FORTINET

Захист інформаційних систем критичної інфраструктури

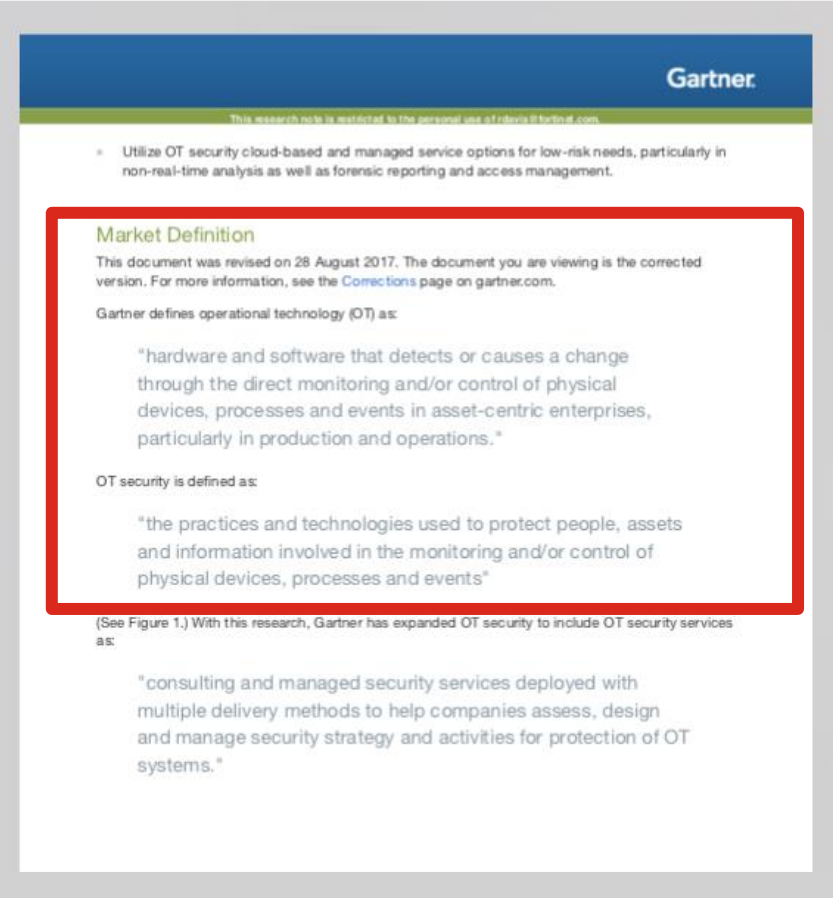
Високоефективні рішення безпеки, розроблені для безпечної та надійної роботи інформаційних систем в ОТ (Операційніх Технологіях).

Київ 2023

Зміст

Виклики кібербезпеки в Операційних Технологіях (ОТ)

Визначення OT, та їх безпеки -Gartner Market Guide



Gartner

This research note is restricted to the personal use of rdavis@fortinet.com.

- Utilize OT security cloud-based and managed service options for low-risk needs, particularly in non-real-time analysis as well as forensic reporting and access management.

Market Definition

This document was revised on 28 August 2017. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner defines operational technology (OT) as:

"hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations."

OT security is defined as:

"the practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events"

(See Figure 1.) With this research, Gartner has expanded OT security to include OT security services as:

"consulting and managed security services deployed with multiple delivery methods to help companies assess, design and manage security strategy and activities for protection of OT systems."

Що таке Операційні Технології (OT)?

«апаратне та програмне забезпечення, яке виявляє або викликає зміни шляхом прямого моніторингу та/або контролю фізичних пристроїв, процесів і подій на підприємствах, орієнтованих на активи, зокрема у виробництві та операційній діяльності».

Що таке безпека операційних технологій?

«практики та технології, що використовуються для захисту людей, активів та інформації, залучених до моніторингу та/або контролю фізичних пристроїв, процесів і подій»

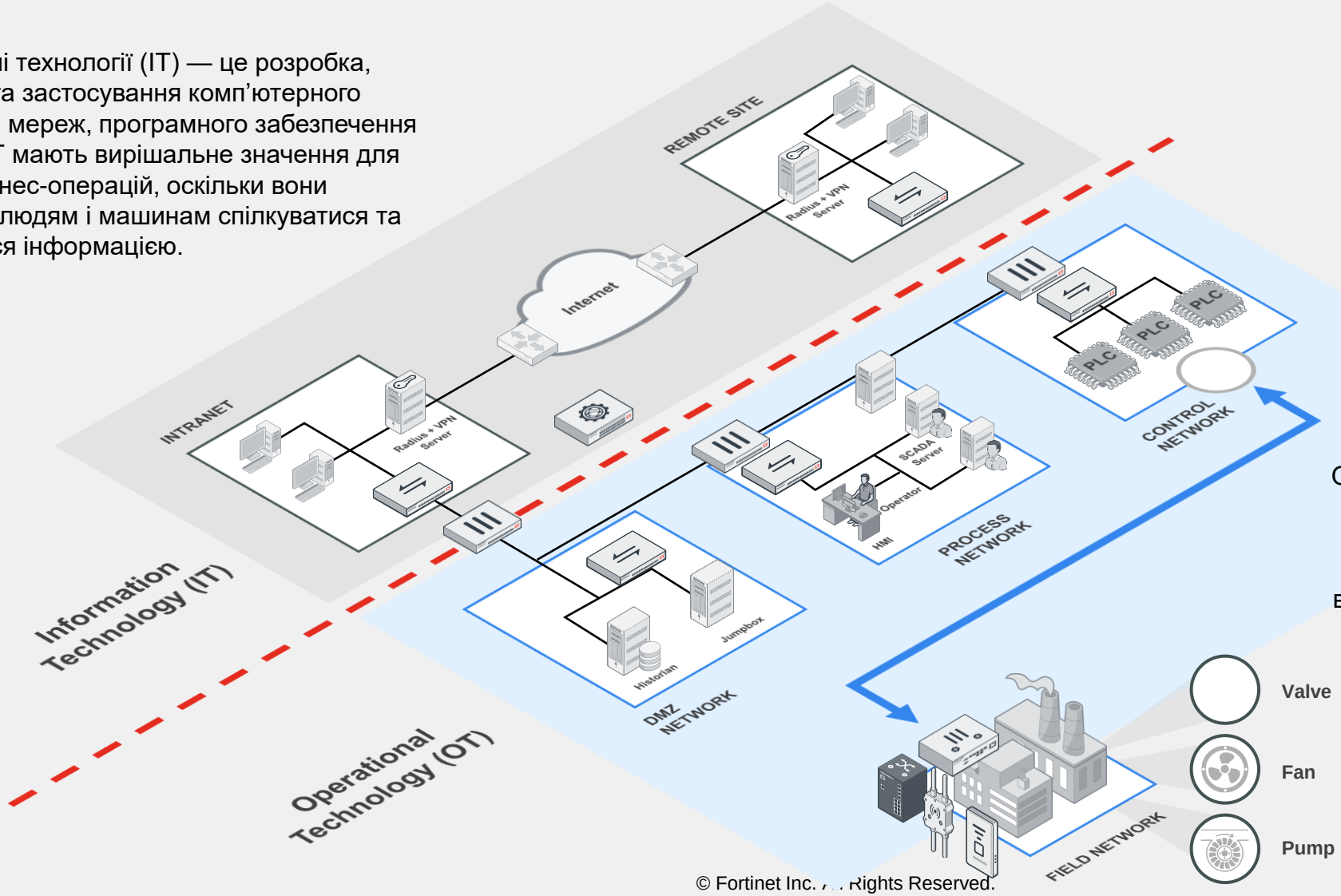
OT відомі також, як SCADA

Supervisory control and data acquisition (SCADA) - це архітектура системи керування в OT

Що таке IT і OT?

Information Technology and Operational Technology (IT/OT)

Інформаційні технології (IT) — це розробка, управління та застосування комп'ютерного обладнання, мереж, програмного забезпечення та систем. IT мають вирішальне значення для сучасних бізнес-операцій, оскільки вони дозволяють людям і машинам спілкуватися та обмінюватися інформацією.



Операційні технології (OT) використовують апаратне та програмне забезпечення для керування промисловим обладнанням і системами. OT контролюють високотехнологічні спеціалізовані системи, наприклад, в енергетичній, промисловій, виробничій, нафтовій і газовій промисловості, робототехніці, телекомунікаціях, утилізації відходів і водопостачанні.

Де ми можемо знайти ОТ?

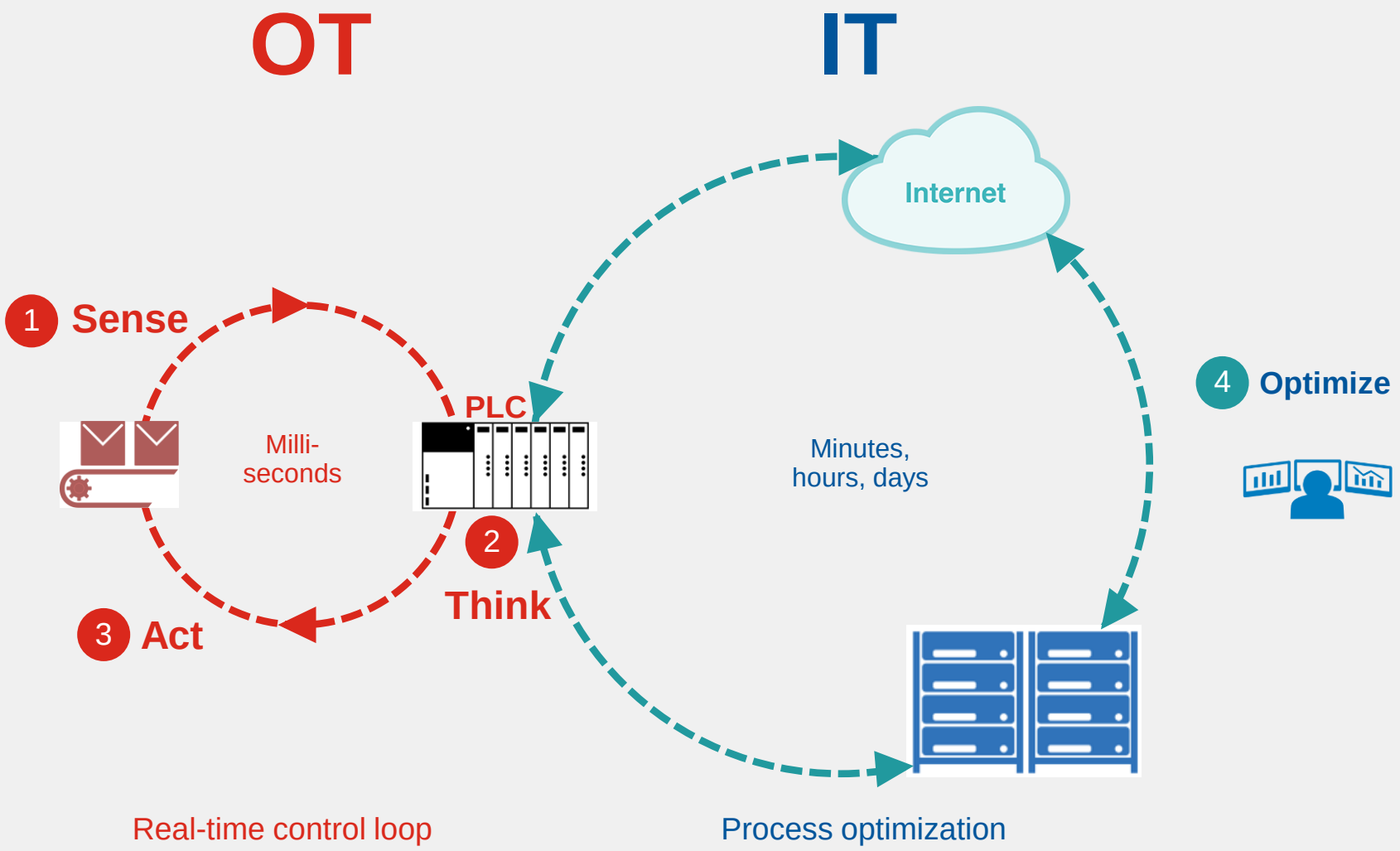
Сектори Критичної Інфраструктури

Цифровізація

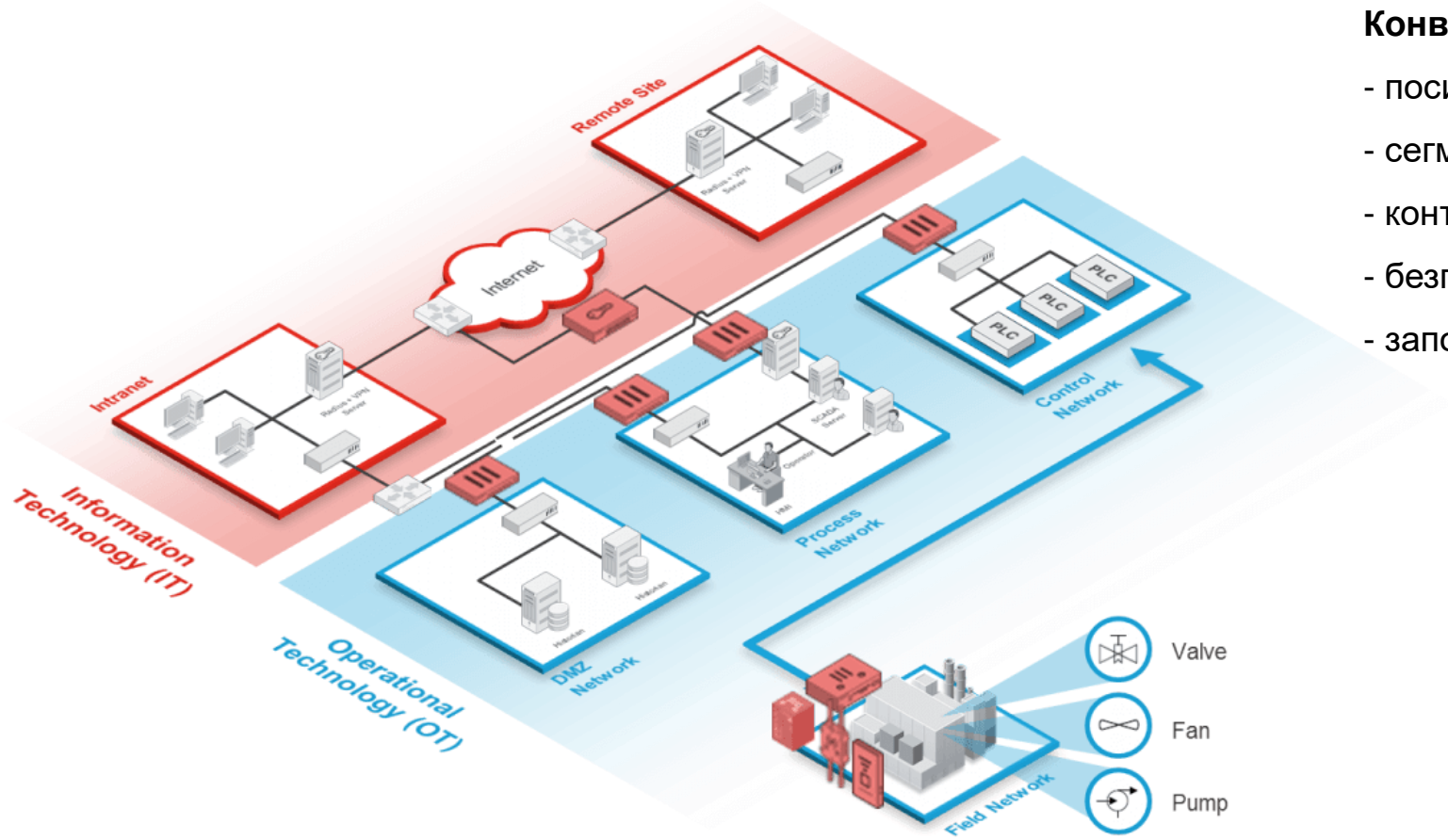
Впливає на всі галузі

Що насправді змінюється в OT?

Оптимізація бізнес-процесів, що сприяє конвергенції IT/OT



Захист взаємопов’язаних IT та OT



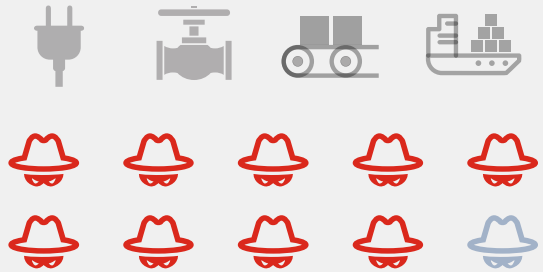
Конвергенція IT і OT

- посилення безпеки пристроїв
- сегментація мережі
- контроль доступу (користувачі, пристрої)
- безпечний бездротовий доступ
- запобігання загрозам в протоколах ICS

Кіберзагрози є реальними для OT

Розкриті інциденти – лише вершина айсберга.

- Збільшення частоти та $ шкоди атак на OT&CI
- Зростання **Ransomware** націленого на OT в ’22 (наприклад: Lockbit, Conti, RaaS)
- **APT групи** є зростаючою загрозою для OT … Нові спонсоровані державою фреймворки для атак на ICS (наприклад, Incontroller)
- Інтенсивна експлуатація **IIoT вразливостей** в OT (наприклад: Ripple20, Mirai botnet, Log4j, BrickerBot,...)
- Високоефективні **Supply-Chain** атаки (атаки на ланцюги постачання) в 2022 (наприклад: Kaseya VSA, Codecov, Fantasy Agrius wiper, ...)
- Розповсюдження через змінні носії у 35%+ початкових векторів атак в інцидентах OT/ICS 2022 року
- Атаки на вразливості MS.Windows (головним чином CVE-2020-1381.Privilege.Elevation) спричинили **найбільшу кількість спрацюваннь IPS у другій половині 2022 ,** більшу за Log4j



9 з 10

Організаційй OT зазнали принаймні одного вторгнення за минулий рік, а **63% мали 3 або більше вторгнень**

Feb ‘23 Fortinet Global Threat Landscape Report
Jun ’22 Fortinet state of OT/ICS Report
Oct ‘22 SANS/Fortinet State of ICS/OT Report

...це впливає на бренд, кредитний рейтинг, конкурентну перевагу, регулювання, ...

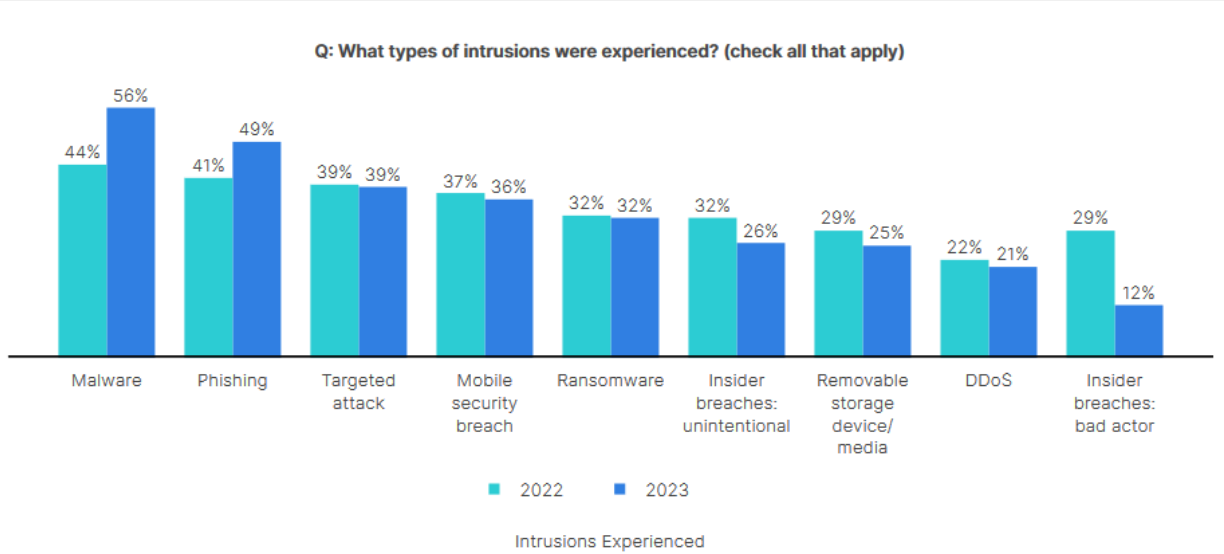
Глобальна статистика по OT користувачах Fortinet – 2023 vs 2022

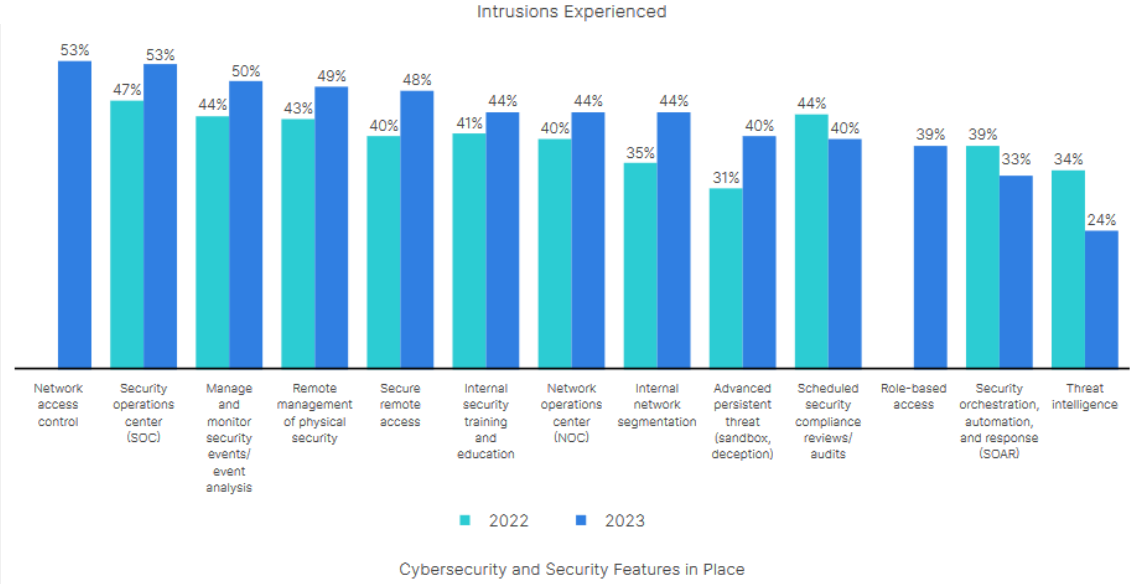
Статистика вторгнень

- Зростання malware та phishing атак

Вдосконалення захисту

- Впровадження NAC
- Розгортання SOC
- Захист віддаленого доступу

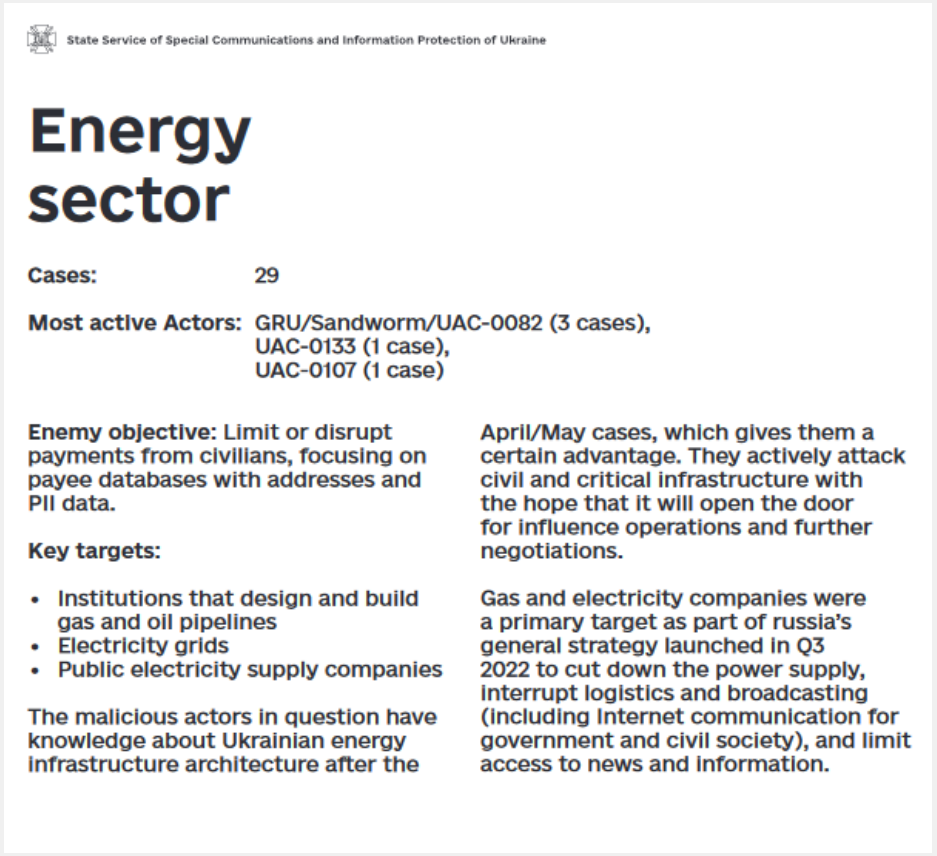




Джерело: State of Operational Technology and Cybersecurity 2023, Fortinet

Звіт ДССЗЗІ за 2022 рік

- Атаки на енергетику та транспорт



State Service of Special Communications and Information Protection of Ukraine

Energy sector

Cases: 29

Most active Actors: GRU/Sandworm/UAC-0082 (3 cases), UAC-0133 (1 case), UAC-0107 (1 case)

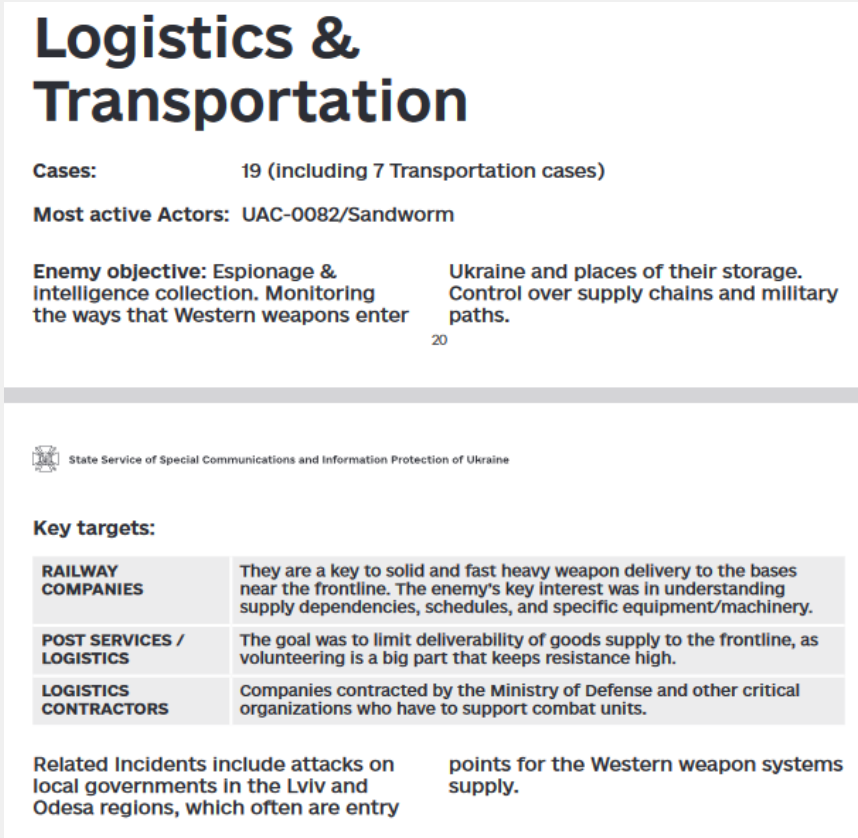
Enemy objective: Limit or disrupt payments from civilians, focusing on payee databases with addresses and PII data.

Key targets:

- Institutions that design and build gas and oil pipelines
- Electricity grids
- Public electricity supply companies

The malicious actors in question have knowledge about Ukrainian energy infrastructure architecture after the April/May cases, which gives them a certain advantage. They actively attack civil and critical infrastructure with the hope that it will open the door for influence operations and further negotiations.

Gas and electricity companies were a primary target as part of russia's general strategy launched in Q3 2022 to cut down the power supply, interrupt logistics and broadcasting (including Internet communication for government and civil society), and limit access to news and information.



Logistics & Transportation

Cases: 19 (including 7 Transportation cases)

Most active Actors: UAC-0082/Sandworm

Enemy objective: Espionage & intelligence collection. Monitoring the ways that Western weapons enter Ukraine and places of their storage. Control over supply chains and military paths.

20

State Service of Special Communications and Information Protection of Ukraine

Key targets:

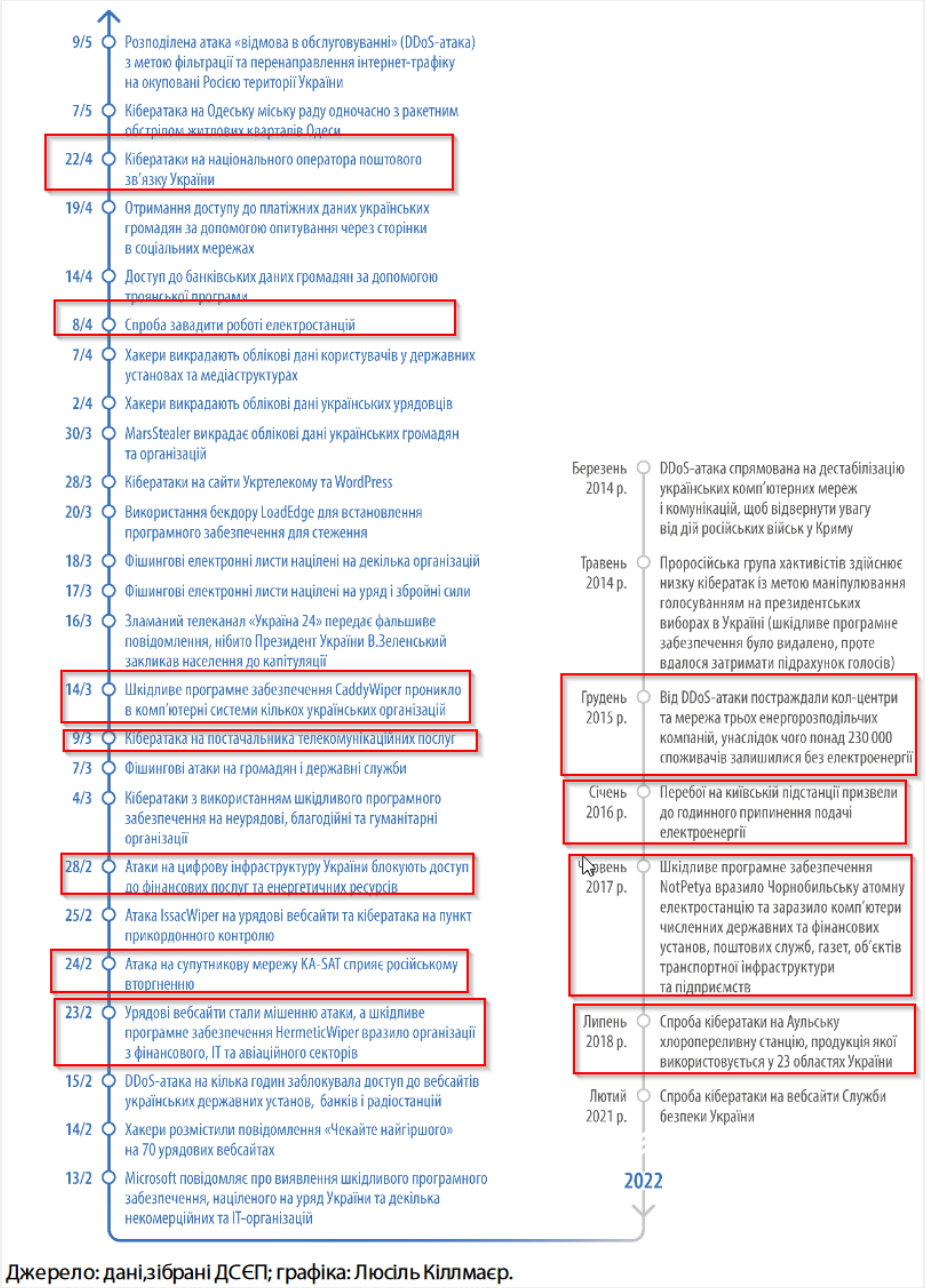
RAILWAY COMPANIES	They are a key to solid and fast heavy weapon delivery to the bases near the frontline. The enemy's key interest was in understanding supply dependencies, schedules, and specific equipment/machinery.
POST SERVICES / LOGISTICS	The goal was to limit deliverability of goods supply to the frontline, as volunteering is a big part that keeps resistance high.
LOGISTICS CONTRACTORS	Companies contracted by the Ministry of Defense and other critical organizations who have to support combat units.

Related Incidents include attacks on local governments in the Lviv and Odesa regions, which often are entry points for the Western weapon systems supply.

Джерело: Russia's Cyber Tactics: Lessons Learned 2022, ДССЗЗІ

Брифінг Дослідницької служби Європейського парламенту

- 30% від атак – націлено на ОТ

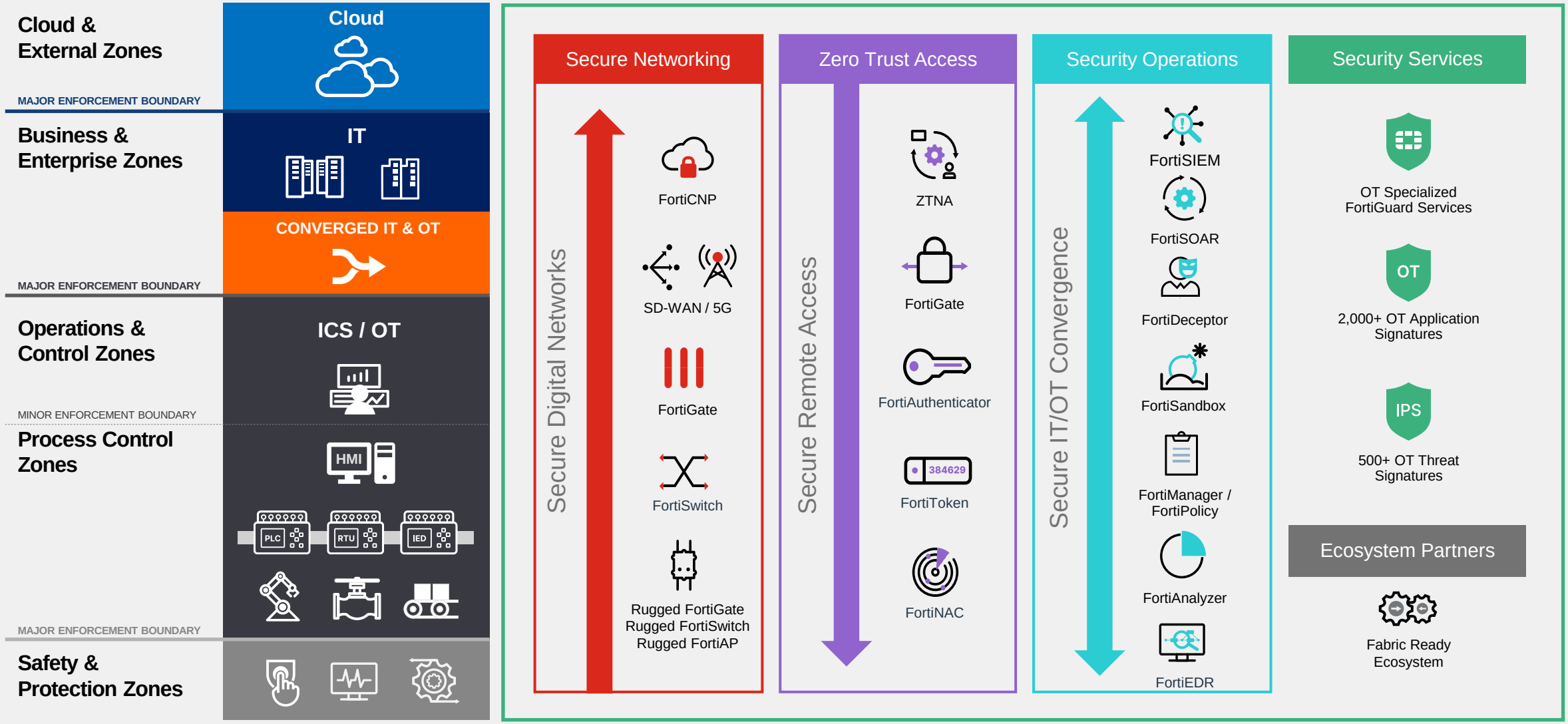


Джерело: дані,зібрані ДСЄП; графіка: Люсіль Кіллмаєр.

Джерело: Війна Росії проти України: хронологія кібератак, Дослідницька служба Європейського парламенту

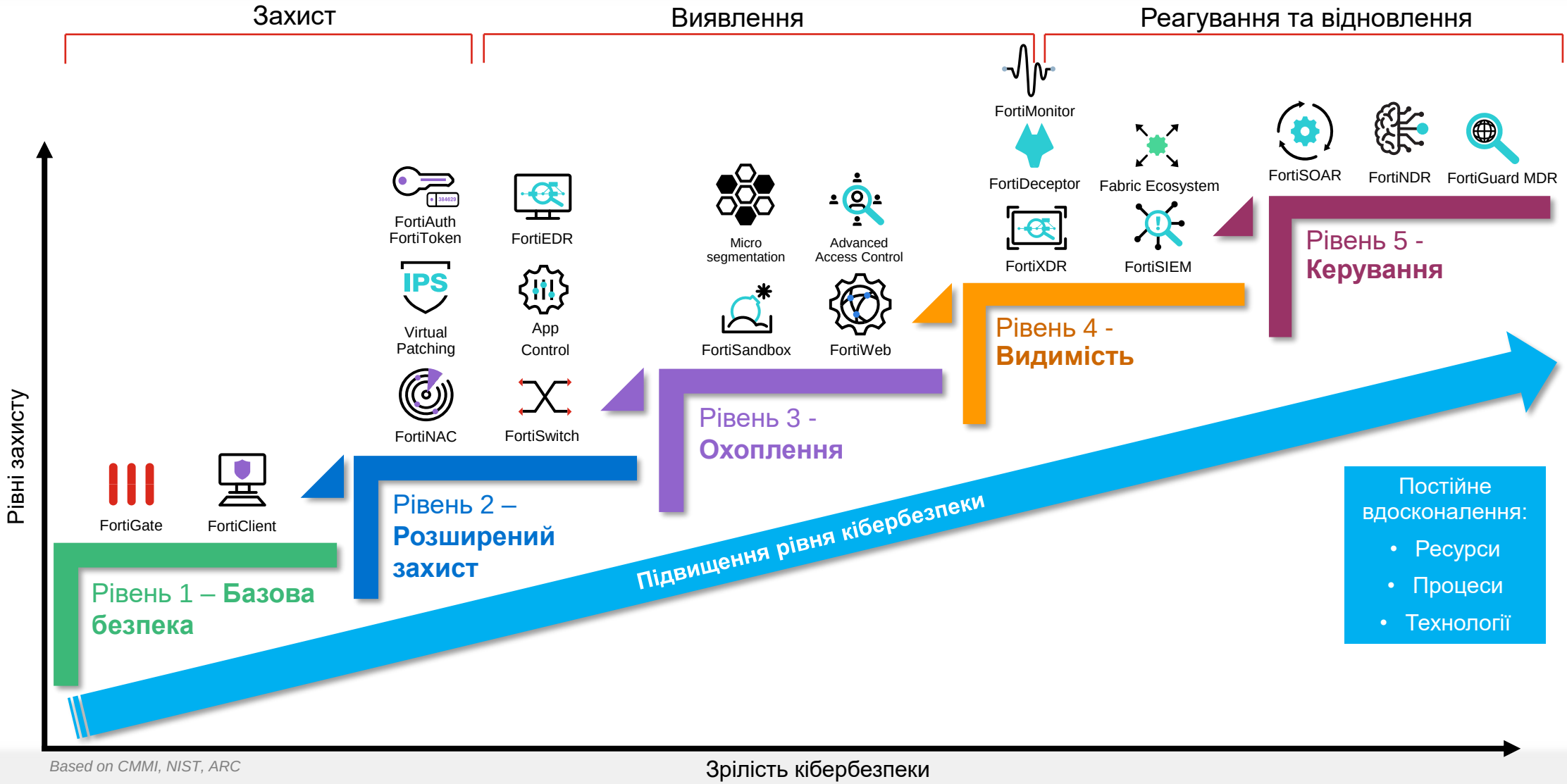
Спеціалізовані рішення для безпеки OT від Fortinet

Security Fabric для Операційних Технологій



Шкала зрілості кібербезпеки

з портфоліо Fortinet



Based on CMMI, NIST, ARC

Спеціалізовані пристрої Fortinet для ICS/OT

FortiGate, FortiSwitch, FortiAP & FortiDeceptor Rugged Series

Захищений (rugged) дизайн
Відсутність вентилятора та використання надійних компонентів забезпечують надійну роботу в агресивних промислових середовищах.

Консолідована архітектура безпеки
FortiGate з консолідованою безпекою FortiOS надає кращий захист і нижчу вартість володіння, ніж багато точкових продуктів.

Простота управління
Дозволяє швидко розгортати, відстежувати стан пристрою та загрози, надаючи актуальні звіти.

FortiGate Rugged Series

FGR-70F
DIN-rail mounted, SoC4-powered, security and VPN gateway

FGR-70F 3G/4G
DIN-rail mounted, SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

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

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

FortiSwitch, FortiAP & FortiDeceptor Rugged

FSR-112D-POE
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.

FortiDeceptor Rugged 100G
Fan-less desktop form factor. AC or DC powered. 6 x 1GbE RJ-45 ports. 1TB SSD storage.

FortiAP Rugged 234F & FortiAP Rugged 432F
External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

Функіонал FortiGate

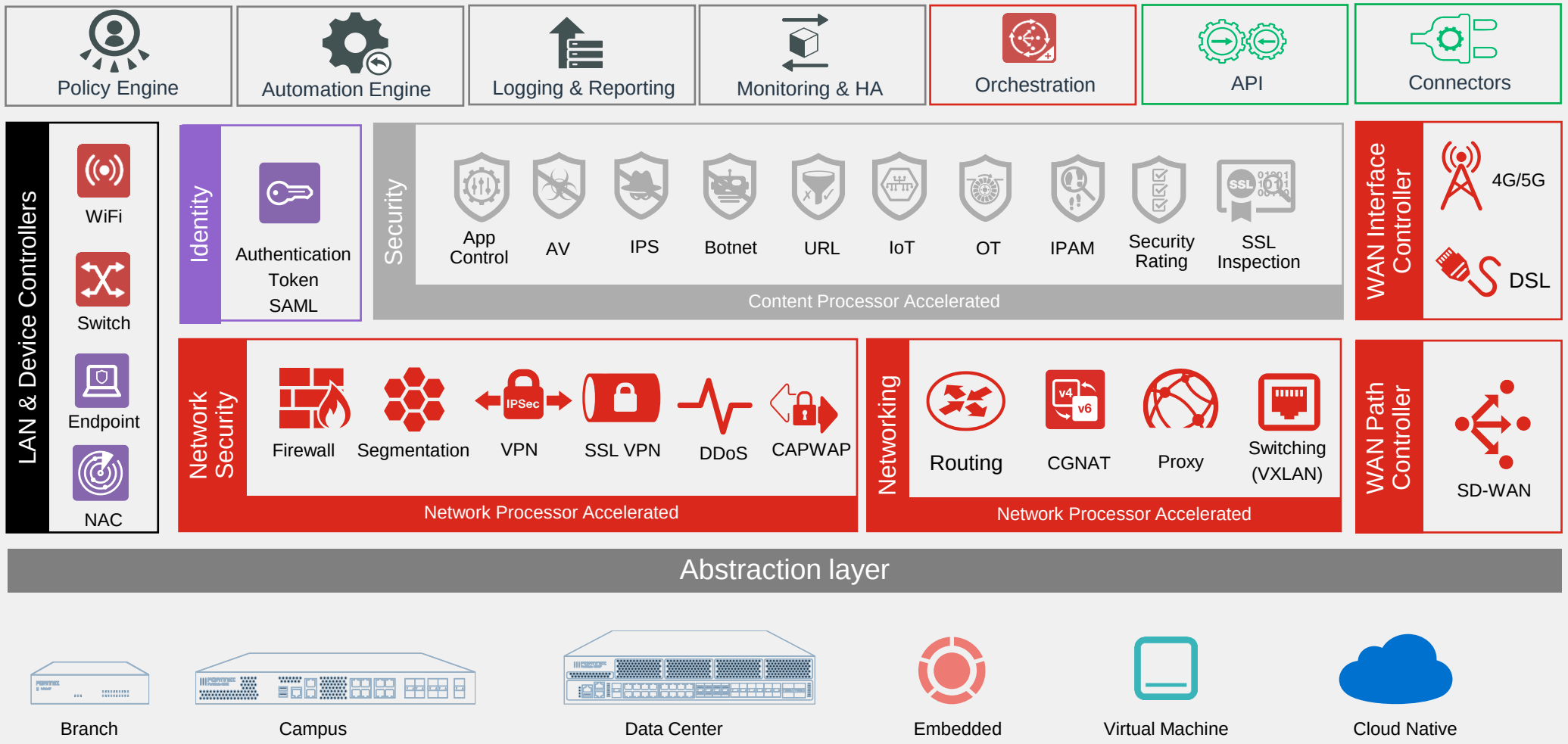
- Security (IPS, FW, OT traffic monitor)
- Encryption (GRE, VXLAN, IPSEC)
- Connectivity (Proxy, VLANs, IPv6.)
- Advance features (SD-WAN)
- Central authentication (LDAP, RADIUS)
- IPS Service (Virtual Patching)
- Industrial Security Service for OT
- IoT Detection Service
- Antivirus, Anti-malware, Bonet, CDR, Virus Outbreak Protection & Sandbox services
- URL, Web, Video DNS Content Filtering
- Wi-Fi
- IPSEC VPN & SSL VPN
- SSL Inspection
- Packet capture triggered by IPS
- Virtual Domains (VDOM)
- Transparent or Proxy

FortiGate – NGFW для OT

FortiGate Rugged Series: порівняння

	FGR-60F/-3G4G	FGR-70F/-3G4G
Firewall (1518 UDP)	6 Gbps	8 Gbps
Concurrent Sessions	600,000	1 Million
New Sessions/Sec	19,000	35,000
IPSec VPN	3.5 Gbps	6.5 Gbps
IPS (Ent. Mix)	950 Mbps	975 Mbps
NGFW (Ent. Mix)	550 Mbps	950 Mbps
Threat Protection (Ent. Mix)	500 Mbps	580 Mbps
Interfaces	4 x GE RJ45 Switch ports, 2 x Shared Media pairs (can be configured with 1 RJ45 Bypass pair)	4x GE RJ45 ports, 1x GE RJ45 bypass port pair (between PORT3 and PORT4), 2x GE RJ45 WAN ports, 2x SFP slots
Storage	-	
Others	IP 20 Rated	IP 40 Rated

FortiOS Network Operating System

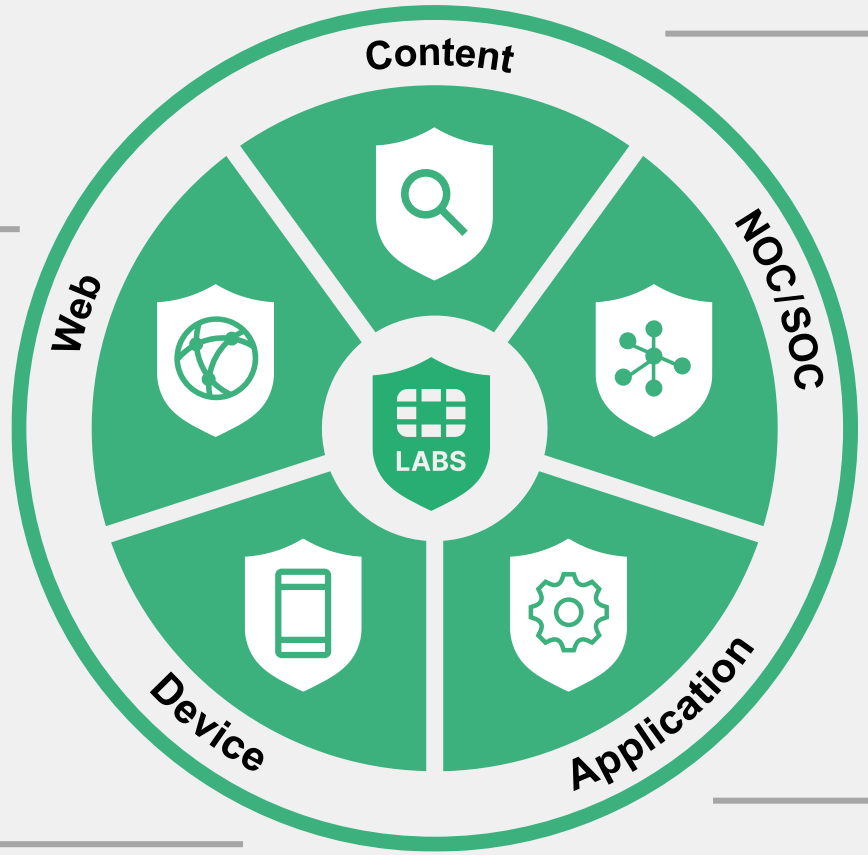


FortiGuard - безпека посилена штучним інтелектом

Web
- URL Filtering
- DNS security
- Secure Web Gateway
- Phishing
- Geo-location
- In-line CASB
- Anti-spam

FortiGuard Labs
- Real-Time Security update
- AI & Machine Learning models developments on both local and large-scale Cloud-driven data lakes
- Zero-Day discovery
- Outbreak Alerts
- Threat Monitoring and Communications
- Industry Alliances

Device Security (IT | OT | IoT)
- Exploit Protection
- Vulnerability Detection
- Virtual Patching
- IPS Known and Zero-Days with Botnet & C2



Content
- AI Sandbox & EDR Behavior
- Polymorphic Anti-Malware | Antivirus
- Mobile Malware
- Credential-stuffing defense

NOC/SOC
- Decoys
- IOC Ingestion and Search
- Advanced Forensics & Threat Hunting
- AI-powered investigation & Automated Integrative IR
- Outbreak Detection services (FAZ, FCT, FOS)
- Automated playbooks and remediation
- Fabric Rating Proactive Assessments and Simplified Migration

Application Security
- Secure Email Gateway
- WAF signatures
- DDOS
- CASB – SaaS Security
- ADC

FortiOS 7.2 підписки

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) Service	•	•	•	•
	URL, DNS and Video Filtering Service	•	•	•	
	FortiGuard Anti-Spam Service		•	•	
	FortiGuard IoT Detection Service	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiGuard AI-based Sandbox Service	•			

FortiOS 7.2 підписки

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	FortiGuard Application Control	*included with FortiCare Subscription*			
	FortiCloud ZTNA Inline CASB Service				
	Internet Service (SaaS) and botnet DB Updates				
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

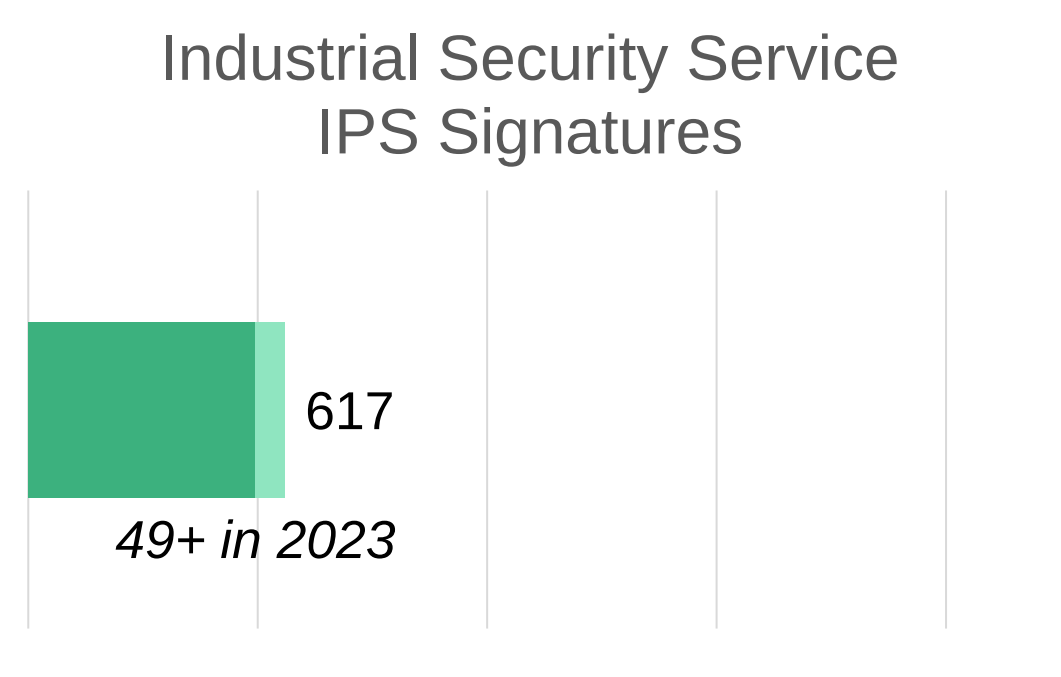
IPS / Application Control для промислових протоколів

2,900+ Granular OT/ICS Application Controls (DNP3 Example)

- DNP3
- DNP3_Abort.File
- DNP3_Activate.Config
- DNP3_Assign.Class
- DNP3_Authenticate.File
- DNP3_Authentication.Error
- DNP3_Authentication.Request
- DNP3_Close.File
- DNP3_Cold.Restart
- DNP3_Confirm
- DNP3_Delay.Measurement
- DNP3_Delete.File
- DNP3_Direct.Operate
- DNP3_Direct.Operate.Without.Ack
- DNP3_Disable.Spontaneous.Messages
- DNP3_Enable.Spontaneous.Messages
- DNP3_Freeze.And.Clear
- DNP3_Freeze.And.Clear.Without.Ack
- DNP3_Freeze.With.Time
- DNP3_Freeze.With.Time.Without.Ack
- DNP3_Get.File.Info
- DNP3_Immediate.Freeze
- DNP3_Immediate.Freeze.Without.Ack
- DNP3_Initialize.Application
- DNP3_Initialize.Data
- DNP3_Open.File
- DNP3_Operate
- DNP3_Read
- DNP3_Record.Current.Time
- DNP3_Response
- DNP3_Save.Configuration
- DNP3_Select
- DNP3_Start.Application
- DNP3_Stop.Application
- DNP3_Unsolicited.Message
- DNP3_Warm.Restart
- DNP3_Write

Сигнатури Industrial Security Service IPS

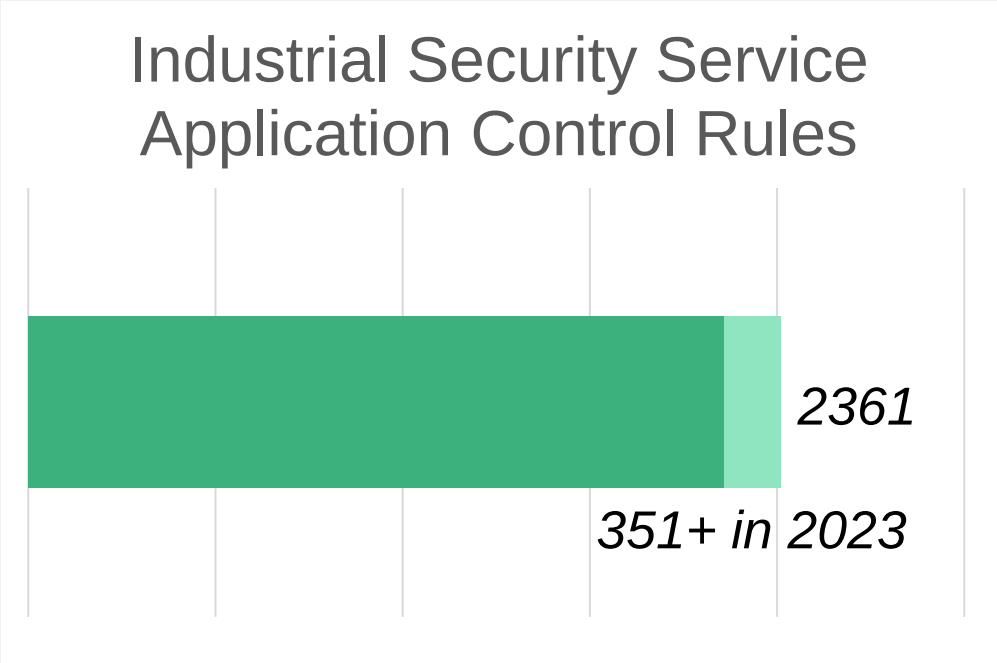
Protections Added	
Advantech	OpenPLC
Delta IA	Rockwell
Eaton	Schneider Electric
Moxa	Siemens
Omron	WECON



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

Сигнатури Industrial Security Service Application Control

Sample Protocols covered, +70	
BACnet	HART
DNP3	LONTalk
Elcom	MELSEC
EtherCAT	MMS
EtherNet/IP	Modbus
FINS	OPC
IEC 60870-6 (TASE 2) /ICCP	Profinet
IEC 60870-5-104	S7
IEC 61850	SafetyNET



Entire list: https://www.fortiguard.com/encyclopedia?type=isapp
Request a signature: https://www.fortiguard.com/faq/appctrlsubmit

FortiGuard Industrial Security Service

Application Control сигнатури з контролем функцій, параметрів і значень

Industrial Security

IEC 60870-5-104 ⇶

IEC 61850 – MMS

IEC 61850 – R-GOOSE

Application Control

IEC 62056 – DLMS/COSEM

IEC 60870-6 – TASE.2/ICCP

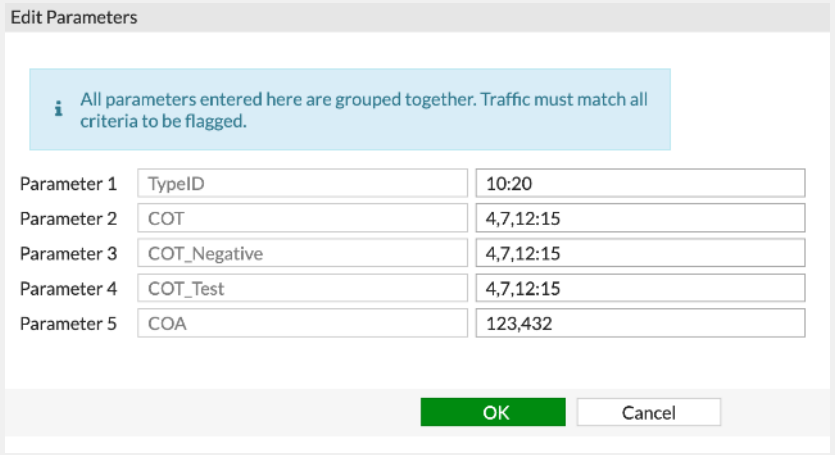
IEEE C37.118 – Syncrophasor

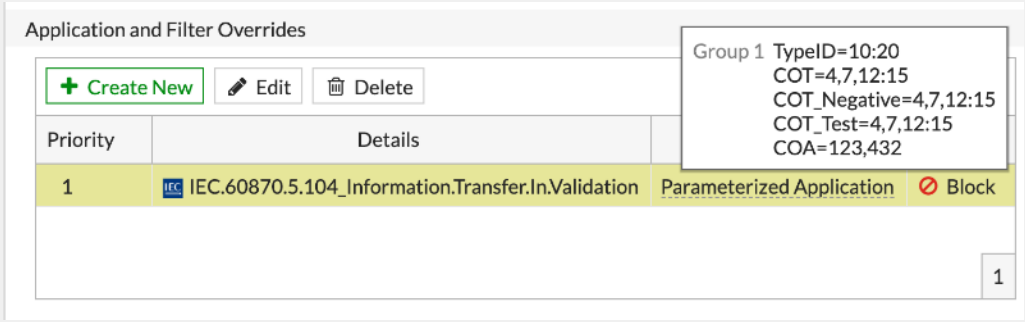
Intrusion Prevention

Modbus TCP ⇶

OPC UA (DA, HDA, AE)

GUI



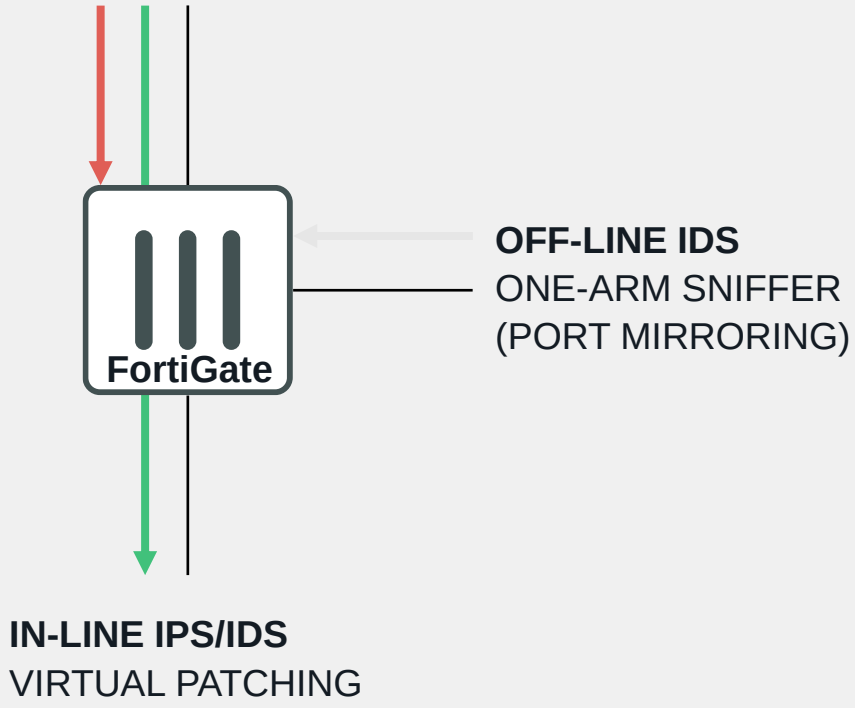


CLI

```
show application list iec104
config application list
    edit "iec104"
        set other-application-log enable
        set unknown-application-action block
        set unknown-application-log enable
        config entries
            edit 1
                set application 49332
                config parameters
                    edit 1
                        config members
                            edit 1
                                set name "TypeID"
                                set value "10:20"
                            next
                            edit 2
                                set name "COT"
                                set value "4,7,12:15"
                            next
                            edit 3
                                set name "COT_Negative"
                                set value "4,7,12:15"
                            next
                            edit 4
                                set name "COT_Test"
                                set value "4,7,12:15"
                            next
                            edit 5
                                set name "COA"
                                set value "123,432"
                            next
                        end
                    next
                end
            next
            edit 2
                set category 2 3 5 6 7 8 12 15 17 21 22 23 25 26 28 29 30 31 32
            next
        end
    next
end
```

⇶ **AND** **OR** Additional parameter, logical operations and ranges are supported

Сценарії використання



- **OFF-LINE IDS**

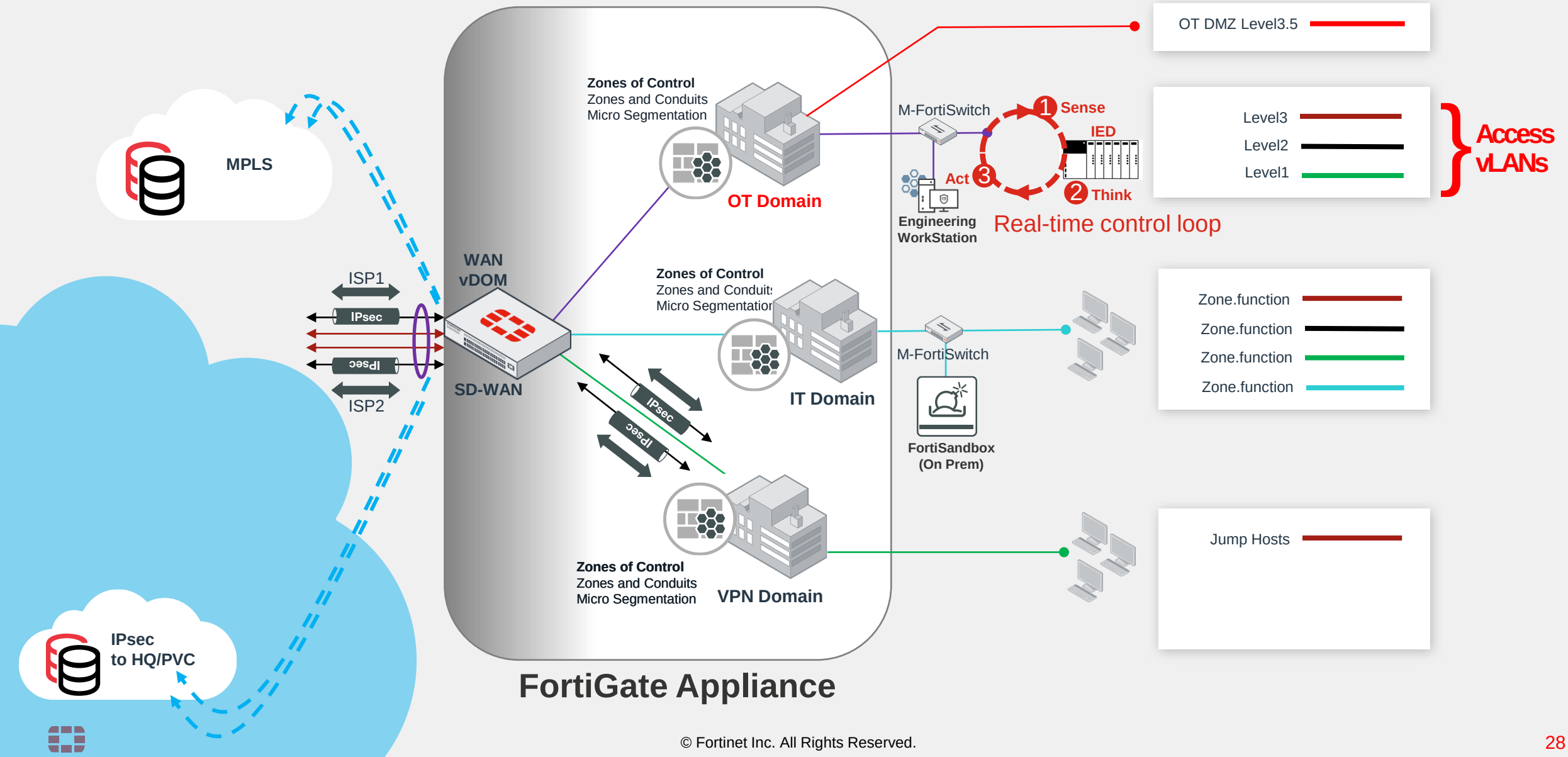
  FortiGate відстежує мережевий сегмент (сегменти) і виявляє атаки, включаючи 0-day атаки.FortiGate отримує копію трафіку від mirror портів. Через нього не протікає nhfasr. FortiGate — мережевий датчик.

- **IN-LINE IPS/IDS**

  Мережевий трафік проходить через FortiGate.Мережеві атаки можуть бути виявлені (IDS) та/або заблоковані (IPS).У режимі IPS вразливі пристрої захищені. Це - virtual patching.

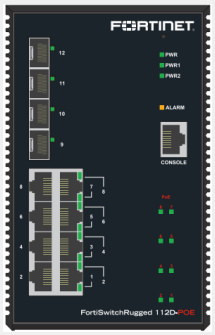
Virtual Domain (VDOM)

Зменшення TCO завдяки консолідації кількох функцій за допомогою одного пристрою NGFW



Рівень доступу - сегментація та мікро-сегментація

FortiSwitch Rugged Series



1. 8x PoE/PoE+ RJ45
2. 4x GE SFP slots

1. 16x GE RJ45 Ports
2. 4x GE SFP slots
3. 8x pairs of Shared Media Interfaces (RJ45/SFP)

	FSR-112D-POE	FSR-124D
Switch Capacity	24 Gbps	56 Gbps
MAC Address Storage	8K	8K
Network Latency (64b)	< 2 µs	< 1 µs
VLANs Supported	4K	4K
Power Supply	Redundant input terminals	Redundant input terminals

FortiSwitch Rugged Series

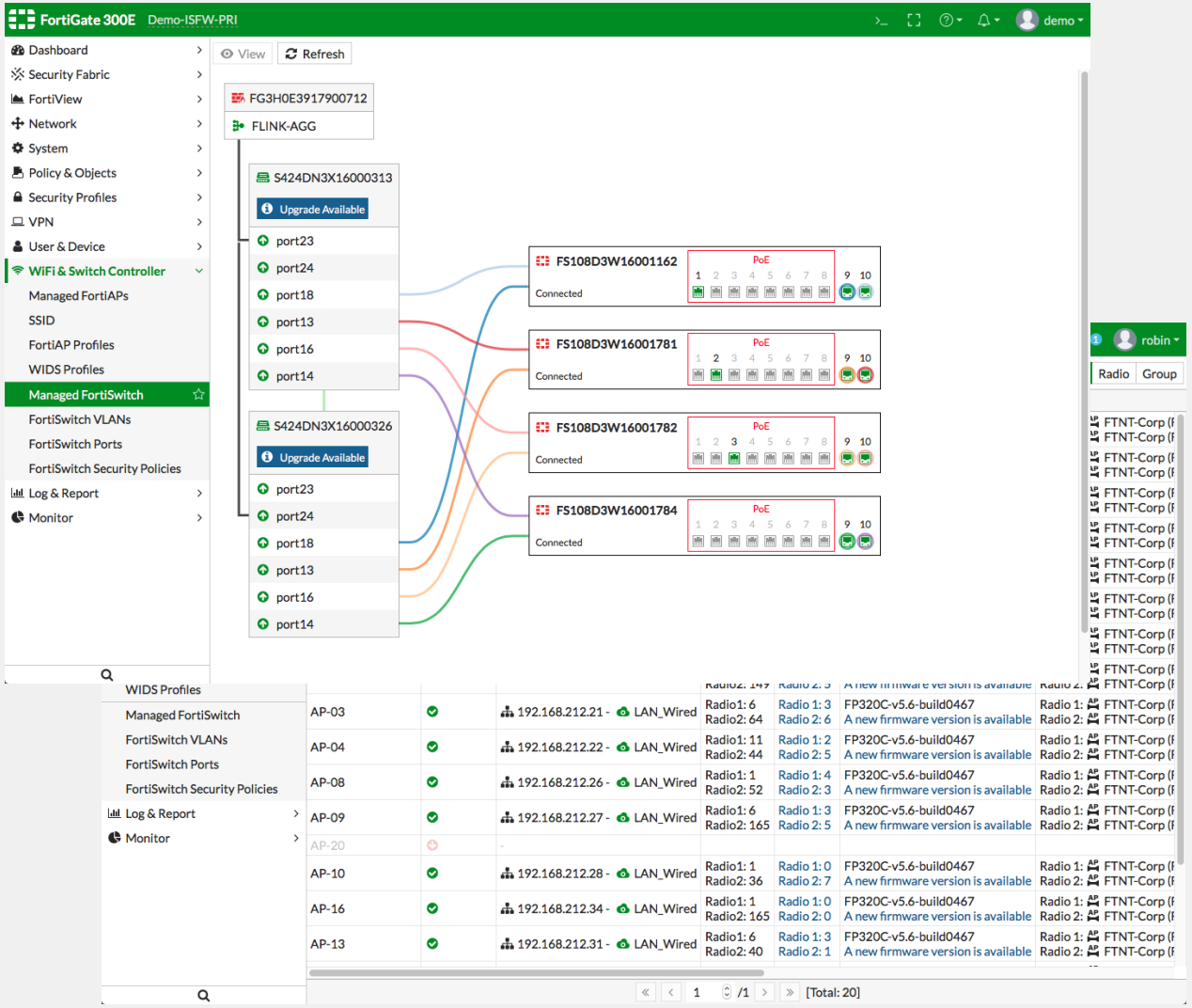
① 12x 1/2.5GE RJ45
② 12x 1/2.5GE GE SFP slots
③ 4x 10GE SFP+ Slots
④ 2x 40GE QSFP+ Slots

	FSR-424F-POE
Switch Capacity	360 Gbps
MAC Address Storage	32k
Network Latency (64b)	< 1 µs
VLANs Supported	4K
Power Supply	Redundant input terminals
Additional Info	*12 port PoE 802.3bt type 3 with maximum 421W limit.

FortiAP

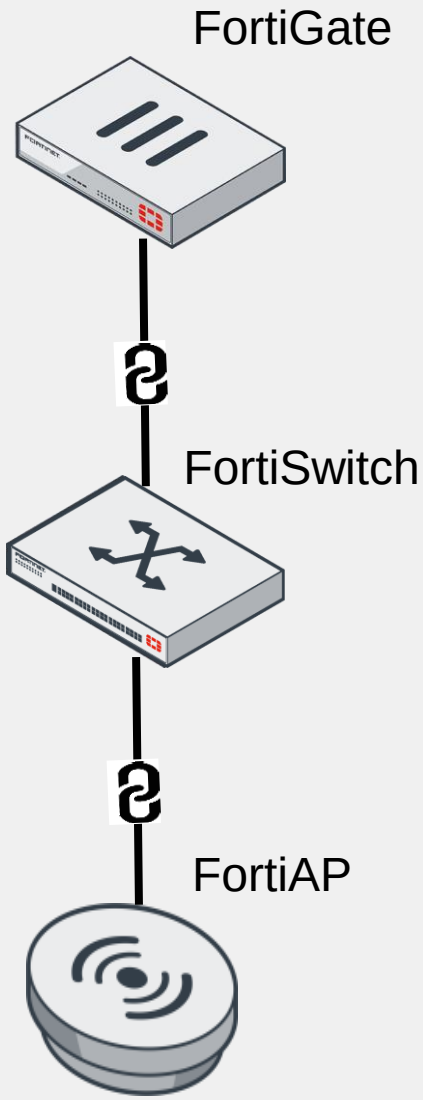
		Wall Plate	Outdoor	Indoor
8x8	3 Radio			802.11ax **FAP-831F**
4x4	3 Radio		802.11ax **FAP-432F**	Wi-Fi 6E **FAP-431/433G** 802.11ax **FAP-431/433F**
4x4	2 Radio			
3x3	2 Radio			
2x2	3 Radio	802.11ax **FAP-23JF**	802.11ax **FAP-234F**	Wi-Fi 6E **FAP-231/233G** 802.11ax **FAP-231F**
2x2	2 Radio			802.11ac W2 **FAP-221/223E**

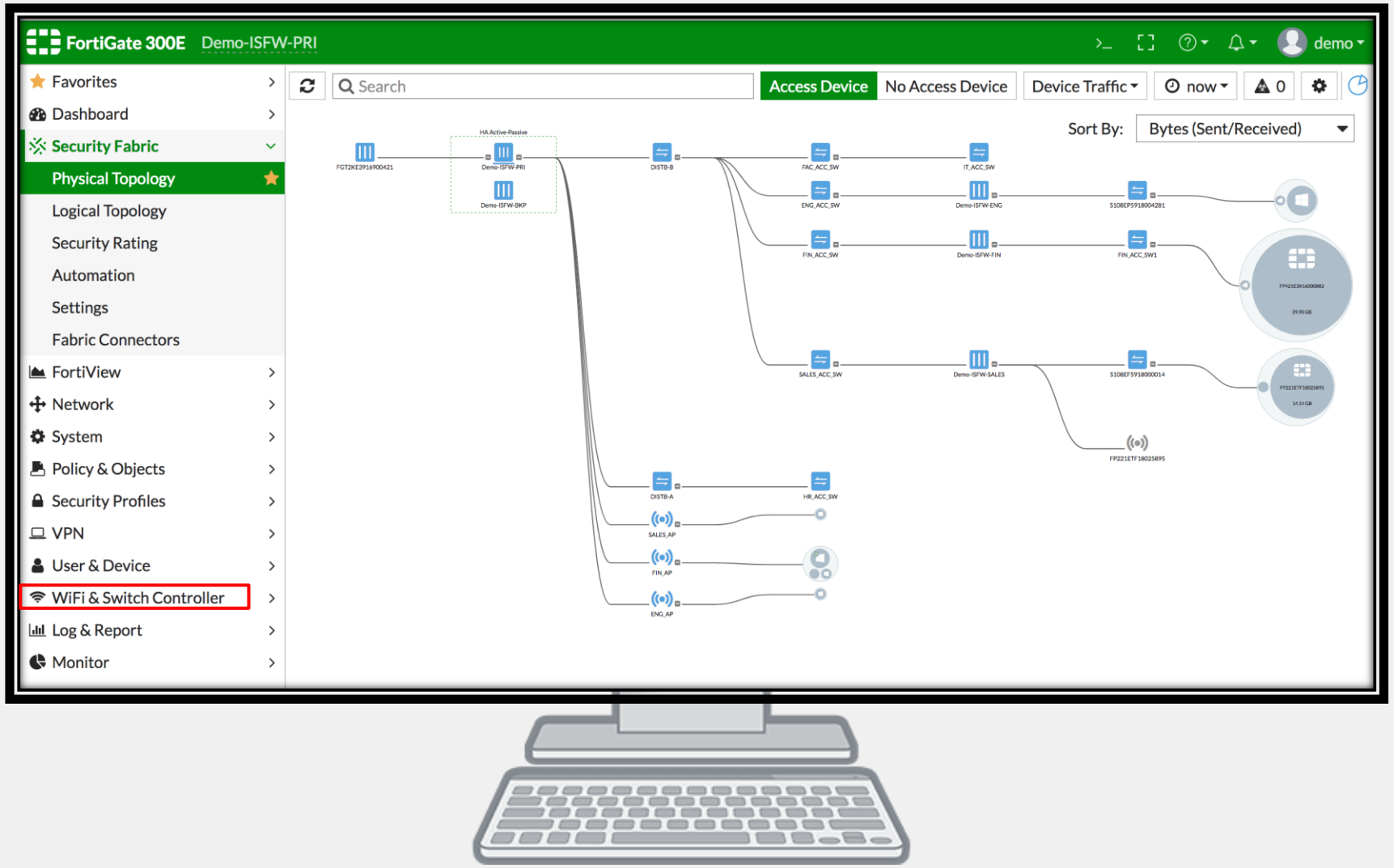
FortiOS: контролер комутаторів та точок доступу



- **FortiGate для керування FortiSwitch/FortiAP**
  - Захист трафіку між інтерфейсами (VLAN, SSID, фізичними)
  - Port level visibility
- **Впровадження кращих практик**
  - ISA99/IEC-62443
  - NIST
  - Defense in Depth
- **Ізоляція, зонування**
  - Сегментація
  - Мікро-сегментація

Керування через FortiLink





FortiOS: NAC

NAC інтегрований в FortiOS

FortiOS з інтегрованим NAC:

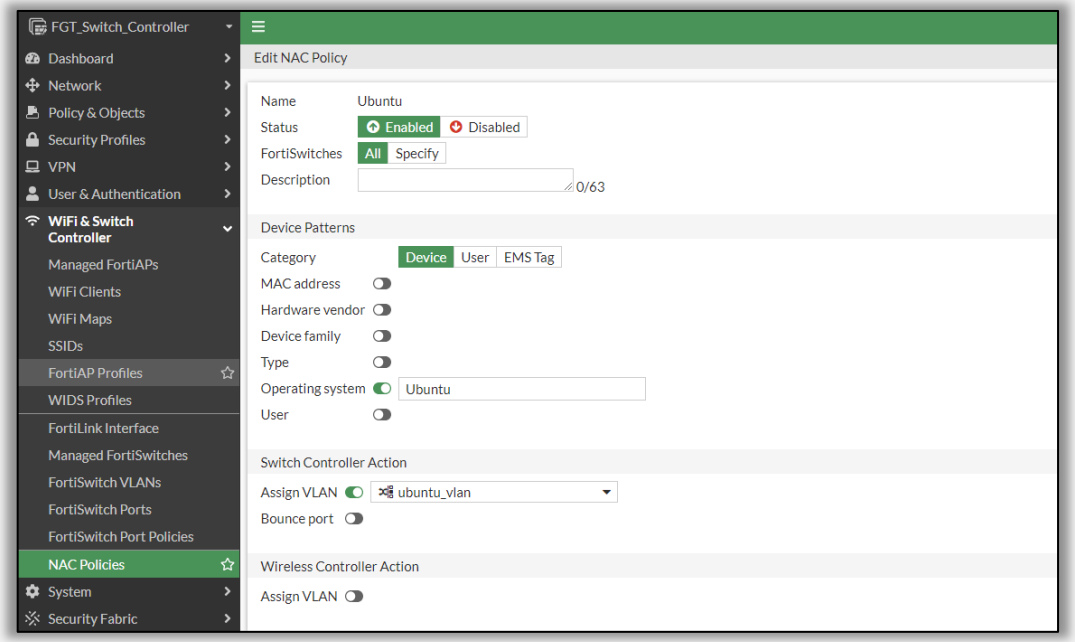
- Політики NAC у FortiOS, що відповідають користувачам або пристроям.
- Режим порту на NAC

Підтримка додаткових умов політики

- EMS tag
- mac_address Wild Card
- Інше

Можливі дії політики

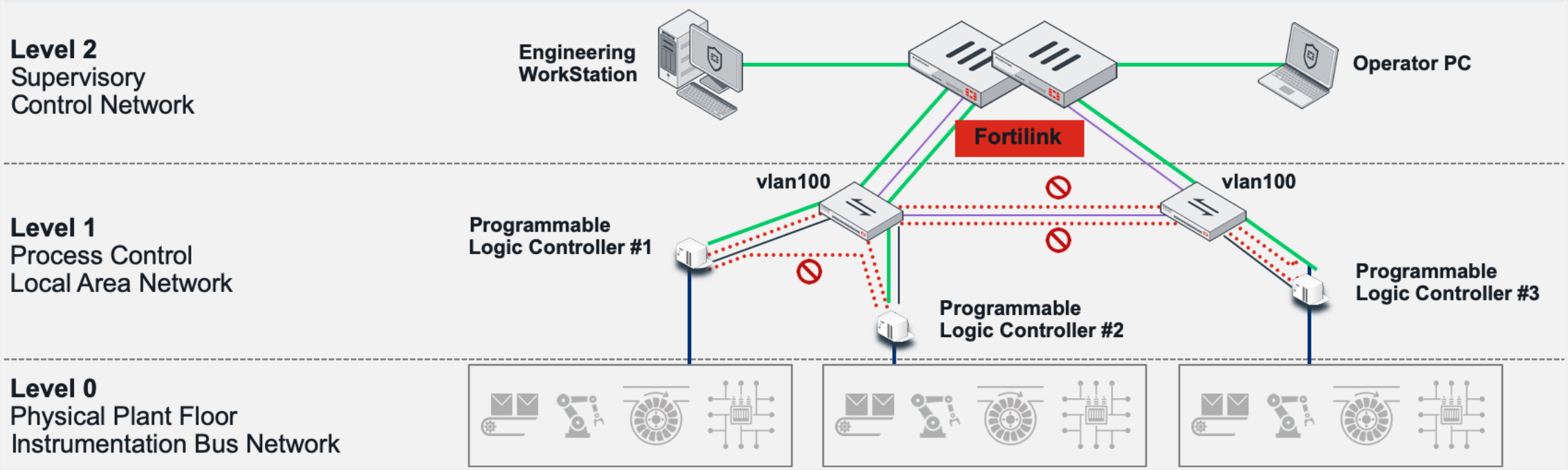
- Перемістити **кінцеву точку/хост** до кінцевого сегмента
- Перемістити **кінцеву точку/користувача** до кінцевого сегмента
- Застосувати політики рівня порту (802.1X AUTH тощо)



port1		NAC		Edge Port Spanning Tree Protocol	onboarding.fortilink (onboarding)	quarantine.fortilink (quarantine)		JOHNLOCUS fe:09:0f:00:29:01 fe:ff:ff:00:00:29	Untrusted
port2		Static		Edge Port Spanning Tree Protocol	contractors	quarantine.fortilink (quarantine)		host8 fe:09:0f:00:2d:01 fe:ff:ff:00:00:2d	Untrusted
port3		Static		Edge Port Spanning Tree Protocol	default_10.fortilink (default_10)	quarantine.fortilink (quarantine)		fe:09:0f:00:00:06	Untrusted
port4		Static		Edge Port Spanning Tree Protocol	default_10.fortilink (default_10)	quarantine.fortilink (quarantine)		fe:09:0f:00:00:07	Untrusted

Мікро-сегментація з Access VLAN

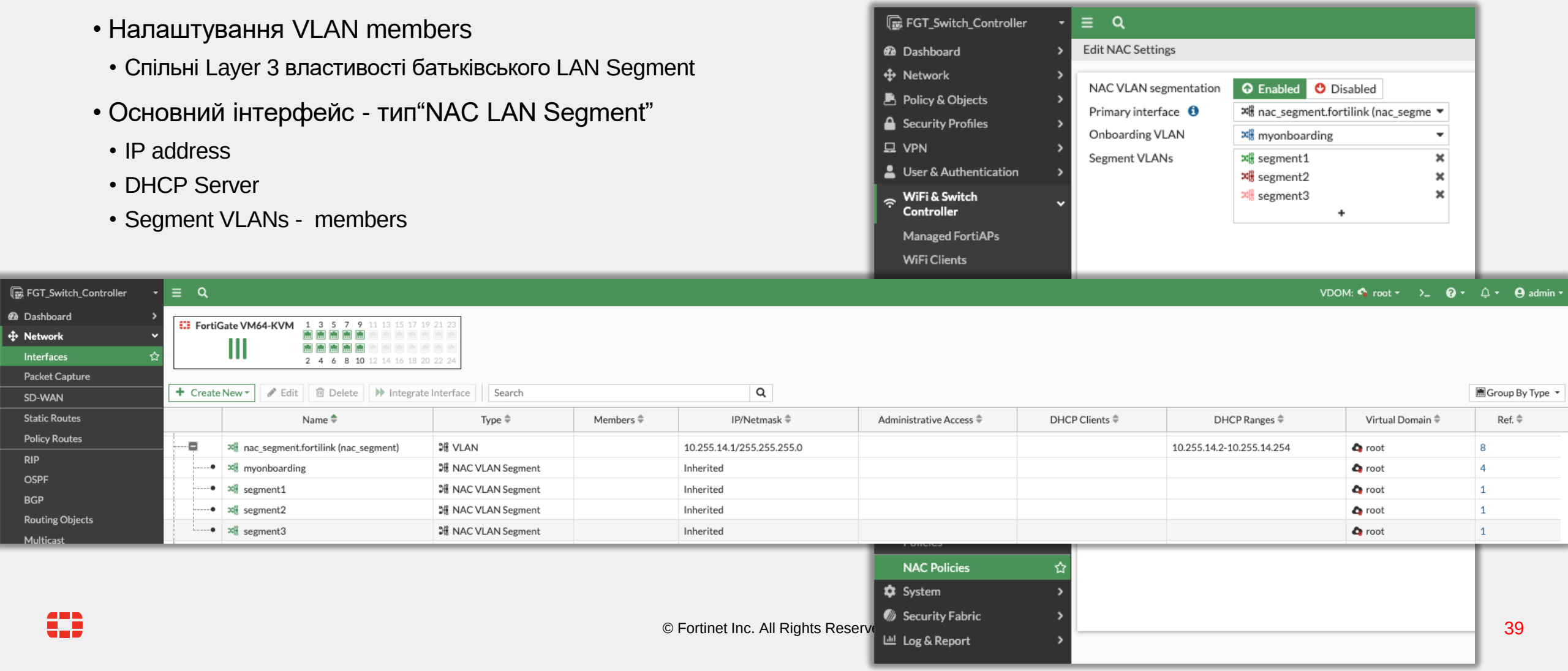
- Host isolation
- Firewall policy to control the L2 communications
- L7 inspection if required



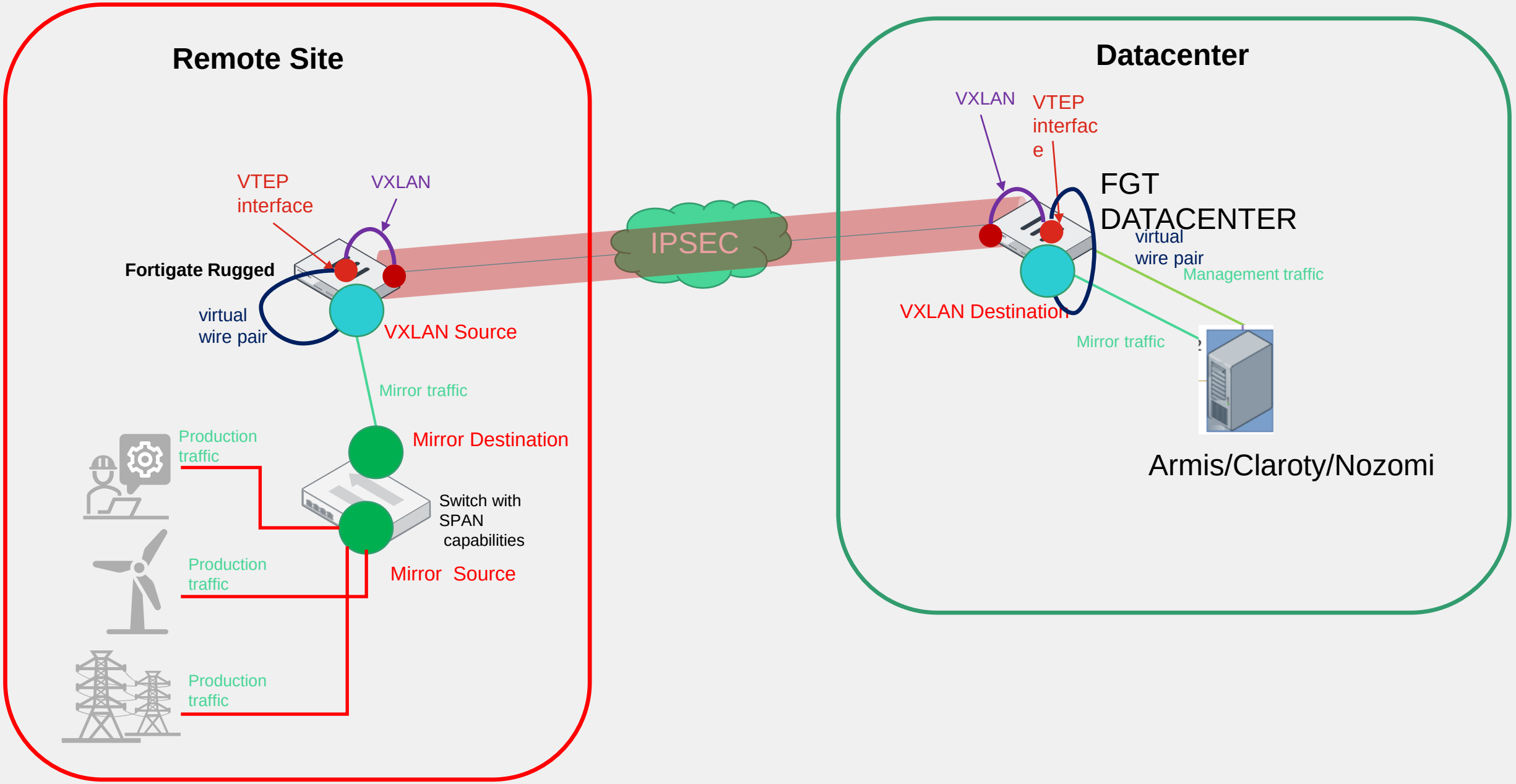
NAC LAN Segments

Вдосконалення мікро-сегментації

- Налаштування VLAN members
  - Спільні Layer 3 властивості батьківського LAN Segment
- Основний інтерфейс - тип“NAC LAN Segment”
  - IP address
  - DHCP Server
  - Segment VLANs - members



Захищений L2 VPN для OT/критичних систем



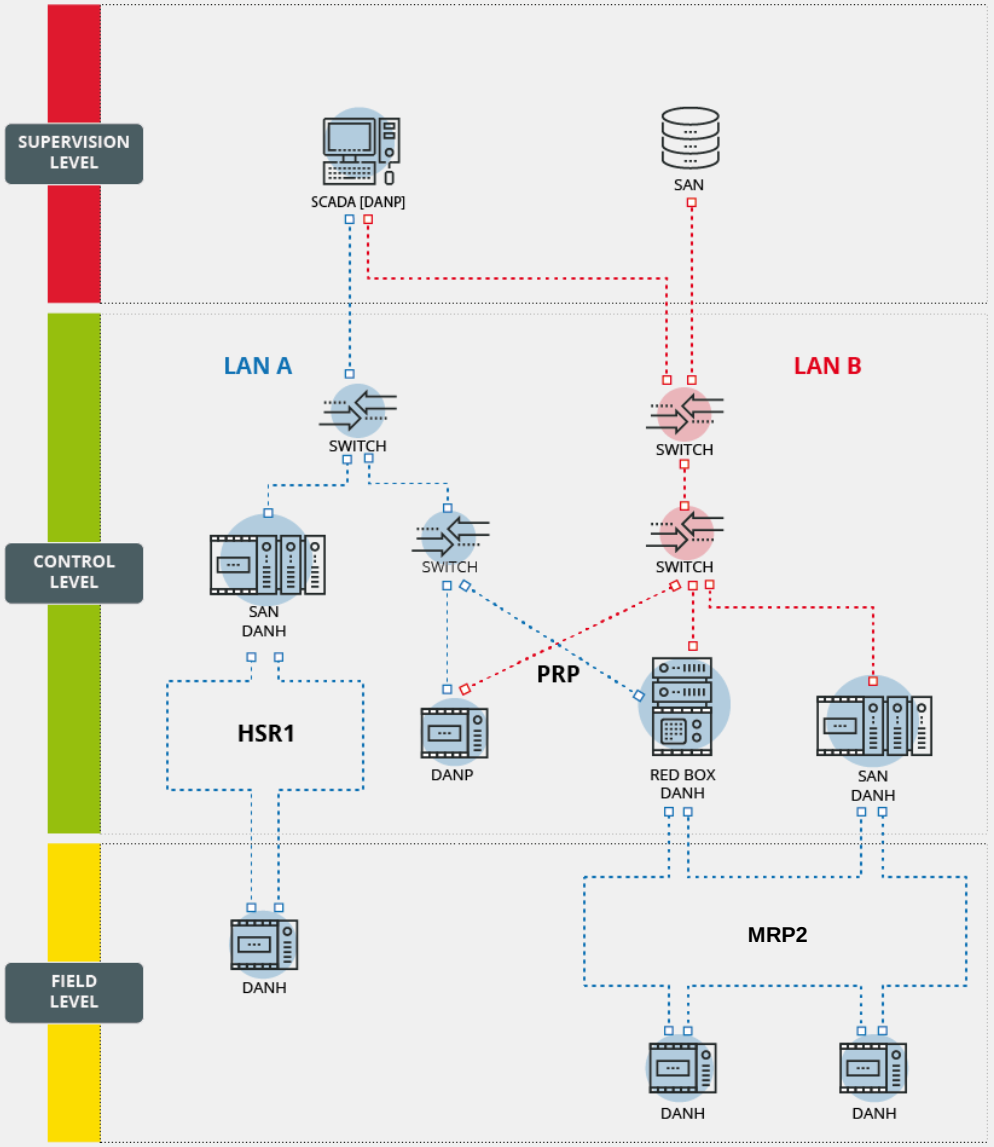
Що означає «Real time» в OT?

Для IEC 61850-8-1 мережі (Substation network)

	Tol	T
SCADA to IED (Client- Server)	800 ms	400ms
IED to IED (interlock)	12ms	4ms
IED to IED (Block reverse)	12ms	4ms

Tol= Application recovery Tolerance
T= Time required for recovery of communication

OT Redundancy L2 protocols



MRP = Media Redundancy Protocols
HSR = High-Availability Seamless Redundancy
PRP = Parallel Redundancy Protocl

MRP vs RSTP

	MRP	RSTP
Topology	Ring	Any (MESH)
Number of switches in ring	50	Max 40
Deterministic reconfiguration	Yes (500/200/30/10ms)	Not guaranteed
Fail-over time vs number of switches	Nearly independent	N* number of switches
Configuration	Simple (Redundancy Manager)	Medium (root, bridge, priority)

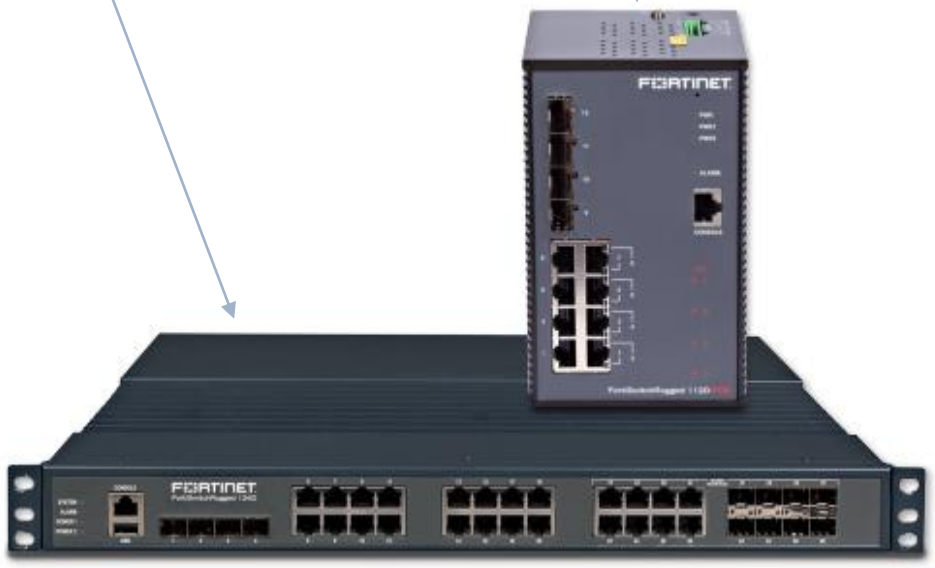
MRP Administration guide

https://docs.fortinet.com/document/fortiswitch/7.2.1/administration-guide/222614/media-redundancy-protocol

Підтримка MRP в FortiSwitch Rugged

FSR-112D-POE - DIN Rail / wall mount

FSR-124D – Rack mount



Feature	GUI Supported	112D-POE	FSR-124D	1xxE, 1xxF	4xxE	200 Series, 400 Series	500 Series	1024D, 1048D, 1048E	3032D, 3032E
SPAN	✓	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗
RSPAN and ERSPAN (IPv4)	✓	🔗 (RSPAN)	🔗	—	🔗	🔗	🔗	🔗	🔗
Flow control	—	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗
MRP	—	✓	✓	—	—	—	—	—	—

Highlights

- Mean time between failure greater than 25 years
- Fanless passive cooling
- DIN-rail or wall-mountable
- Power over Ethernet capable including PoE+
- Redundant power input terminals

Key Features

Sturdy IP30 Construction

- Built to ingress protection 30 standards, the construction is designed to perform while enduring hostile conditions

Passive Cooling

- With no fan and no moving parts, the mean time between failure is greater than 25 years

Redundant Power Inputs

- Maximizes network availability by eliminating the down time associated with failure of a power input

Power over Ethernet Capability

- Seamless integration of peripheral devices such as cameras, sensors, and wireless access points into the network

FortiNAC

Варіанти використання FortiNAC

Inventory Management
- Консолідована видимість
- Комплексне покриття

Micro Segmentation
- Гранульована
- Динамічна
- Контекстна

Compliance
- Оцінка
- Аудити

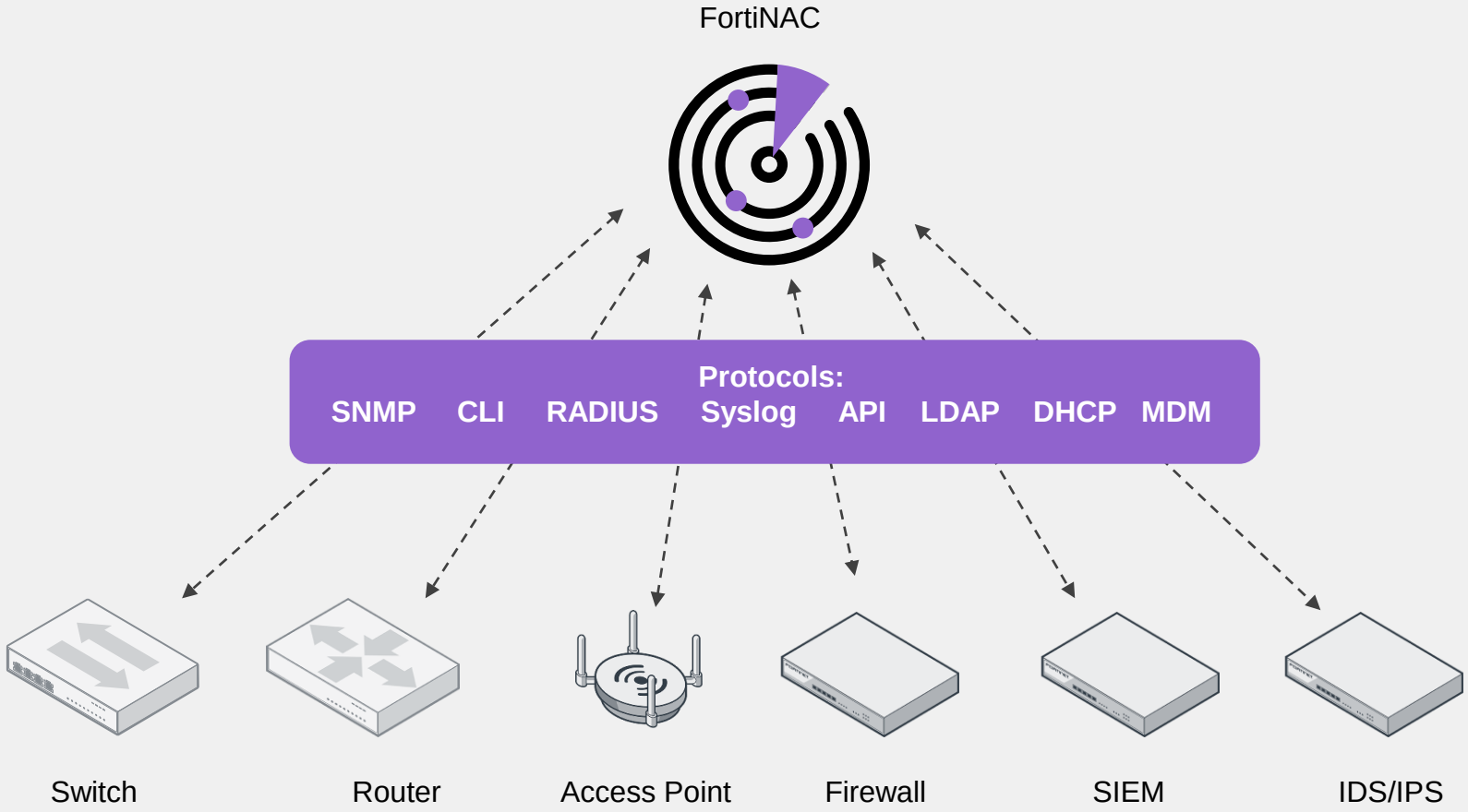
Zero Trust для пристроїв

Command Center with 3rd Party Intel Sharing

Automated Process
- Виконання політики
- Стримування загрози
- Зміна дозволів

Onboarding
- BYOD пристрої
- Різні типи користувачів
- Captive Portal

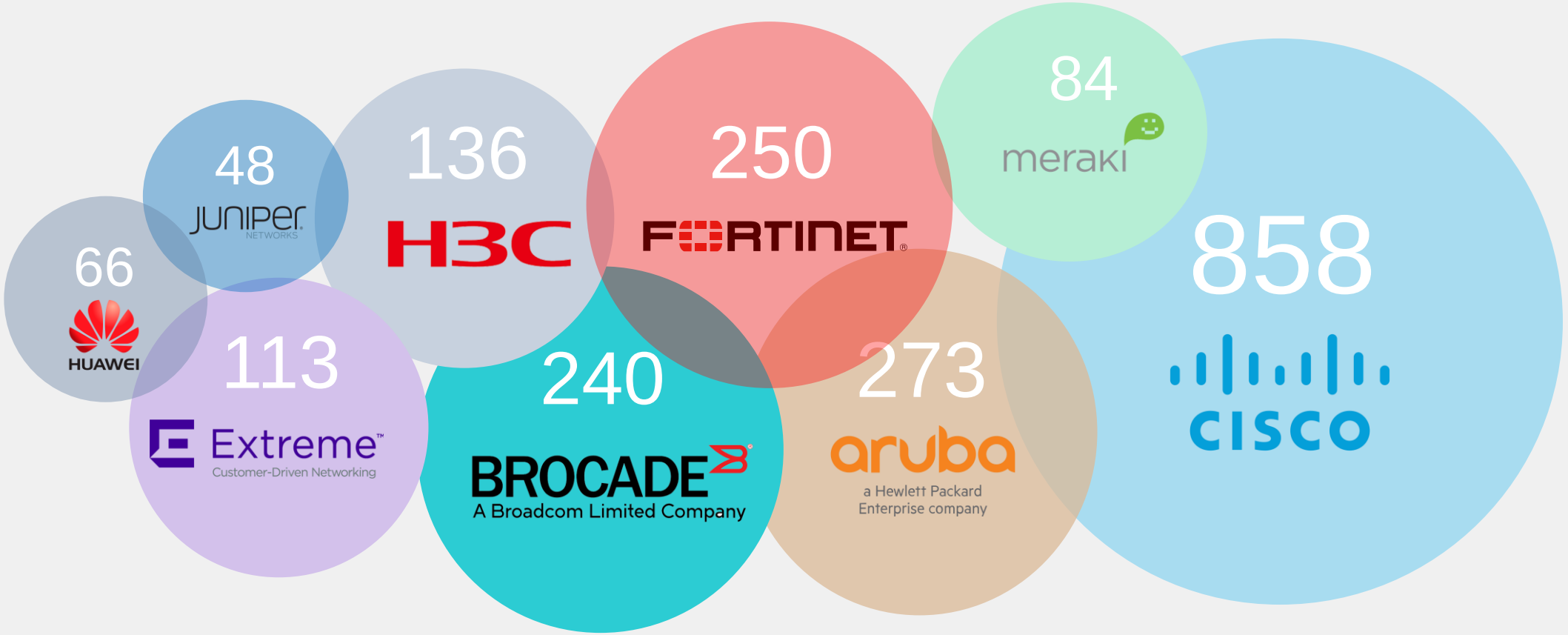
Взаємодія FortiNAC з пристроями інших виробників



Взаємодія з більшістю мережевої інфраструктури корпоративного класу

Покриття підтримуваного мережевого обладнання

Охопленя продуктів становить ~75% мережевого ринку



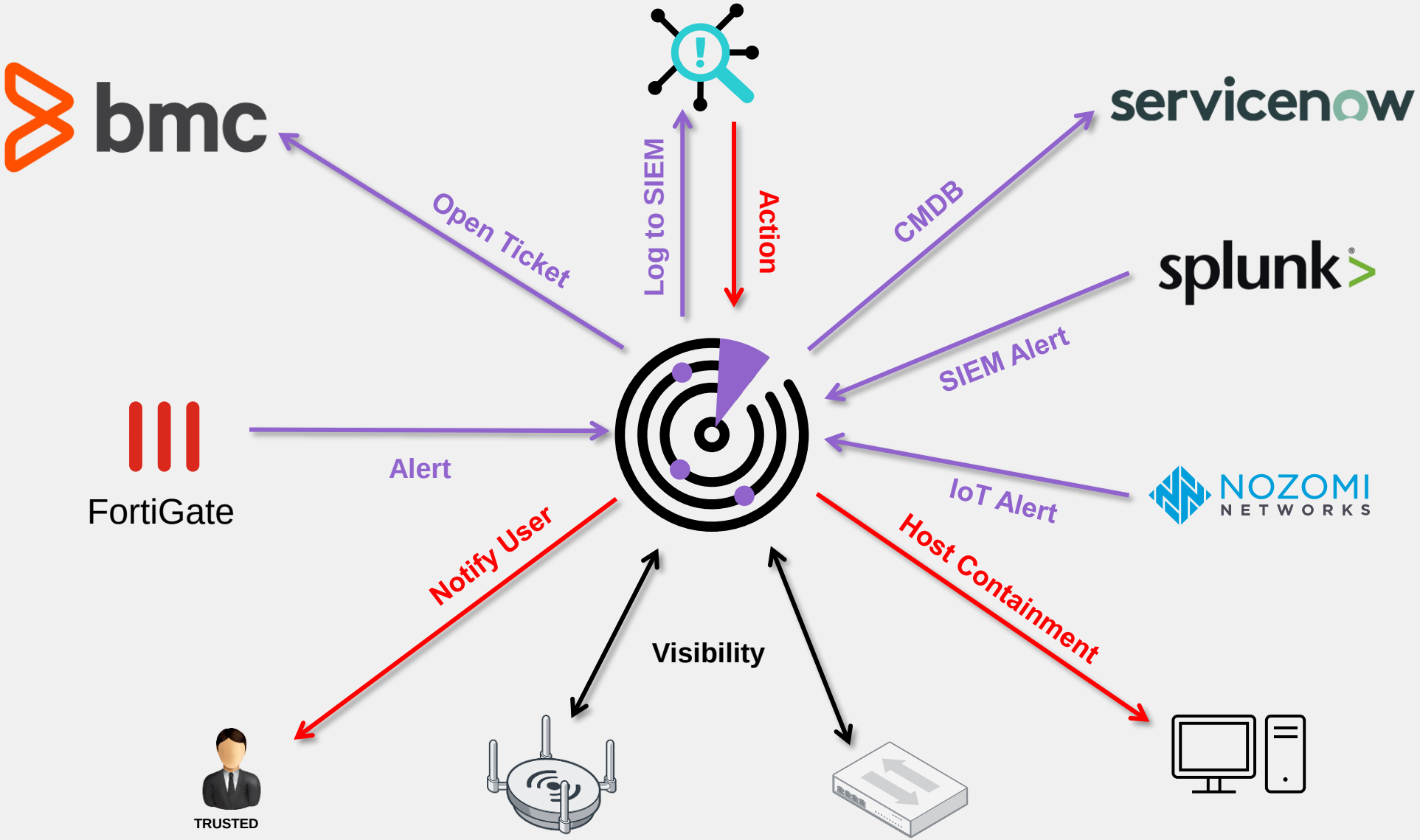
95 Vendors

- Networking
- Security
- Carrier
- Industrial

2432 Models

- Switches, APs, Controllers,
- Data Center, Enterprise, SMB
- Modular, 1U, Ruggedized

Автоматизація та керування безпекою



Профілювання пристроїв

Швидко, точно, без перешкод і безперервно

- 20+ методів профілювання (пасивних і активних)
- Правила створюються на основі методів профілювання та використовуються для оцінки виявлених пристроїв
- Правила можна ранжувати в послідовності та мати перехресні посилання на інформацію про пристрій.
- Коли пристрої відповідають правилам, то встановлюються атрибути, наприклад тип пристрою, роль, група тощо.

Passive Methods

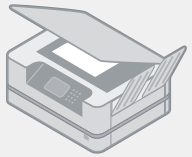
- DHCP Fingerprinting
- FortiGate
- FortiGuard
- IP Range
- Location
- Network Traffic
- Passive
- Persistent Agent
- RADIUS Request
- Vendor OUI

Action Methods

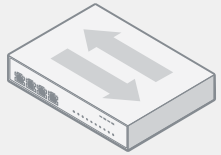
- Active
- NMAP
- HTTP/HTTPS
- ONVIF
- Script
- SNMP
- SSH
- TCP
- Telnet
- UDP
- WinRM
- Windows Profile

Приклад роботи FortiNAC

Безперервне профілювання пристроїв

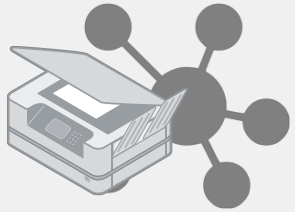


1. Принтер підключений до мережі



2. MAC notification trap відправлено до FortiNAC

3. FortiNAC визначає пристрій, як принтер та назначає налаштування порта



4. FortiNAC дозволяє швидко встановити принтер та налаштувати безпеку в Fabric

Стримування розповсюдження загроз на рівні доступу

1. FSSO підключення через FGT, виявлення зараження

2. FGT виявляє загрозу та відсилає подію до FortiNAC

3. FortiNAC ізолює пристрій на рівні доступу

4. Вірус ізольовано на рівні комутатора

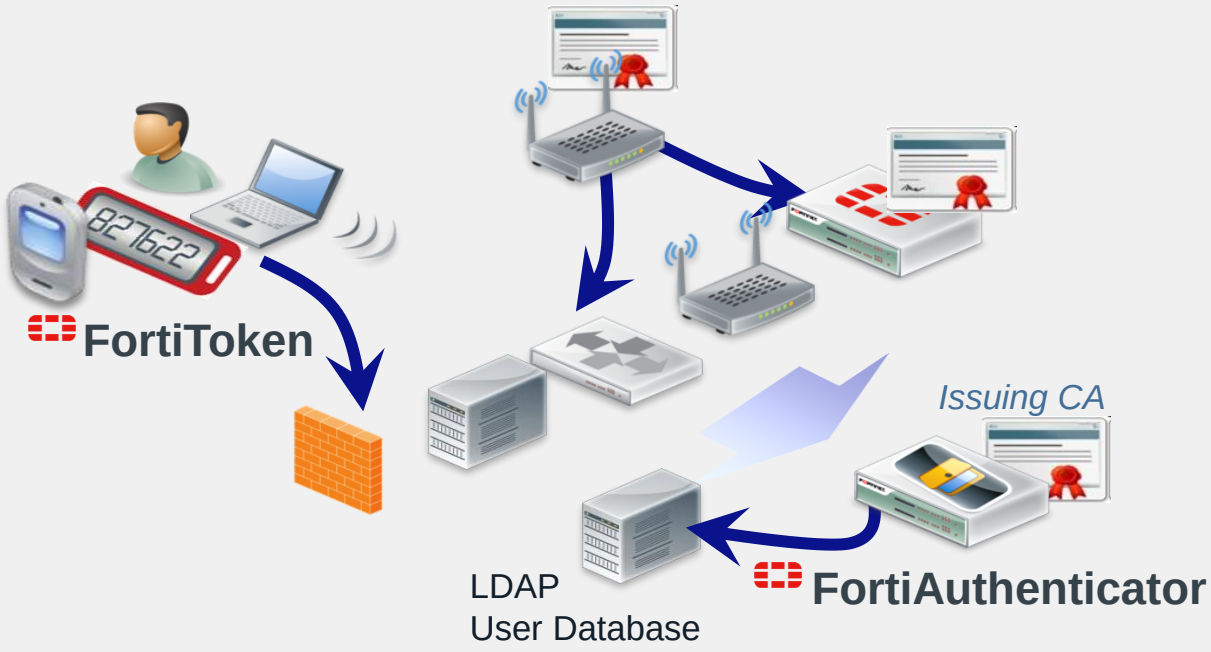
Безпечна аутентифікація

FortiAuthenticator

Appliance | Virtual Machine | Cloud

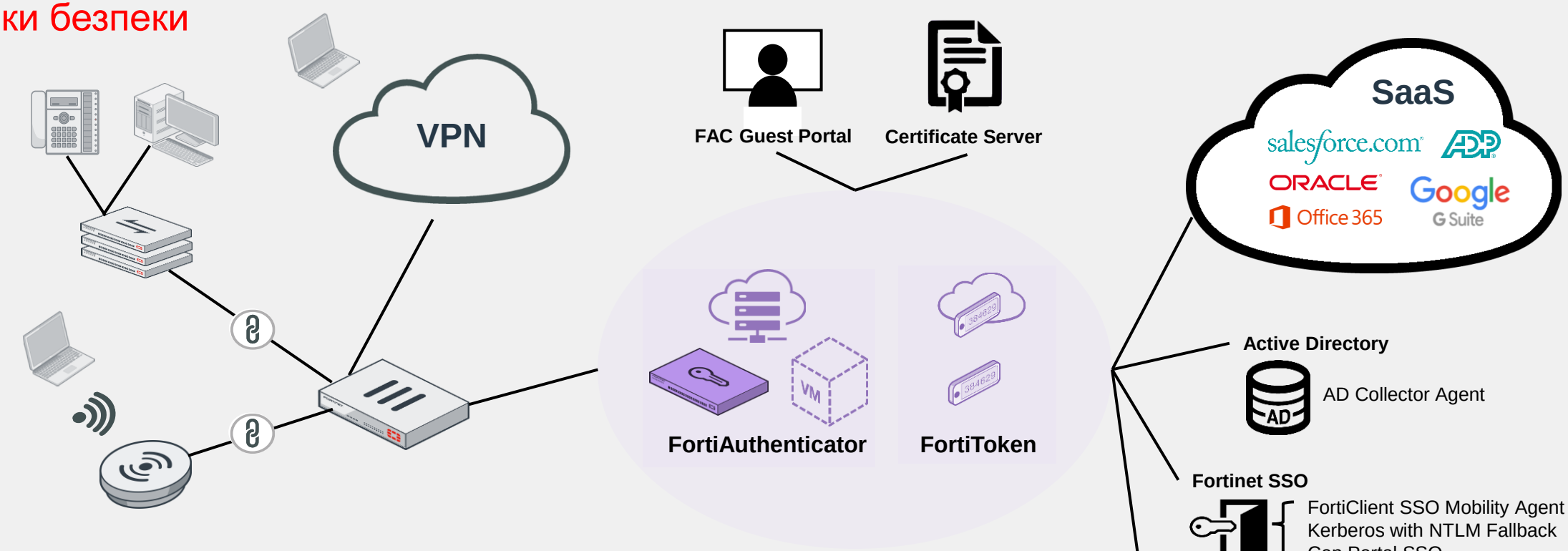
Управління ідентифікацією, контроль доступу користувачів та MFA

- Прозора ідентифікація користувачів мережі та застосування політики, керованої ідентифікацією, у корпоративній мережі з підтримкою Fortinet
- Безпечна багатофакторна/OTP аутентифікація в організації в поєднанні з FortiToken
- Керування сертифікатами для корпоративного бездротового зв'язку та VPN
- Гостьове керування для безпеки дротової та бездротової мережі
- Підтримка Single Sign On для внутрішніх і хмарних мереж



Fortinet керування ідентифікацією та доступом

Встановлення ідентифікації за допомогою надійної аутентифікації є важливою умовою ефективної політики безпеки



- **Authentication and Authorization**
  – Role based access and control
- **Fortinet Single Sign On**
- **Single Sign On**
  – via SAML, RADIUS, etc

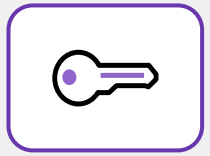
- **Two Factor Authentication**
- **Certificate Management**
- **Time Based Enabled Authentications**
- **Self Service Portal**

Компоненти IAM

FortiAuthenticator

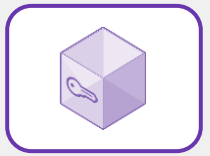
- Безстрокова ліцензія. Жодних прихованих витрат
- Апаратний або віртуальний пристрій

Appliance



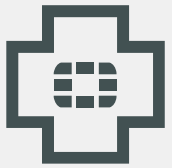
3 Available models
100 – 240K users
User upgrade SKUs

Virtual Machine



100 – 1M + users
User upgrade SKUs

Services



FortiCare

FortiToken

- Проста безстрокова ліцензія. Жодних прихованих витрат
- Апаратні форм-фактори USB, кредитна карта, брелок
- Мобільний додаток з технологією PUSH

FortiToken Mobile

FortiToken 200B/200BCD

FortiToken 220

FortiToken 300

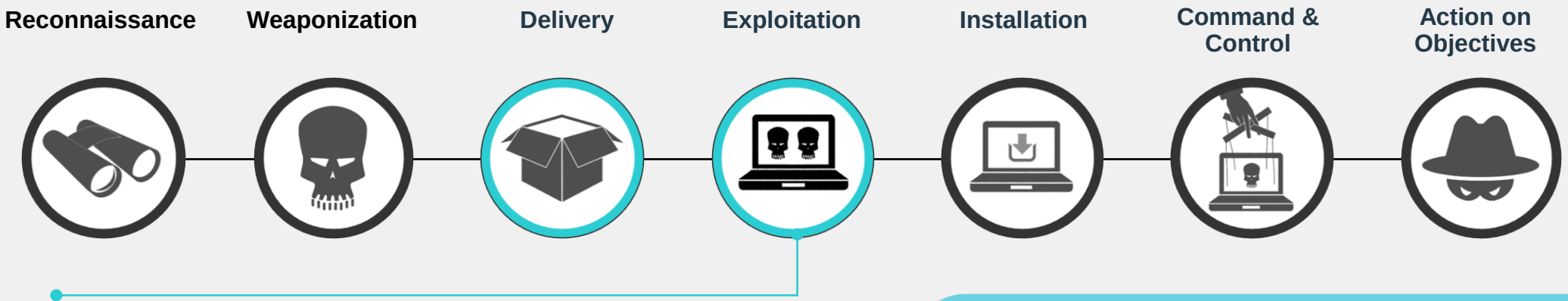
FortiToken 400 (Passwordless)

One-Time-Passcode (OTP) | Certificate | FIDO Key

Пісочниця для OT

Sandboxing

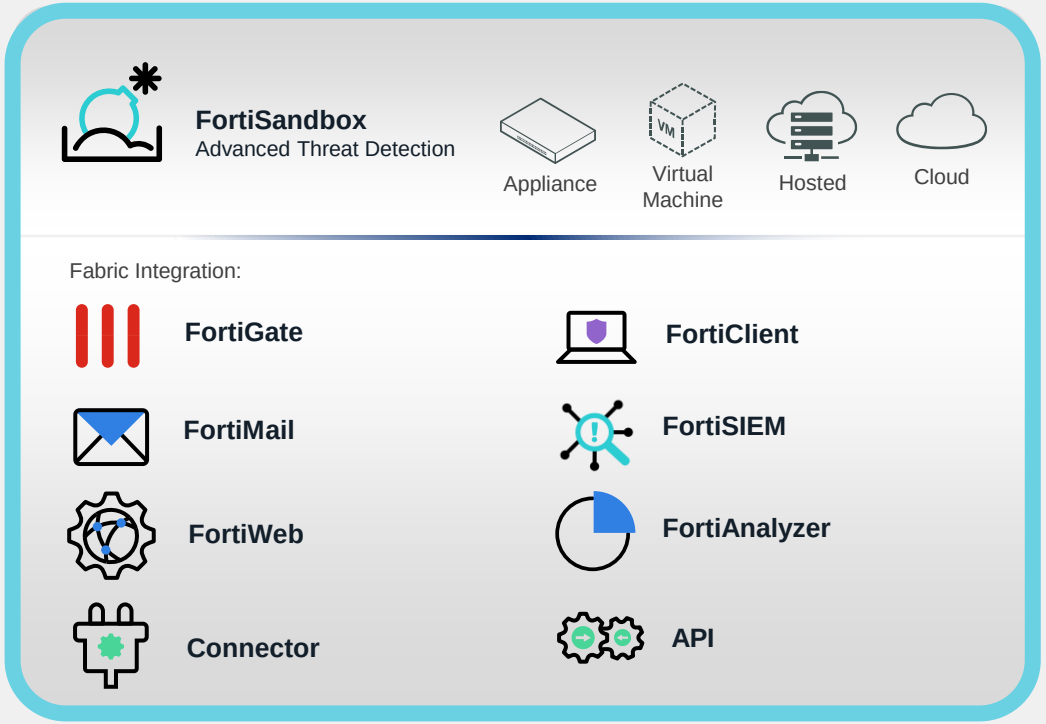
Блокування розширених загроз



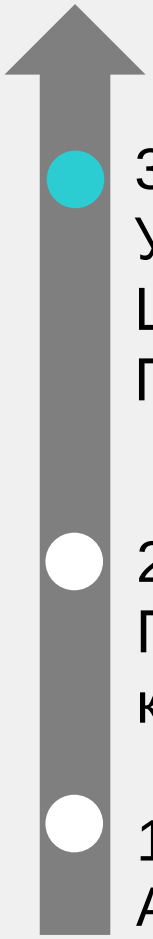
Sandbox

FortiSandbox

Пісочниця **3-го покоління** посилена **Machine Learning** & **Deep Learning**, **інтегрується** до будь-якої існуючої інфраструктури безпеки та надає **автоматичний** захист як в IT, так і в OT середовищах.



Еволюція пісочниці

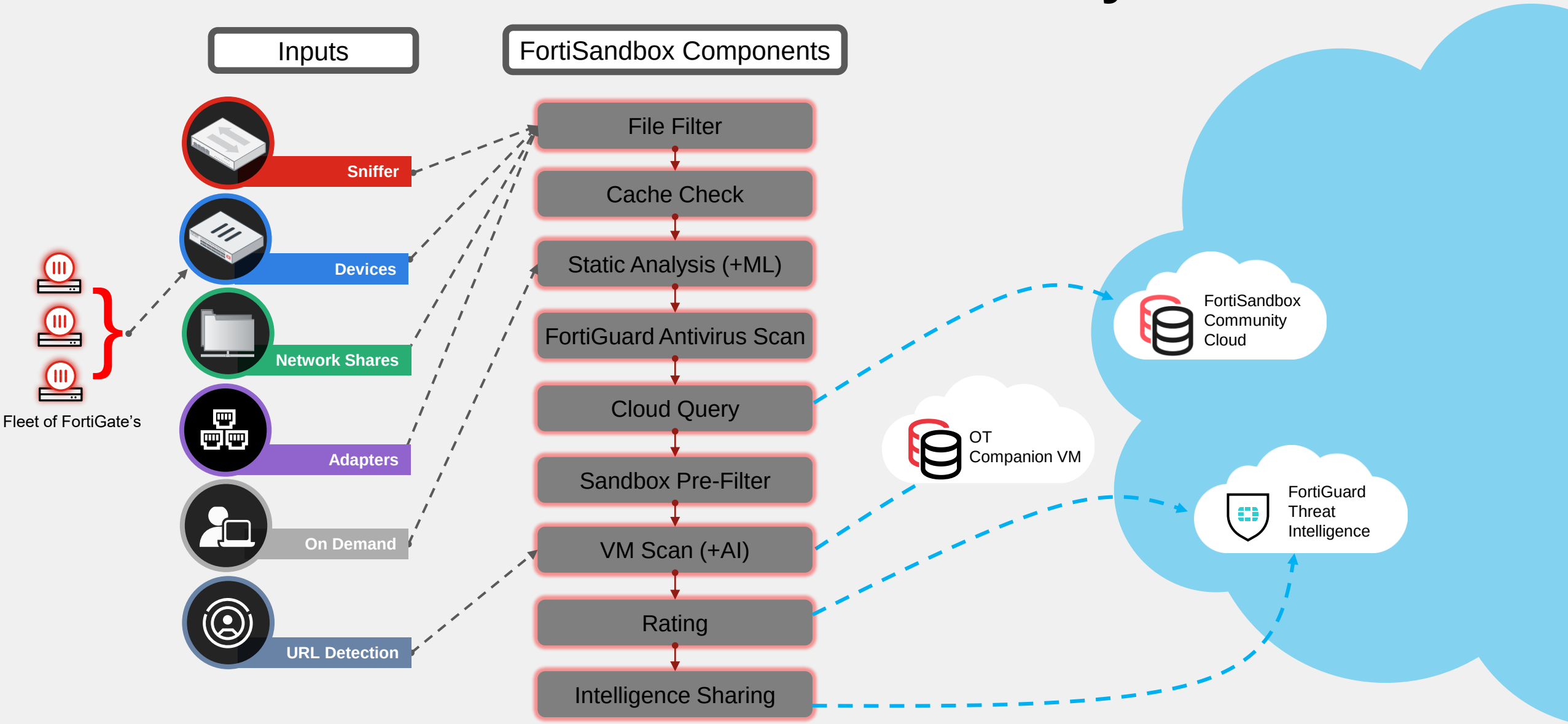


3-е покоління
Удосконалений механізм виявлення: пісочниця на основі ШІ
Широке охоплення: гнучке розгортання та підтримка аналізу загроз IT/OT
Підтримка процесів SOC: прискорення реагування та розслідування

2-е покоління
Платформний підхід до ізольованого програмного середовища: елементи керування безпекою інтегровані з пісочнецею

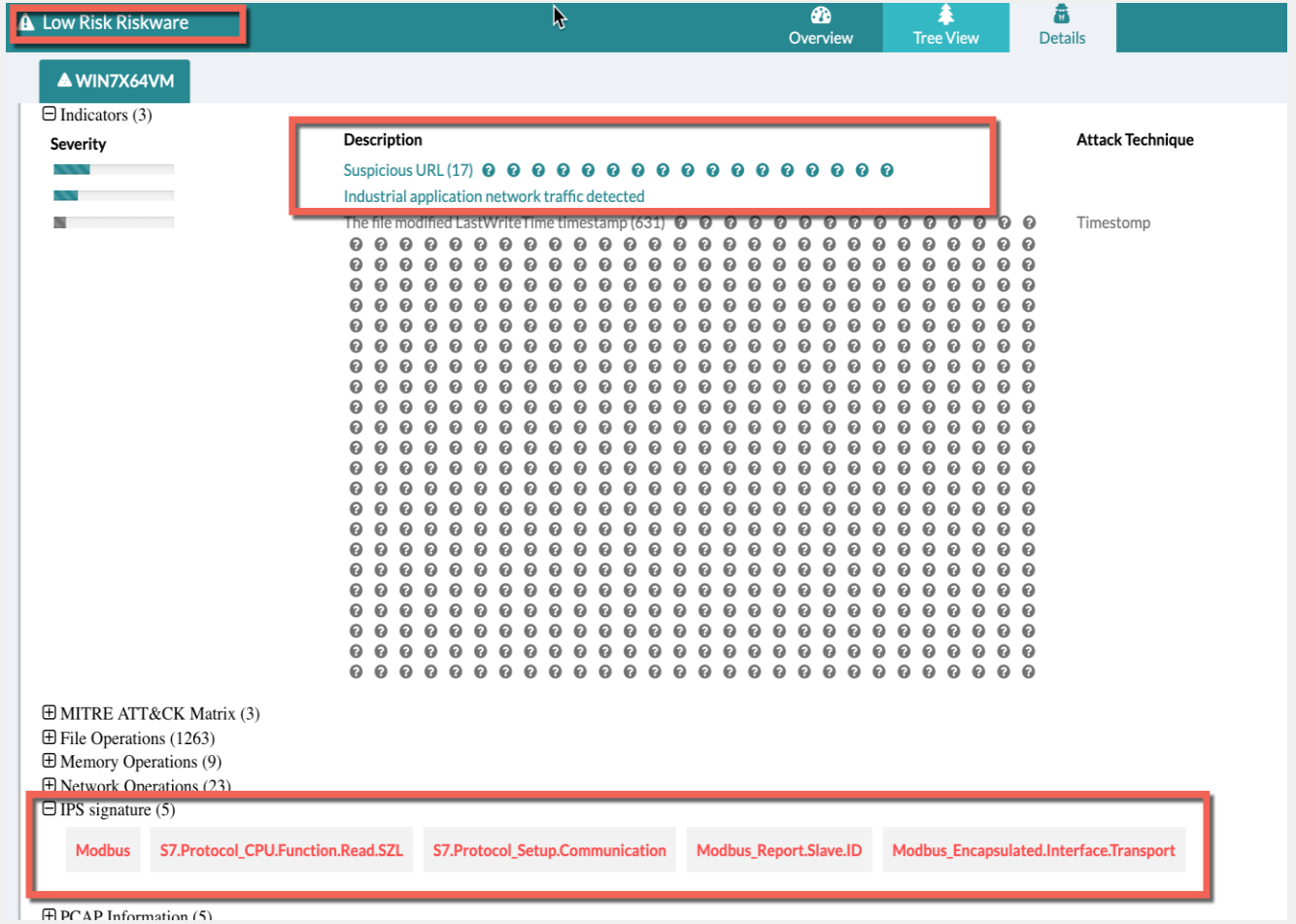
1-е покоління
Автономна пісочниця: окрема пісочниця для кожного вектора загрози

FortiSandbox: Ключові компоненти сканування



SCADA/ICS Sandboxing

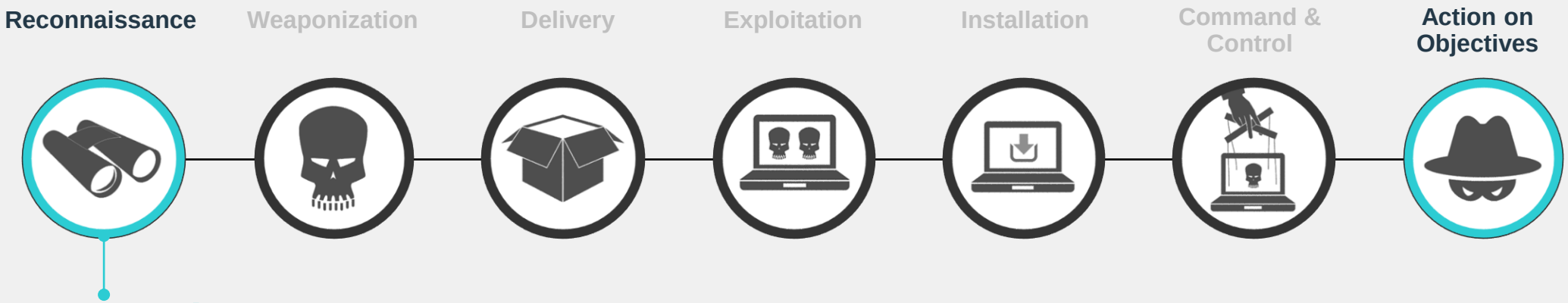
- Уніфіковане виявлення загроз нульового дня для сегментів IT та OT
- Включає симулятор SCADA/ICS у процес пісочниці
- Під час аналізу об’єкта можна виявляти шкідливе програмне забезпечення, націлене на OT, яке отримує доступ до служб:
  - ✓ ModBus
  - ✓ S7comm
  - ✓ SNMP
  - ✓ BACnet
  - ✓ IPMI
  - ✓ Та інших..



Deception технологія для OT

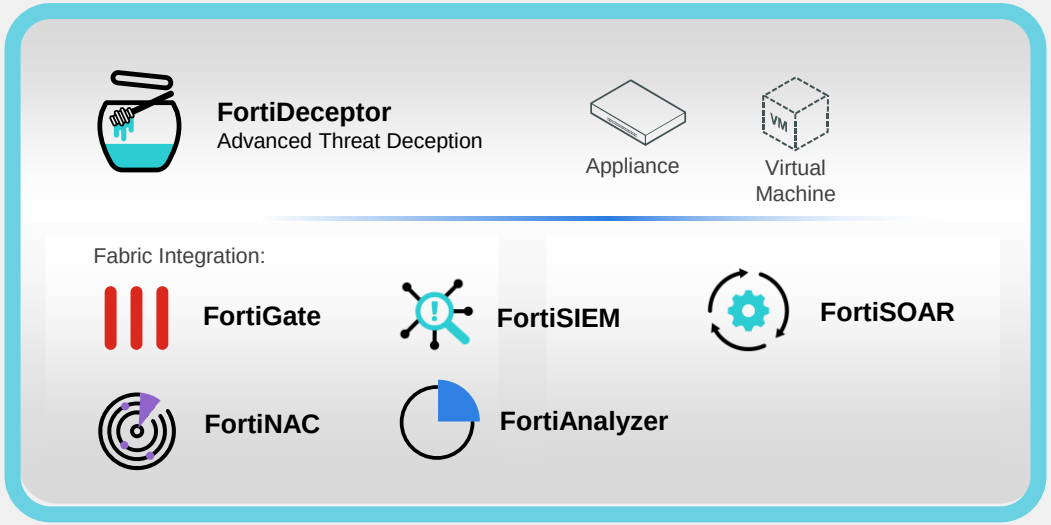
FortiDeceptor

Порушення дії загроз



FortiDeceptor

Вдосконалена система захисту від загроз, призначена для **ОБМАНУ**, **ВИКРИВАННЯ** та **УСУНЕННЯ** зовнішніх і внутрішніх загроз на ранніх етапах атаки та проактивного блокування цих загроз до того, як станеться будь-яка значна шкода.



Deception — це більше, ніж Honeypot

	Honeypot	Deception Technology
	Призначений для виявлення зовнішніх загроз	Спеціальна платформа(decoys, breadcrumbs, lures, etc.) розроблена для виявлення та стримування атак всередині мережі
Автентичність	Легко ідентифікується зловмисниками	Високоаутентичні приманки змішані з виробничим середовищем
Простота розгортання та експлуатації	Відсутність централізованої системи розгортання. Трудомісткі для розгортання та масштабування	Швидке розгортання (2-4 години) і простота в обслуговуванні, 85% розгортання автоматизовано
Масштабованість	Неможливо масштабувати в кількох/обмежених середовищах	Розгортання глобально у фізичному, віртуальному та хмарному середовищах, IT/OT/IoT
Взаємодія	Низька взаємодія – обмежені інструменти для аналізу та реагування	Висока взаємодія – забезпечує широкий аналіз атак, розслідування, автоматизацію ізоляції та численні інтеграції, щоб допомогти прискорити аналіз загроз і реагування на інциденти

Для чого Deception Technology для OT середовищ?

Критичні активи не виправляються або не контролюються

- Системи ICS не мають безпеки за своєю конструкцією та нестійкі до змін
- Періоди технічного обслуговування є дорогими та вимірюються місяцями/роками
- Різноманітні активи різних постачальників (застарілі ОС, нестандартні пристрої та протоколи)

Межа між IT та OT зменшується

- ICS більше не ізольовані від корпоративних чи інших мереж

Підрозділи безпеки обмежені

- Високий рівень хибних позитивних сповіщень, розслідується < 5%.
- Прогалини в навичках кібербезпеки

Decoy та Lure в FortiDeceptor

Якв різниця?

Decoy

VM що виконується в FortiDeceptor

Lure

Агент на пристрої в продуктиві

FortiDeceptor в дії…

Раннє виявлення. Стримування кібератак. Зменшення ризику.

Комплексне виявлення, закриття прогалин у видимості, відволікання зловмисників від чутливих активів, зміна балансу на користь захисника

Decoys/Lures в FortiDeceptor

Local Windows Decoy
- Windows 7
- Windows 10

Custom Windows Decoy
- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Windows Lure / Tokens
- SMB
- RDP
- TCP Port Listener
- SQL (MS-Server)
- Cache Credentials
- Fake Network Connection
- SQL ODBC
- SAP Connector
- FTP
- HoneyDocs (Office & PDF & Excel)

VPN Decoy
- FortiOS

VPN Lures
- SSLVPN

Linux Decoy
- Ubuntu 16.0.4
- Ubuntu 18.0.4
- CentOS

Linux Lure / Tokens
- ESXi
- ELK
- MySQL
- Tomcat

Cloud Decoys
- AWS
- AZURE
- GCP

IoT Decoys
- Cisco Router
- IP Camera
- Printers (HP,Lexmark,Brother)
- UPS

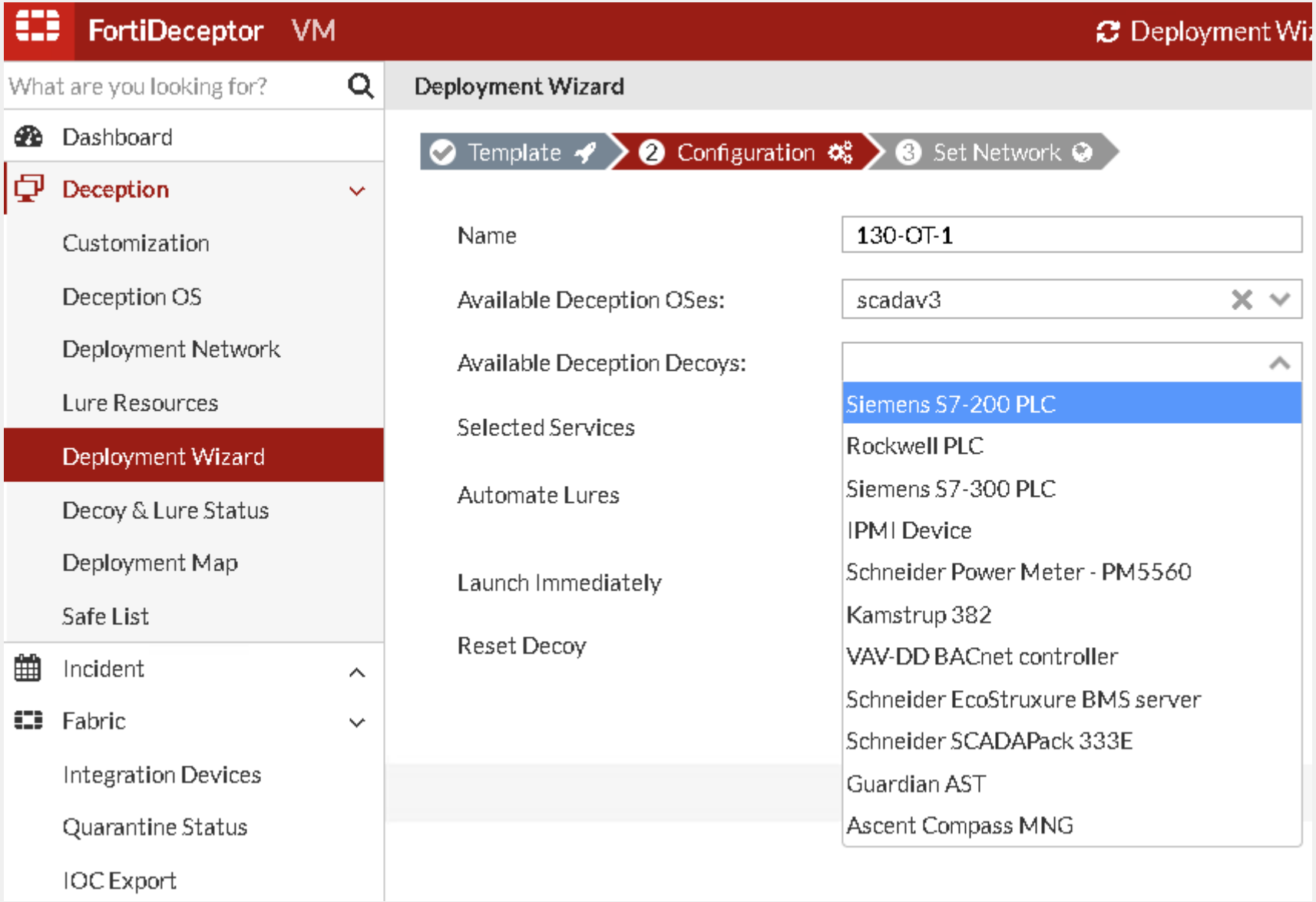
VoIP Decoys
- SIP
- XMPP
- MQTT

Application Decoys
- SAP
- ERP
- POS
- GIT

Medical Decoys
- PACS
- DICOM
- Infusion Pump

SCADA Decoy
- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM (Siemens)
- BACNET
- IPMI
- TRICONEX (Schneider)
- GUARDIAN-AST
- IEC 60870-5-104
- EtherNet/IP (Rockwell)
- DNP3
- SRTP (GE IP Series 90-30)
- MOXA (NPORT)
- SCADABR (MGMT)

Підтримка OT в FortiDeceptor



Інтеграція з рішеннями інших виробників

Рідна та загальна інтеграція

Вбудована інтеграція автоматизації

- FGT-REST-API
- FGT-WEBHOOK
- PAN-XMLAPI
- FNAC-WEBHOOK
- WMI-Disable
- FortiEDR-Isolation
- Cisco-ISE
- Microsoft-ATP
- CrowdStrike-Isolation
- FSM-Watch-List
- Checkpoint-FW-Isolation

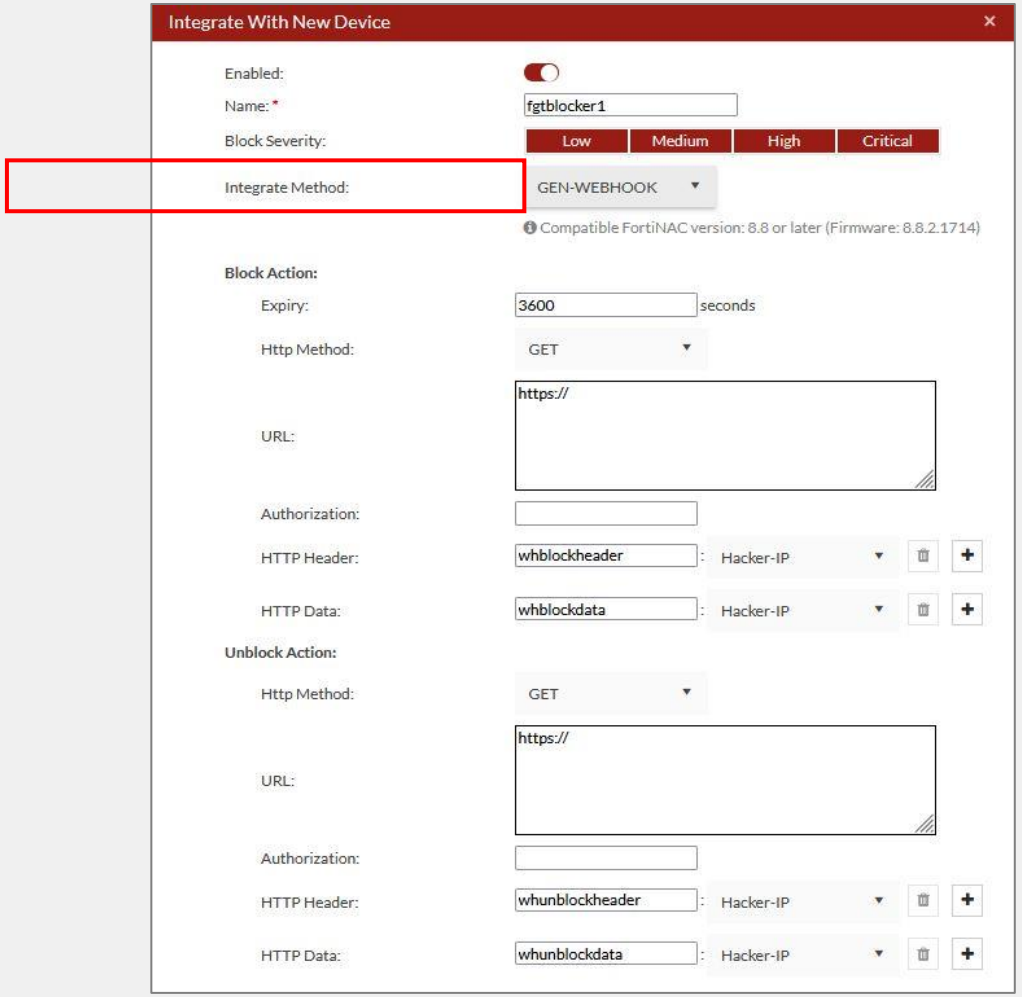
Загальна інтеграція автоматизації

- GEN-WEBHOOK (generic API call)

IOC Export

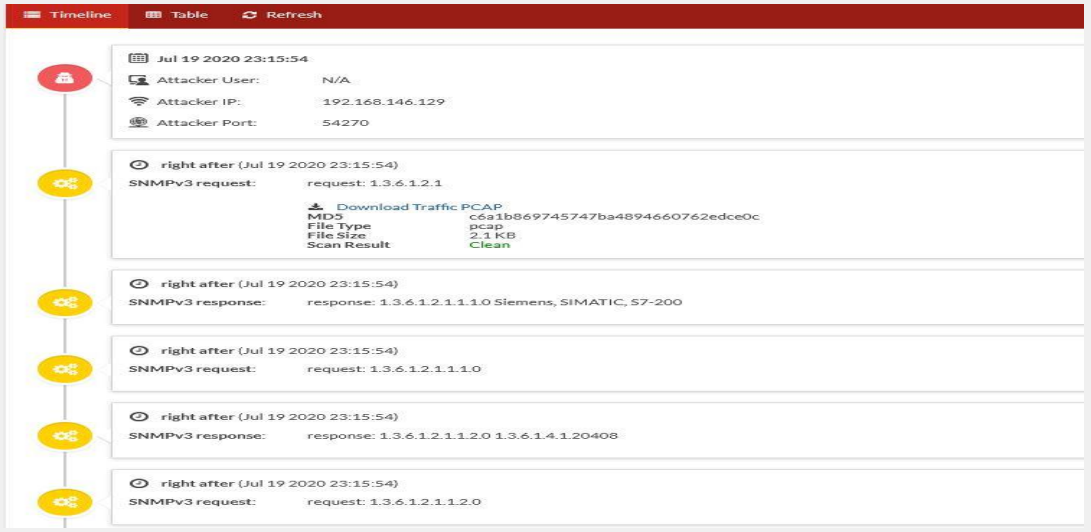
- STIX/TAXII

Syslog Log Streaming

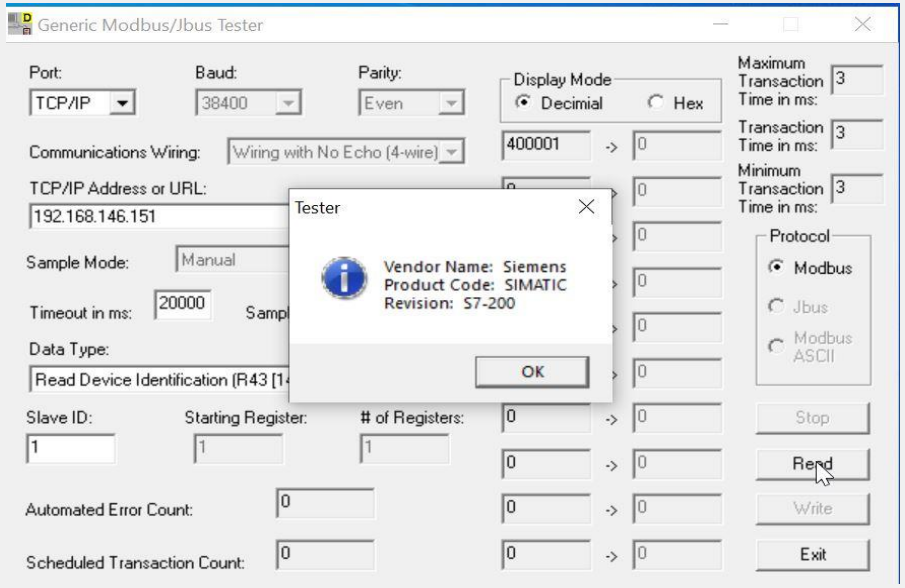


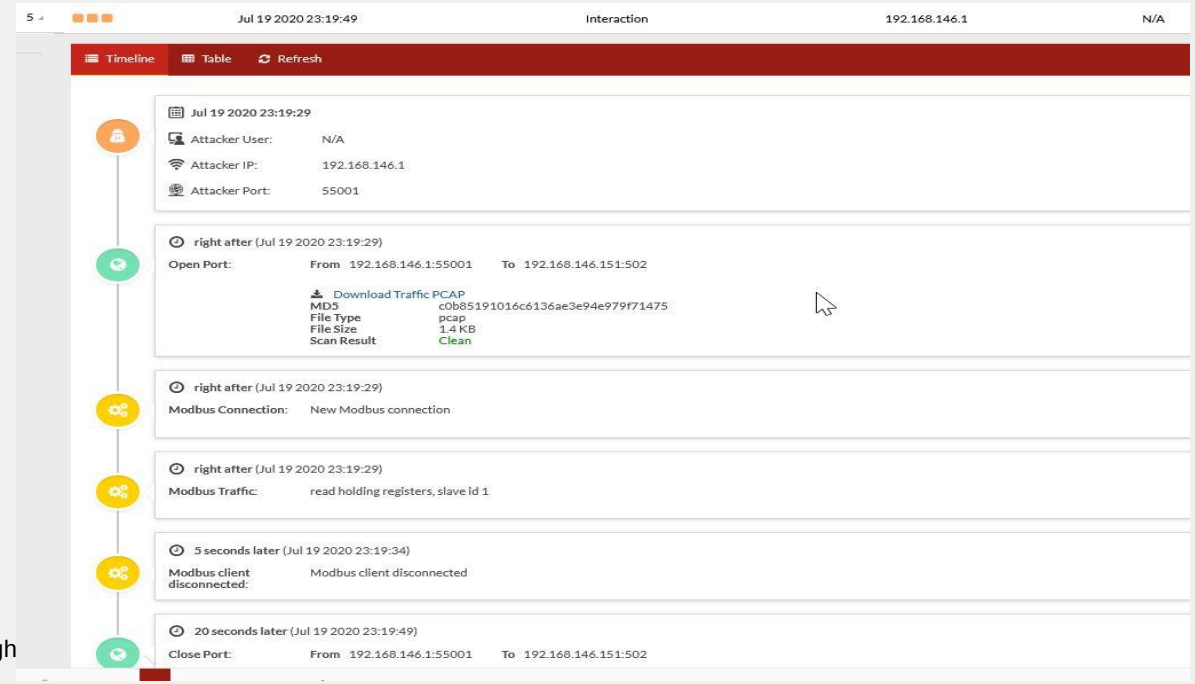
SCADA Attack Simulation – FortiDeceptor

SNMP Query for stealth Device discovery



MODBUS RD/WR Query for retrieving and changing the configuration



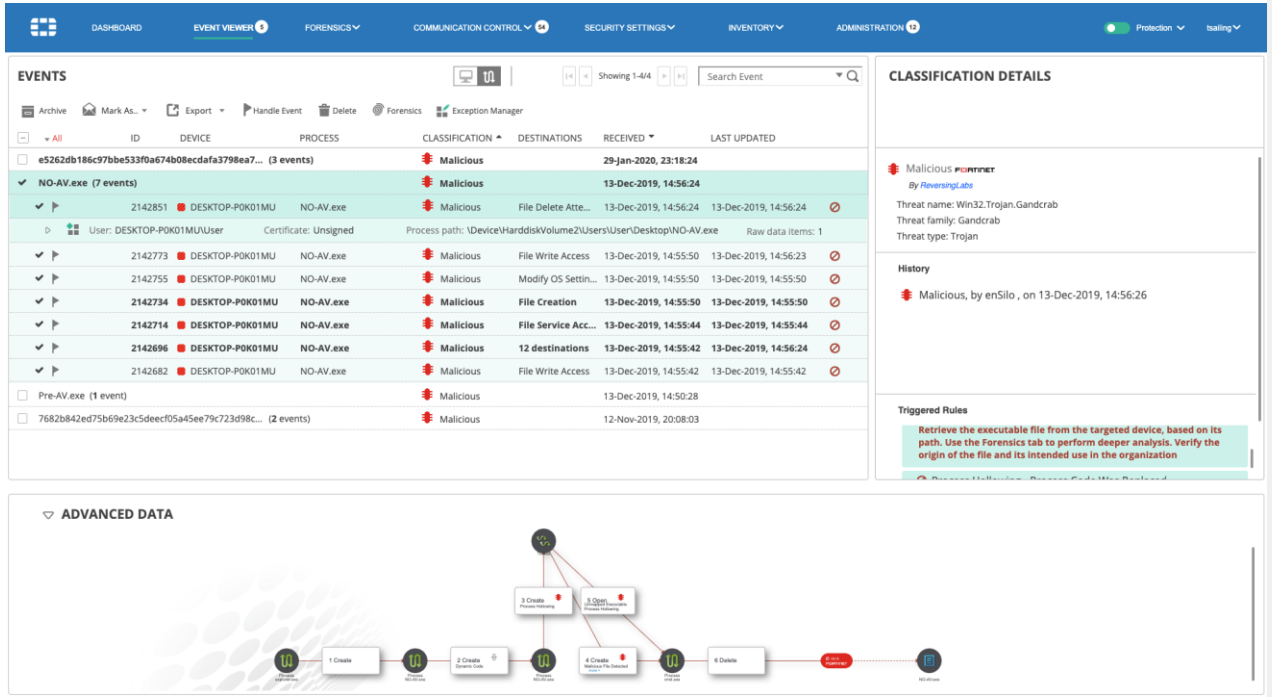


FortiEDR

FortiEDR

Розширений автоматизований захист кінцевої точки, виявлення та реагування

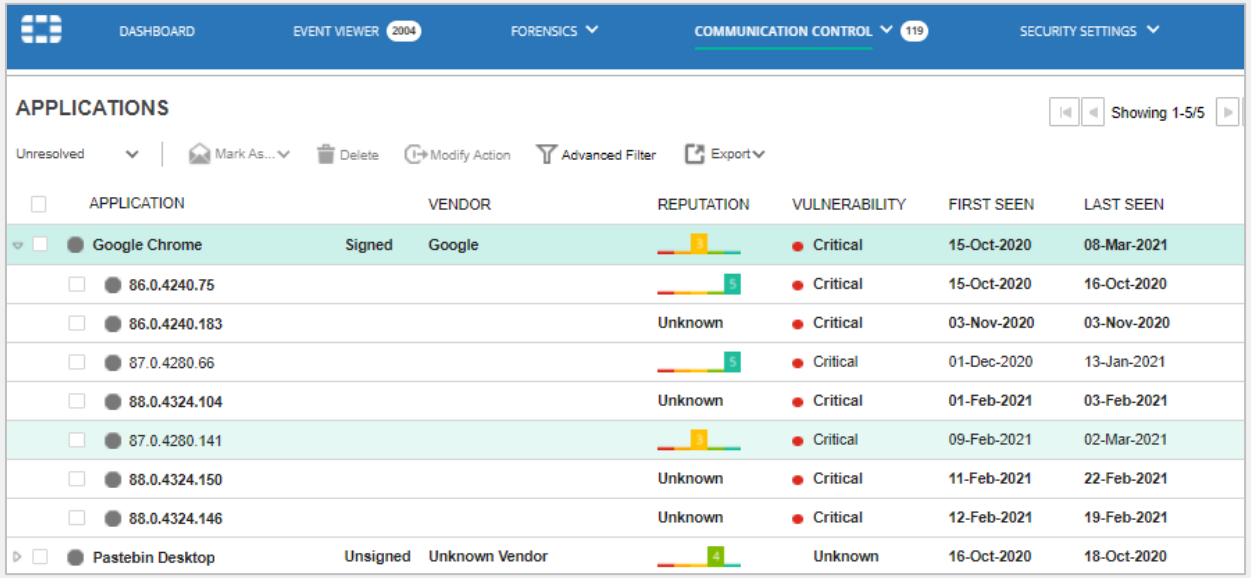
- Виявлення, передбачення, запобігання
- Виявлення та знешкодження в реальному часі
- Playbook-based реагування на інциденти
- У реальному часі та автоматично
- Ефективні операції безпеки
- Мінімальний вплив на бізнес



Дослідження і передбачення

ЗМЕНШЕННЯ ПОВЕРХНІ АТАКИ

- Виявлення сторонніх пристроїв та IoT
- Сканування додатків, вразливостей
- Risk-based проактивні політики, virtual patching

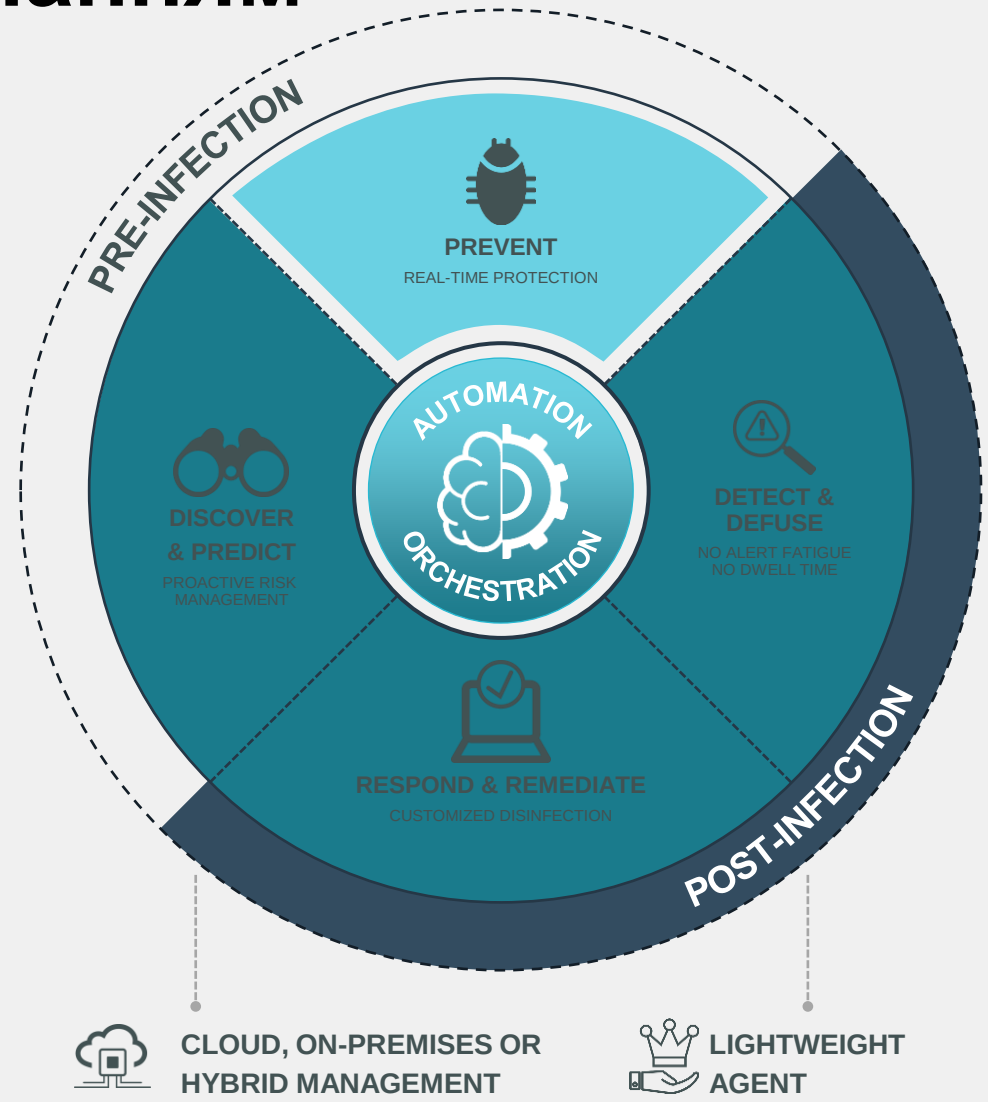


Anti-Malware з машинним навчанням

ЗАХИСТ В РЕАЛЬНОМУ ЧАСІ

- Машинне навчання, kernel-based AV
- Оновлювана база даних в хмарі
- Незмінно найвищий рейтинг

POLICY NAME	RULE NAME	ACTION	STATE
Execution Prevention			
	Malicious File Detected	Block	Enabled
	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
	Sandbox Analysis - File was sent to the sandbox for analysis	Log	Disabled
	Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
	Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
	Suspicious File Detected	Block	Enabled
	Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
	Unconfirmed File Detected	Block	Enabled

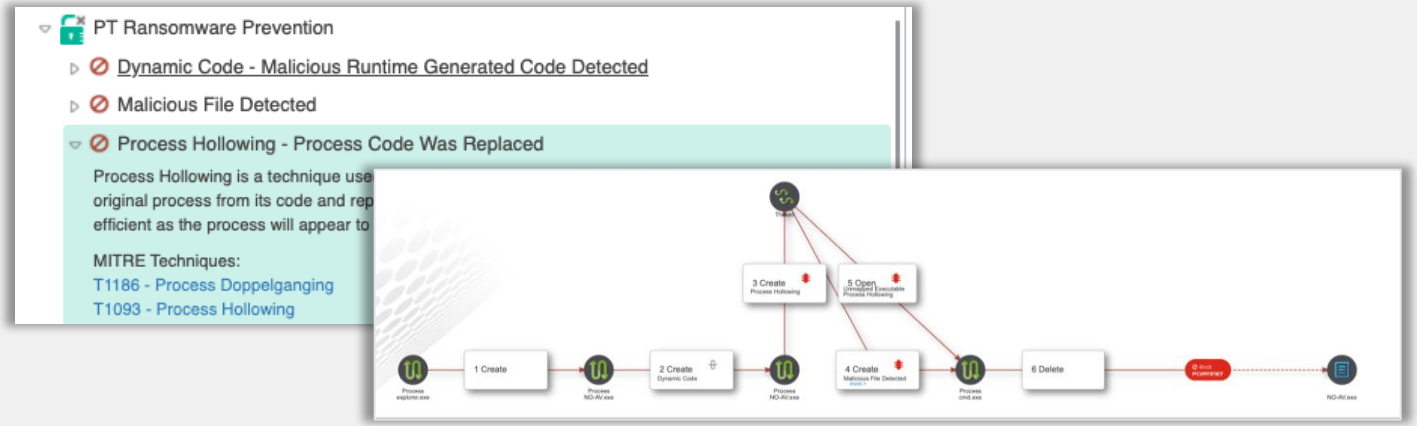


Виявлення та знешкодження

ВИЯВЛЕННЯ, ЗНЕШКОДЖЕННЯ ТА АУДИТ

Patent Number US2016149887A1

- Трасування та аналіз стека ОС
- Блокування зламів у реальному часі - навіть після успішного проникнення
- Блокування комунікацій - Data exfiltration, lateral movement, C&C
- Заборона доступу до файлової систем – захист від шифрування ransomware, модифікацій реєстру

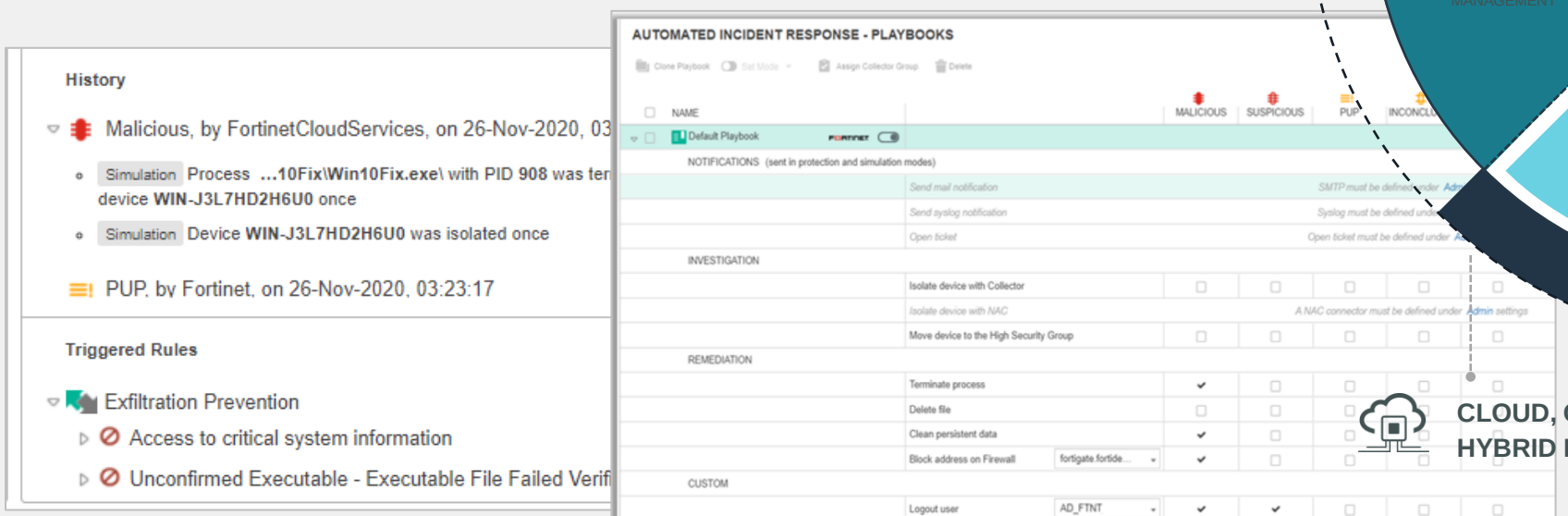


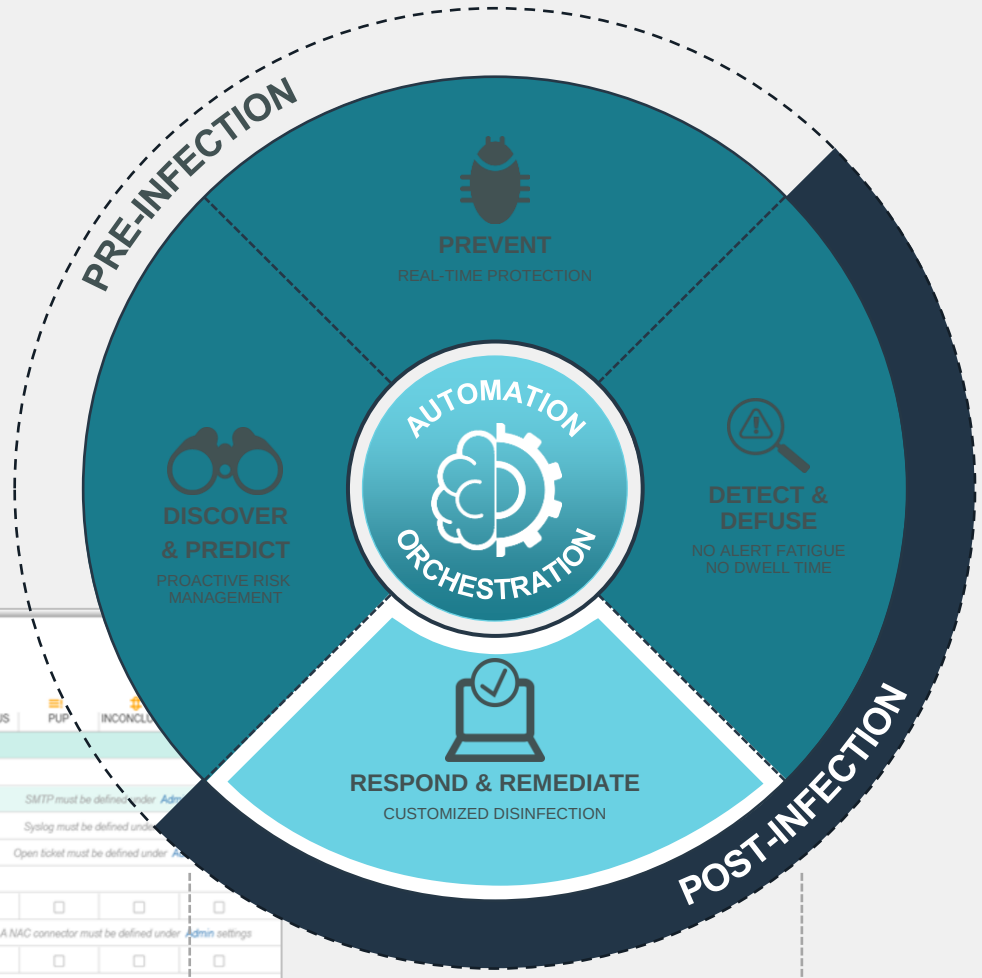
Реагування і виправлення

РЕАГУВАННЯ НА ІНЦИДЕНТИ

Fortinet Ref.: 19154; FORT-035200

- Автоматизована постійна (пере-)класифікація подій
- Настроювані playbooks на основі групи пристроїв і класифікації загроз
- eXtended автоматизовані реагування та виправлення





CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

LIGHTWEIGHT AGENT

FEDR підтримка операційних систем

- **Windows**
  - XP SP2/SP3
  - 7, 8, 10 and 11

- **Windows Server**
  - 2003 R2 SP2
  - 2008 R1 SP2
  - 2008 R2
  - 2012
  - 2012 R2
  - 2016
  - 2019
  - 2022

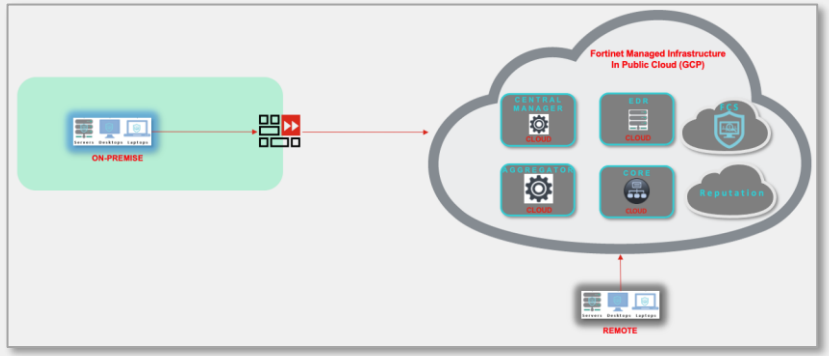
- **Linux Distributions**
  - Red Hat Enterprise (6.x, 7.x, 8.x)
  - CentOS (6.x, 7.x, 8.x)
  - Ubuntu (16.04, 18.04, 20.04
  - Oracle Linux (7.x , 8.x)
  - Amazon Linux AMI 2 (2018)
  - Open SUSE Linux
  - SUSE Linux Enterprise (11.x, 12.x, 15.x)
  - Debian*
  - Fedora*

- **VDI Environment**
  - VMware Horizons 6
  - Citrix XenDesktop/XenApp 7

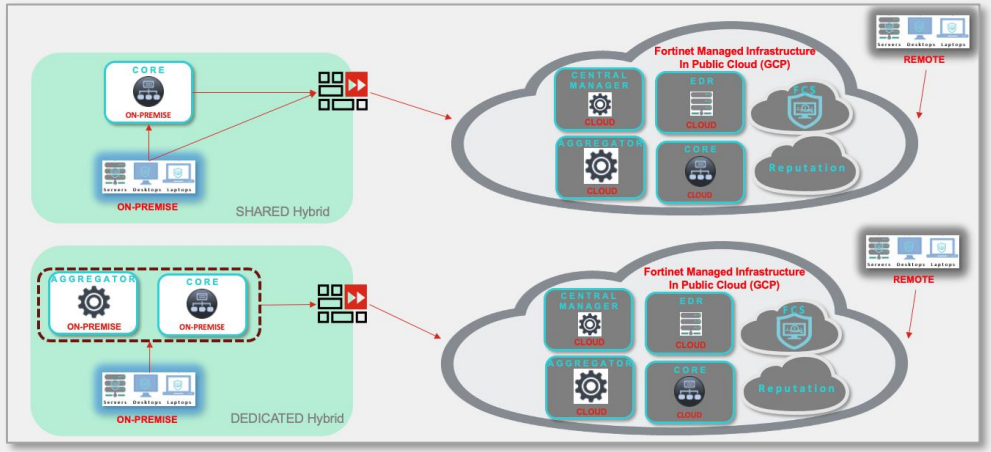
- **MACOS**
  - Yosemite (10.10)
  - El Capitaine (10.11)
  - Sierra (10.12)
  - High Sierra (10.13)
  - Mojave (10.14)
  - Catalina (10.15)
  - Big Sur (11)
  - Monterey (12)

FEDR варіанти розготання

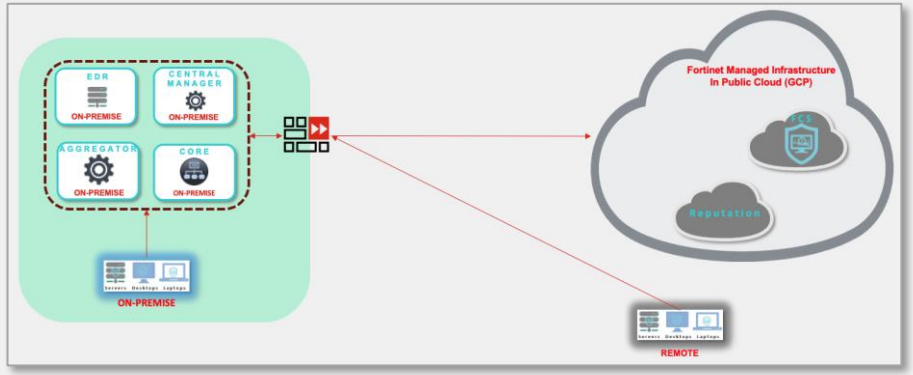
1. **Cloud** = Усі компоненти в хмарі



2. **Hybrid** = On Premise та в хмарі



3. **On-Premise** = Усі компоненти on-prem (та з’єднання з FCS).



Інтеграція FortiXDR з фабрикою

eXtended Detection

FortiGate
- Telemetry sharing

FortiMail
- Telemetry sharing

FortiSandbox
- Threat Intelligence Sharing

= XDR

eXtended Response

FortiGate
- automatic blocking of malicious destination IP

FortiNAC
- Isolation actions

FortiSIEM
- Alert and log sharing

FortiSOAR
- Extended workflow automation

3rd Party Ticketing
- Create cases, pass case information

3rd Party Security Products
- Using the REST API + Custom Connectors

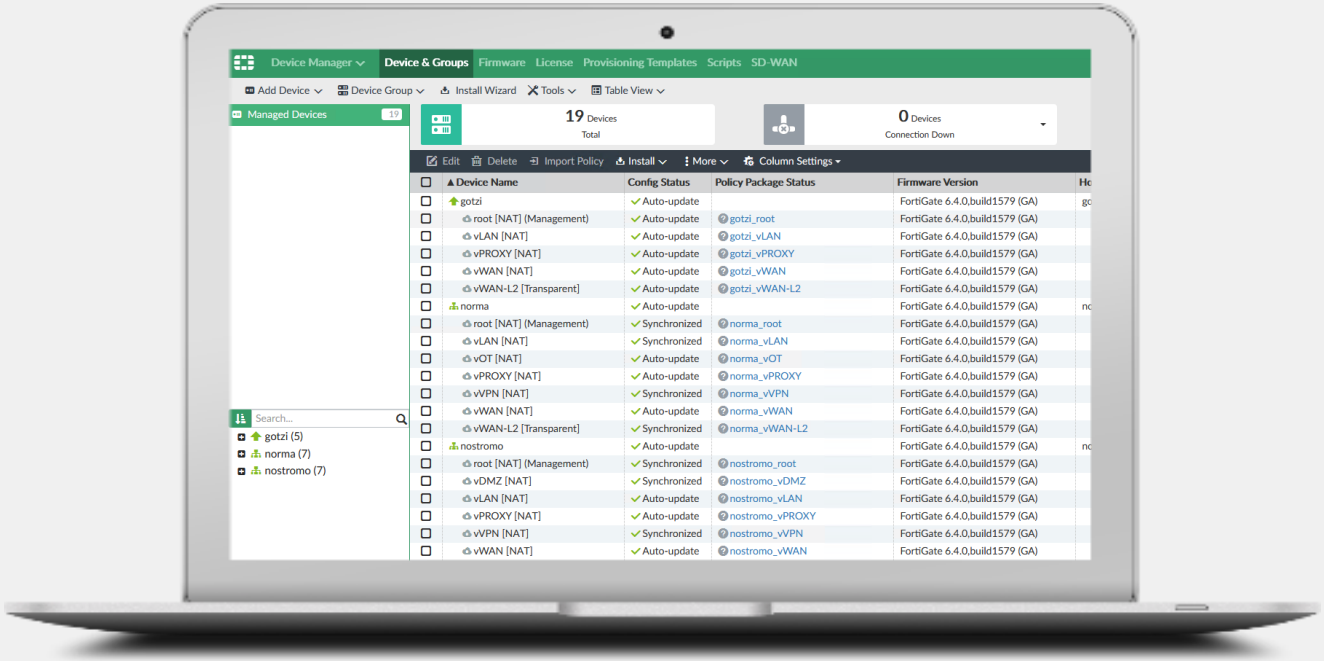
Управління безпекою, аналітика та автоматичне реагування для OT

FortiManager

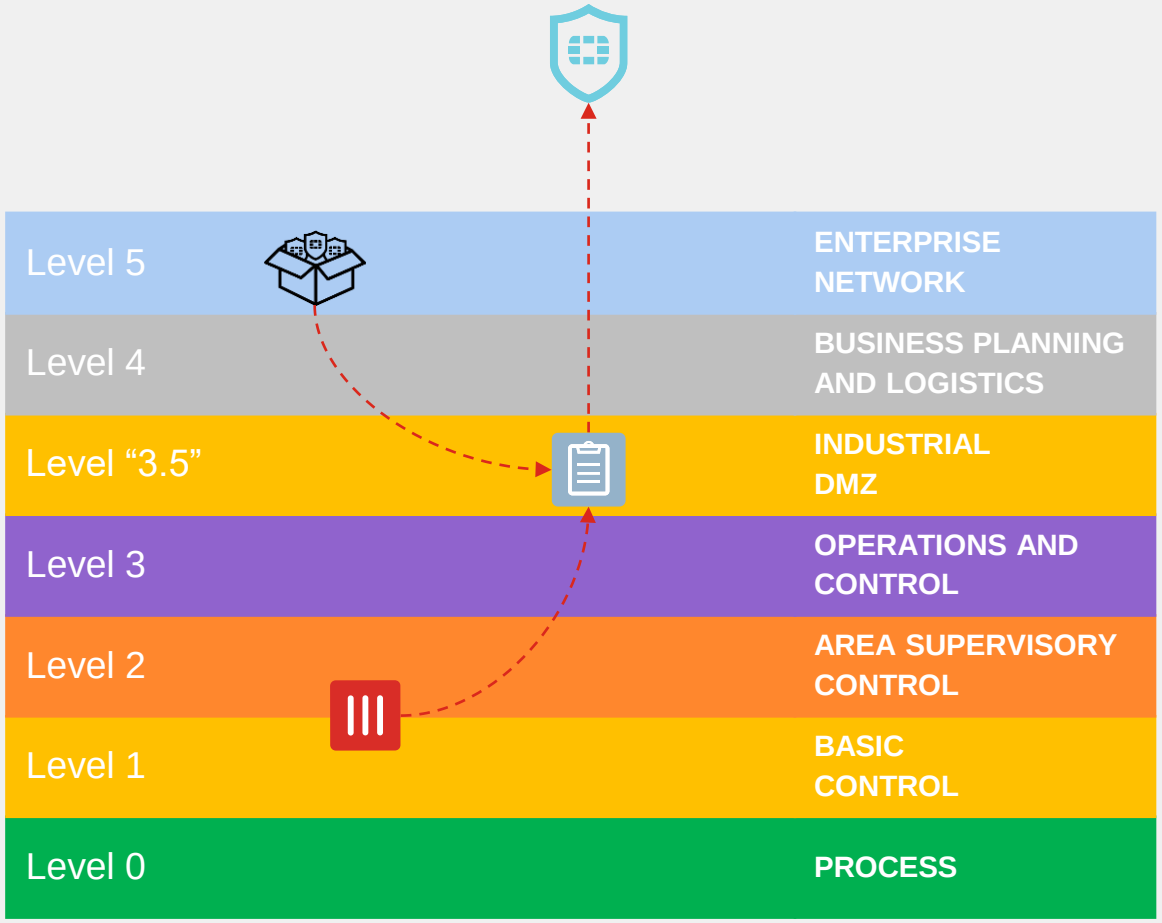
Appliance | Virtual Machine | Hosted | Cloud

Ефективне керування інфраструктурою безпеки Fortinet будь-якого розміру, від кількох до тисяч пристроїв

- Просте централізоване налаштування, уніфікація політик, керування оновленнями та наскрізний моніторинг мережі
- Розділення адміністрування великих інсталяцій з ADOM
- Централізована панель керування NGFW, IPsec, маршрутизацією, FortiSwitche, FortiAP тощо
- Локальна база оновлень FDS для ізольованих середовищ
- Автоматизація через JSON/XML API



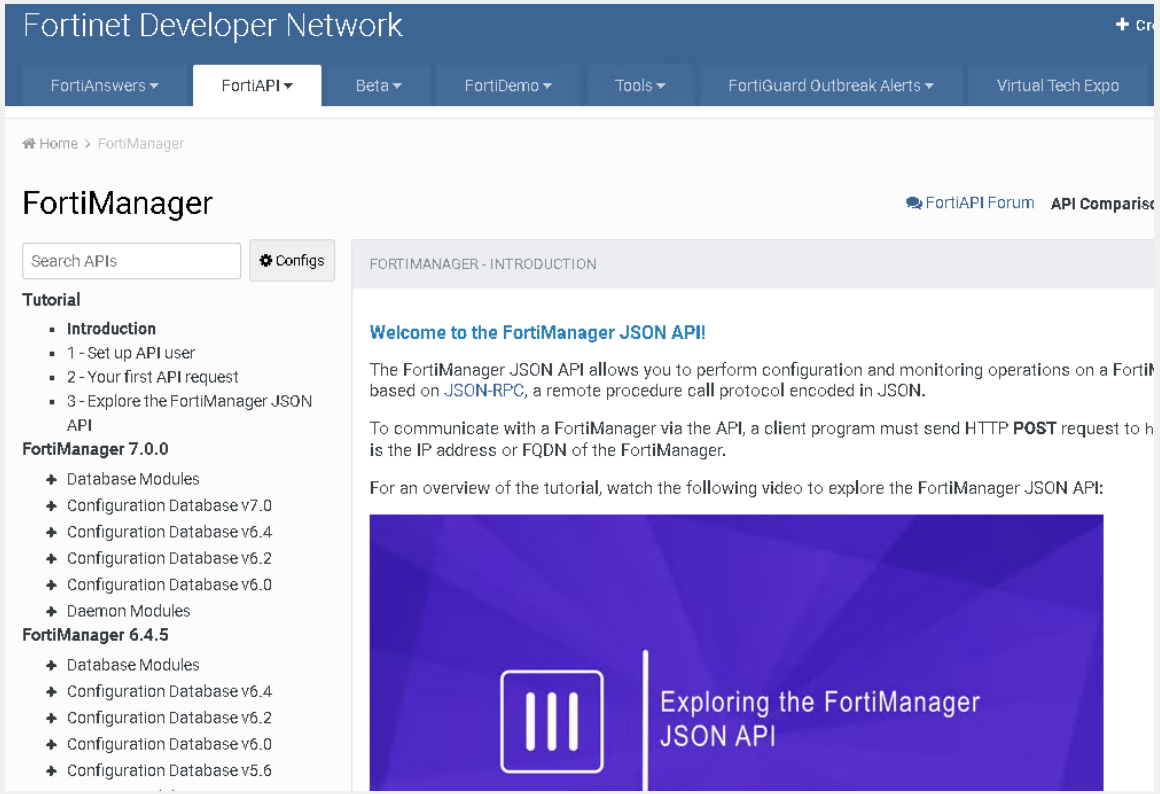
FortiManager як локальний сервер оновлень FDS



- FortiManager як FortiGuard Distribution Server (FDS)
  - Достатньо BASE license
  - Синхронізує оновлення з FortiGuard Distribution Network (FDN)
  - Альтернативно – ручне (offline) завантаження оновлень
- FortiGate налаштовуються використовувати FortiManager як local FDS
  - Надає Web Filtering database
  - Надає всі потрібні пакети оновлень FortiGates
  - FDN для FGT, FPX, FSA, FCT тощо..

Автоматизація

FortiManager API's



ЗАДАЧА

- Інтеграція в існуючу екосистему
- Інтелектуальна автоматизація, ініціалізація пристроїв у виділених ADOM тощо.

МОЖЛИВОСТІ

- REST API
- DevOps – Ansible, Terraform etc.
- SDK

ПЕРЕВАГИ

Підвищення операційної ефективності та результативності

FortiAnalyzer

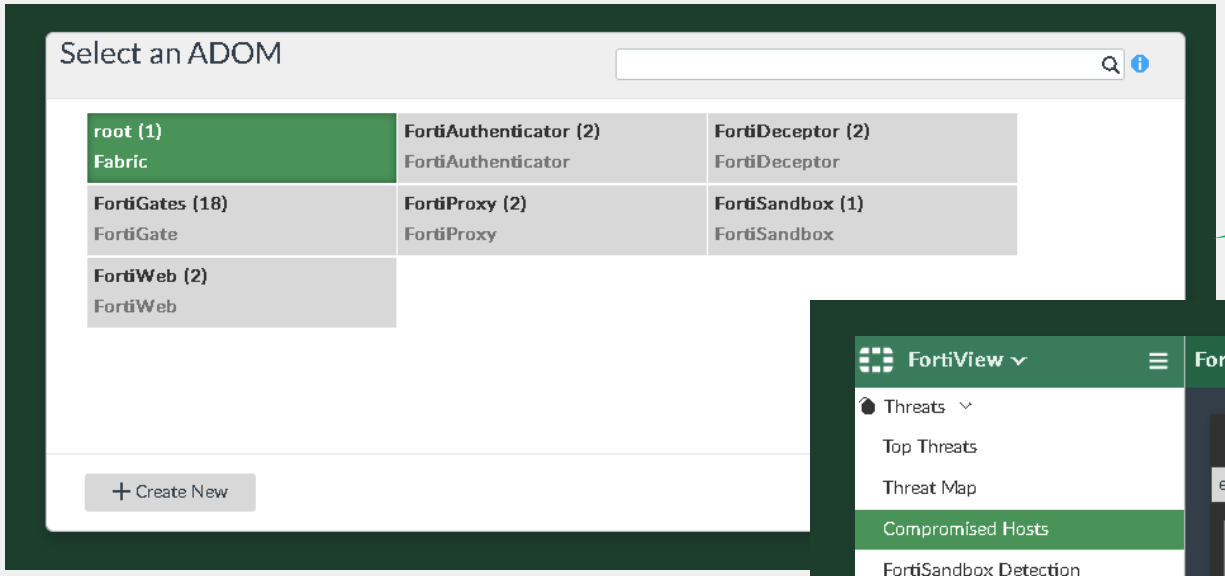
Security Fabric управління журналами, аналітика та звітність

FortiAnalyzer

- ✓ Наскрізне керування безпекою + журнали безпеки з виявленням/аналітикою в реальному часі
- ✓ Єдина платформа для видимості IT, NOC & SOC
- ✓ Розширений захист від загроз із можливостями автоматизації Security Fabric

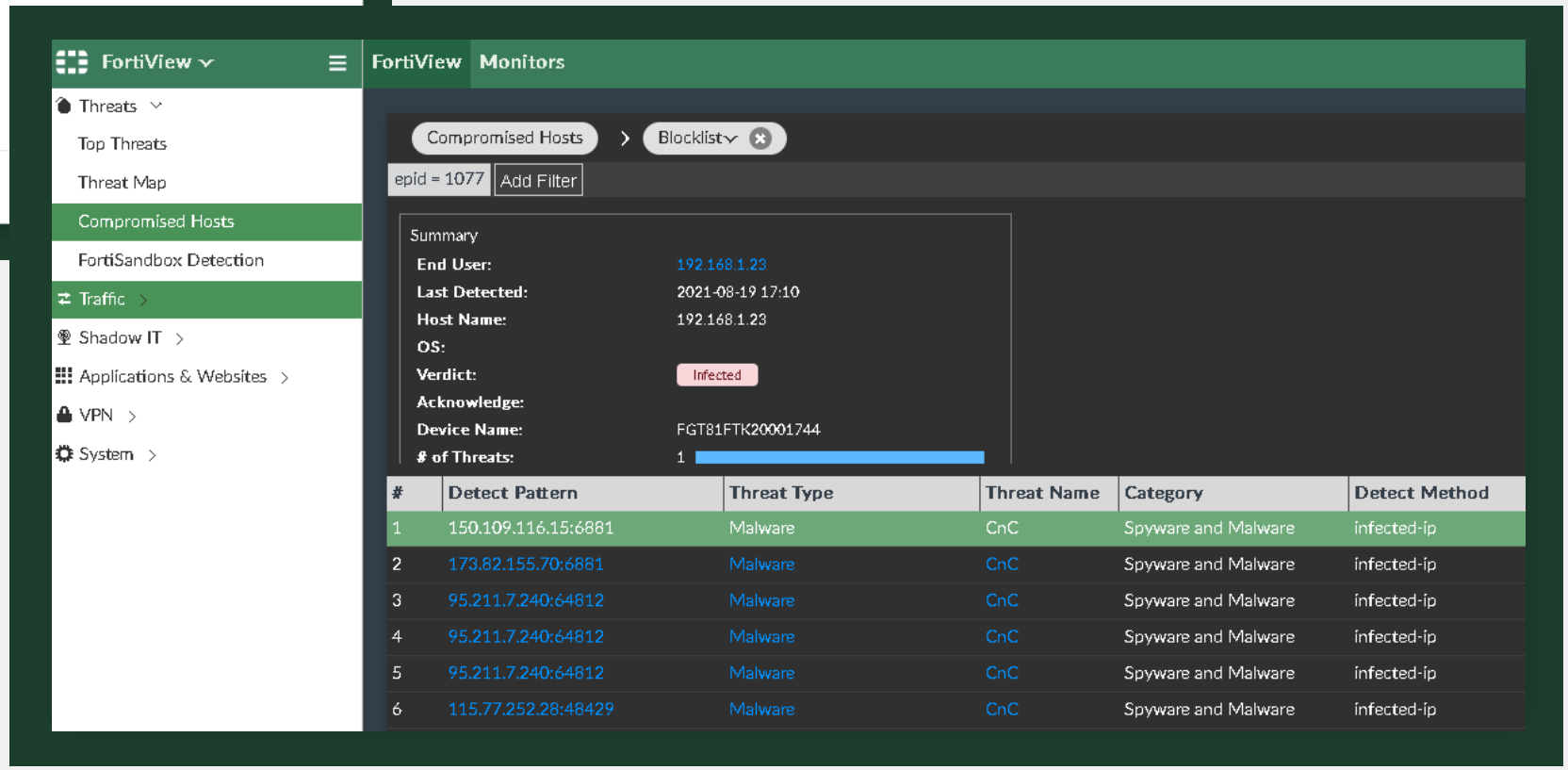
SOC and NOC teams can use FortiAnalyzer for IOC, event handling and reporting

FortiAnalyzer – повна підтримка Security Fabric



Targeted ADOMs per device types and/or tenants.

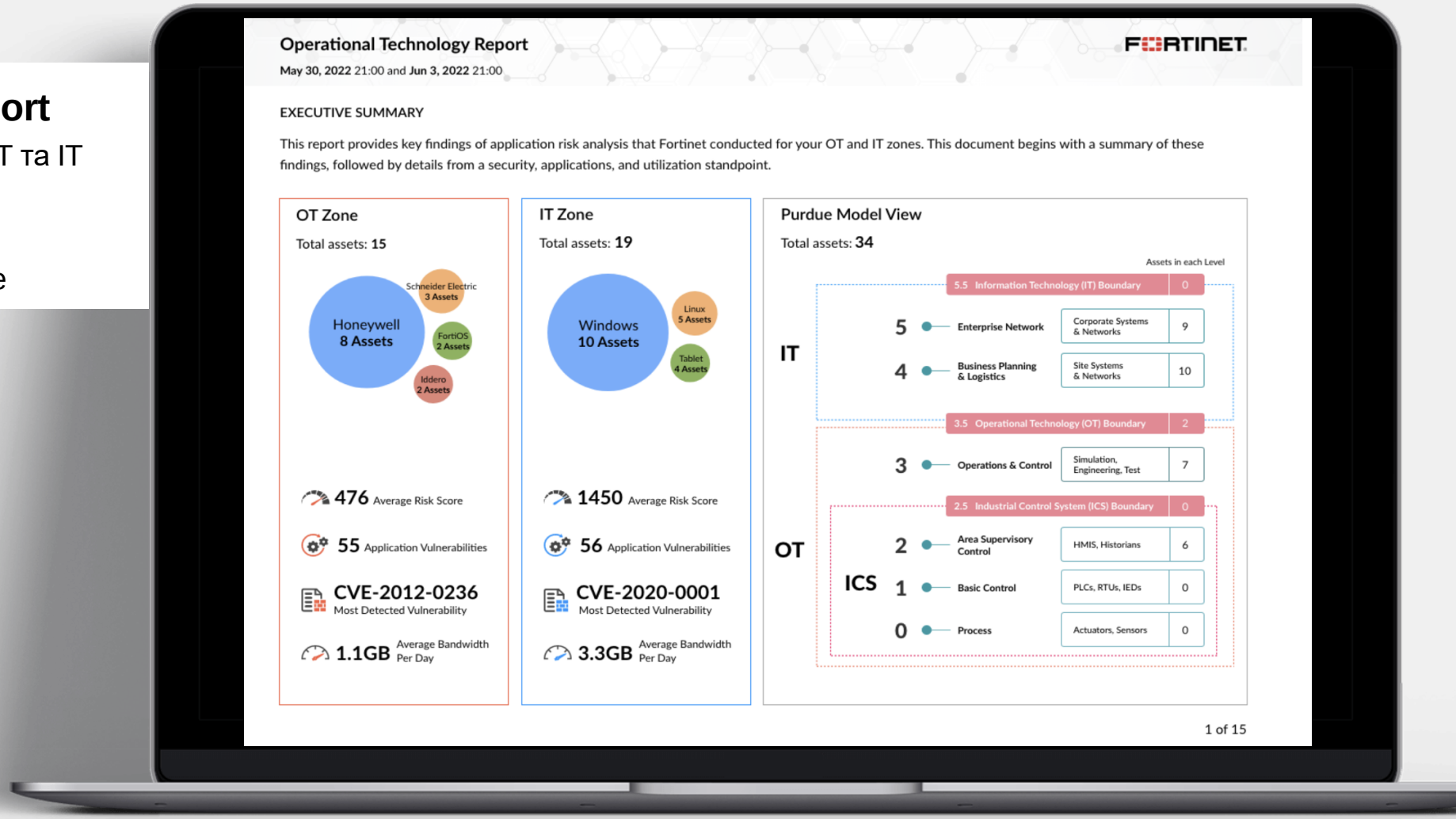
IoC's, Top Threats, Sandbox ratings in a Single Pane of Glass.



Звітність для OT

Operational Technology Report

- Аналіз ризиків програми для зони OT та IT
- Виявлення сліпих зон і прихованих ризиків
- Відображення активів моделі Purdue



FortiSIEM

Appliance | Virtual Machine | Cloud

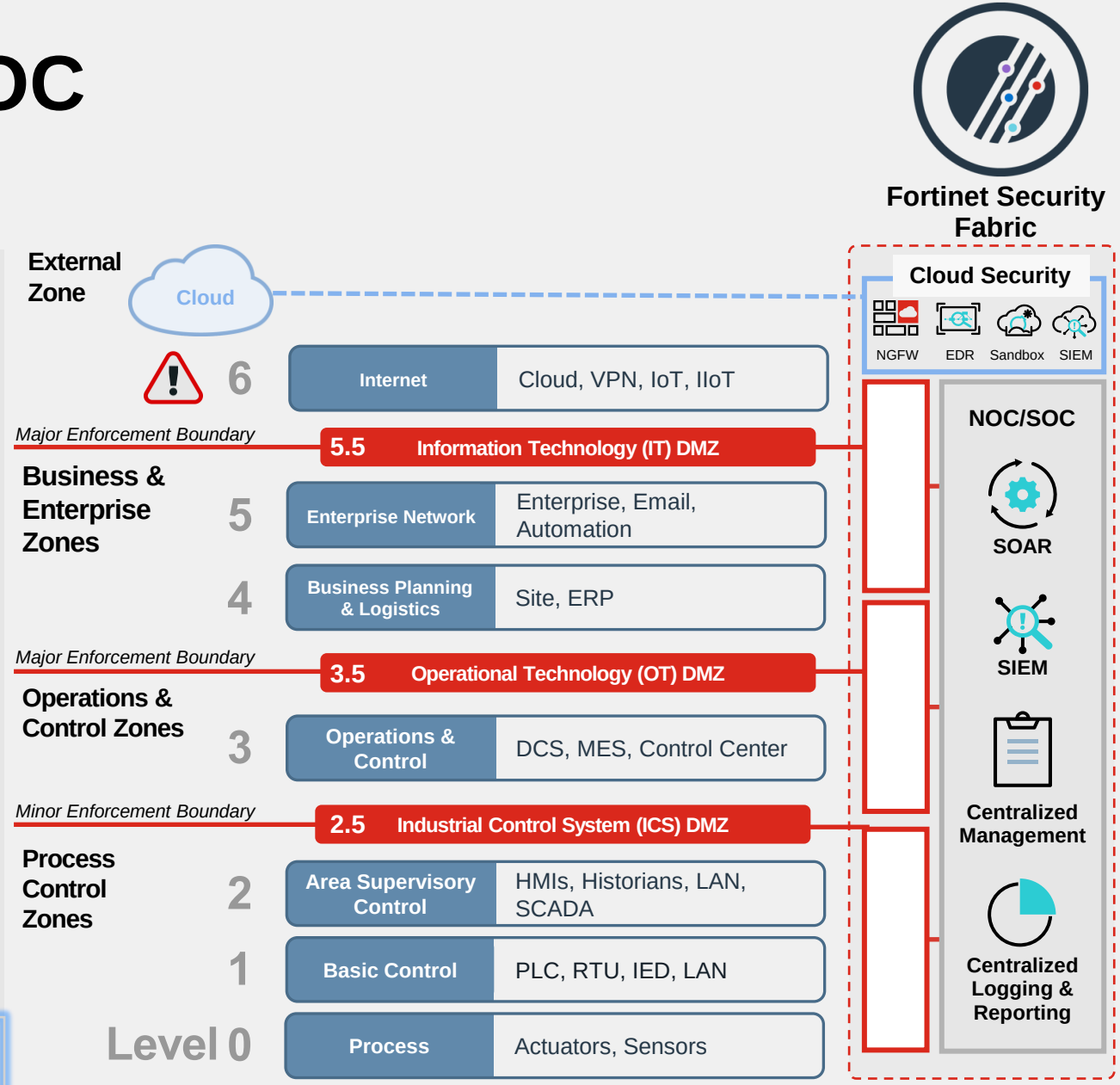
Уніфікована кореляція подій та управління ризиками для сучасних мереж

- Виявлення активів
- Швидка інтеграція та масштабованість
- Автоматизація із бібліотекою реагувань
- Централізована консоль для швидкого вирішення проблем
- Підтримка Multi-tenancy та RBAC

NOC / SOC

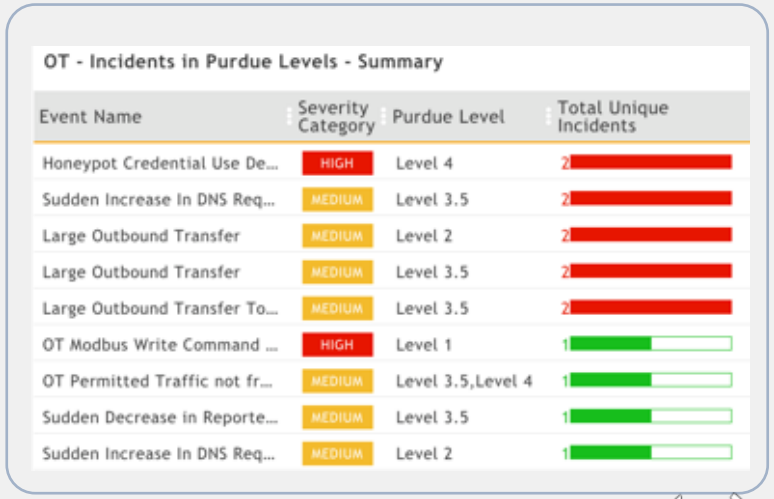
3 FortiSIEM

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



OT Specific Capabilities

- FortiSIEM можна розгорнути локально, гібридно або в хмарі, включаючи спеціальні інструменти та інтеграції OT.
- Налаштування відповідно до конкретних випадків використання OT
- Інтеграція моніторингу OT і Enterprise
- Сканування пристроїв та додавання в CMDB FortiSIEM
- Моніторинг роботи та продуктивності пристроїв



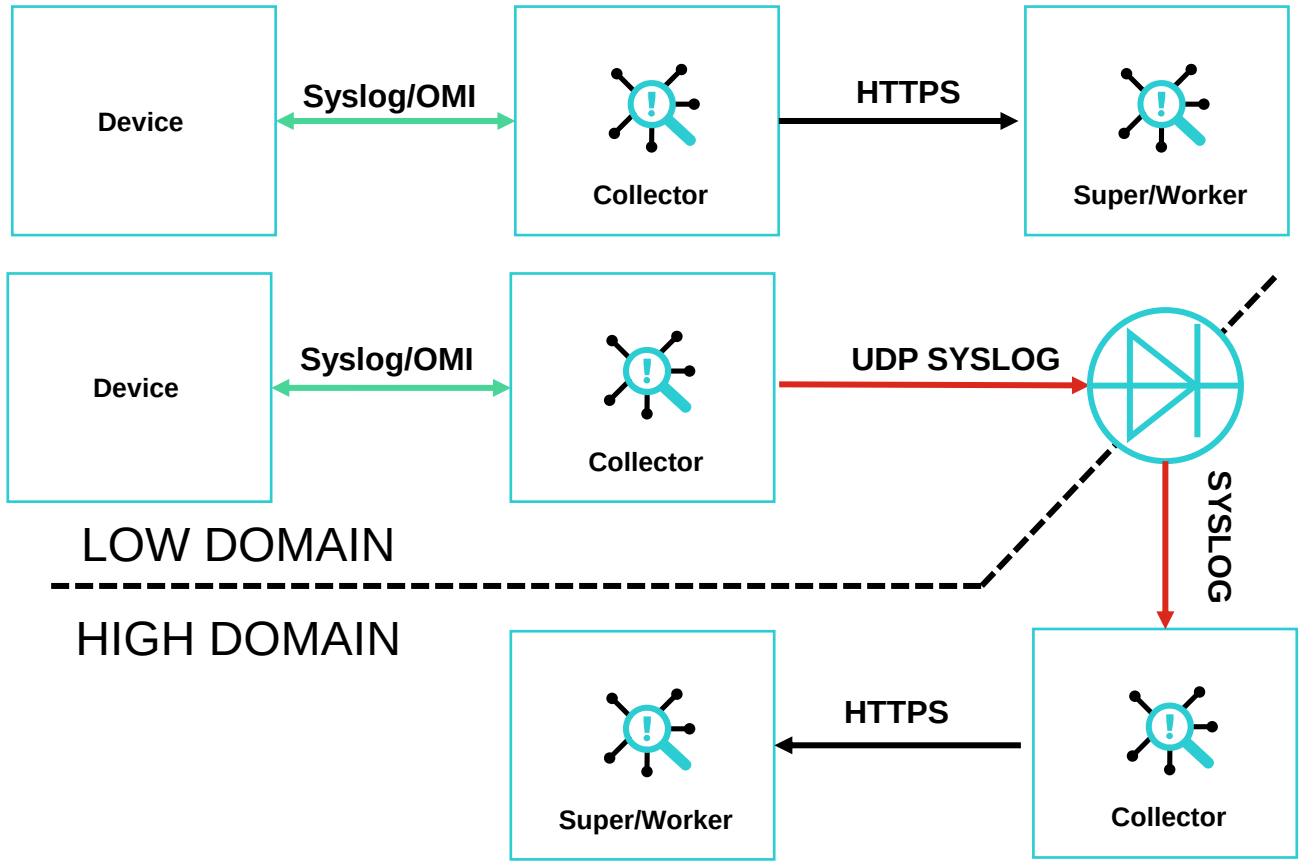
OT - Incidents in Purdue Levels - Summary

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

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

Середовища високого рівня надійності

Отримання подій через Data Diodes



Headless Collector

ЗАДАЧА

- Підтримка середовищ високої надійності, які вимагають проходження логів через мережеві діоди даних

ЯК

- Налаштування Collectors на відсилання syslog через діоди данних

ПЕРЕВАГИ

- **Гарантія того, що дані не можуть перетікати з високих доменів до низьких**
- **Гарантія часто потрібна в ОТ та державних середовищах**

Підтримка продуктів інших виробників

300+ Integrations across vendors and applications

Service Desks & Cloud

ConnectWise, ServiceNow, BMC Software Remedy, Jira, Salesforce, Microsoft Azure, aws, Office 365, okta

Security & Intelligence

Fortinet, Cisco, paloalto Networks, websense, tenable, CYBERX, VirusTotal, DRAGOS, Symantec, Qualys, FireEye, CrowdStrike, Cisco AMP for Endpoints, Trend Micro, McAfee, STIX, TAXII, NOZOMI NETWORKS, CLAROTY

Applications

ORACLE, Microsoft SQL Server, GitLab, Apache, MySQL, NGINX, Exchange, SQUID

Operating Systems

Microsoft, redhat, Linux, debian, fedora, hp, CentOS, ORACLE

Infrastructure

Fortinet, Cisco, DELL, hp, BlueCoat, Juniper Networks, HUAWEI

Platforms

aws, Microsoft Azure, Alibaba Cloud, vmware, NUTANIX, Microsoft Hyper-V, KVM

FORTINET

FortiSOAR

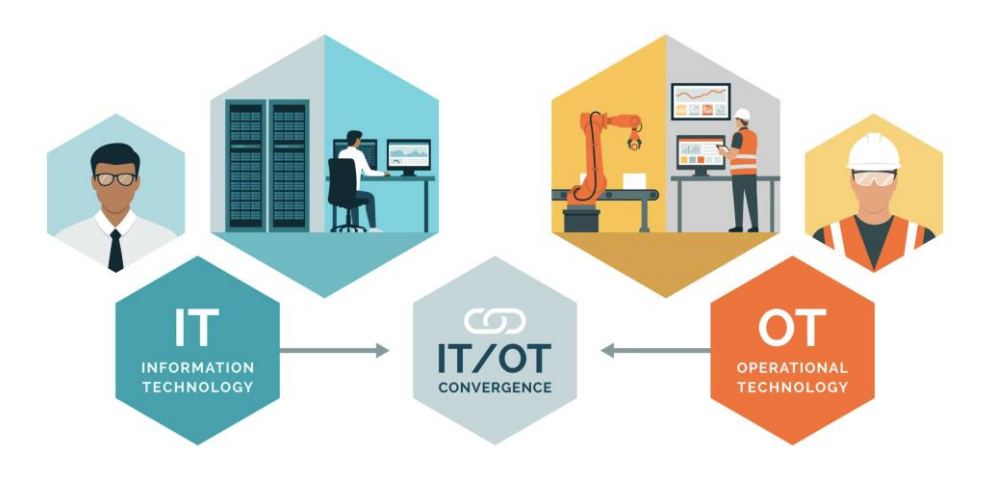
Appliance | Virtual Machine | Cloud

Уніфікована автоматизація безпеки та реагування для сучасних SOC/NOC

- Уніфіковане управління реагуванням на інциденти
- Оптимізація SOC
- Автоматизація сортування сповіщень
- Співпраця в SOC
- Корпоративна масштабована архітектура Active/Active HA, Distributed Multi-Tenancy

Як FortiSOAR може допомогти в OT?

Незалежне від постачальника, добре інтегроване рішення, яке заповнює таку необхідну прогалину в організації зв'язку між різними розрізненими системами/середовищами



Переваги FortiSOAR

- Понад 450 галузевих інтеграцій, включаючи комплексну інтеграцію з рішеннями Fortinet Security Fabric.
- Випробувано в ізольованих середовищах
- Провідна в галузі, запатентована система оркестрації/автоматизації безпеки з вбудованою контекстуалізацією MITRE ATT&CK ICS
- Агент FortiSOAR для доступу/зв'язку в сегментованих мережах і багатокористувацька модель для сценаріїв управління/оркестрації на кількох сайтах
- Вбудоване керування активами, керування threat inelligence, керування вразливостями, керування скануванням тощо для OT/IT
- Автоматизує управління відповідністю до вимог в секторах OT.
- Корпоративне рішення RBAC для забезпечення політик доступу до даних
- Пропонує готові, добре досліджені Solution Packs для скорочення часу на створення нових рішень з нуля
- Готові до OT Solution Packs для управління Threat Intel в OT, управління активами (модель Purdue), оцінки ризику тощо

Інтеграції для автоматизації в структурі Fortinet і системах/продуктах OT

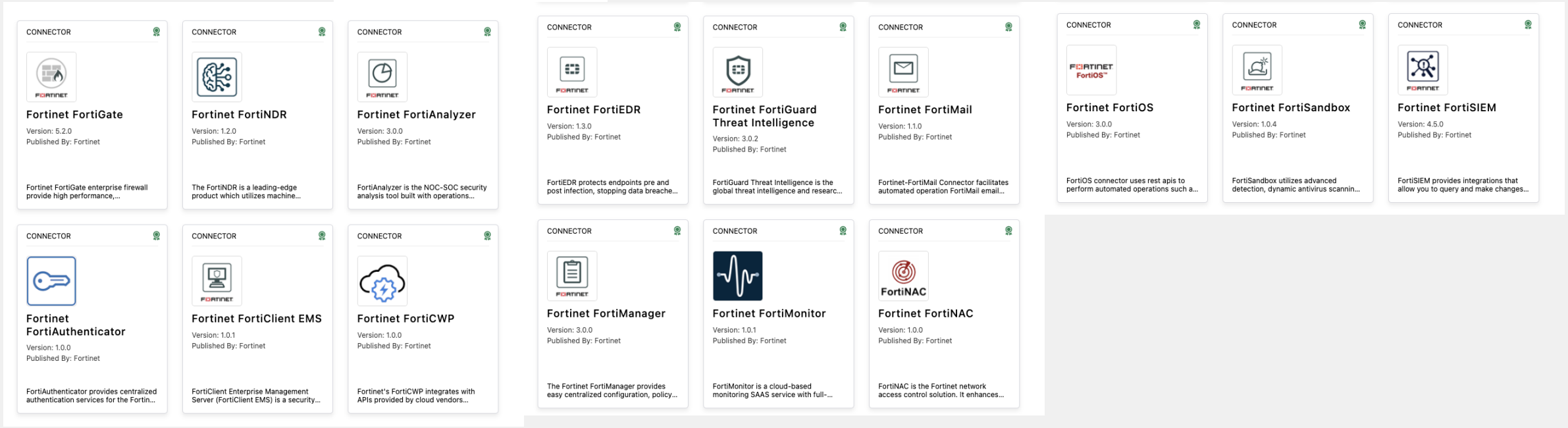
NOZOMI NETWORKS

CLAROTY

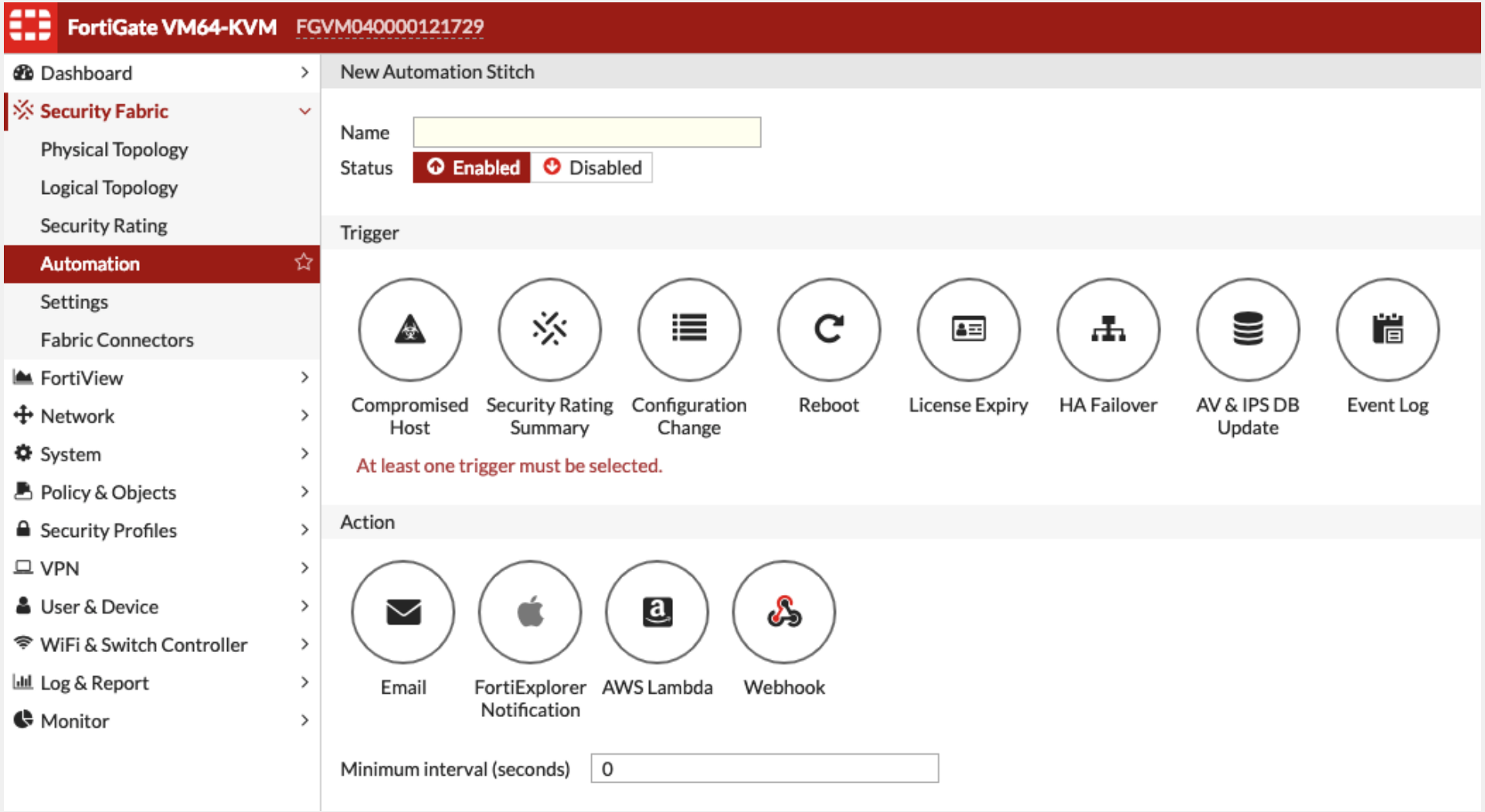
SCADAfence

FORESCOUT

everbridge



Автоматизація Security Fabric вбудована в FortiOS

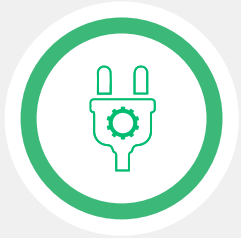


Партнерська екосистема

Розширення Платформи

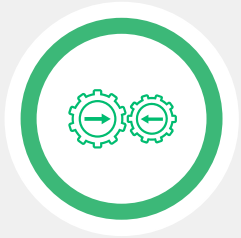
Завдяки інтеграції з найбільшою галузевою екосистемою кібербезпеки

400+ security fabric інтеграцій екосистеми



Fabric Connector

Глибока інтеграція, розроблена Fortinet, автоматизує операції та політики безпеки



Fabric API

Розроблена партнерами інтеграція з використанням Fabric API забезпечує широку видимість та доповнення функціоналу

Fabric DevOps

Сценарії DevOps, розроблені спільнотою, автоматизують налаштування мережі та безпеки, конфігурацію та оркестрацію

Extended Fabric Ecosystem

Інтеграція через обмін індикаторами та технологіями з іншими постачальниками

Extensive Cybersecurity Ecosystem

450+ Open Ecosystem Integrations

Fabric Connectors (13)

Fortinet-developed deep integrations that automate security operations and policies

aws, aruba a Hewlett Packard Enterprise company, cisco, Google Cloud, IBM Cloud, Microsoft Azure, ORACLE, servicenow, Symantec.

Fabric APIs (248)

Partner-developed integrations using Fabric APIs that provide broad visibility with end-to-end solutions

DELL, DRAGOS, EQUINIX, intel, Megaport, rubrik, Security Bridge, SIEMENS Ingenuity for life, splunk>, tufin

Fabric DevOps (10)

Community-driven DevOps scripts that automate network and security provisioning, configuration, and orchestration

aws, Google Cloud, HashiCorp, Microsoft Azure, openstack., ORACLE, RED HAT ANSIBLE Tower, refactr, vmware

Extended Security Fabric Ecosystem (200+)

Collaboration with threat sharing organizations and integrations with other vendor products

CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA, Firewalls, Switching, Wireless, Endpoint Security

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

Figures as of June 30, 2021

SCADA/Industrial Control

Fabric API партнерство в вертикалі OT

Fabric API

Приклад інтеграції Fortinet - Nozomi Networks

Пасивний моніторинг у реальному часі гарантує відсутність впливу на продуктивність і забезпечує видимість на різних рівнях мереж керування та процесів

Non-intrusive Passive Monitoring | **In-line Protection**

In-line розділення між IT та OT середовищами

Глибоке розуміння всіх ключових протоколів SCADA, відкритих і закритих

Deep SCADA Understanding | **Active Traffic Control**

Проактивна фільтрація шкідливого та неавторизованого мережевого трафіку

Автоматично вивчає поведінку ICS і виявляє підозрілі дії

Behavioral Analysis | **Security Policy Enforcement**

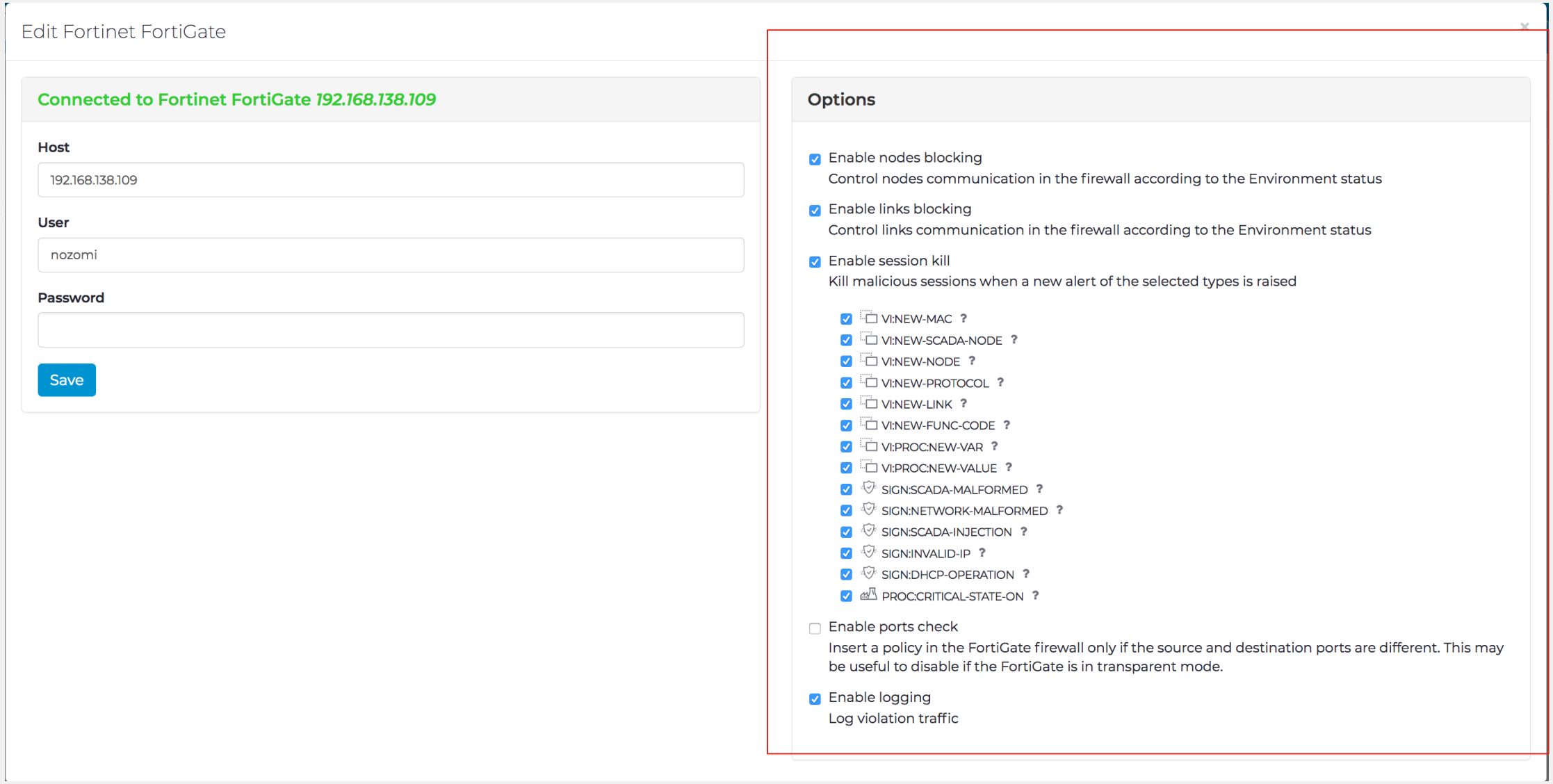
Гнучкість для застосування політик безпеки з різним ступенем деталізації

Turn–key Internal and Perimeter Visibility

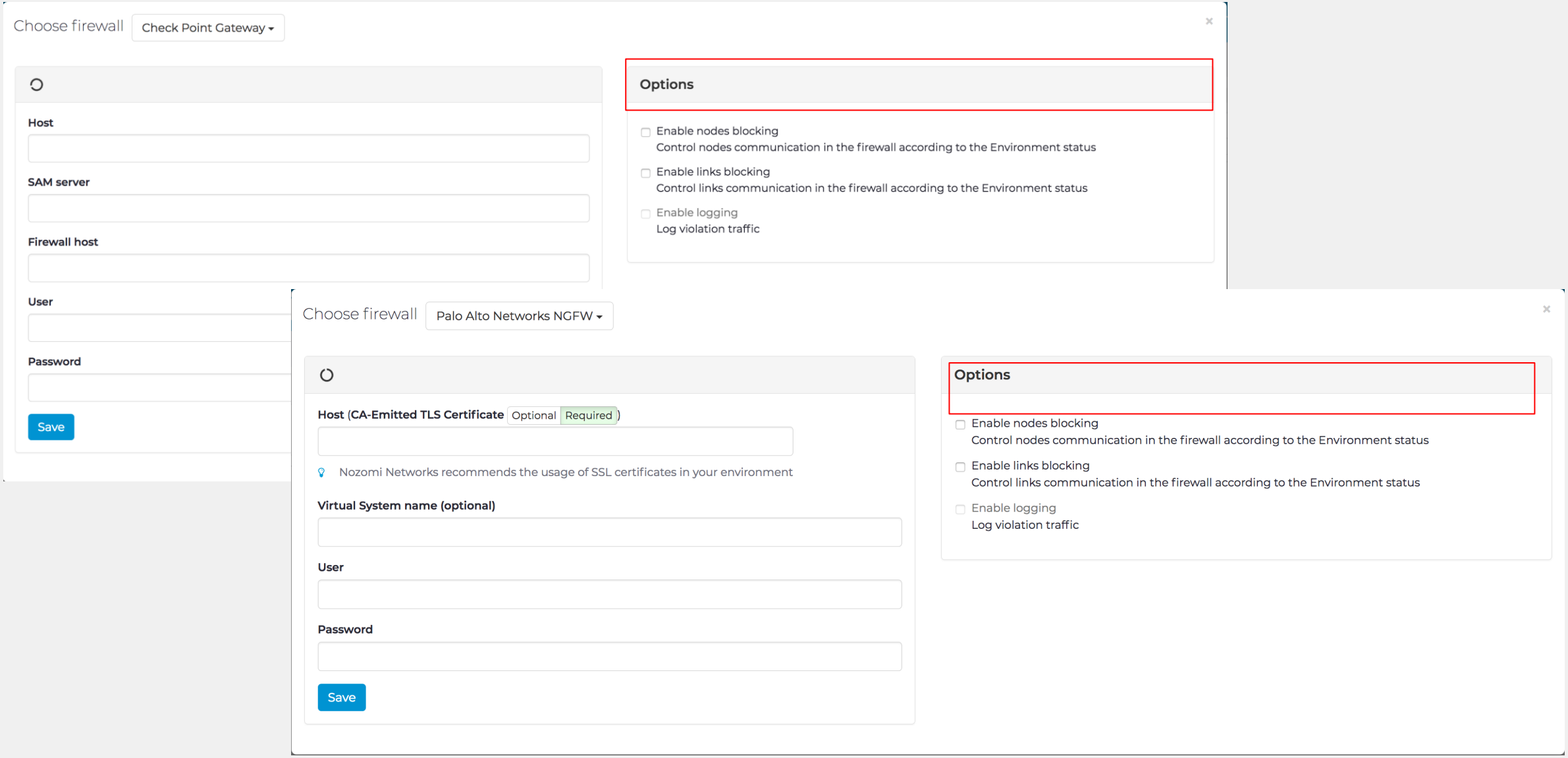
Fine Tuning, Control and Monitoring of the Firewall Ruleset

Proactive SCADA Security

Fortinet інтеграція з Nozomi



Інші виробники



Приклади впроваджень

Надання спеціальних рішень OT для безпечного виробництва

9

Рішень Fortinet мають рейтинг «Рекомендовано» від NSS Labs[1]

Найбільша екосистема партнерів із безпеки OT

Високопродуктивна перевірка нешифрованого та зашифрованого вмісту SSL/TLS

OT-специфічна база threat intelligence отримана завдяки **15+** років співпраці з виробниками

[1] “Independent Validation of Fortinet Solutions,” Fortinet, October 14, 2019.

Київенерго

Видимість і безпека в мережах IT і OT

ЗАГАЛЬНІ ВІДОМОСТІ

- Комплексне рішення для покращення безпеки та видимості мережі OT
- Вимога сегментувати свої IT- та OT-мережі одна від одної

ПОТРЕБИ ЗАМОВНИКА

- Сегментація з NGFW, включаючи можливості роботи в агресивних середовищах
- MFA аутентифікація користувачів
- Менеджмент і аналітика
- IPSEC VPN

РІШЕННЯ ВІД FORTINET

- Security Fabric – FG rugged, FMG, FAZ, FSW, FCT EMS
- MFA аутентифікація з FortiToken та FAC
- IPSec VPN ЦОД - підстанції.

OT замовники Fortinet

Основні переваги рішень Fortinet

Security Integration	Monitoring and Management	Ruggedized Appliances	Insider Threat Protection	OT-Specific Threat Intelligence
• Fabric-ready конектори забезпечують вбудовану інтеграцію зі сторонніми рішеннями • Екосистема API. • Наскрізна інтеграція з одним постачальником	• Централізована видимість • Централізоване керування	• Пристрої безпеки, розроблені для всіх середовищ розгортання	• Аналітика поведінки користувачів і суб’єктів (UEBA). • Сегментація на основі намірів на базі FortiGate NGFW • Технологія приманки FortiDeceptor	• 15+ років співпраці з виробниками • Експерти з 30+ роками досвіду роботи з безпекою OT • Найбільша партнерська екосистема OT


FORTINET