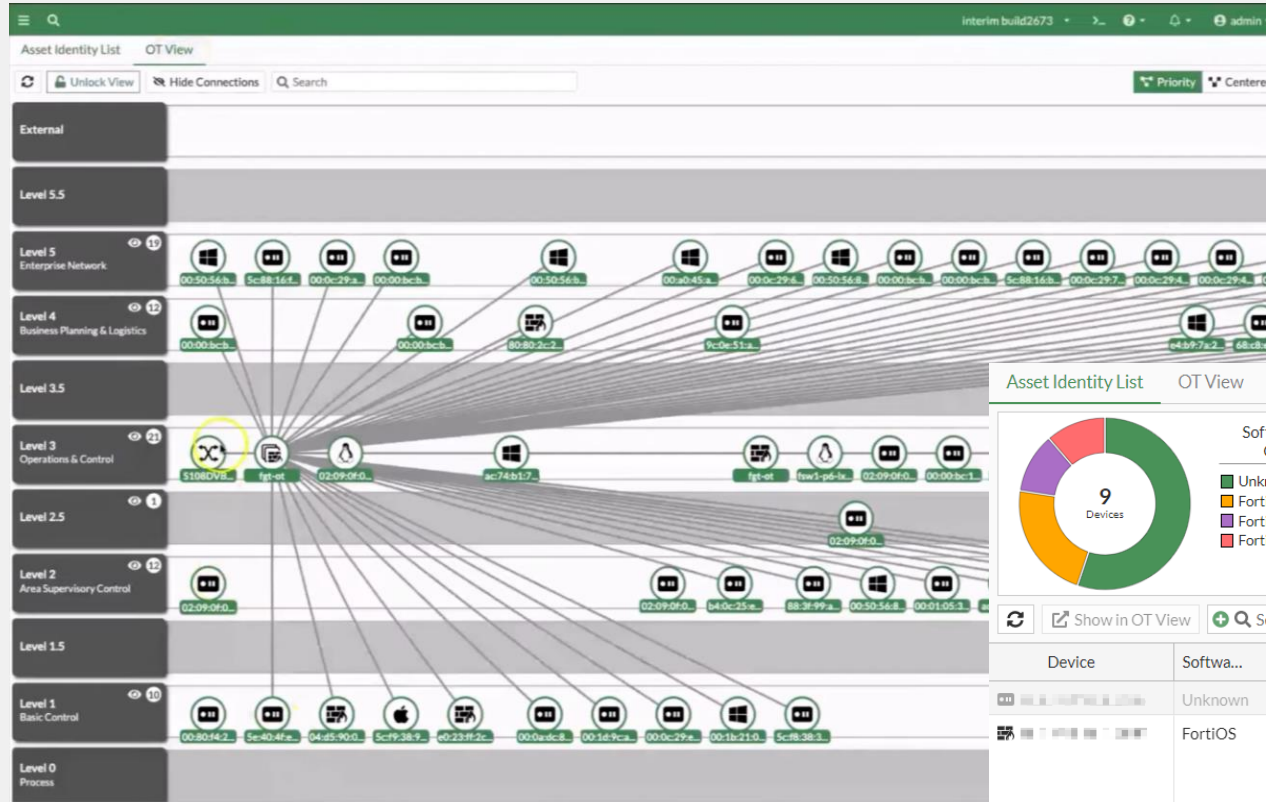
* Pas de maatregelen toe behorende bij het weerstandsniveau (SL1-4) van het object *

© Fortinet Inc. All Rights Reserved.

18

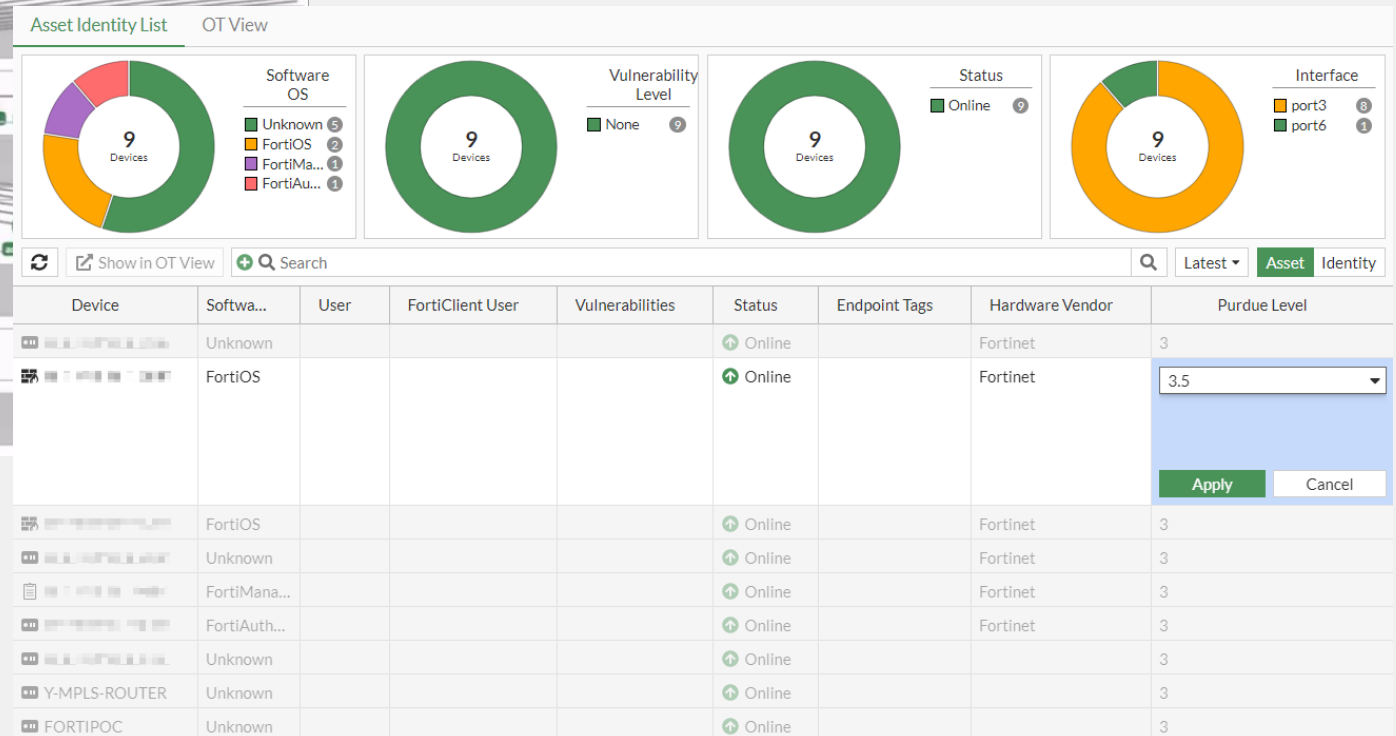
FortiGuard Attack Surface Security Service

(Security, Compliance and Risk Ratings, IoT Detection and IoT Vulnerability Correlation)



“

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



FortiGuard Attack Surface Security Service

(Security, Compliance and Risk Ratings, IoT Detection and IoT Vulnerability Correlation)

OTCSE-FortiGate-OT

Favorites

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Physical Topology

Logical Topology

Security Rating

Automation

Fabric Connectors

External Connectors

Asset Identity Center

Log & Report

Asset Identity List

OT View

9 Devices

Show in OT View

Device

00:0c:29:05:56:e6

ENGWS

HENDRO-PC

00:0c:29:71:2b:25

00:0c:29:71:2b:2f

00:0c:29:71:2b:4d

00:0c:29:71:2b:57

00:0c:29:cb:63:44

55:55:55:55:55:55

View IoT Vulnerabilities for Device ENGWS

Search

Vulnerability ID	Type	Severity	Reference	Description	Patch Signature ID
IoT Application: Mozilla Firefox 110.0 68					
83468	Other		CVE-2009-4102	Sage 1.4.3 and earlier extension for Firefox performs certain opera...	
78103	Other		CVE-2009-2469	Mozilla Firefox before 3.0.12 does not properly handle an SVG ele...	
74293	Other		CVE-2009-1597	Mozilla Firefox executes DOM calls in response to a javascript: URI ...	
68821	Other		CVE-2008-4059	The XPConnect component in Mozilla Firefox before 2.0.0.17 allow...	
65166	Other		CVE-2007-4013	Multiple unspecified vulnerabilities in (1) Net6Helper.DLL (aka Net...	
64530	Other		CVE-2007-2176	Unspecified vulnerability in Mozilla Firefox allows remote attacker...	
64172	Other		CVE-2007-0981	Mozilla based browsers, including Firefox before 1.5.0.10 and 2.x b...	
62984	Other		CVE-2006-5160	** DISPUTED ** Multiple unspecified vulnerabilities in Mozilla Firef...	
62953	Other		CVE-2006-5159	** DISPUTED ** Stack-based buffer overflow in Mozilla Firefox allo...	
62332	Buffer Errors		CVE-2006-2788	Double free vulnerability in the getRawDER function for nsIX509C...	
62314	Other		CVE-2006-2787	EvalInSandbox in Mozilla Firefox and Thunderbird before 1.5.0.4 al...	
62283	Code Injection		CVE-2006-2779	Mozilla Firefox and Thunderbird before 1.5.0.4 allow remote attac...	
61771	Other		CVE-2006-1723	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2...	
61788	Other		CVE-2006-1726	Unspecified vulnerability in Firefox and Thunderbird 1.5 before 1.5...	
61727	Other		CVE-2006-1529	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2...	
61479	Other		CVE-2006-0748	Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before...	
83468	Other		CVE-2009-4102	Sage 1.4.3 and earlier extension for Firefox performs certain opera...	
78103	Other		CVE-2009-2469	Mozilla Firefox before 3.0.12 does not properly handle an SVG ele...	
74293	Other		CVE-2009-1597	Mozilla Firefox executes DOM calls in response to a javascript: URI ...	
68821	Other		CVE-2008-4059	The XPConnect component in Mozilla Firefox before 2.0.0.17 allow...	
65166	Other		CVE-2007-4013	Multiple unspecified vulnerabilities in (1) Net6Helper.DLL (aka Net...	
64530	Other		CVE-2007-2176	Unspecified vulnerability in Mozilla Firefox allows remote attacker...	
64172	Other		CVE-2007-0981	Mozilla based browsers, including Firefox before 1.5.0.10 and 2.x b...	

Close



FortiGuard OT Security Service

(OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules)

Allen-Bradley DF-1 →	Ether-S-Bus →	MMS →	Profinet IO →
Allen-Bradley PCCC →	Ether-S-I/O →	Modbus TCP/IP ⇌	Rockwell FactoryTalk View SE
Beckhoff AMS →	EtherCAT →	Moxa Modbus RTU →	Rockwell FactoryTalk ViewPoint
BSAP	Ethernet POWERLINK	Moxa UDP Device Discovery	Schneider UMAS →
BACnet →	EtherNet/IP-CIP →	MTConnect	SECS-II/GEM →
CC-Link →	FactorySuite NMXSVC	Niagara Fox	Siemens OCG ATCS →
CN/IP CEA-852 →	FL-NET →	oBIX	Siemens LOGO →
CoAP →	GE EGD	OCPP →	Siemens S7 →
DDSI-RTPS	GE SRTP →	Omron FINS →	Siemens S7 1200 →
Digi ADDP →	Hart IP →	OPC AE →	Siemens S7 Plus →
Digi RealPort (Net C/X)	IEC 60870-5-104 ⇌	OPC Common →	Siemens SIMATIC CAMP →
Digi RealPort (Net C/X) DNP3 ⇌	IEC 60870-6 (ICCP/TASE.2) →	OPC DA →	STANAG 4406 Military Messaging
Direct Message Profile →	IEC 61850 →	OPC DA Automation	STANAG 5066
DLMS/COSEM(IEC62056) →	IEC 61850-90-5 R-GOOSE	OPC HDA →	Triconex TSAA →
DNP3 →	IEC 61850-90-5 R-SV	OPC HDA Automation →	TriStation →
ECHONET Lite →	IEEE 1278.2 DIS →	OPC UA →	Veeder-Root ATG
ECOM100	IEEE C37.118 Synchrophasor →	OpenADR →	Vnet/IP
ELCOM 90 →	KNXnet/IP (EIBnet/IP) →	OSIsoft Asset Framework	WITSO
Emerson DeltaV	LonTalk IEC14908-1 CNP →	OSISoft PI	
Emerson ROC	Mitsubishi MELSEC →	Profinet CBA →	

FortiGuard Industrial Security Service provides broader coverage for Industrial Control System and Operational Technology applications and protocols through Application Control (AppCtrl) and IPS signatures. **For an up-to-date list of supported signatures, please visit fortiguard.com.**

→ message layer policy ⇌ message and parameter policy (FortiOS v6.4 and above)





FortiGuard OT Virtual Patching

IEC-62443:
FR 7 Maintenance, SR 7.6 Security Updates



FortiGuard Virtual Patching for OT

IPS OT Signatures

Detect OT/IoT
Network
Assets



Query for
Vulnerabilities



Populate
Asset Identity
Center



Deploy
Virtual Patch
Profile

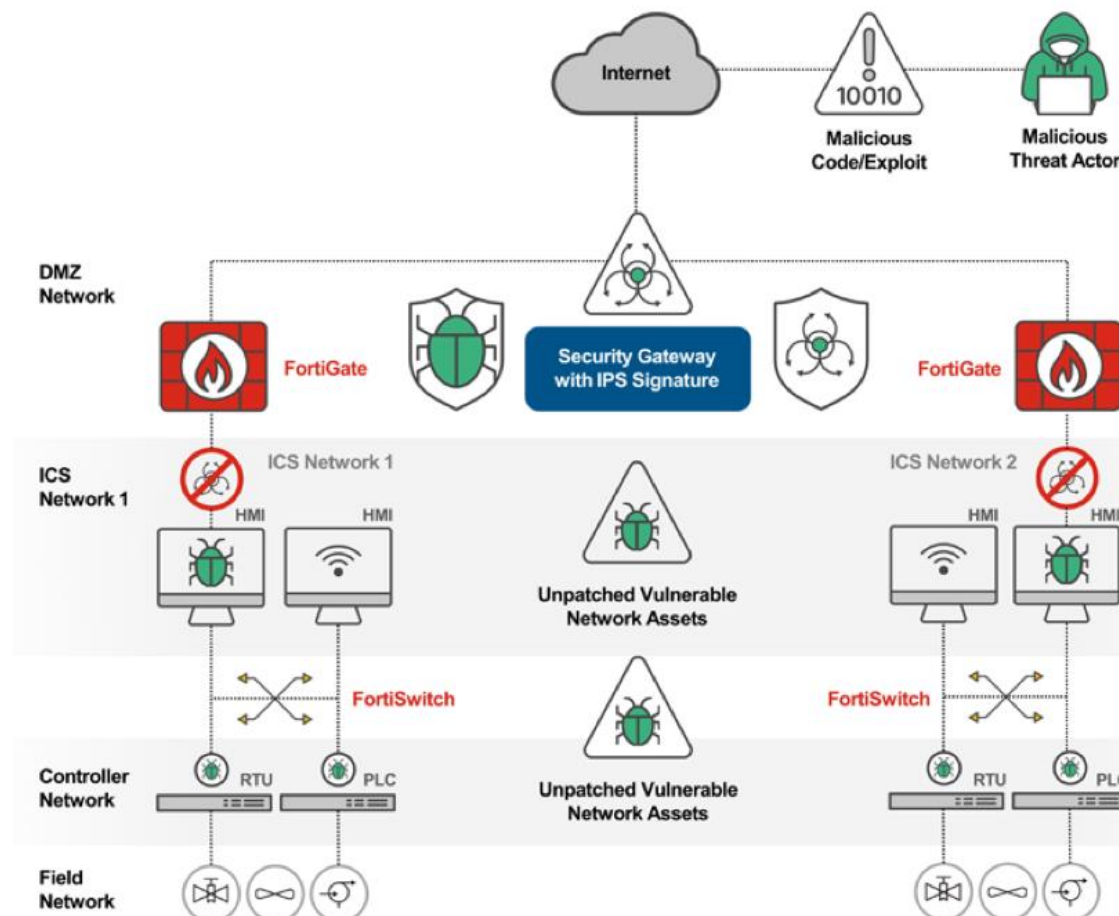


Figure 2: Virtual patching in ICS/OT networks

FortiGuard Virtual Patching for OT

IPS OT Signatures



M580 Safety PLC patches

Last week, on Patch Tuesday, Schneider Electric published a bunch of updates to advisories. Except for one, they were all the Modicon M580 Safety PLC. The latest firmware SV4.21 solves a lot of issues in one go: CVE-2018-7240...7242, CVE-2019-6841...6847, CVE-2021-27779, CVE-2021-22789...22792, CVE-2020-28895, CVE-2020-35198, CVE-2022-37300...37301, CVE-2021-22786, CVE-2022-45788...45789, CVE-2023-25619...25620 and CVE-2023-6408.

Now in itself it is good that the vulnerabilities are solved, but what surprised me is that the oldest one is from 2018. Six years waiting for a patch? You might think that perhaps it wasn't a dangerous vulnerability? Not quite so – CVSS score 9.8 for CVE-2018-7241. Remember that this is a safety PLC, can the safety of the system still be guaranteed when it is hacked?

Why does it have to take so long? Obviously, a safety PLC firmware bug isn't "quickly" solved. The functionality of the safety PLC needs to be guaranteed, so a lot of testing and certification (by Schneider and notified bodies like TuV) is needed: SIL3/IEC 61508/IEC 61511, SIL CL3/IEC 62061, PLe Cat. 4/ISO 13849-1, CIP Safety IEC 61784-3. Not trivial indeed. Notified bodies are busy, may take half a year or so. But – six years? That the patch works is not too difficult to determine – it is also in the "normal" M580 CPU, so any problems there would be quickly known, no need to wait for multiple years just to be sure. Anyway, only Schneider can say why it took so long.

Of course patches could have been provided earlier, if Schneider wanted to do so: in 2018, 2019, 2020, 2021, 2022, 2023 and 2024. This would have meant a lot of work for asset owners. Updating all vulnerabilities together in one go, M580 Safety PLC owners will love it, only one patch round instead of a dozen! Probably also saves on additional testing and recertification of the systems the M580 Safety PLC is protecting on the





Best Practice #03: Monitor and Control Access to Digital Assets and Networks



IEC-62443:

Foundational Requirement (FR1), SR 1.1 Human user Identification and Authentication



IEC/ISA 62443-3-3

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

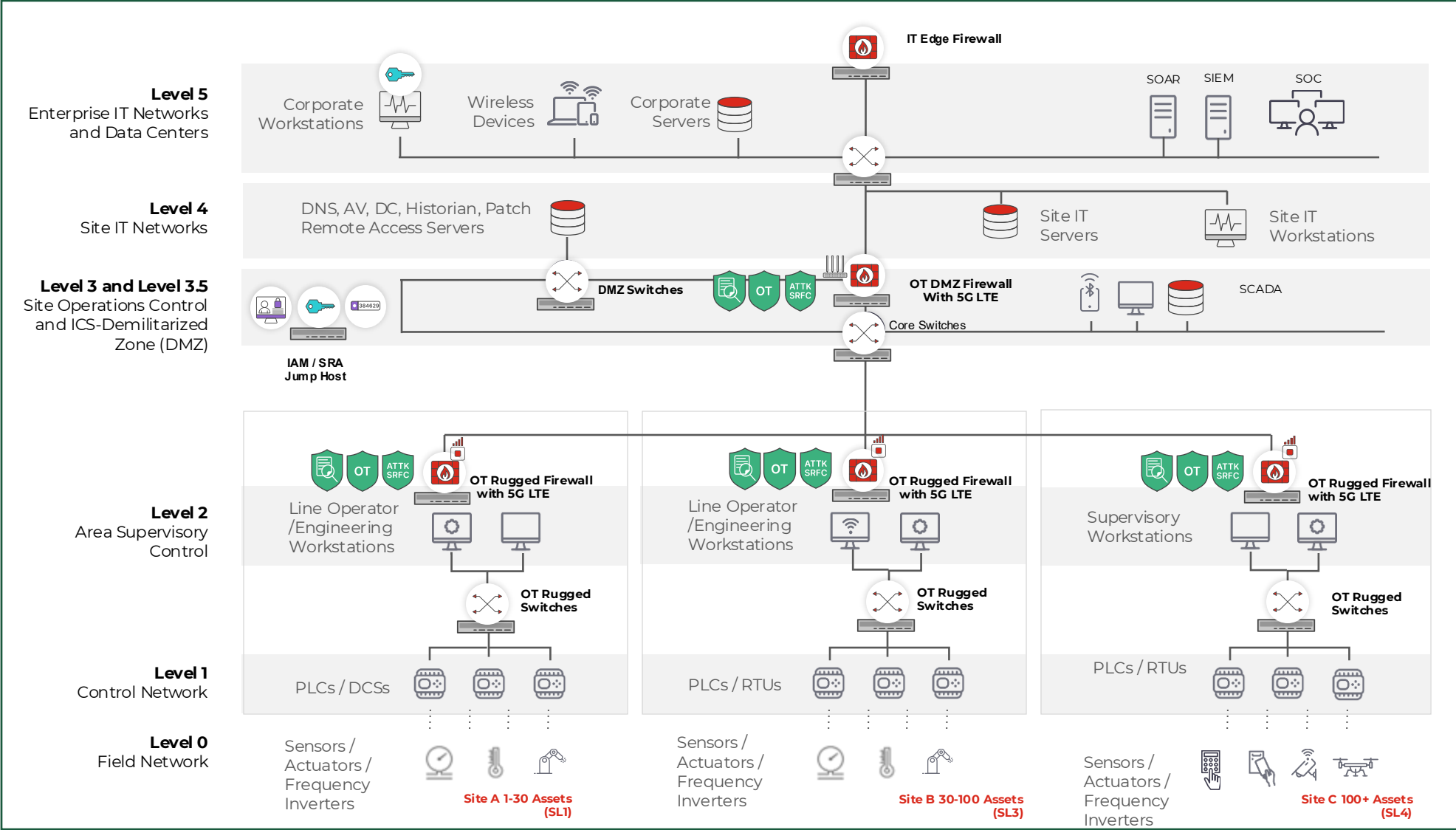
Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and authentication control (IAC)					FR 1 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager		
FR 1 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.1 RE 1 – Unique identification and authentication		✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiPAM C: Product(s) integration.
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration.
SR 1.1 RE 3 – Multifactor authentication for all networks				✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration.



Monitor and Control Access to Digital Assets and Networks

Zero Trust for OT



Network Segmentation

Connectivity (5G)
With Secure SDWAN

Deep OT Visibility and
Security Services

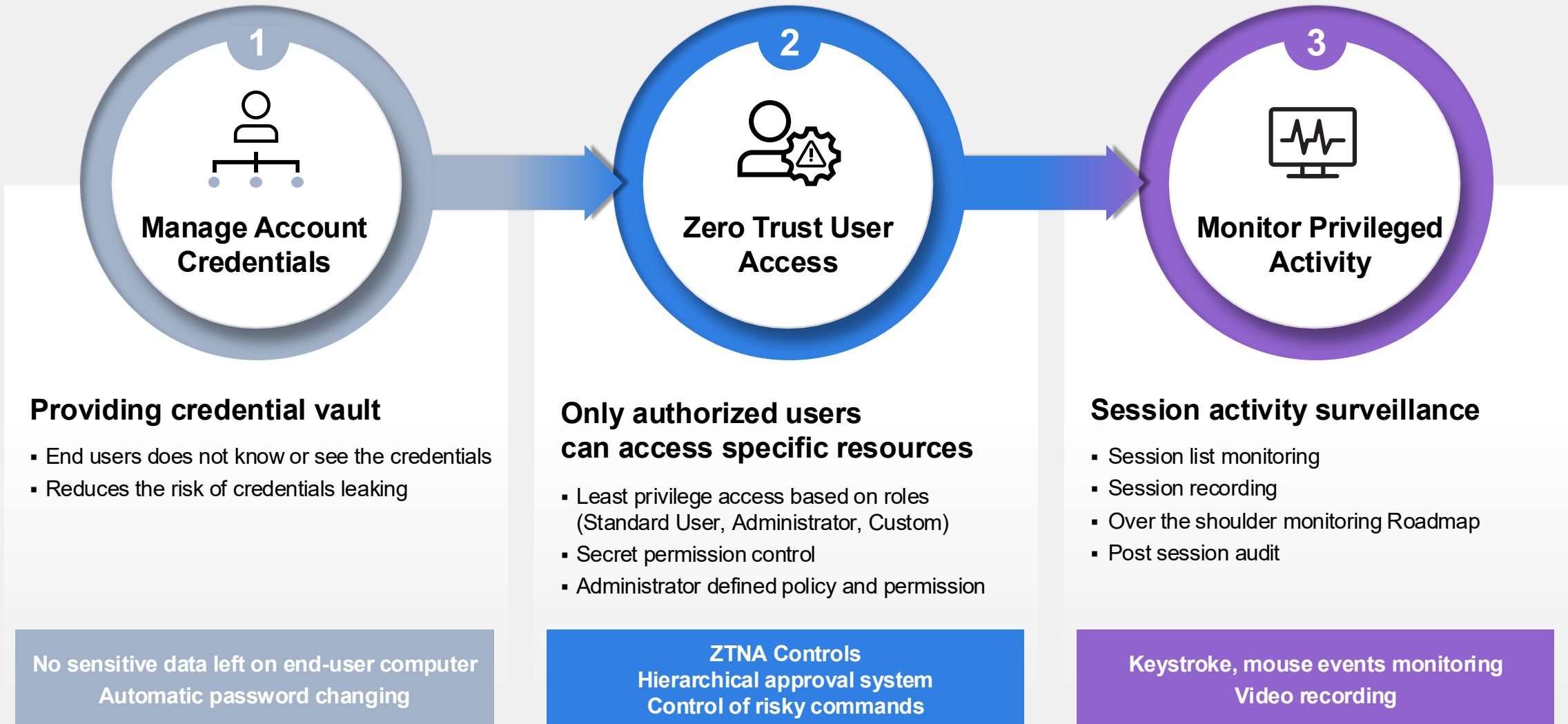
Zero-Trust Access
for OT



* Pas de maatregelen toe behorende bij het weerstandsniveau (SL1-4) van het object *

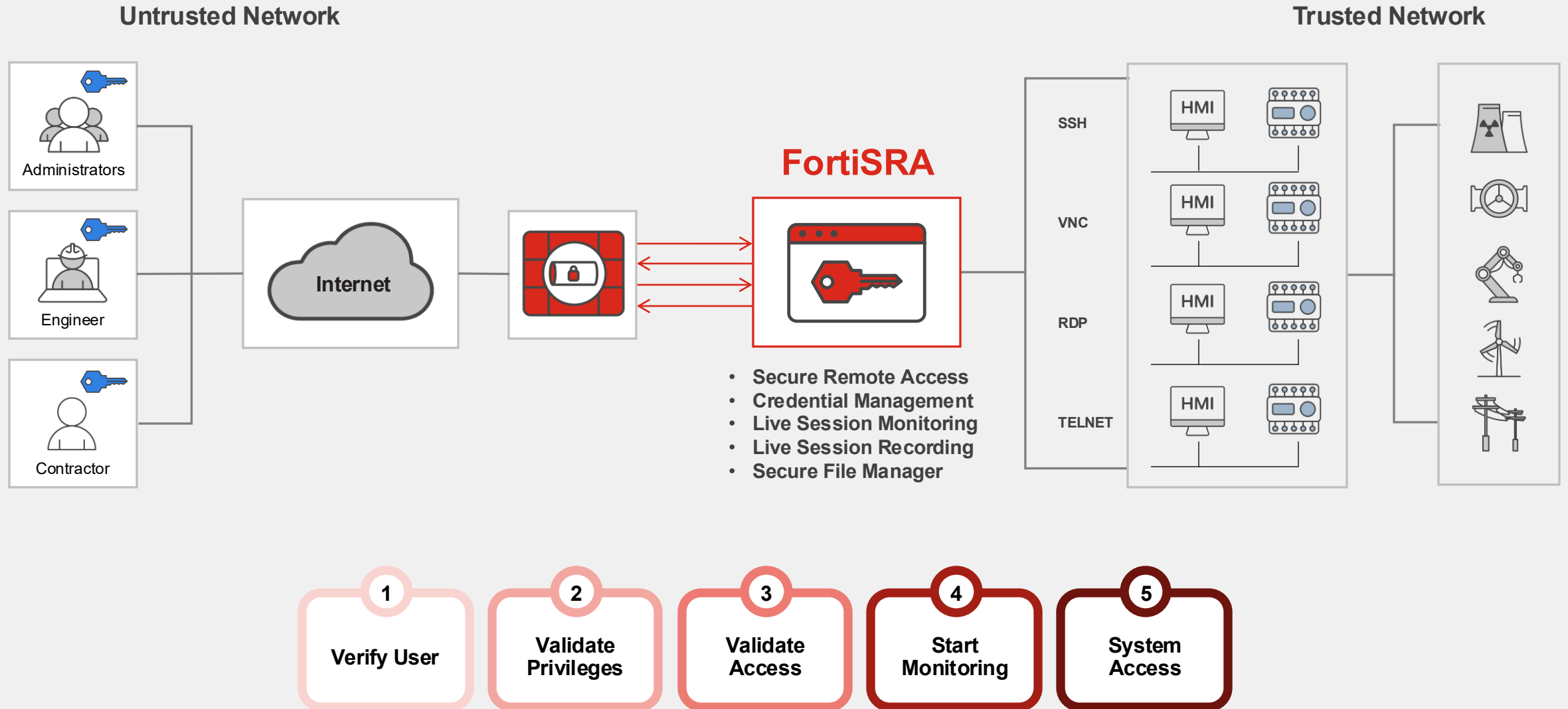
Monitor and Control Access to Digital Assets and Networks

FortiPAM/SRA



Monitor and Control Access to Digital Assets and Networks

Secure Remote Access – An Agentless Solution





Must-Do #4: Implement Proactive Measures for Threat Detection and Prevention

Compliance Reference:

NIST CSF Detect – Security Continuous Monitoring (DE.CM)-4, -5

NIST CSF Respond – Mitigation (RS.MI)-1, -2, -3

ISA/IEC 62443-2-1:2009 4.3.4.3.8, 4.3.4.5.6, 4.3.4.5.10

ISA/IEC 62443-3-3:2013 SR 2.4, SR 3.2, SR 5.1-5.4



Implement Proactive Measures for Threat Detection and Prevention

7.4 SR 3.2 – Malicious code protection

7.4.1 Requirement

The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

7.4.2 Rationale and supplemental guidance

The control system should use protection mechanisms to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means.

NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

E.2.7. Deception Technology

A deception technology uses decoy data and/or devices placed across the network to lure attackers away from legitimate assets. Decoys can range from access credentials and files to complete endpoints. When a threat actor interacts with a decoy, it triggers an alarm to alert cyber defenders to its presence. Defenders can then choose to further monitor the adversary for intelligence or immediately mitigate the threat. Because decoys do not actively interact with other network components, deception technologies can support malicious activity monitoring and detection without jeopardizing the controlled process.



Defense in depth is needed

[illegible]

Daniel Sarica · 2e
Founder/Security Architect @ ...
2 w · Bewerkt · 

+ Folgen ✕

After reviewing hundreds of enterprise security implementations, I've found that most organizations only leverage 30-40% of their NGFW capabilities against advanced threats.

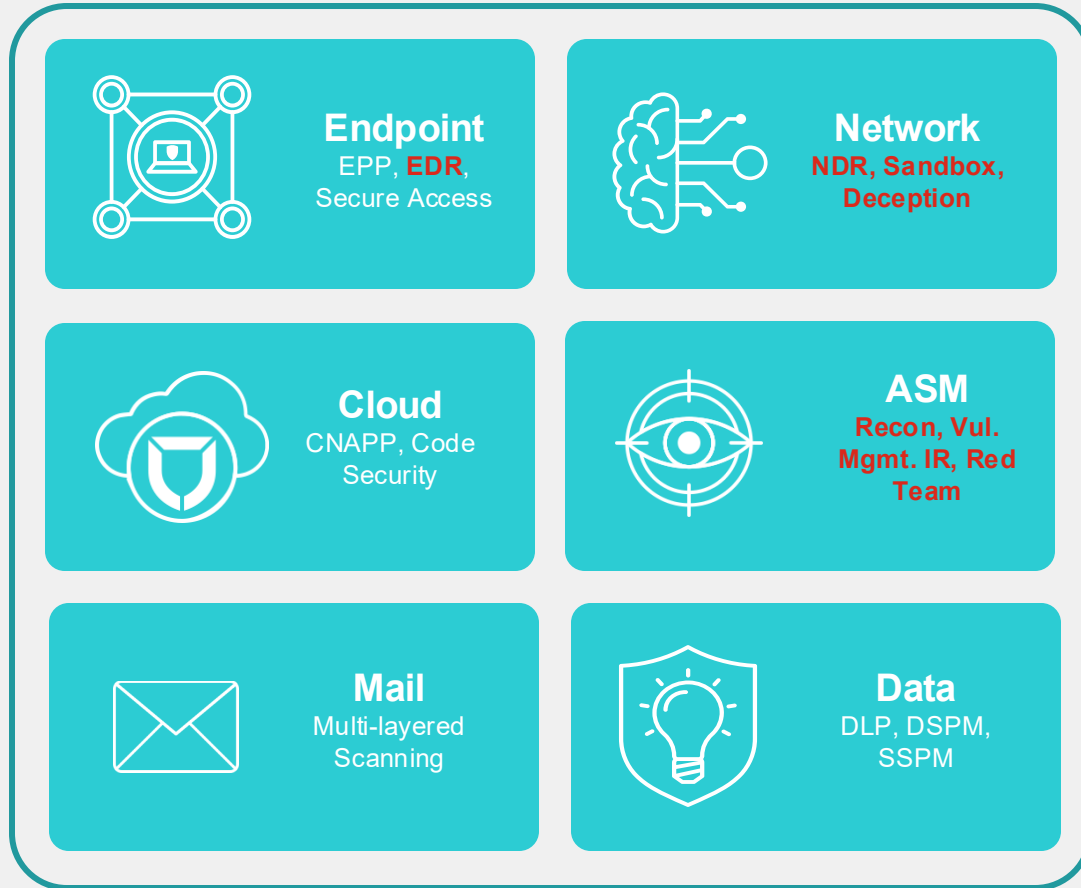
The blue highlights across this MITRE framework, represent areas where properly configured NGFWs provide protection. This is more comprehensive than most security teams realize.

Is your NGFW configured to address these 12 MITRE ATT&CK tactics?

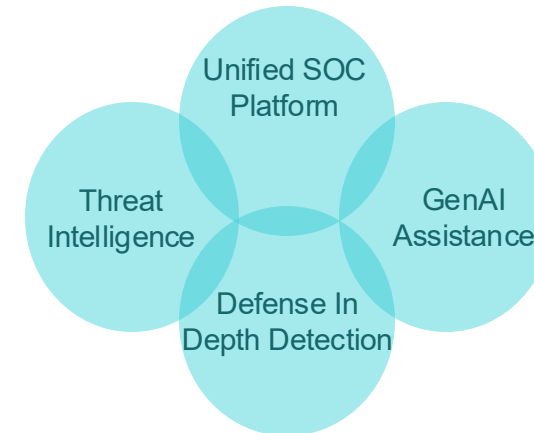


Solutions for Defense In Depth and Advanced Detection

Solutions to aid protection, close vulnerabilities, and identify and respond to stealthy attackers



Fortinet Security Operations Platform



Comprehensive

Best-in-class products for the end-to-end security needs of any size organization

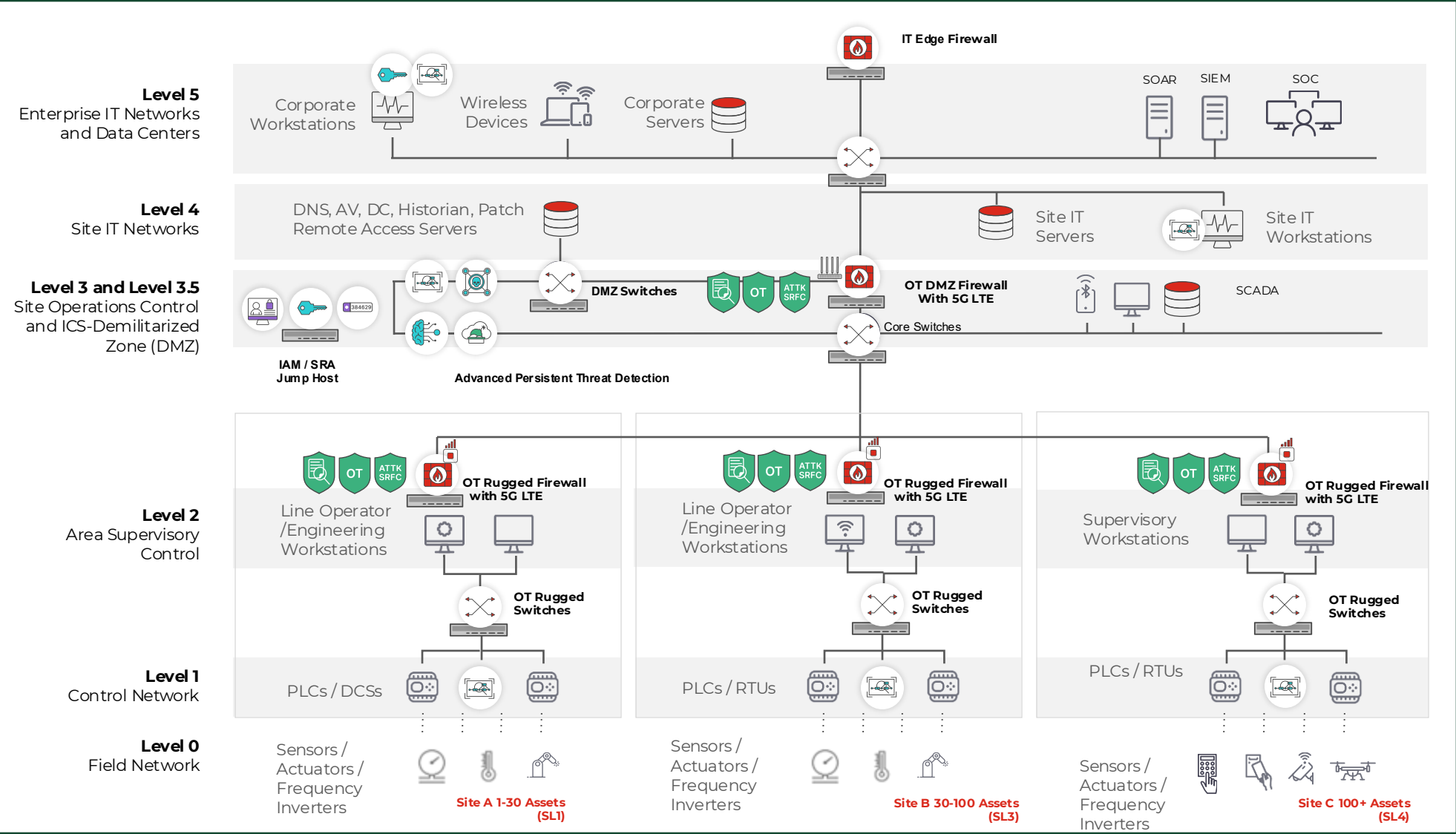
Integrated

Platform approach and tight integration across Fortinet and multivendor environments

Automated

GenAI assistance and built-in automation turbocharge security operations

Solutions for Defense In Depth and Advanced Detection



- Network Segmentation
- Connectivity (5G) With Secure SDWAN
- Deep OT Visibility and Security Services
- Zero-Trust Access for OT
- Advanced Persistent Threats



* Pas de maatregelen toe behorende bij het weerstandsniveau (SL1-4) van het object *



Overview – FortiDeceptor Decoys, Lures, and Tokens

Local Windows Decoys

- Windows 7
- Windows 10

Custom Windows Decoys

- Windows 7
- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- RedHat Enterprise Linux 7.9

Windows Lures/Tokens

- SMB
- RDP
- SMTP
- ICMP
- FTP
- TCP Port Listener
- NBNSSpoofSpotter
- SWIFT Lite 2
- SQL (MS-Server)
- Cache Credentials
- SQL ODBC
- SAP Connector
- HoneyDocs (Office / PDF / Excel)



VPN Decoys

- FortiOS



VPN Lures

- SSLVPN

Linux Decoys

- Ubuntu 16.0.4
- Ubuntu 18.0.4
- CentOS
- MacOS
- Outbreak Alerts



Linux Lures/Tokens

- SSH
- SAMBA
- TCP Port Listener
- ICMP
- Radius
- FTP
- ESXi
- ELK
- GIT
- MariaDB (MySQL)
- Tomcat (Webserver)
- SCADABR (MGMT)



IoT Decoys

- Cisco Router
- TP-Link Router
- IP Camera
- Printers (HP, LX, BR)
- UPS
- SWIFT VPN Gateway



VoIP Decoys

- SIP
- XMPP
- MQTT
- 4G/5G-3GPP



Application Decoys

- SAP
- ERP
- POS



Cloud Decoys



Medical Decoys

- PACS / Infusion Pump
- DICOM
- SPACECOM
- INFUSOMAT (Braun)



OT Decoys

- Schneider Electric
 - Modicon M241
 - PowerMeter PM-5560
 - EcoStrucure BMS Server
 - SCADAPack 333E
- Siemens
 - S7-200 PLC
 - S7-300 PLC
 - S7-1500 PLC
- Rockwell Automation
 - Rockwell PLC
 - 1769-L16ER/B LOGIX5316ER
 - 1769-L35E Ethernet Port
- Niagara
 - Niagara4 Station
 - NiagaraAX Station
- Phoenix Contact AXC 1050
- MOXA NPORT 5110
- GUARDIAN-AST
- GE PLC 90 (SRTP)
- Liebert Spruce UPS
- VAV-DD BACnet controller
- Kamstrup 382
- Ascent Compass MNG
- IPMI Device
- Modicon M580
- PowerLogic ION7650
- Emerson iPro by Dixell
- C-More HMI





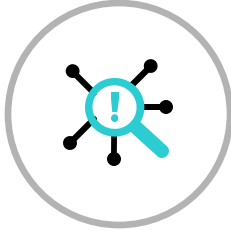
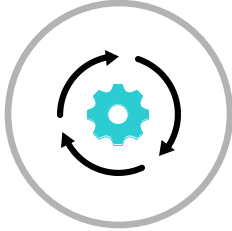

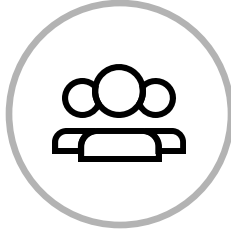


OT Lures

- HTTP/HTTPS
- FTP
- TFTP
- SNMP
- TELNET
- MODBUS
- S7COMM
- BACNET
- IPMI
- MOXA
- TRICONEX
- ENIP (EtherNet/IP)
- DNP3
- IEC 60870-5-104
- PROFINET
- KAMSTRUP
- Guardoan-AST



Fortinet Security Fabric and Third-party Integrations

FortiGate	FortiNAC	FortiSandbox	FortiEDR	FortiSIEM	FortiSOAR	FortiAnalyzer	Third-Party
							
<ul style="list-style-type: none">• Dynamic rule blocking based on attack trigger• OT/IoT Threat detection• Quarantine attacker/malware (TIC IOC)	<ul style="list-style-type: none">• Endpoint/device isolation automation based on attack trigger• OT/IoT threat detection	<ul style="list-style-type: none">• Provide malware analysis for malicious code captured by decoys• Enrich threat detection with attack IOCs	<ul style="list-style-type: none">• Enrich threat detection with attack IOCs• Built-in security and analytics reporting	<ul style="list-style-type: none">• Correlation rules detection based on false data (Tokens)• Reduce false-positive alerts to improve team efficiency	<ul style="list-style-type: none">• Orchestrate response based on attack trigger• Enhance MDR workflows with threat intelligence IOCs	<ul style="list-style-type: none">• Improve threat detection with attack IOCs• Built-in security and analytics reporting	<ul style="list-style-type: none">• Generic REST-API wizard enables integrate with third-party tools for mitigation & remediation• Native (built-in) 3rd party connectors

FortiDeceptor: Improved Threat Detection & Response



Must-Do #5: Streamline Security Operations Across NOC and SOC

NIS 2: cyber incident reporting (24Hrs) and IR forensics sharing (7 days)

NIST CSF Detect – Anomalies and Events (DE.AE)-1, -2, -3

NIST CSF Respond – Analysis (RS.AN)-1, -2, -3

ISA 62443-2-1:2009 4.4.3.3, 4.3.4.5.6 - 4.3.4.5.8

ISA 62443-3-3:2013 SR 2.8 - 2.12, SR 3.9, SR 6.1, 6.2

Streamline NOC and SOC

6.10 SR 2.8 – Auditable events

6.10.1 Requirement

The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

10.3 SR 6.1 – Audit log accessibility

10.3.1 Requirement

The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

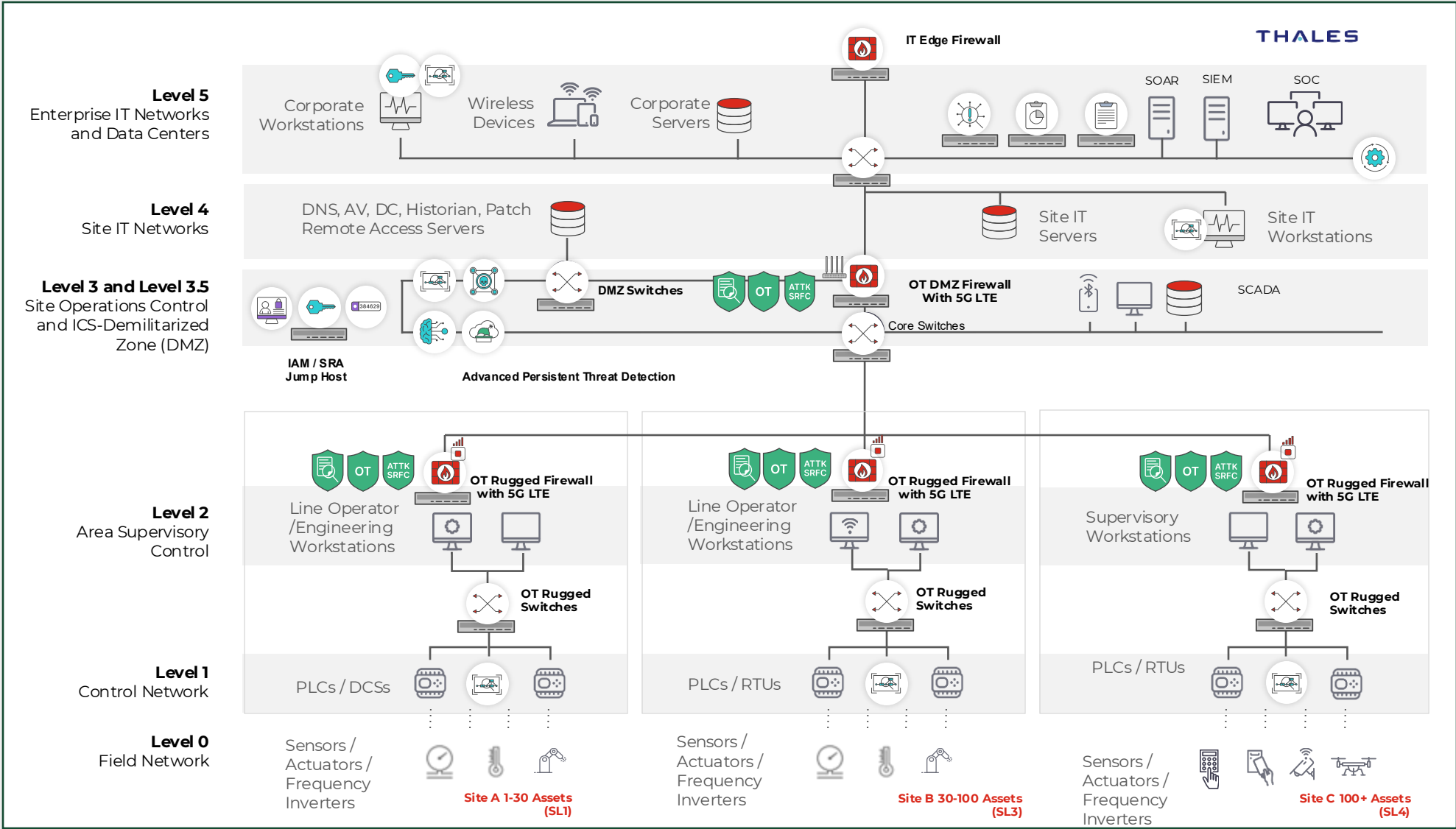
10.4 SR 6.2 – Continuous monitoring

10.4.1 Requirement

The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.



Solutions for Defense In Depth and Advanced Detection



- Network Segmentation
- Connectivity (5G) With Secure SDWAN
- Deep OT Visibility and Security Services
- Zero-Trust Access for OT
- Advanced Persistent Threats
- Integrated SOC and NOC for IT and OT



* Pas de maatregelen toe behorende bij het weerstandsniveau (SL1-4) van het object *

SOCaaS by Fortinet

Fortinet professionals for critical 24x7 security operations.

Global Response Teams

- SOC
- Data Center

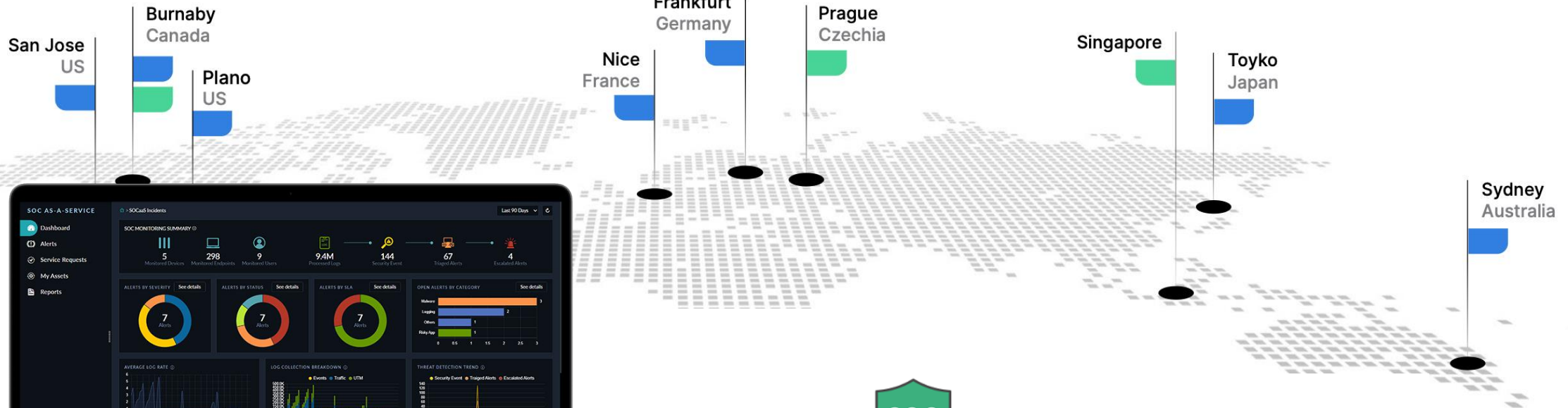
99.99%
Availability

24x7x365
Service Hours

Unlimited
Log Capacity

Fabric Devices
Ingest Log Data

Fast & Simple
Onboarding



Critical Escalation Times

P1, Priority 1: 15 minutes

P2, Priority 2: 45 minutes

P3, Priority 3: 90 minutes

P4, Priority 4: 6 hours



Fortinet Turnkey SecOps Platform

Solution Specs



Turnkey SOC Platform

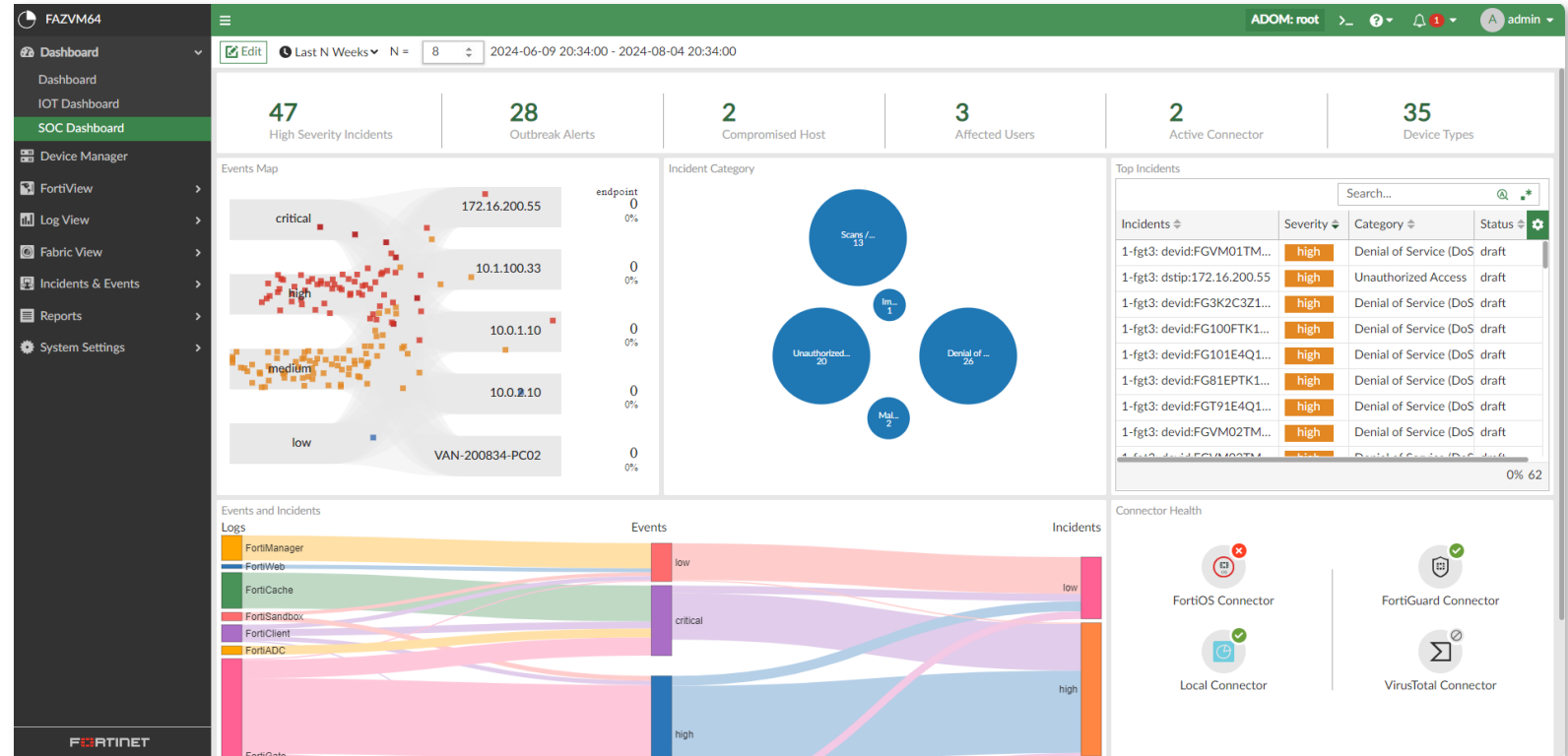
Use Cases:

Unified Visibility and Management

Threat Analysis and Hunting

SOC Automation

AI-Assistance



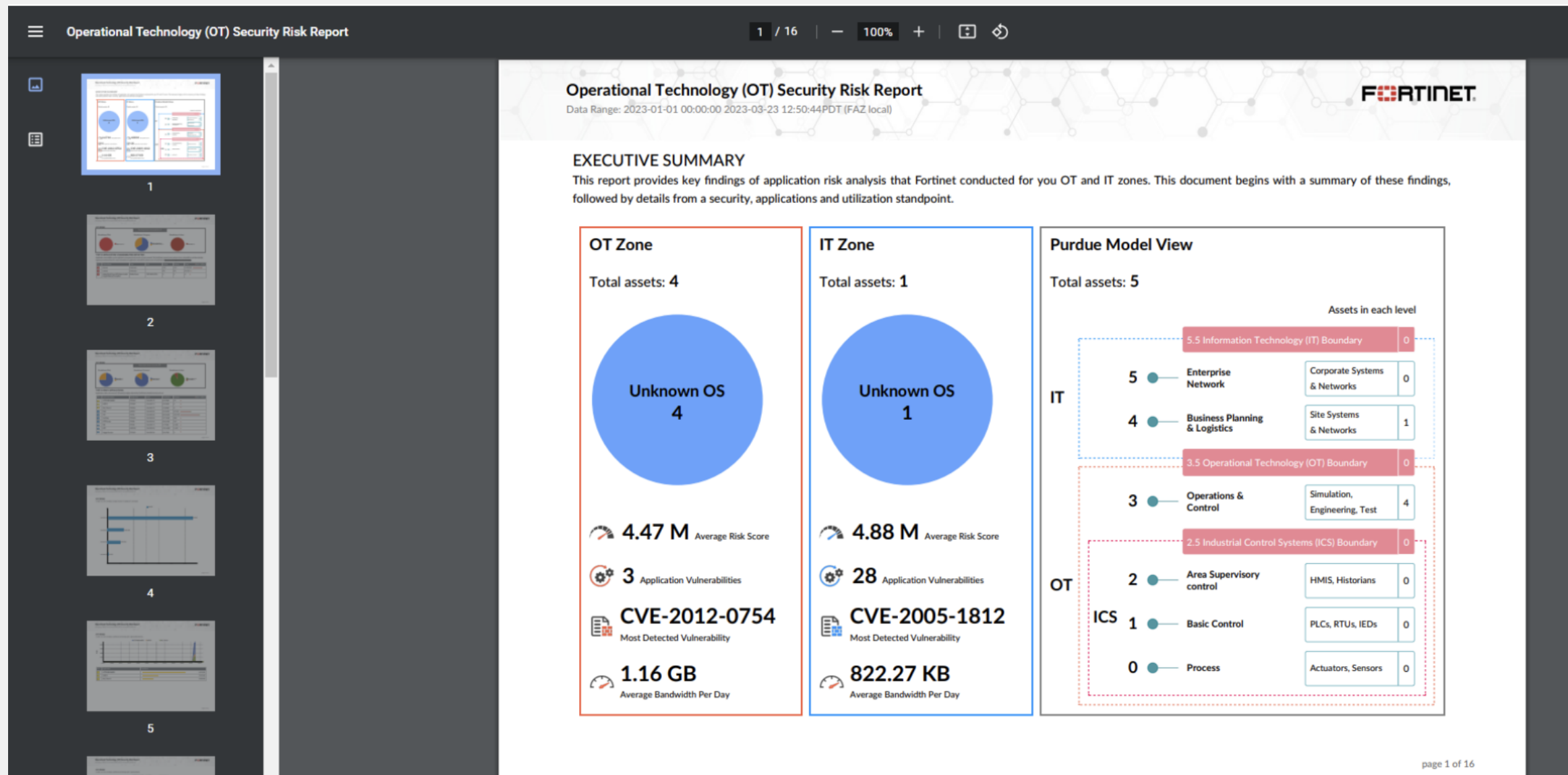
Unified Data Lake

Provides centralized log collection and analysis with a single view of alerts, incidents, configurations

SOC Dashboard

Unified visibility across SOC, email, endpoints, and IoT, enabling automated threat detection, risk assessment, and policy-driven security enforcement.

FortiAnalyzer 7.4.0



Advanced SOC Platform



FortiSIEM

Enterprise visibility,
compliance, threat
detection & response



FortiSOAR

Centralized automation
of incident management
and any SOC activity

Enterprise
Event Collection



Advanced Threat
Detection



Investigation
& Response

Working together or independently
to power the Enterprise & MSSP SOC

Enterprise Threat Detection

Multivendor event collection, behavioral threat detection, and comprehensive SIEM features

Automation Everywhere

FortiSOAR playbooks and creation within SIEM. Full SOAR platform for any SecOps/enterprise workflow

Embedded GenAI Assistant

Integrated FortiAI assistant to aid analyst efficiency and effectiveness

Scalability & Deployment Flexibility

Scales to meet the needs of the most demanding organizations. Available as SaaS and software.

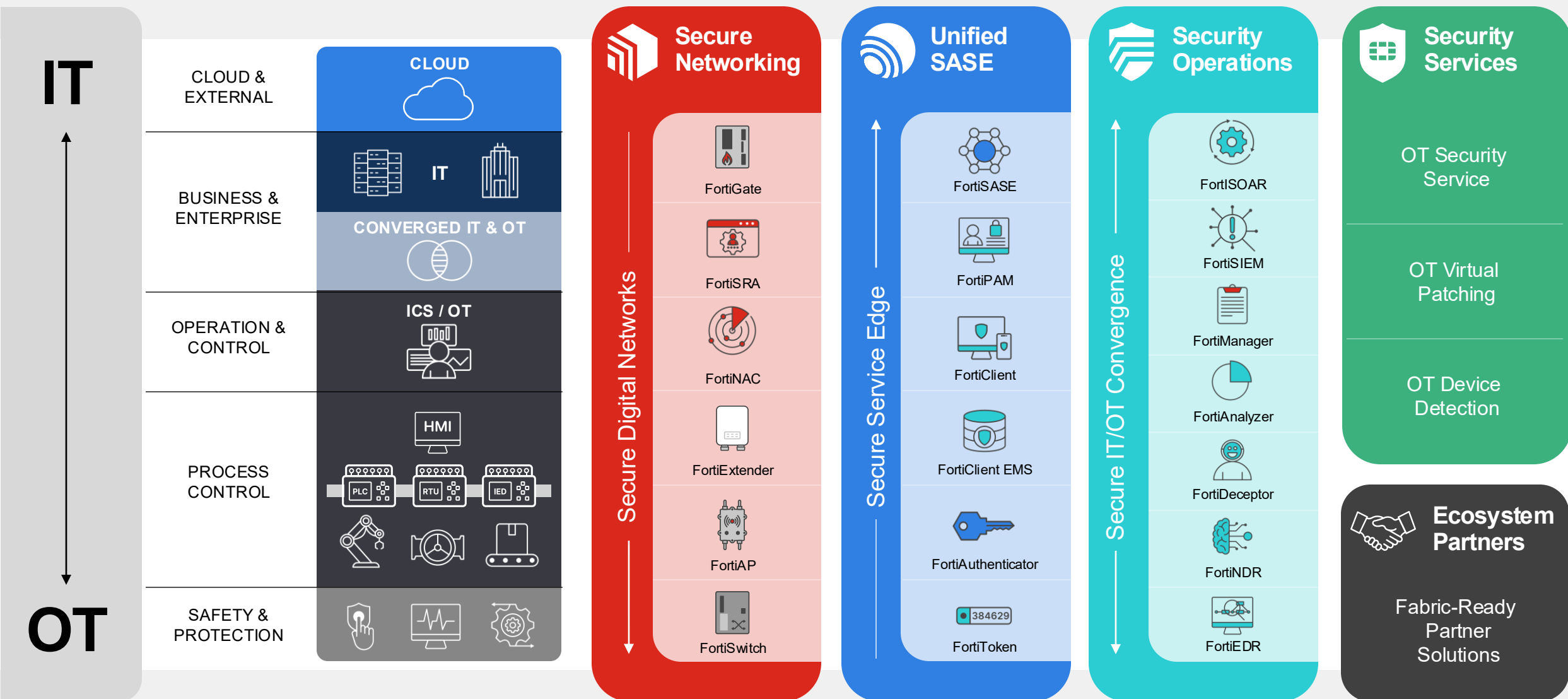
Integrated with FortiAnalyzer Data Lake





Protecting Operational Technology Summary

Fortinet's OT Security Platform Solution





What's Next





FORTINET®