

The Fortinet logo, featuring the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is stylized with a red and white grid pattern. A registered trademark symbol (®) is located to the right of the word. The logo is positioned on a white, rounded rectangular background that overlaps the top and left sides of the slide.

**FORTINET®**

# Operational Technology Fortinet Tanum

Q2 2025

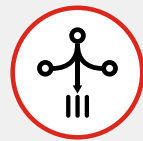
# Fortinet Rugged Product Portfolio

FortiGate Rugged, FortiSwitch Rugged, FortiAP Rugged



## Ruggedized Design

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



## Consolidated Security Architecture

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



## Ease of Management

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

## FortiGate Rugged Series



### FGR-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 (VDM)
- 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



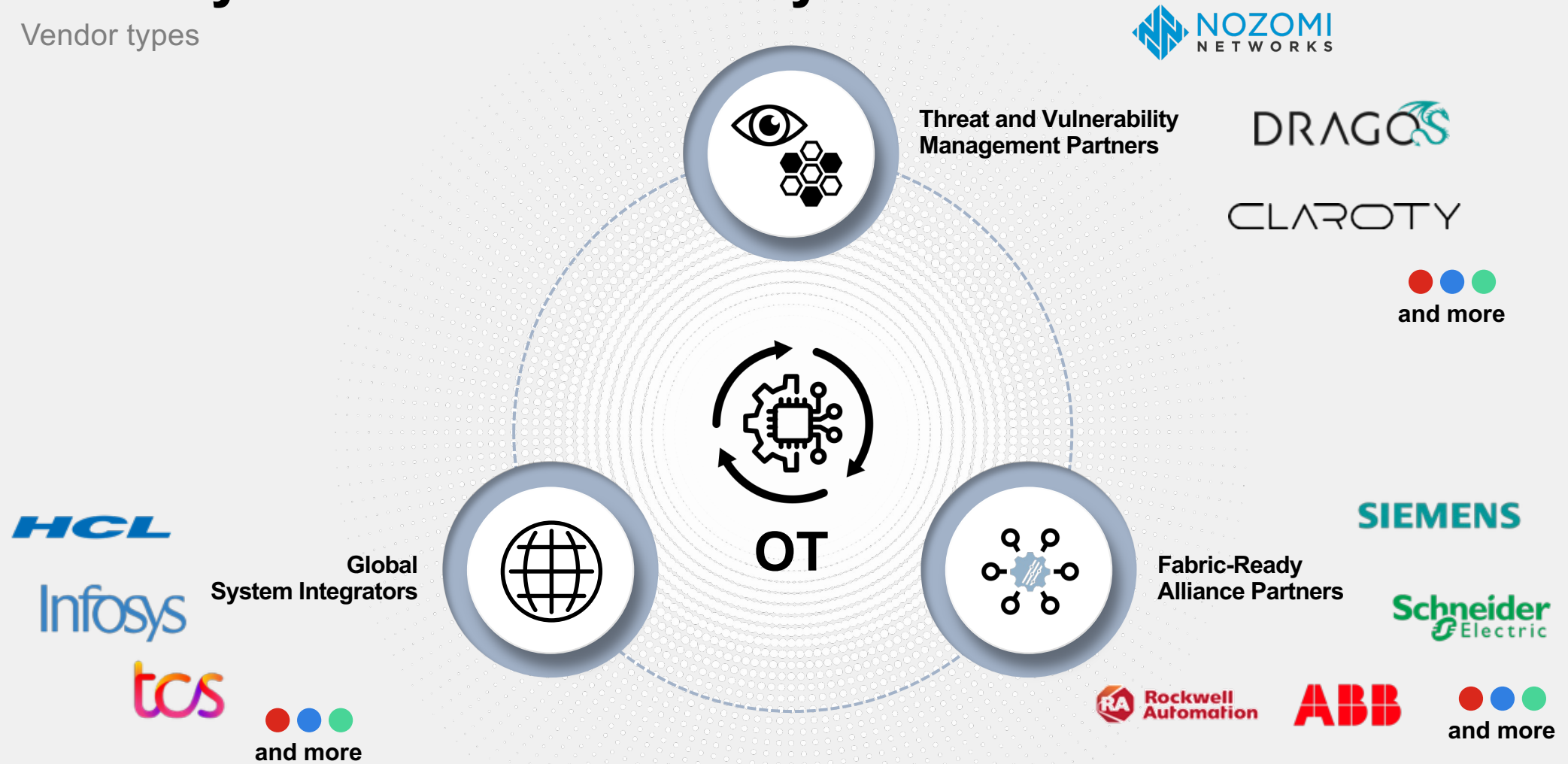
### FortiAP Rugged 432FR

External Antennas  
C1D2/IP67, Indoor/Outdoor Use  
PoE Powered  
Wall- and pole-mountable  
Wi-Fi Alliance Certified



# Security Fabric Partner Ecosystem

Vendor types



© Fortinet Inc. All Rights Reserved.

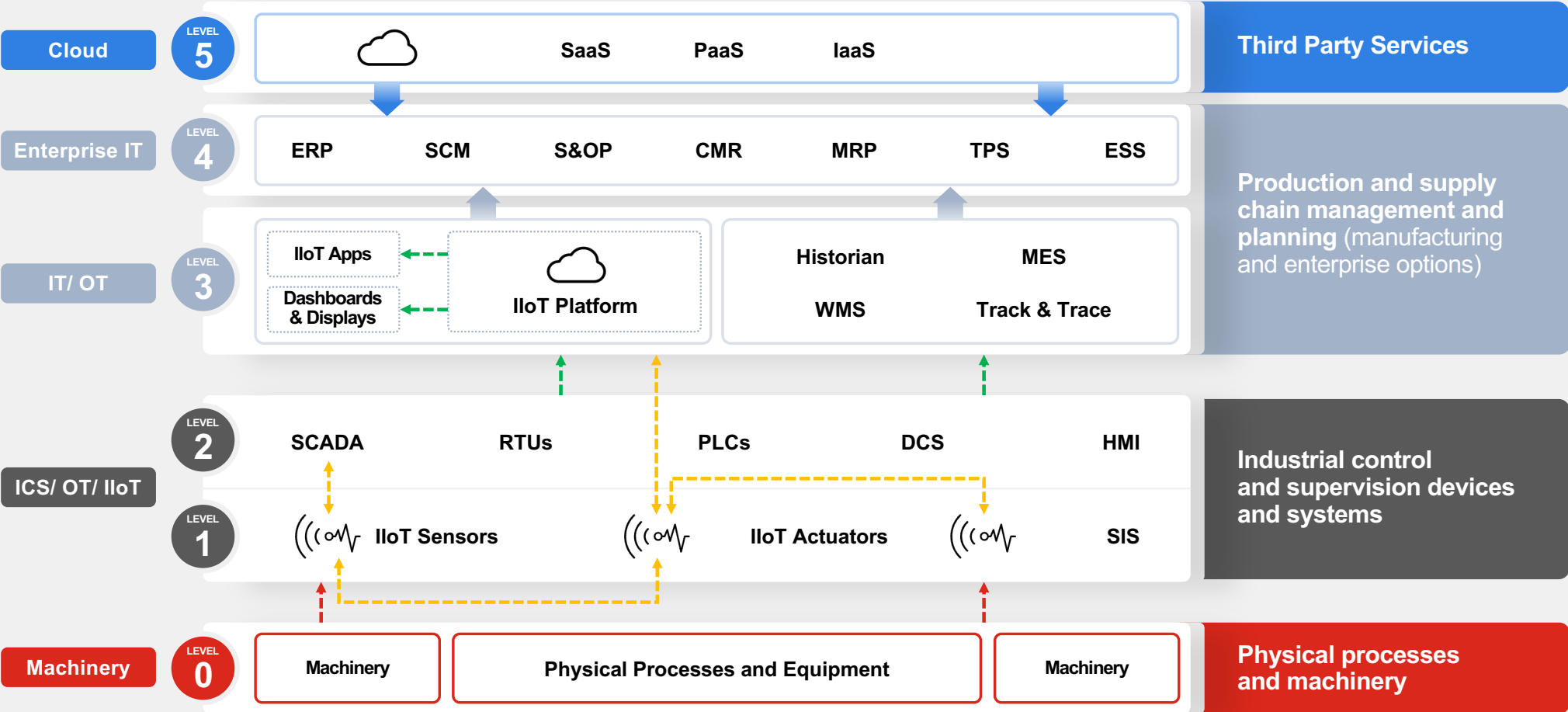


# Security Fabric Deployment for IT/OT/IloT





# Example IT, OT and IIoT Converged Infrastructure







# FortiGate Rugged 70F / 70F-3G4G

Released Feb 2023

## Product Information



## Key Differentiators

-  ASIC-based NGFW/ NGIPS
-  Secure SD-WAN
-  Specialized IPS for ICS/OT
-  3<sup>rd</sup> party integrations

## Industry Compliance



## Product Literature

Datasheet, Quickstart Guide

## Key Benefits



**Ruggedized NGFW**  
comply with industrial requirements and certifications to ensure reliable operations in harsh conditions



**Optimal User Experience**  
ASIC-based processor for high-speed NGFW/ NGIPS performance



**Cost-effective**  
compact design with integrated networking, security, wireless, and secure SD-WAN features



**Centralized Visibility**  
support for unified logging, reporting, and management for centralized control over security operations



# FortiGate Rugged 70G-5G-DUAL

Ideal for remote locations and harsh environments

## ✓ Secure Adaptive Edge

Integrated 5G, SD-WAN, ZTNA app gateway, and security into one compact appliance simplifies architecture and operations

## ✓ High-performance Ruggedized Design

Purpose-built ASIC for high-speed NGFW/NGIPS performance; comply with industrial requirements and certifications for reliable operations in harsh environment with dual DC power inputs

## ✓ Dual Active/Active 5G Connectivity

Faster deployment and mobility with dual-5G and dual-SIM modem for dual-active 5G WAN links and additional redundancy

## ✓ Centralized Visibility & Security

End-to-end visibility, orchestration and security protecting assets and improving digital experience



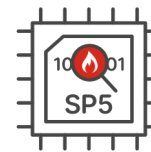
6x GE RJ45 (includes 1x bypass) and 2x GE SFP

## Fortinet Advantage

Patented ASIC radically increases the speed, scale, efficiency while greatly improving user experience, reducing footprint and power requirements



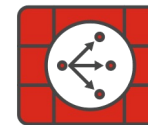
reddot winner 2024



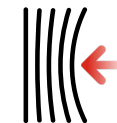
ASIC Acceleration



Energy efficiency



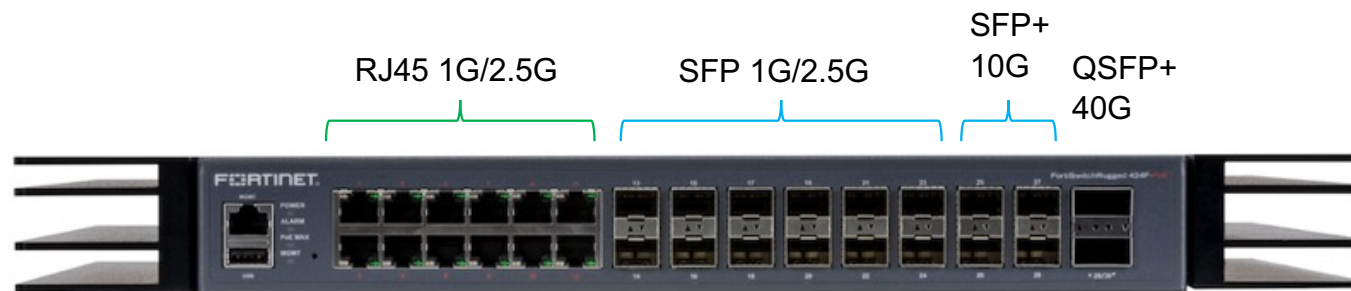
Secure SD-WAN



Resilient Design



# FortiSwitch Rugged (FSR) 424F-POE



Forwarding Capacity (Duplex): 360Gbps Line Rate

## FSR-424F-POE

**PRP** – IEC 62439-3 Clause 4

**HSR** – IEC 62439-3 Clause 5

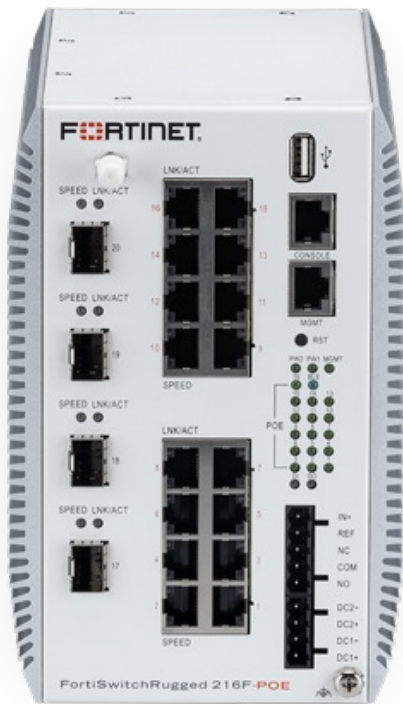
**PTP** – IEEE 1588v2

(Supports Power Profile IEEE C37.238-2017)

Specifications	FSR-424E-POE
Downlinks	12 x 1/2.5G RJ45 + 12 x 1/2.5G SFP
Uplinks	4 x 10G SFP+ 2 x 40G QSFP+
POE (60W per port)	420W Budget
Power Supply	18-125VDC (Redundant)
Industrially Hardened	Fan-less, IP40 IEC 61850-3, IEEE 1613



# FortiSwitch Rugged (FSR) 216F-POE



## FortiSwitch Rugged 216F-POE

- DIN type, IP40, fan-less design
- 16x 1GbE RJ45 POE/POE+, 360W power budget
- 4x 10G SFP+
- 1x RJ45 Serial Port for Console
- 1x RJ45 Ethernet Port for Management
- 2x DC Power Inputs 12V – 57V DC (Redundant)
- IEC 61850-3, IEEE 1613
- Dimensions: 180mm (H) x 116mm (W) x 170mm (D/L)

## Key Differentiators



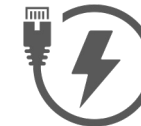
### Rugged IP40 Design

Resiliency for Harsh Environments  
Dual DC Power Inputs



### Fault Detection

Fault Relay and Alarm inputs



### 802.3bt POE

802.3bt POE support up to 240W



### Hardware Security Switch

Restricts hardware security options  
to only authorized personnel with  
physical access to the device





# FortiExtender Vehicle for Secure Mobility

Rugged FortiExtender with integrated Wi-Fi for Mobile Fleets



FEV	211F
Cellular	CAT-12 LTE
Top D/L Speed	600Mbps
Deployment	Vehicle/OT
Benefit	Wi-Fi, Dual-SIM Public Safety
Connection	7-36VDC
Support	North America/Global



# FortiAP Rugged 432FR

FAP-432FR – Certified for ATEX environments

## **FortiAP 432FR: C1D2 certified based on 432F**

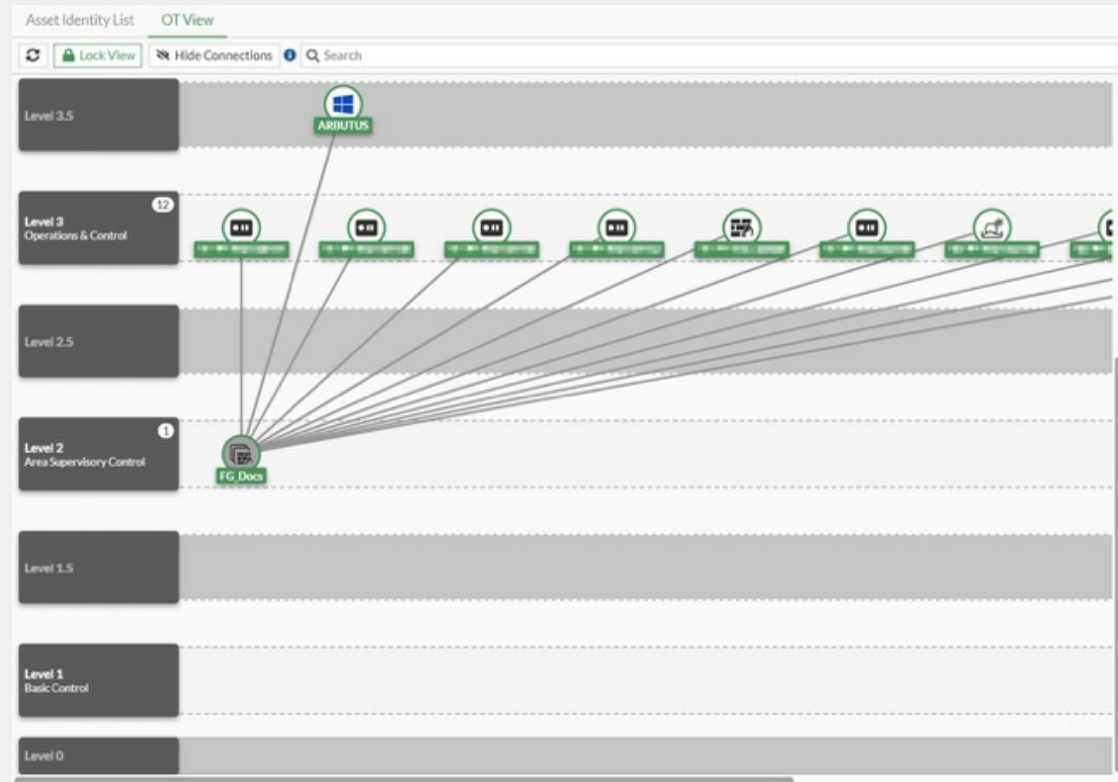
- 802.11ax Tri-Radio 2.4 GHz + 5 GHz + scanning
- 4x4 MU-MIMO; 6 External Antennas
- Up to 1147 Mbps + 2402 Mbps
- BLE for beacons and location discovery
- IP67, -40C – 60C
- PoE power
- 2.5G Ethernet + 1G Ethernet w PoE output



# FortiOS Asset Identity Center – OT View

Released in FortiOS 7.2

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



Link: <https://docs.fortinet.com/document/fortigate/7.2.0/new-features/498242/add-ot-asset-visibility-and-network-topology-to-asset-identity-center-page>



# FortiOS OT View – Asset and Network Flow Info

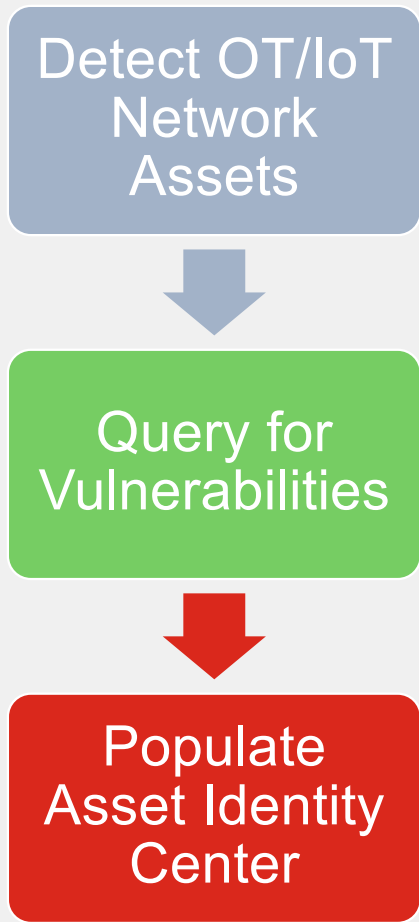
Partly Released

The image displays three overlapping screenshots of the FortiOS OT View interface. The leftmost screenshot shows a network topology diagram with various nodes and connections. The middle screenshot shows a detailed view of a device's network flow information, including a table of policies and a line graph of traffic volume. The rightmost screenshot shows a similar view for a different device, also with a line graph.

Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	FortiGate
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	22,148	2	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	26,518	2	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	21,718	2	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	20,098	2	FortiGate-01F
4 from-hub-test-lookupspeke_0	Firewall	wan2	vlan-fortilink (local)	9,198	1	FortiGate-01F
2	Firewall	wan2	vlan-fortilink (local)	9,908	1	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	17,918	2	FortiGate-01F
9	Firewall	wan2	vlan-fortilink (local)	36,848	2	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	11,728	1	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	11,538	1	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	8,148	1	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	7,788	2	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	5,268	1	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	5,178	1	FortiGate-01F
Implicit Deny	Local IPv4	wan2	vlan-fortilink (local)	4,588	1	FortiGate-01F
1	Firewall	wan2	vlan-fortilink (local)	348	1	FortiGate-01F
Implicit Deny	Firewall	unknown-0	unknown-0	2,278	2	FortiGate-01F
800	Firewall	unknown-0	unknown-0	1,848	3	FortiGate-01F
Local IPv4	Local IPv4	wan2	vlan-fortilink (local)	1,348	1	FortiGate-01F



# FortiGuard OT Device Detection



Summary Charts:

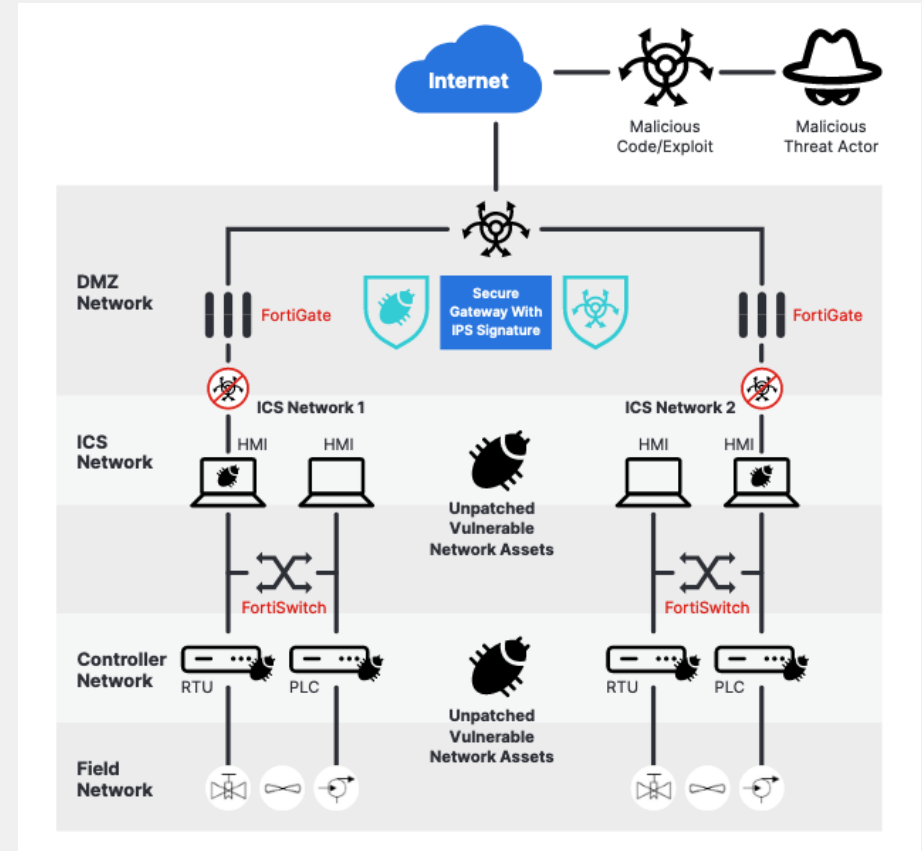
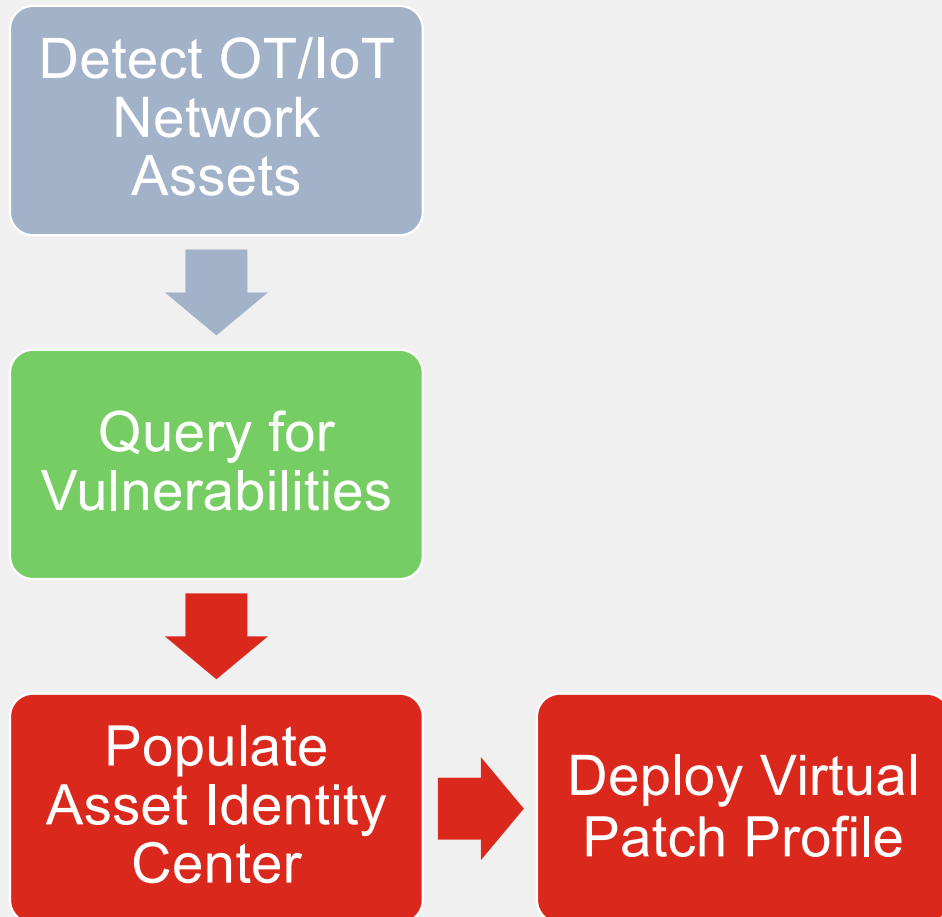
- Software OS:** 43 Devices. Legend: Unknown (20), Linux (12), macOS (6), Windows (5).
- Vulnerability Level:** 43 Devices. Legend: None (23), Critical (2), High (4), Medium (2).
- Status:** 43 Devices. Legend: Online (43).
- Interface:** 43 Devices. Legend: port4 (23), port3 (20), port6 (1), port5 (1).

Device	Software OS	Address	User	FortiClient User	Vulnerabilities	Status	Endpoint Tags
Robin Foster PC	macOS	10.1.0.10	Robin Foster	Robin Foster	6 2 41 5	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients
Charlie Fischer PC	Linux	10.1.0.13	Charlie Fischer	Charlie Fischer	10 9 16 5	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients ZTNA IP: Corporate Linux Endpoints ZTNA MAC: Corporate Linux Endpoints
Unknown Device	Unknown	10.100.55.102				Online	
Unknown Device	Unknown	10.100.55.1				Online	
Unknown Device	Unknown	10.100.55.101				Online	
Sidney Ramos PC	macOS	10.1.0.12	Sidney Ramos	Sidney Ramos	1 3 4	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients
Caden Wallace Laptop	macOS	10.1.0.21	Caden Wallace	Caden Wallace	6 5 26 2	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients
Shay Nicholson Laptop	Linux	10.1.0.6	Shay Nicholson	Shay Nicholson	1 5 6 1	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients ZTNA IP: Corporate Linux Endpoints ZTNA MAC: Corporate Linux Endpoints
Jordan Garrison PC	macOS	10.1.0.18	Jordan Garrison	Jordan Garrison	4 24 9	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients
Lee Khan PC	Linux	10.1.0.8	Lee Khan	Lee Khan	7 5 14	Registered - Online - On-Net	ZTNA IP: all_registered_clients ZTNA MAC: all_registered_clients ZTNA IP: Corporate Linux Endpoints ZTNA MAC: Corporate Linux Endpoints

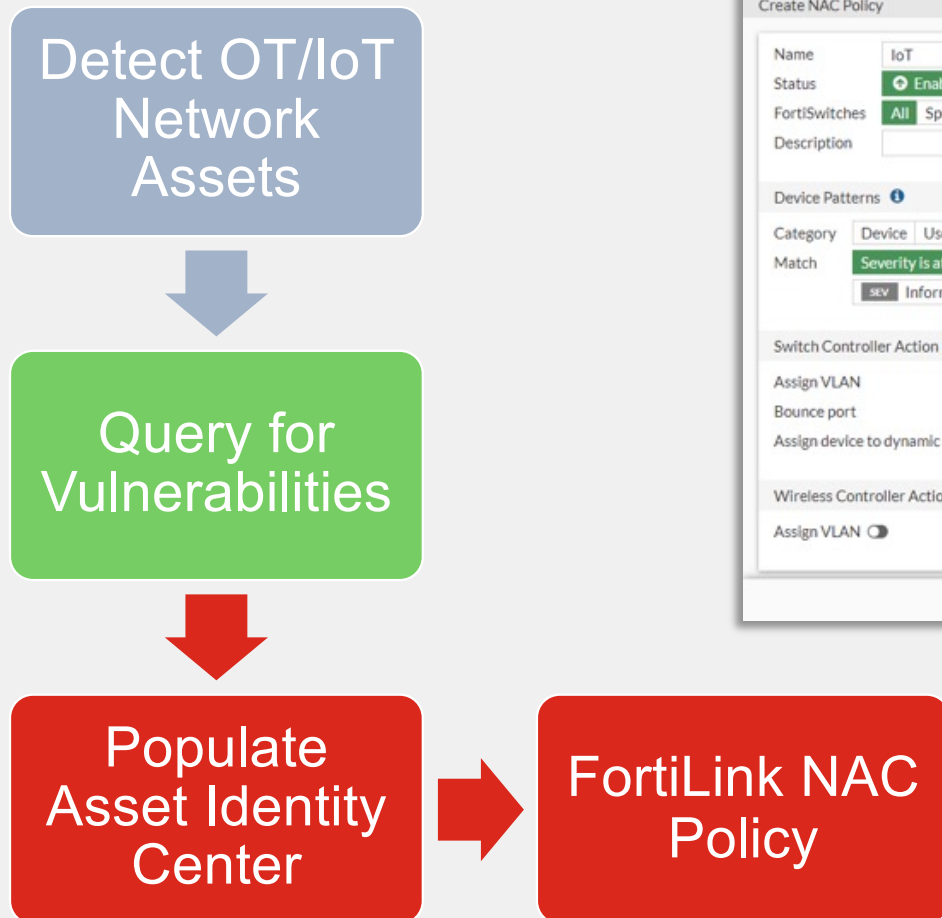




# FortiOS OT Virtual Patching



# FortiOS FortiLink NAC OT Auto-Quarantine



Create NAC Policy

Name: IoT

Status:  Enabled  Disabled

FortiSwitches: All Specify

Description: /0/63

Device Patterns

Category: Device User EMS Tag Vulnerability

Match: Severity is at least Specify

SEV: Information

Switch Controller Action

Assign VLAN:  vlan300

Bounce port:

Assign device to dynamic address:

Wireless Controller Action

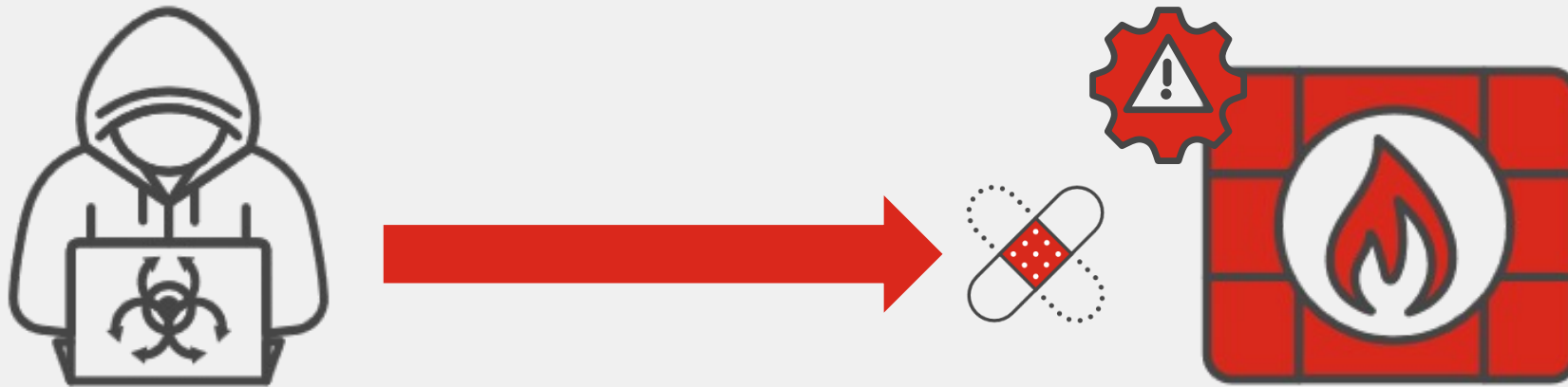
Assign VLAN:

Name	Patterns	Assign
NAC Policies		
IoT	SEV Information SEV Low SEV Medium SEV High SEV Critical	vlan300
FortiSwitch Onboarding VLAN and VLAN Segmentation		



# Virtual Patching Local-in Management Interface

FortiOS 7.4.x



“ Virtual patching is enabled for the local-in policy, for example following scenarios:

- FortiGate with an SSL VPN vulnerability
- FortiGate with a web GUI vulnerability
- FortiGate with both an SSL VPN and web GUI vulnerability



# FortiGuard OT Security Service

OT Application Control and IPS Signatures

## Operational Technology Security Service

The FortiGuard Operational Technology (OT) Security Service for FortiGate combines IPS and Application Control signatures tailored to OT environments, enabling asset owners and operators to detect and protect against network-level threats while gaining extensive visibility into OT applications and protocols.

Search



ID Lookup  Encyclopedia

**3,172**

Number of Protocol Rules

**698**

Number of IPS Rules

**1,200**

Number of OT Virtual Patch rules

**1,086**

Number of OT App Detection rules

## Version Updates

OT Threat

28,814

1 week ago

Modified (1)



# FortiGuard OT Security Service Coverage

Application Control Signatures – ICS/OT Applications and Protocols

<b>Allen Bradley CSP</b>	EtherNet/IP-CIP →	MTConnect	Schneider UMAS →
Allen-Bradley DF-1 →	Ewon Talk2M Access	Niagara Fox	<b>SECS-II/GEM</b> →
<b>Allen-Bradley PCCC</b> →	Ewon Talk2M VPN	oBIX	<b>SEL Fast Message</b> →
BACnet →	Ewon.M2web	<b>OCCP</b> →	Siemens LOGO →
Beckhoff.AMS →	FactorySuite NMXSVC	Omron FINS →	Siemens OCG ATCS →
Bristol BSAP	FL-NET →	OPC AE →	Siemens S7 →
CC-Link →	GE EGD →	OPC Common →	Siemens S7 1200 →
CN/IP CEA-852 →	GE SRTP →	OPC DA →	<b>Siemens S7 Plus</b> →
CoAP →	Hart IP →	OPC DA Automation →	Siemens SIMATIC CAMP →
DDSI-RTPS	IEC 60870-5-104 ⇄	OPC HDA	Siemens.Epoc.EDM
Digi ADDP →	IEC 60870-6 (ICCP/TASE.2) →	OPC HDA Automation →	STANAG 4406 Military Messaging
Digi RealPort (Net C/X)	IEC 61850 →	OPC UA →	STANAG 5066
Digi RealPort (Net C/X) DNP3 ⇄	IEC 61850-90-5 R-GOOSE	OpenADR →	ToolsNet Open Protocol
Direct Message Profile →	IEC 61850-90-5 R-SV	OSIsoft Asset Framework	<b>TRDP</b> →
DLMS/COSEM(IEC62056) →	IEEE 1278.2 DIS →	OSIsoft PI	Triconex TSAA →
<b>DNP3</b> →	IEEE C37.118 Synchrophasor →	Profinet CBA →	TriStation →
ECHONET Lite →	Inductive Automation Ignition Gateway	Profinet IO →	Unitronics PCOM →
ECOM100	KNXnet/IP (EIBnet/IP) →	Rockwell FactoryTalk AssetCentre	<b>V2G.EXI</b>
ELCOM 90 →	LonTalk IEC14908-1 CNP →	Rockwell FactoryTalk Diagnostic	<b>V2G.SDP</b>
Emerson DeltaV	<b>Matrikon OPC Tunneller</b>	Rockwell FactoryTalk Live Data	Veeder-Root ATG
Emerson ROC	Mitsubishi MELSEC →	Rockwell FactoryTalk RNA Alarming	Vnet/IP
Ether-S-Bus →	MMS →	Rockwell FactoryTalk RNA Server Ping	<b>WITS0</b>
Ether-S-I/O →	<b>Modbus RTU</b> →	Rockwell FactoryTalk View SE	<b>WITSML</b> →
EtherCAT →	Modbus TCP/IP ⇄	Rockwell FactoryTalk ViewPoint	
Ethernet POWERLINK	Moxa UDP Device Discovery	SafetyNET p →	

Recent additions/updates

→ message layer policy ⇄ message and parameter policy

For an up-to-date list of supported signatures, please visit [fortiguard.com](https://www.fortiguard.com).

Entire list: <https://www.fortiguard.com/services/ots> Submit new (signature) request: <https://www.fortiguard.com/faq/appctrlsubmit>





# OT Vulnerability Protection

650+ OT IPS Signatures

## OT Vulnerability Protections—Select Vendors

ABB	ETIC	Moxa	Ricon
Advantech	Fuji	mySCADA	Rockwell
AVEVA	GE	OAS	Schneider
B&R Automation	Iconics	Omron	SEL
Contec	Inductive Automation	Osprey	Siemens
Delta IA	InHand Networks	Pepperl+Fuchs	Sierra Wireless
DUT CCE	KeySight	PnP SCADA	WECON
Eaton	Korenix	PTC	Wibu Systems



# Signature Packages for IoT Devices

Released in FortiOS 7.2

“The signature packages are updated when FortiGate has a valid IoT Detection Service license.

Although the signature packages are available in FortiOS 7.2.0, you cannot apply the signatures to network traffic. Support for this functionality is coming in future FortiOS releases.

FortiGuard Distribution Network		FortiGuard.com	
Outbreak Prevention	✔ Licensed (Expiration Date: 2022/08/26)	FortiGuard.com	4.75 MB
SD-WAN Network Monitor	✔ Licensed (Expiration Date: 2022/08/26)	FortiGuard Download	275.39 MB
Security Rating	✔ Licensed (Expiration Date: 2022/08/26)	FortiGuard Query	162.31 kB
Industrial DB	✔ Licensed (Expiration Date: 2022/08/26)	FortiGate Cloud Sandbox	0 B
FortiPAM	✔ Licensed (Expiration Date: 2022/08/26)	OCVPN	0 B
IoT Detection Service	✔ Licensed (Expiration Date: 2022/08/26)	SDNS	0 B
IoT Detection Definitions	🕒 Version 20.00308	FortiToken Registration	0 B
FortiGate Cloud	✔ Activated	SMS Service	0 B
FortiGate Cloud Log Retention	✔ Licensed (Expiration Date: 2022/08/25)		

[Upgrade Database](#) [Logout](#)

[Apply](#)



# FortiAnalyzer OT Focused Dashboard and Reports

Partly released

- *OT View Dashboard*
- *OT Security Risk Report*
- *OT Security Compliance Report*
  - *CIS Top 20*
  - *IEC 62443-3-3*
  - *NERC CIP*
  - *and more...*

*Requires FAZ OT Security Service license*



# FortiAnalyzer OT Focused Dashboard and Reports

**00Copy of Template - CIS Controls Security Rating Report**  
Data Range: 2023-04-30 00:00:00 2023-05-29 23:59:59 PST

**EXECUTIVE SUMMARY**

CIS Controls Compliance Results

48 Total

- 72.92% Compliant
- 27.08% Non-Compliant

**OVER VIEW**

CIS CRITICAL SECURITY CONTROL

CIS Control	CIS Name
<b>CIS Control 1</b>	<b>Inventory and Asset Management</b>
L CIS Control 1.1	Establish and maintain an accurate and up-to-date inventory of all information systems and assets, including those owned, leased, or managed by the organization, and the support functions and services used by those systems and assets.
L CIS Control 1.2	Address unauthorized access, use, modification, disclosure, destruction, and loss of information systems and assets.
<b>CIS Control 3</b>	<b>Data Protection</b>
L CIS Control 3.3	Configure data protection for information systems and assets.
L CIS Control 3.10	Encrypt sensitive information.
L CIS Control 3.12	Segment data flows.

**NERC CIP Compliance Security Rating Report (OT)**  
Nov 30, 2023 21:00 and Dec 3, 2023 21:00

Requirement	Title
<b>CIP-002-5.1.a</b>	<b>Cyber Security - BES Cyber System Security</b>
Requirement 1	Each Responsible Entity shall:
Part 1.1	Identify each of the high impact BES Cyber Systems within the organization, including those owned, leased, or managed by the organization, and the support functions and services used by those systems and assets.
Part 1.2	Identify each of the medium impact BES Cyber Systems within the organization, including those owned, leased, or managed by the organization, and the support functions and services used by those systems and assets.
Part 1.3	Identify each asset that could be used to impact BES Cyber Systems according to Attachment 1, Section 1.1.
Part 2.1	Review the identifications and update them if there are changes on a calendar month basis, even if it has no impact on the BES Cyber System.
Part 2.2	Have its CIP Senior Management review and approve the identifications required by Requirement 1, even if it has no impact on the BES Cyber System.
<b>CIP-003-8</b>	<b>Cyber Security - Security Information and Event Management</b>
Requirement 1	Each Responsible Entity shall have more documented cyber security information and event management systems:
Part 1.1	For its high impact and medium impact BES Cyber Systems.
Part 1.2	For its assets identified in Attachment 1, Section 1.1.

**NIST CSF Report**  
Jan 30, 2024 21:00 and Feb 3, 2024 21:00

**EXECUTIVE SUMMARY**

Aggregated NIST CSF Check Results

272 Total

- 70% NIST CSF Passed: 191
- 30% NIST CSF Failed: 81

Security Fabric Posture

1853 Total

- 52.29% Passed: 726
- 30.39% Failed: 715
- 11.76% Unmet: 212
- 5.56% Exempt: 200

**OVER VIEW**

NIST CSF CYBERSECURITY FRAMEWORK V1.1

Category	Description	Failed, Unmet or Exempt (# of Device)	Passed (# of Device)
<b>IDAM</b>	<b>Identity: Asset Management</b>	82	104
L IDAM-1	Physical devices and systems within the organization are inventoried	25	30
L IDAM-2	Software platforms and applications within the organization are inventoried	14	19
L IDAM-3	Organizational communication and data flows are mapped	15	18
L IDAM-4	External information systems are catalogued	10	8

2 of 7

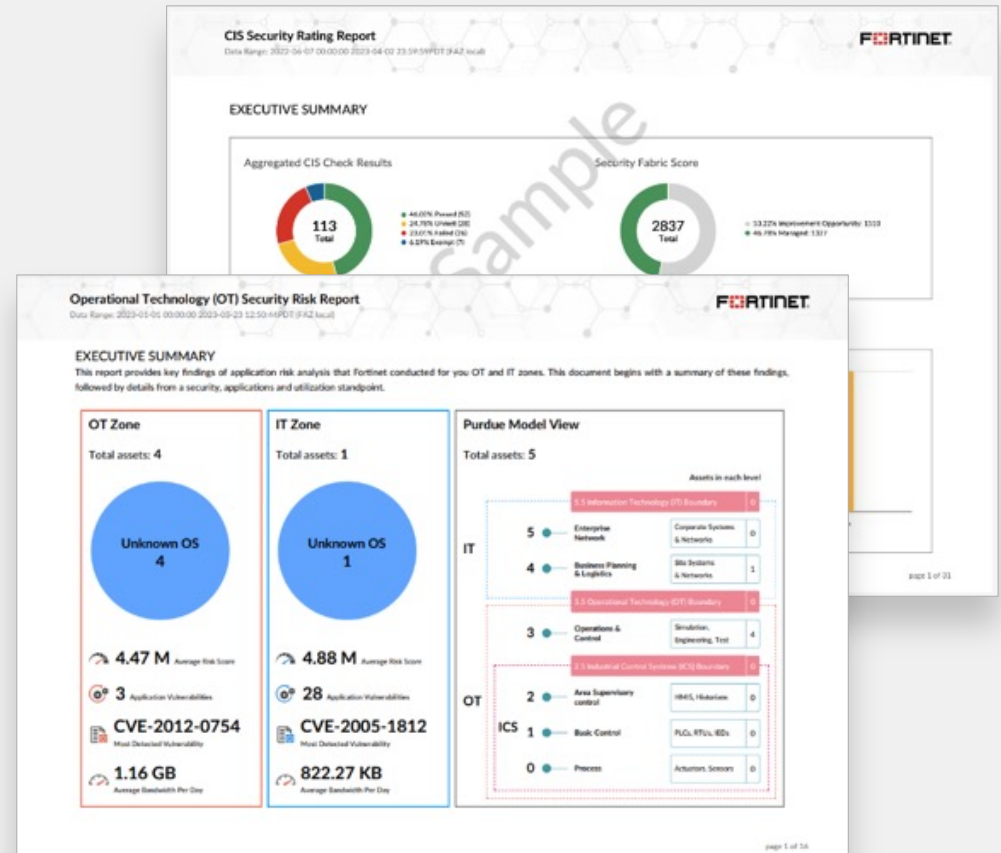


# FortiAnalyzer OT Vulnerability Management

Partly released

- MITRE ATT&CK for ICS
- Asset to vulnerability mapping
- KEV identification and reporting

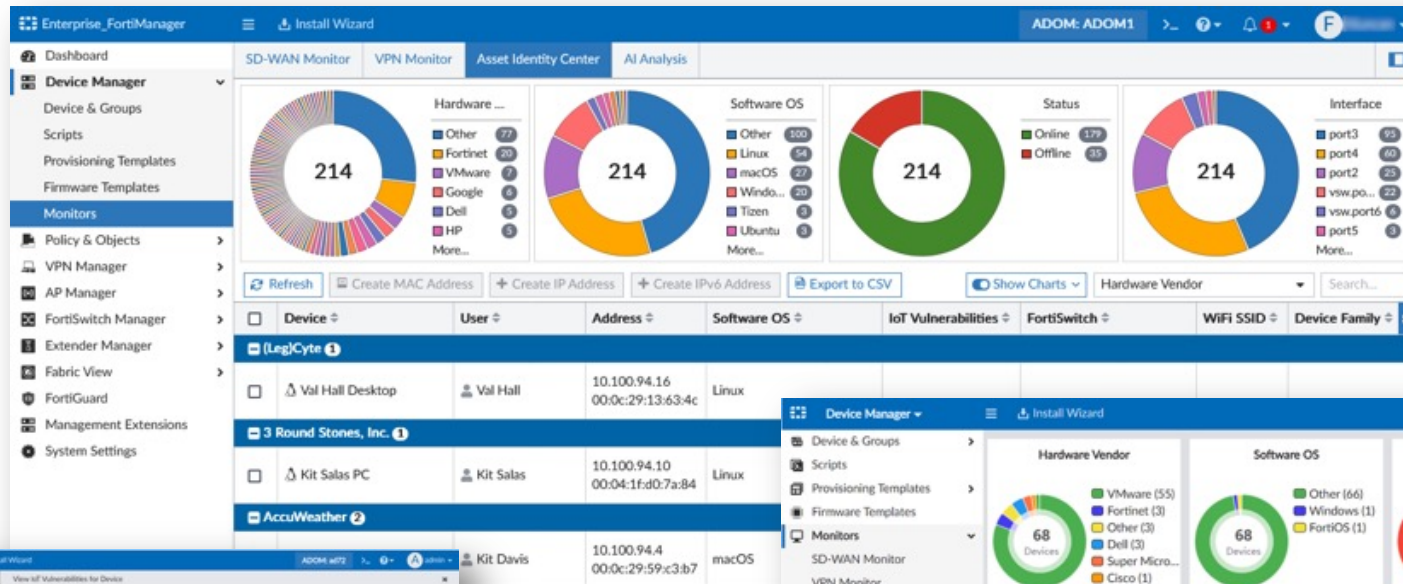
*Requires FAZ OT Security Service*





# FortiManager Asset Identity Center Improvements

FortiManager v7.4.x



*single pane of glass*

View of Vulnerabilities for Device

Vulnerability ID	Severity	Reference	Description
1214	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by CVE. This affects D4200 before 1.1.30.3.
1214	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by authentication bypass. This affects D4200.
1214	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by incorrect configuration of security settings.
1217	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by authentication bypass. This affects D4200.
1218	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated user.
1240	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated user.
1241	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated user.
1242	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by command injection by an authenticated user.
1259	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by stored XSS. This affects D4200 before 1.1.
1243	Critical	CVE-2020-10341	Certain NETGEAR devices are affected by stored XSS. This affects D4200 before 1.1.

Device Manager - Asset Identity Center

Device	User	Address	Software OS	IoT Vulnerabilities	FortiSwitch
Val Hall Desktop	Val Hall	10.100.94.16 00:0c:29:13:63:4c	Linux		
Kit Salas PC	Kit Salas	10.100.94.10 00:04:1f:d0:7a:84	Linux		
Kit Davis		10.100.94.4 00:0c:29:59:c3:b7	macOS		
78ac:44:19:a7:5c		10.59.8.27 78ac:44:19:a7:5c	Other identified device		
80:81:82:83:84:85		178.10.199.186 80:81:82:83:84:85	Other identified device	3	21
b0:7b:25:b8:91:22		10.59.8.25 b0:7b:25:b8:91:22	Other identified device		
e8:1c:ba:7d:77:0e		10.59.8.4 e8:1c:ba:7d:77:0e	FortiOS		



# Purdue Model Based Event Correlation

Available in FortiSIEM v6.5

“*Business Services is a logical grouping of Devices and Applications.*

*Model your OT Devices under the Business Service in FortiSIEM.*

The screenshot displays the FortiSIEM CMDB interface. The left sidebar shows a navigation tree with categories: Devices, Applications, Users, Business Services (expanded), and CMDB Reports. Under Business Services, the following items are listed: IT Srvc, Biz Srvc, Compliance, Operational Technology (highlighted), and Ungrouped. The main content area shows the breadcrumb path: CMDB > Business Services > Operational Technology. Below this, there are buttons for 'New', 'Edit', and 'Delete', along with a dropdown menu set to 'Discovered by All' and a search bar. A table lists the levels of Operational Technology:

Name	Members
Level 5	0
Level 4	2
Level 3.5	1
Level 3	0
Level 2	1
Level 1	2
Level 0	0

Below the table, there is a 'Members' section with an 'Auto expand' checkbox. A table lists the members of Level 1:

Type	Name	Running On	Access IP
Device	PLC1-PCN-A2		192.168.100.197
Device	PLC1-PCN-A1		192.168.100.195



# MITRE ATT&CK for ICS Dashboards

Released in FortiSIEM 6.5

“Three MITRE ATT&CK dashboards for ICS are created to show Rule coverage, Incident coverage and Kill Chain analysis for ICS Techniques.

Currently 84 ICS ATT&CK Technique detection rules are provided out of the box and similar support for other vendors can be added.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Link: <https://docs.fortinet.com/document/fortisiem/6.5.0/release-notes/482665/whats-new-in-6-5-0#MITRE>



# Support for Various OT Technologies

Released in FortiSIEM 6.5

“*FortiSIEM supports these operational technology applications/ devices for discovery and monitoring.*”

- APC Netbotz Environmental Monitor
- APC UPS
- Claroty Continuous Threat Detection
- Cybereason
- Dragos Platform (Dragos Worldview Threat Feed Integration)
- Generic UPS
- Hirschmann SCADA Firewalls and Switches
- Liberty FPC
- Liberty HVAC
- Liberty UPS
- Microsoft Defender for IoT (Was CyberX OT/IoT Security)
- Nozomi Central Management Control (CMC)
- Nozomi SCADAguardian (Asset Discovery)
- OTORIO RAM2 (Risk Assessment, Monitoring and Management)
- VMware NSX-vSphere



# FortiSRA Secure Remote Access

**Agentless Secure Remote Access  
for OT**



## **Manage Remote Access**

Ensure only authorized users have access in a policy of least privilege



## **Manage Privileged Credentials**

Store credentials securely and automatically create and rotate passwords



## **Monitor and Record Sessions**

Post session audit and ability to terminate sessions in real-time



# FortiDeceptor OT/IoT and Medical IoT Decoys

Released in FortiDeceptor 4.2

“Expanded the Medical decoy and added Braun Infusomat pump.

Many vulnerabilities discovered in the Braun Infusomat pump product that exists widely in healthcare organization and become a target for threat actors.

The current FortiDeceptor decoy OS are:

Windows	Windows 7, Windows 10, Windows 2016 and Windows 2019
Linux	Ubuntu Desktop, CentOS, ESXi and ELK
IoT/OT	SCADA version 3, Medical OS, and IoT OS.
VPN	Fortinet SSL-VPN (FG-60E, FG-100F, FG-1500D, FG-2000E, FG-3700D)
Customized Windows	Windows 10, Windows Server 2016, Windows Server 2019

The current FortiDeceptor application decoys are:

Application Decoys	POS OS, ERP OS PACS and SAP
--------------------	-----------------------------

The current FortiDeceptor lure services are:

Windows	RDP, SMB, TCPListener, NBNSspoofSpotter, ICMP and FTP
Linux	SSH, SAMBA, TCPListener, HTTP, HTTPS, GIT, ICMP and FTP
IoT/OT	HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, ENIP, Kamstrup, DNP3, Telnet, PACS-WEB, PACS, DICOM server, Infusion Pump (TELNET), Infusion Pump (FTP), POS-WEB, ERP-WEB, GUARDIAN-AST, IEC104, Jetdirect, Printer-WEB, IP Camera-WEB, UPnP, RTSP, CDP, TP-link WEB, CWMP, SAP DISPATCHER and SAP WEB
SSL VPN	HTTPS
Customized Windows	RDP, SMB, NBNSspoofSpotter, MSSQL, IIS (HTTP/HTTPS) and ICMP

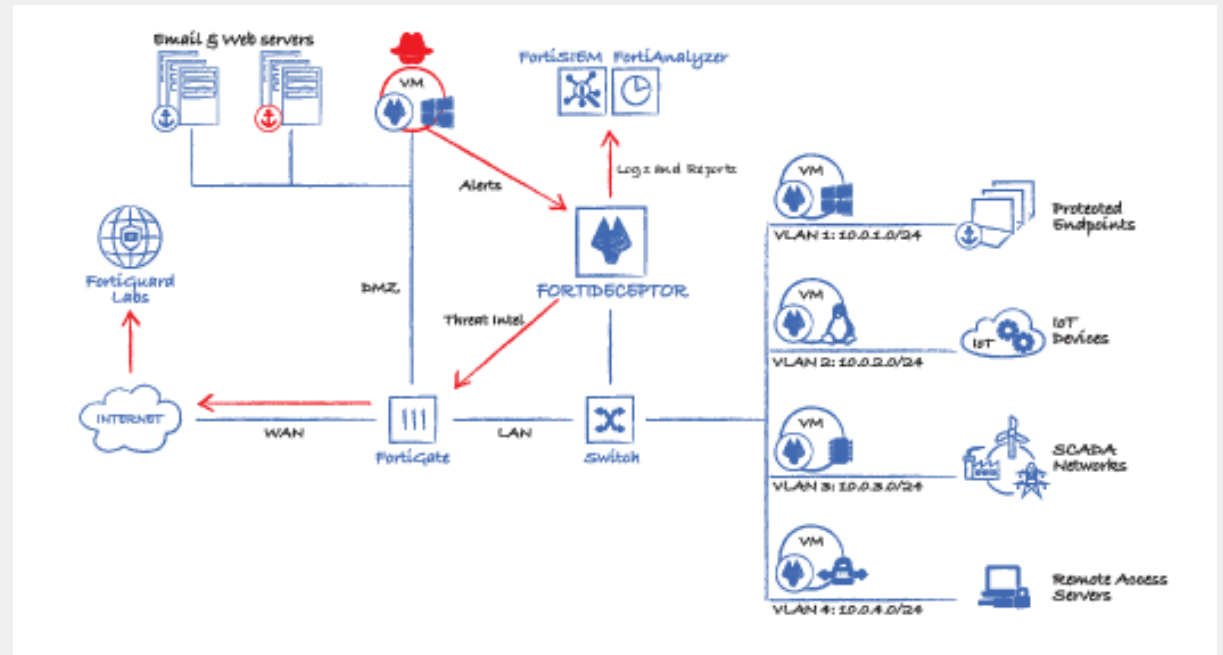


# FortiDeceptor Network Asset Discovery Module

Released in FortiDeceptor 4.2

“The asset discovery generates the network asset inventory using passive network sniffing for network threat visibility and decoy deployment automation.

The network asset discovery supports both IT and IoT/OT networks.

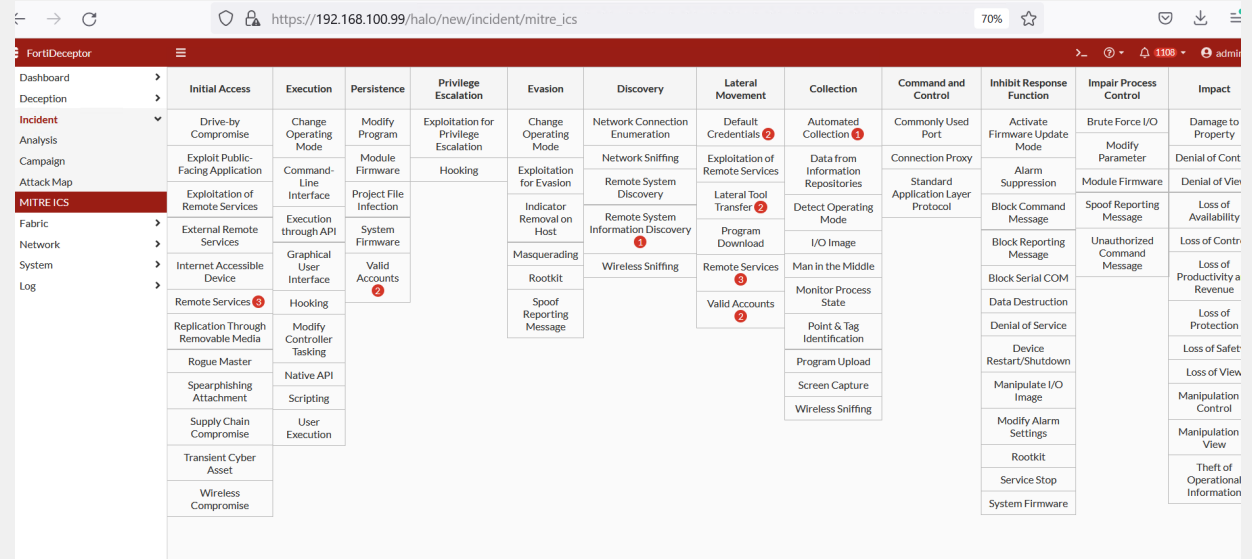




# FortiDeceptor MITRE ATT&CK for ICS

Released in FortiDeceptor 4.3

“FortiDeceptor 4.3.0 supports MITRE ICS framework, both as an independent menu and also inside the incident alert itself, to provide better visibility to incident alerts in the ICS network.



# 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
- NBNSpoofSpotter
- 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

- Azure
- AWS
- Google Cloud



## Medical Decoys

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



## OT Decoys

- Schneider Electric
- Modicon M241
- PowerMeter PM-5560
- EcoStructure BMS Server
- SCADAPack 333E
- Modicon M580
- PowerLogic ION7650
- 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
- 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



# FortiNDR OT Features

On Premises Deployment



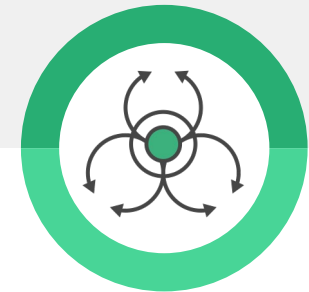
## OT Coverage

- Industrial Security IDS/ IPS
- Application Control
- Device Inventory
- 15+ protocols support
- 50 vendors & applications



## Machine Learning

- Identify applications based on FortiGuard OT Security Service
- Build baseline from customer traffic
- Identify anomalies



## Malware Detection

- Detect OT-specific Malware
- Virtual Security Analyst™
- Artificial Neural Networks

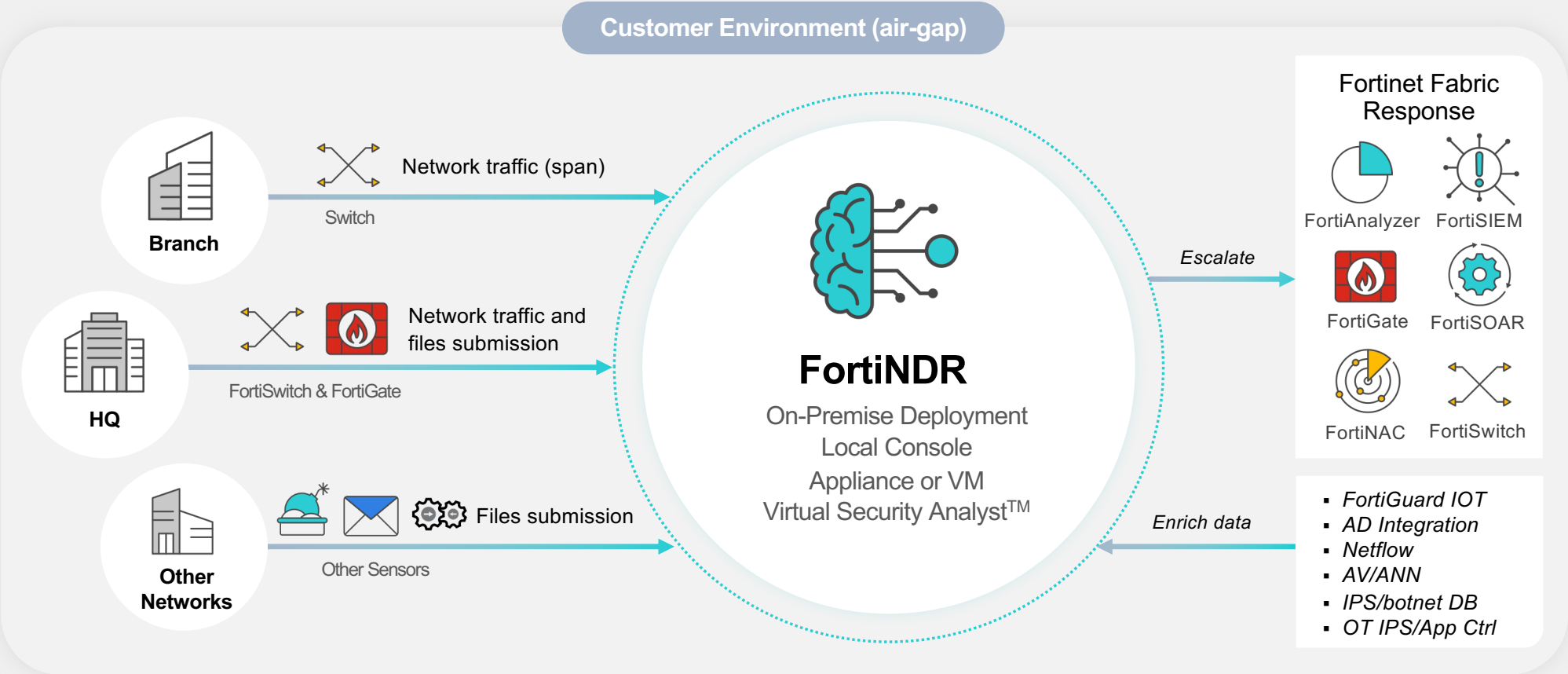
*Another interesting attack using the Industroyer.V2 malware targeted a Ukrainian high-voltage substation*

<https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper>

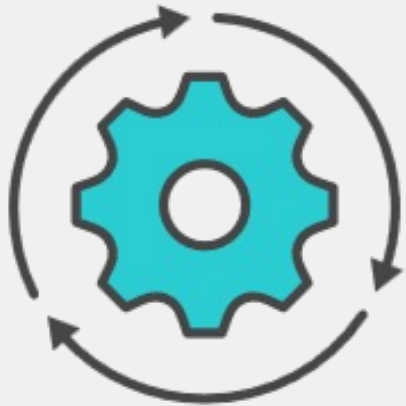


# FortiNDR OT Integration

## On-premises SOC Deployment



# FortiSOAR OT Updates



- “ • *Asset Management with OT Context*
- *IT/OT Overview Dashboard*
- *MITRE ATT&CK for ICS Dashboard*
- *OT Compliance Management – US BOD 22-01, NERC CIP*
- *OT Partner Integrations – OTbase, etc.*
- *OT Threat-Intel Management and KEV correlation*
- *OT View Dashboard – Purdue Model Context*



# FortiSOAR MITRE ATT&CK for ICS Framework

“FortiSOAR offers integrated MITRE ATT&CK for Industrial Control Systems Framework and provides pre-made playbooks for Recommended Mitigations based on the MITRE Technique detected.

The screenshot displays the FortiSOAR interface. The top section, titled 'Dashboard', shows a 'MITRE ATT&CK Thread Spread' with columns for various techniques: Initial Reconnaissance, Privilege Escalation, Lateral Movement, Discovery, Initial Access, Impact, Persistence, Execution, Command and Control, Collection, and Exfiltration. Below this, a detailed view of 'Alert-562' is shown, identifying it as a 'Stuxnet peer to peer communication attempt'. The alert details include source and destination IP addresses, ports, and the target asset 'win7 host1-PC'. A 'Recommended Mitigation' section lists three items: MDP28 (Operating System Configuration), MDP34 (Limit Hardware Installation), and MDP42 (Disable or Remove Feature or Program), each with a brief description of the mitigation action.



# FortiSOAR OT/IT Overview Dashboards

“FortiSOAR added OT/IT overview dashboards to visualize Asset and Alert overview across Purdue Levels. For example,

- Metrics based on Purdue Model and asset distribution
- Metrics on important vulnerabilities
- Metrics on OT risks
- Metrics around Common Techniques
- Metrics around top alerts
- Metrics around MTTD/MTTR






# FortiSOAR NERC CIP Compliance Package

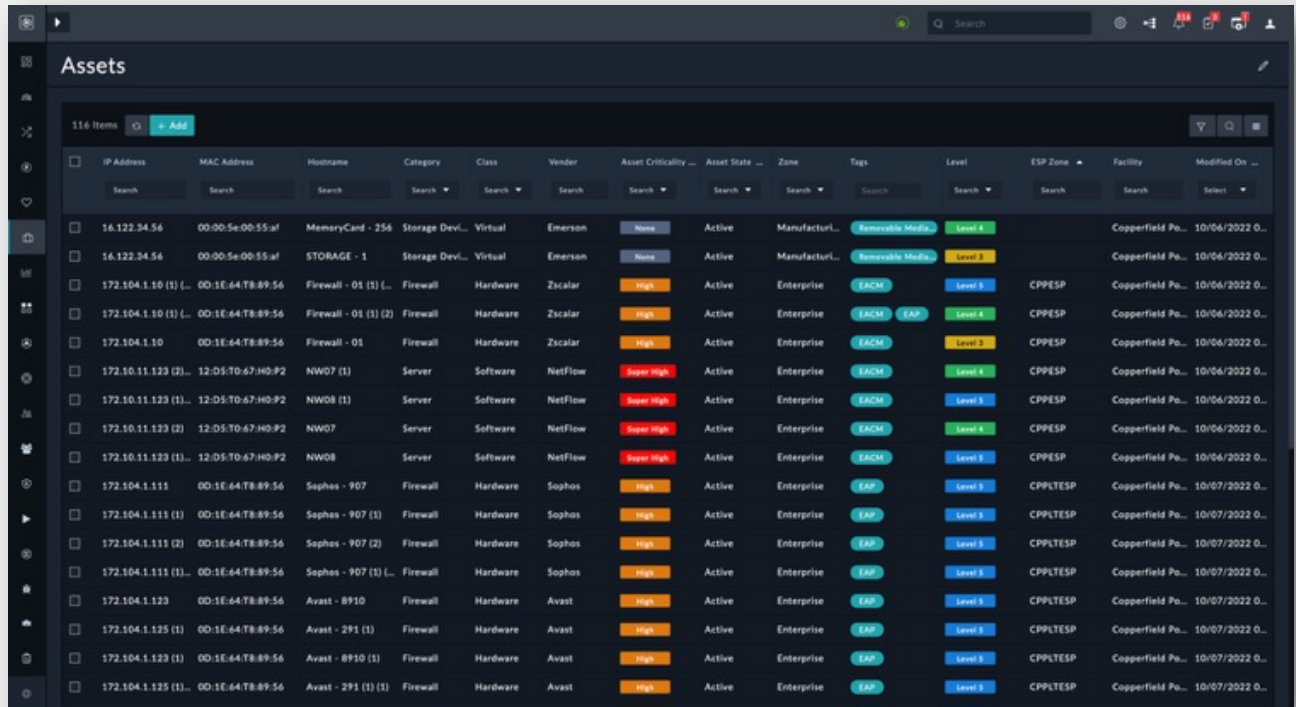
The image displays a collage of screenshots from the FortiSOAR NERC CIP Compliance Package software interface. The primary screenshot in the foreground is titled "BES Cyber System - Impact Evaluation". It features a navigation flowchart with five steps: Start, Associated Assets, Entity & Control Systems, Impact Rating Criteria, and Summary. Below the flowchart, the interface displays the "Evaluated Impact Level: High" and a message: "Based on your selection, the Great Wind Energy - Plant GWE41 system is assessed with a High impact level." A section titled "Here is the list of provided input." lists three categories of input: Entity Type (Generator Operator (GOP), Reliability Coordinator (RC), Transmission Operator (TOP)), Digital Control Systems (Control Center / Backup Control Center, Blackstart Resource), and Criteria (The system is used by and located at a Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability equal to or exceeding 1500 MW in a single interconnection, where no single Generation Resource is rated at 1500 MW or higher). Other screenshots in the background show a "Dashboard" with "Cyber Systems by Impact" (3 BES Cyber Systems) and "Cyber Systems - Entity Type vs Digital Control" bar charts.



# FortiSOAR Asset Management with OT Context

 FortiSOAR added,

- *OT tailored Asset Management modules for Assets, Scans, Vulnerabilities*
- *Zone/Level Context based on Purdue Model*
- *Solution packs for Vulnerability Management and Orchestration*
- *Integrations with 3<sup>rd</sup> party VM vendors like Qualys, Tenable, Rapid7 and the likes*

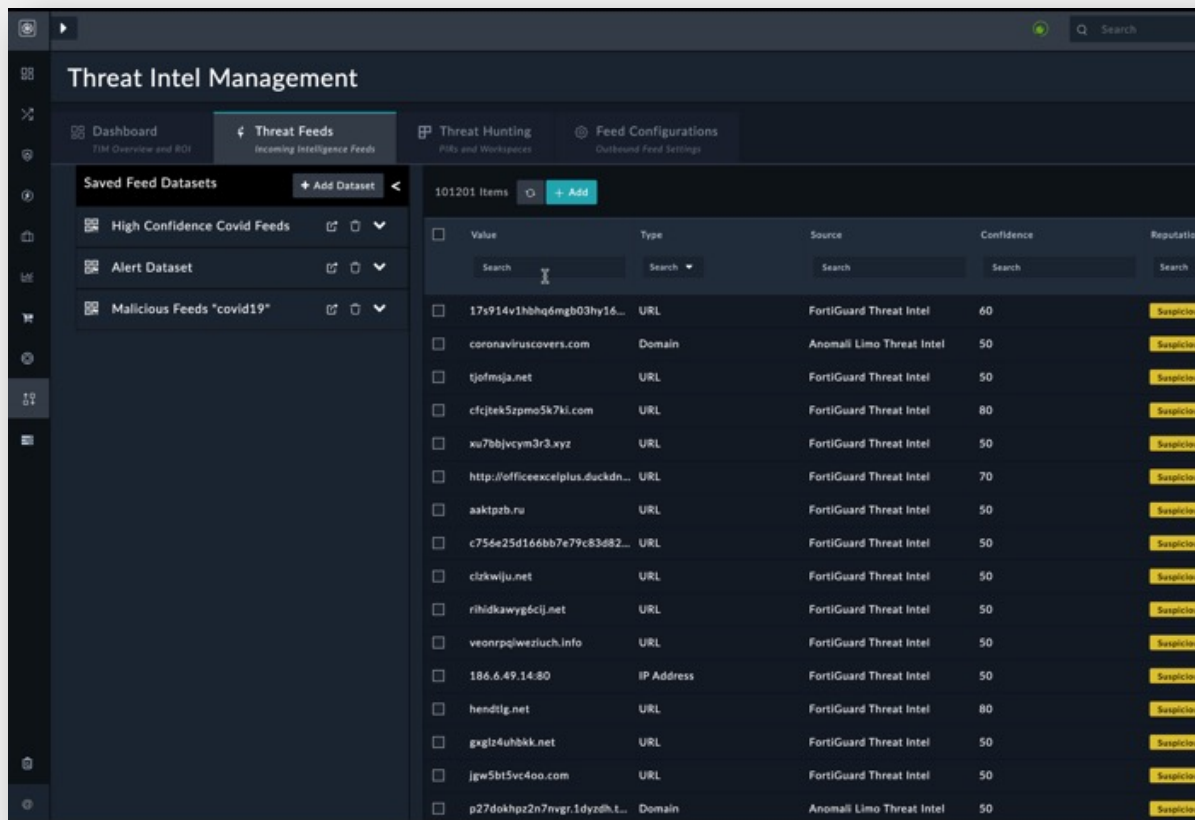


IP Address	MAC Address	Hostname	Category	Class	Vendor	Asset Criticality	Asset State	Zone	Tags	Level	ESP Zone	Facility	Modified On
16.122.34.56	00:00:5e:00:55:af	MemoryCard - 256	Storage Dev...	Virtual	Emerson	None	Active	Manufactur...	Removable Media	Level 4		Copperfield Po...	10/06/2022 0...
16.122.34.56	00:00:5e:00:55:af	STORAGE - 1	Storage Dev...	Virtual	Emerson	None	Active	Manufactur...	Removable Media	Level 2		Copperfield Po...	10/06/2022 0...
172.104.1.10 (1)	00:1E:64:T8:89:56	Firewall - 01 (1)	Firewall	Hardware	Zscaler	High	Active	Enterprise	EACM	Level 3	CPPEP	Copperfield Po...	10/06/2022 0...
172.104.1.10 (1)	00:1E:64:T8:89:56	Firewall - 01 (1) (2)	Firewall	Hardware	Zscaler	High	Active	Enterprise	EACM EAP	Level 3	CPPEP	Copperfield Po...	10/06/2022 0...
172.104.1.10	00:1E:64:T8:89:56	Firewall - 01	Firewall	Hardware	Zscaler	High	Active	Enterprise	EACM	Level 2	CPPEP	Copperfield Po...	10/06/2022 0...
172.10.11.123 (2)	12:05:70:67:H0:P2	NW07 (1)	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 4	CPPEP	Copperfield Po...	10/06/2022 0...
172.10.11.123 (1)	12:05:70:67:H0:P2	NW08 (1)	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 3	CPPEP	Copperfield Po...	10/06/2022 0...
172.10.11.123 (2)	12:05:70:67:H0:P2	NW07	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 4	CPPEP	Copperfield Po...	10/06/2022 0...
172.10.11.123 (1)	12:05:70:67:H0:P2	NW08	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 3	CPPEP	Copperfield Po...	10/06/2022 0...
172.104.1.111	00:1E:64:T8:89:56	Sophos - 907	Firewall	Hardware	Sophos	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.111 (1)	00:1E:64:T8:89:56	Sophos - 907 (1)	Firewall	Hardware	Sophos	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.111 (2)	00:1E:64:T8:89:56	Sophos - 907 (2)	Firewall	Hardware	Sophos	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.111 (1)	00:1E:64:T8:89:56	Sophos - 907 (1)	Firewall	Hardware	Sophos	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.123	00:1E:64:T8:89:56	Avast - 8910	Firewall	Hardware	Avast	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.125 (1)	00:1E:64:T8:89:56	Avast - 291 (1)	Firewall	Hardware	Avast	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.123 (1)	00:1E:64:T8:89:56	Avast - 8910 (1)	Firewall	Hardware	Avast	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...
172.104.1.125 (1)	00:1E:64:T8:89:56	Avast - 291 (1) (1)	Firewall	Hardware	Avast	High	Active	Enterprise	EAP	Level 3	CPPLTESP	Copperfield Po...	10/07/2022 0...



# FortiSOAR Threat-Intel Management

Integration with FortiGuard and 3<sup>rd</sup> party OT security solutions



The screenshot displays the FortiSOAR Threat Intel Management interface. The main panel shows a list of 101201 items. The table below represents the data shown in the interface:

Value	Type	Source	Confidence	Reputation
17s914v1hbhq6mgb03hy16...	URL	FortiGuard Threat Intel	60	Suspicious
coronaviruscovers.com	Domain	Anomali Limo Threat Intel	50	Suspicious
tjofmsja.net	URL	FortiGuard Threat Intel	50	Suspicious
cfctek5zpmo5k7ki.com	URL	FortiGuard Threat Intel	80	Suspicious
xu7bbjvcym3r3.xyz	URL	FortiGuard Threat Intel	50	Suspicious
http://officeexcelplus.duckdn...	URL	FortiGuard Threat Intel	70	Suspicious
aaktptz.ru	URL	FortiGuard Threat Intel	50	Suspicious
c754e25d166bb7e79c83d82...	URL	FortiGuard Threat Intel	50	Suspicious
clzkwju.net	URL	FortiGuard Threat Intel	50	Suspicious
rihidkawy6clj.net	URL	FortiGuard Threat Intel	50	Suspicious
veonrpgweziuch.info	URL	FortiGuard Threat Intel	50	Suspicious
186.6.49.14.80	IP Address	FortiGuard Threat Intel	50	Suspicious
hendtlg.net	URL	FortiGuard Threat Intel	80	Suspicious
gxgtz4uhkk.net	URL	FortiGuard Threat Intel	50	Suspicious
jgw5bt5vc4oo.com	URL	FortiGuard Threat Intel	50	Suspicious
p27dohpz2n7nvr.1dyzth.L...	Domain	Anomali Limo Threat Intel	50	Suspicious

“FortiSOAR added OT specific threat-intel management

- Multiple threat feed integrations, normalized single pane view of threat feeds. FortiGuard lookup and feed included.
- Includes full threat intelligence lifecycle: Planning & Direction, Collection, Processing, Analysis, Production and Dissemination, and Feedback.
- FortiGuard Industrial Security Service integration coming soon



# FortiSOAR Security Fabric Integrations

“Seamless integrations for security orchestration and automation across Fortinet Security Fabric solutions.”

Connector Name	Version	Published By	Description
Fortinet FortiGate	5.2.0	Fortinet	Fortinet FortiGate enterprise firewall provide high performance...
Fortinet FortiNDR	1.2.0	Fortinet	The FortiNDR is a leading-edge product which utilizes machine...
Fortinet FortiAnalyzer	3.0.0	Fortinet	FortiAnalyzer is the NOC-SOC security analyst tool built with operations...
Fortinet FortiEDR	1.3.0	Fortinet	FortiEDR protects endpoints pre and post infection, stopping data breach...
Fortinet FortiGuard Threat Intelligence	3.0.2	Fortinet	FortiGuard Threat Intelligence is the global threat intelligence and resarc...
Fortinet FortiMail	1.1.0	Fortinet	Fortinet-FortiMail Connector facilitates automated operation FortiMail email...
Fortinet FortiOS	3.0.0	Fortinet	FortiOS connector uses rest apis to perform automated operations such a...
Fortinet FortiSandbox	1.0.4	Fortinet	FortiSandbox utilizes advanced detection, dynamic antivirus scannin...
Fortinet FortiSIEM	4.5.0	Fortinet	FortiSIEM provides integrations that allow you to query and make changes...
Fortinet FortiAuthenticator	1.0.0	Fortinet	FortiAuthenticator provides centralized authentication services for the Fortn...
Fortinet FortiClient EMS	1.0.1	Fortinet	FortiClient Enterprise Management Server (FortiClient EMS) is a security...
Fortinet FortiCWP	1.0.0	Fortinet	Fortinet's FortiCWP integrates with APIs provided by cloud vendors...
Fortinet FortiManager	3.0.0	Fortinet	The Fortinet FortiManager provides easy centralized configuration, policy...
Fortinet FortiMonitor	1.0.1	Fortinet	FortiMonitor is a cloud-based monitoring SAAS service with full...
Fortinet FortiNAC	1.0.0	Fortinet	FortiNAC is the Fortinet network access control solution. It enhances...



**F****RTINET**®