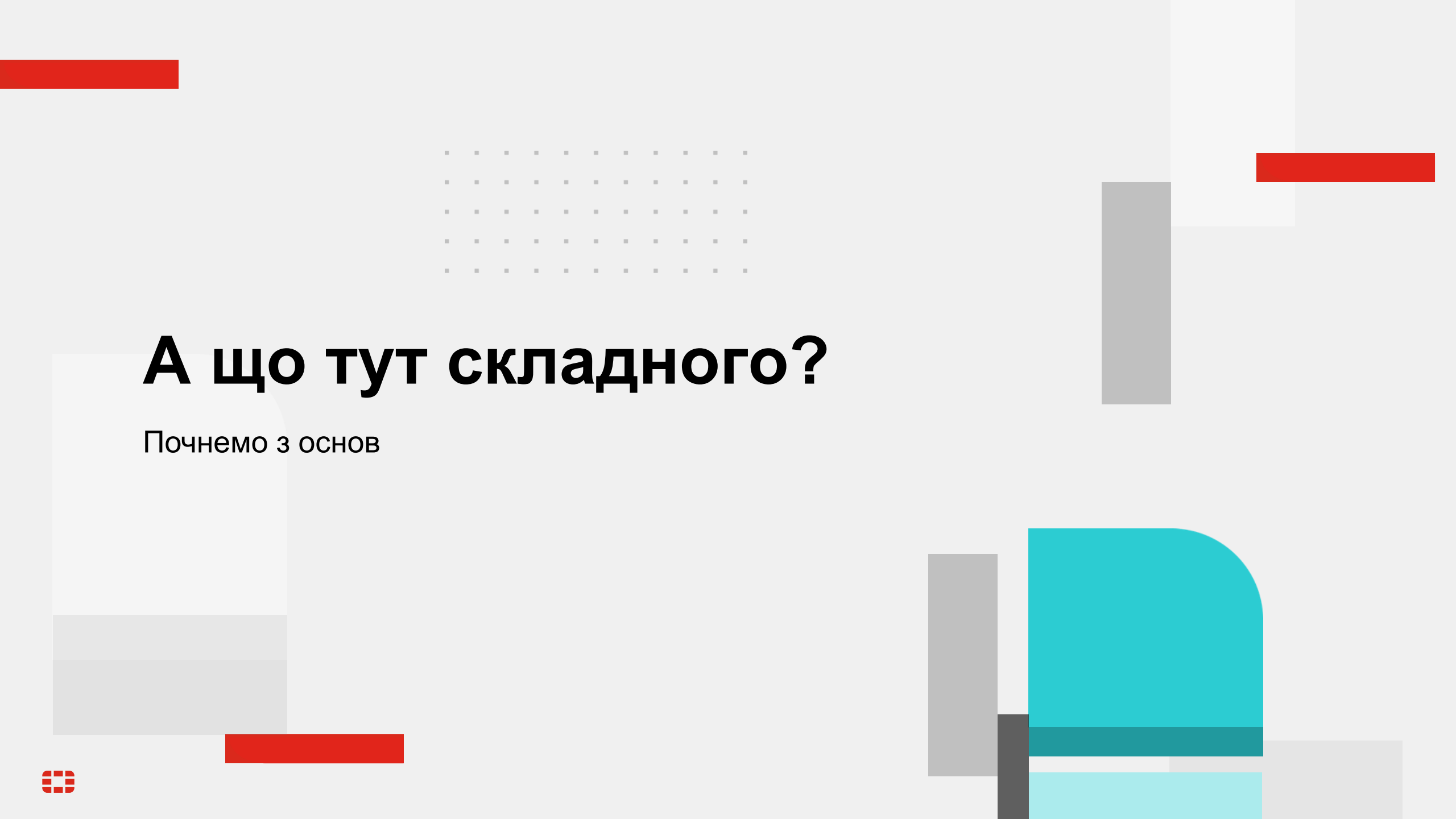




Гібридні мережі з Fortinet Fabric Management Center. Побудова, адміністрування та безпека.

Євгеній Таран, Systems Engineer



А що тут складного?

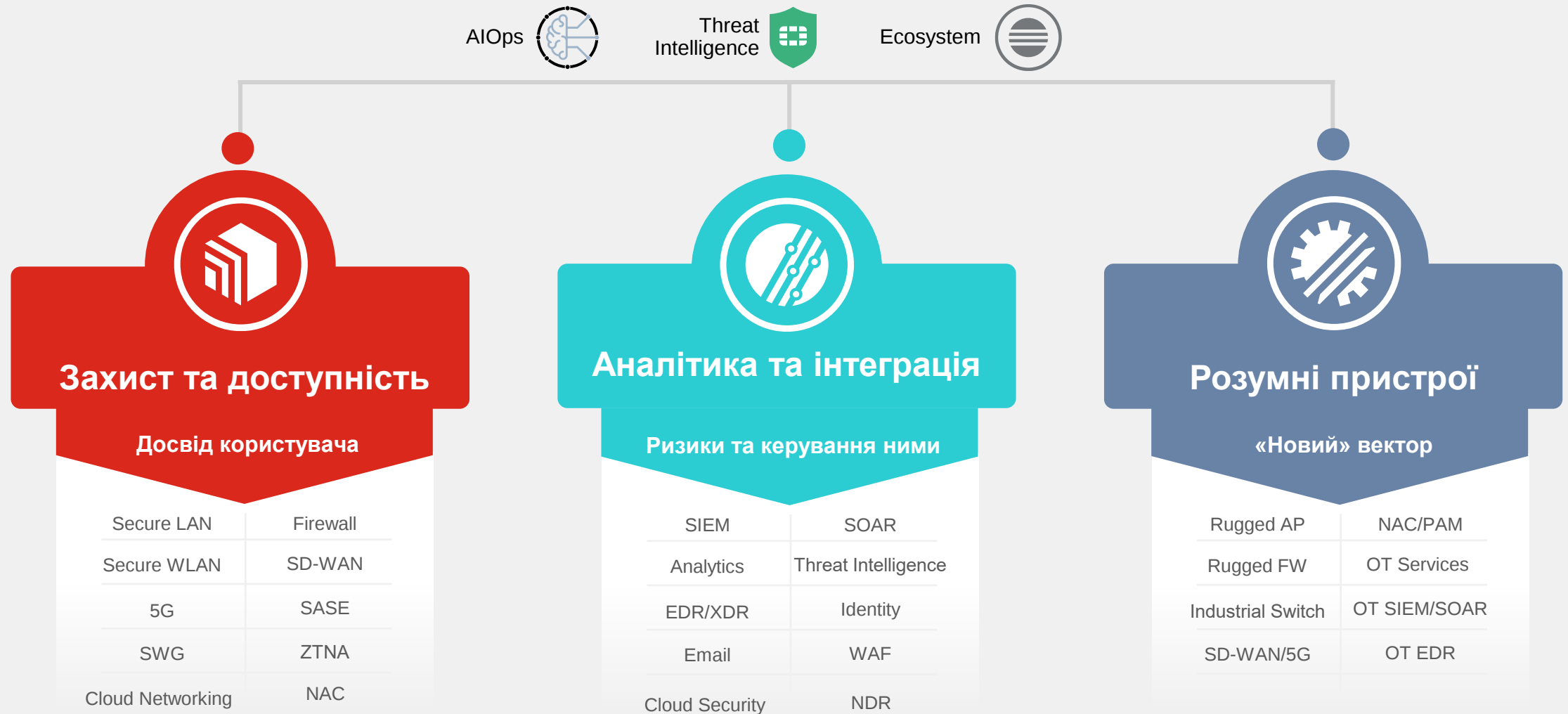
Почнемо з основ

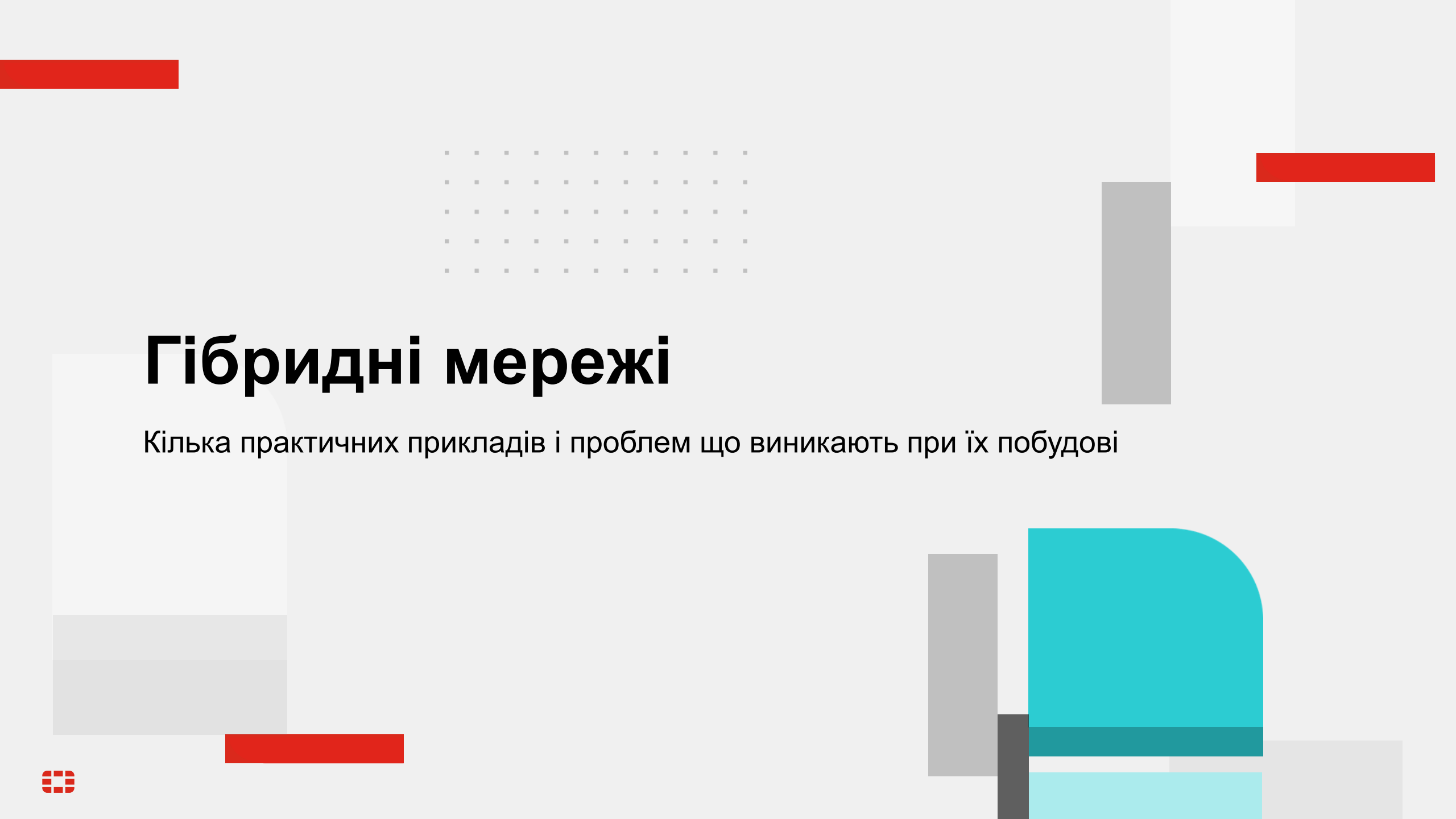


Безпека – це комплекс



Кожний напрям – свої рішення



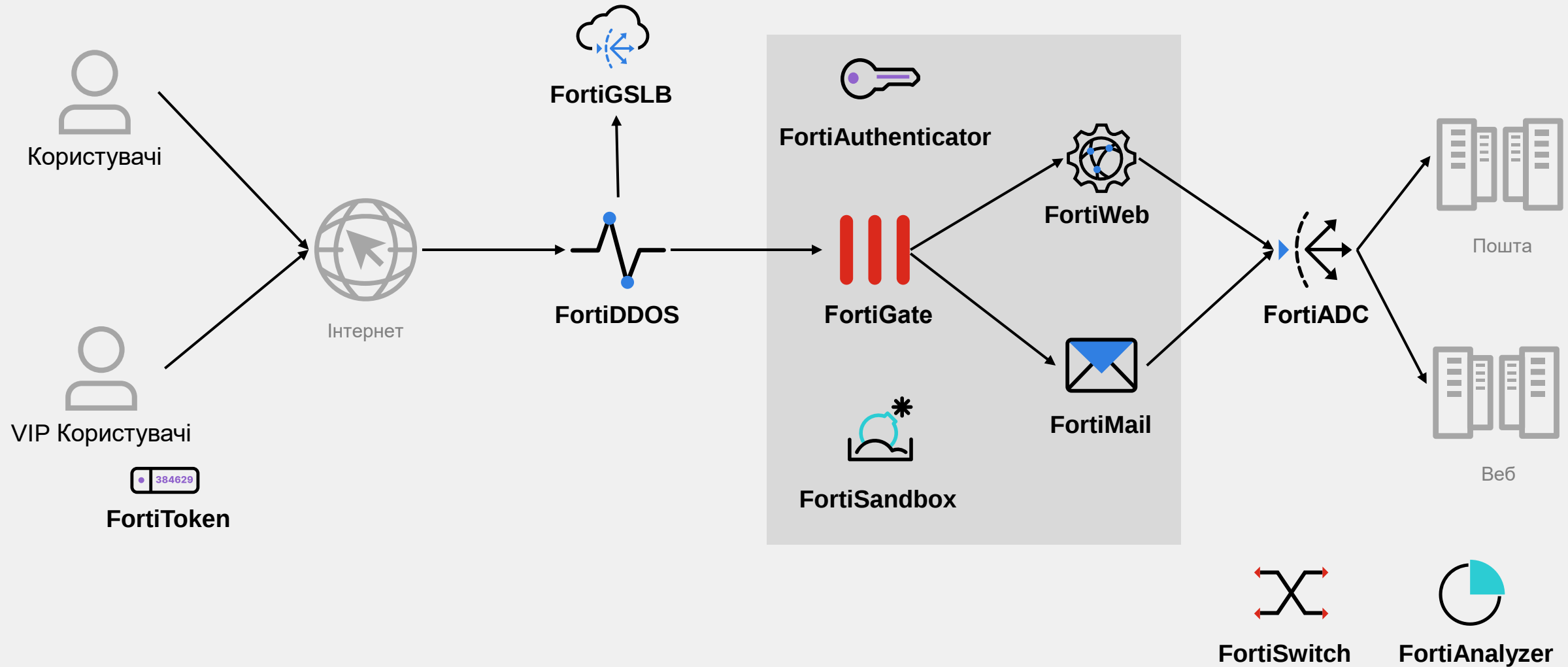


Гібридні мережі

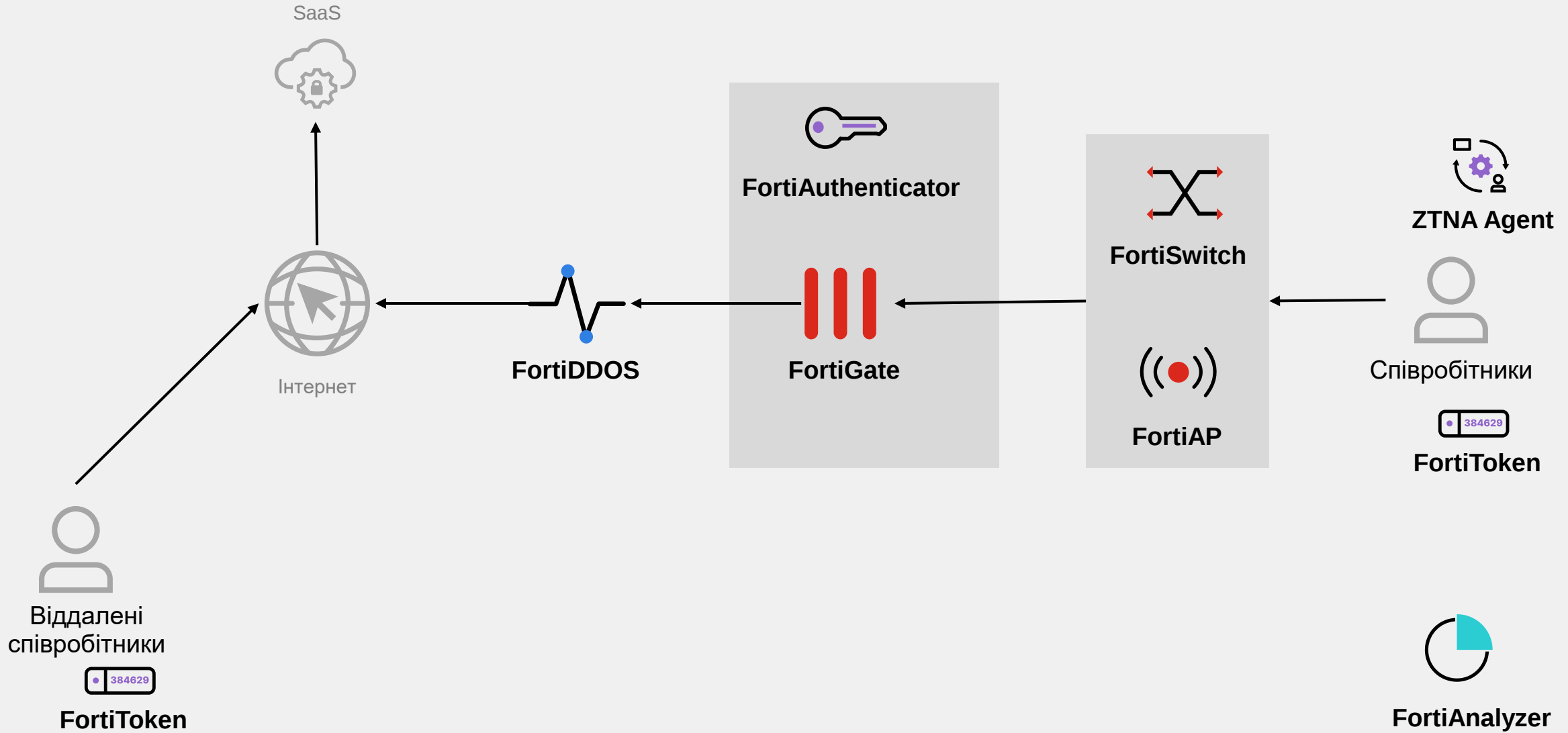
Кілька практичних прикладів і проблем що виникають при їх побудові



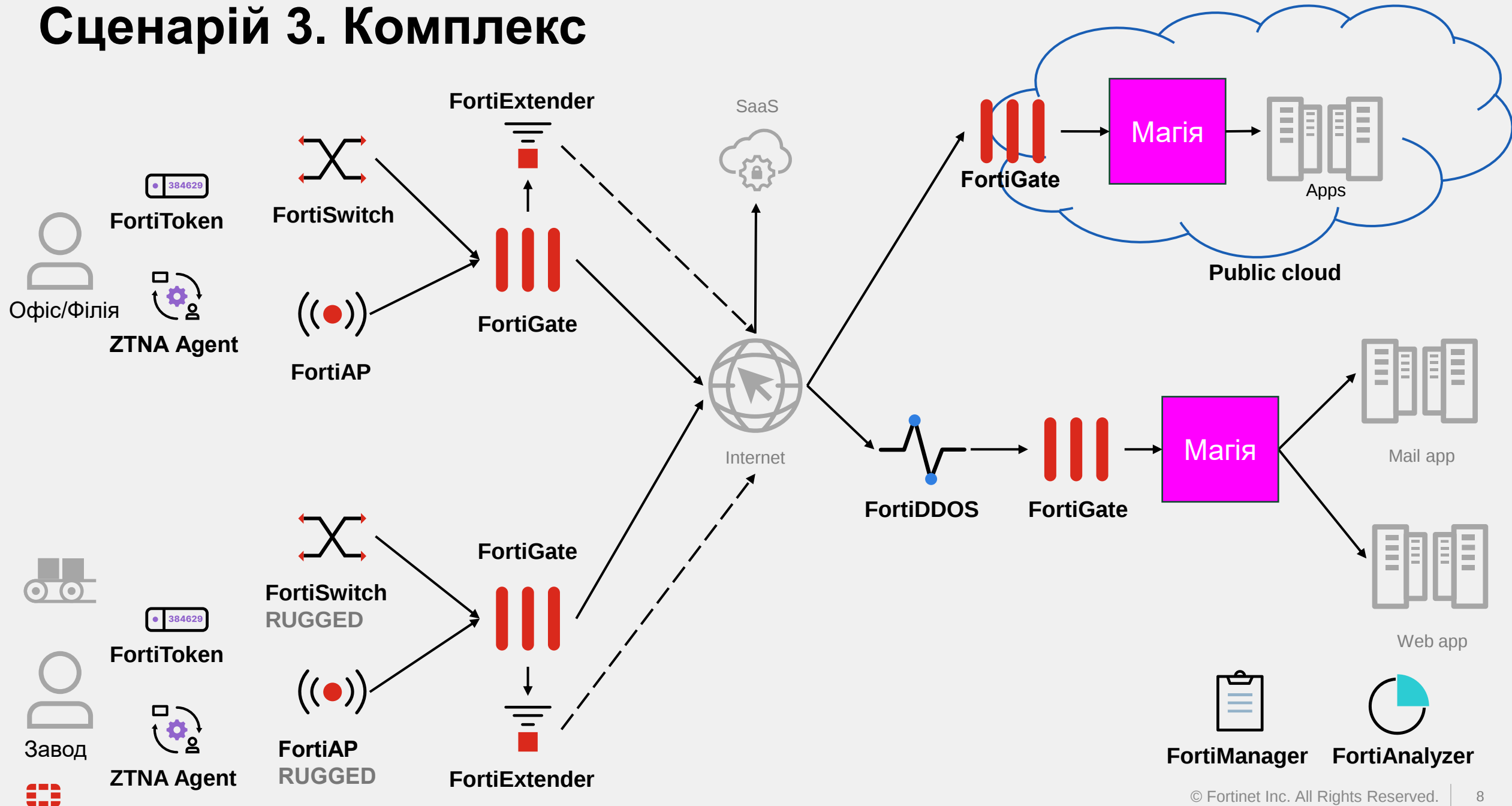
Сценарій 1. Публікація веб/поштового сервісу



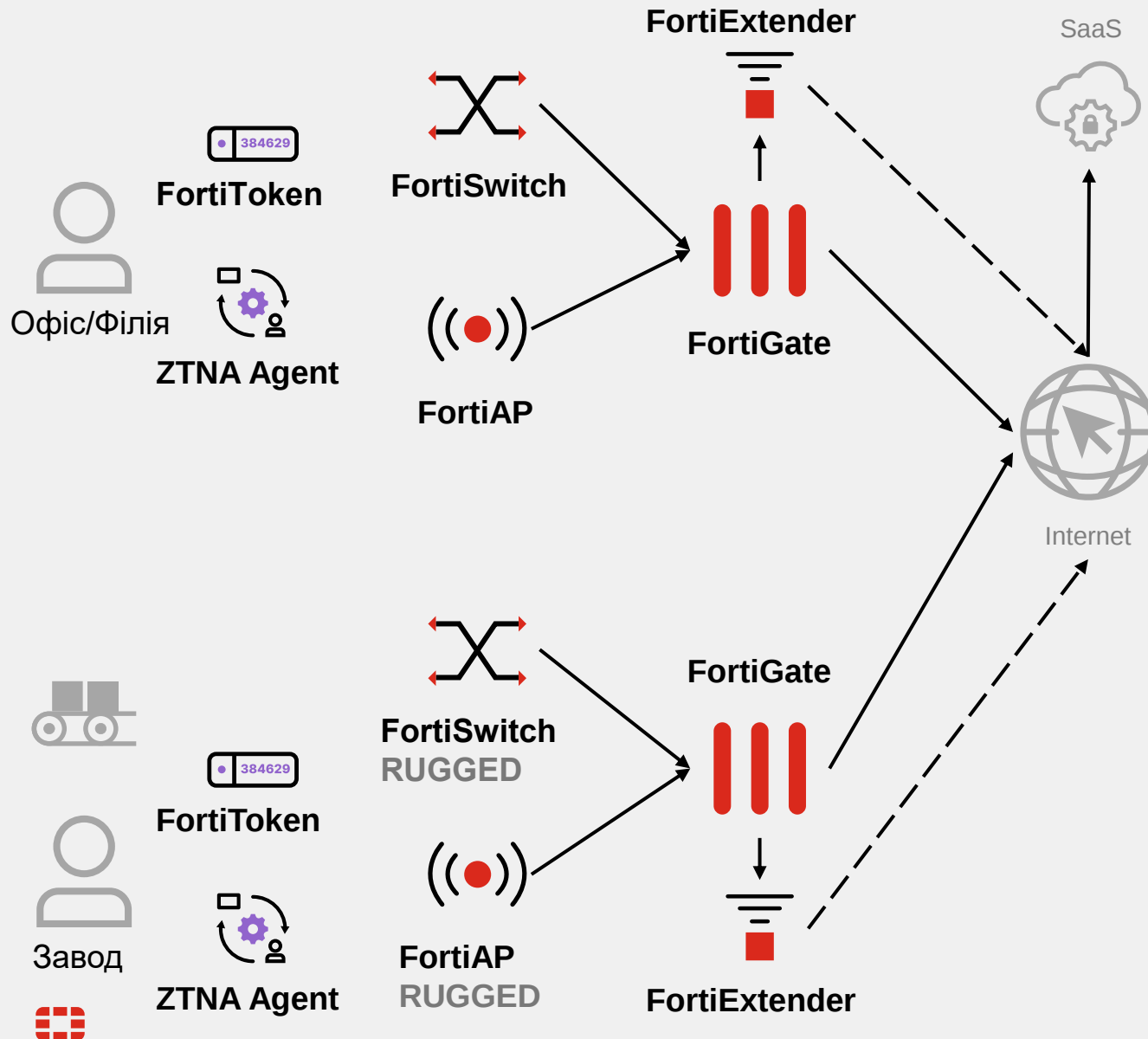
Сценарій 2. Безпека співробітників



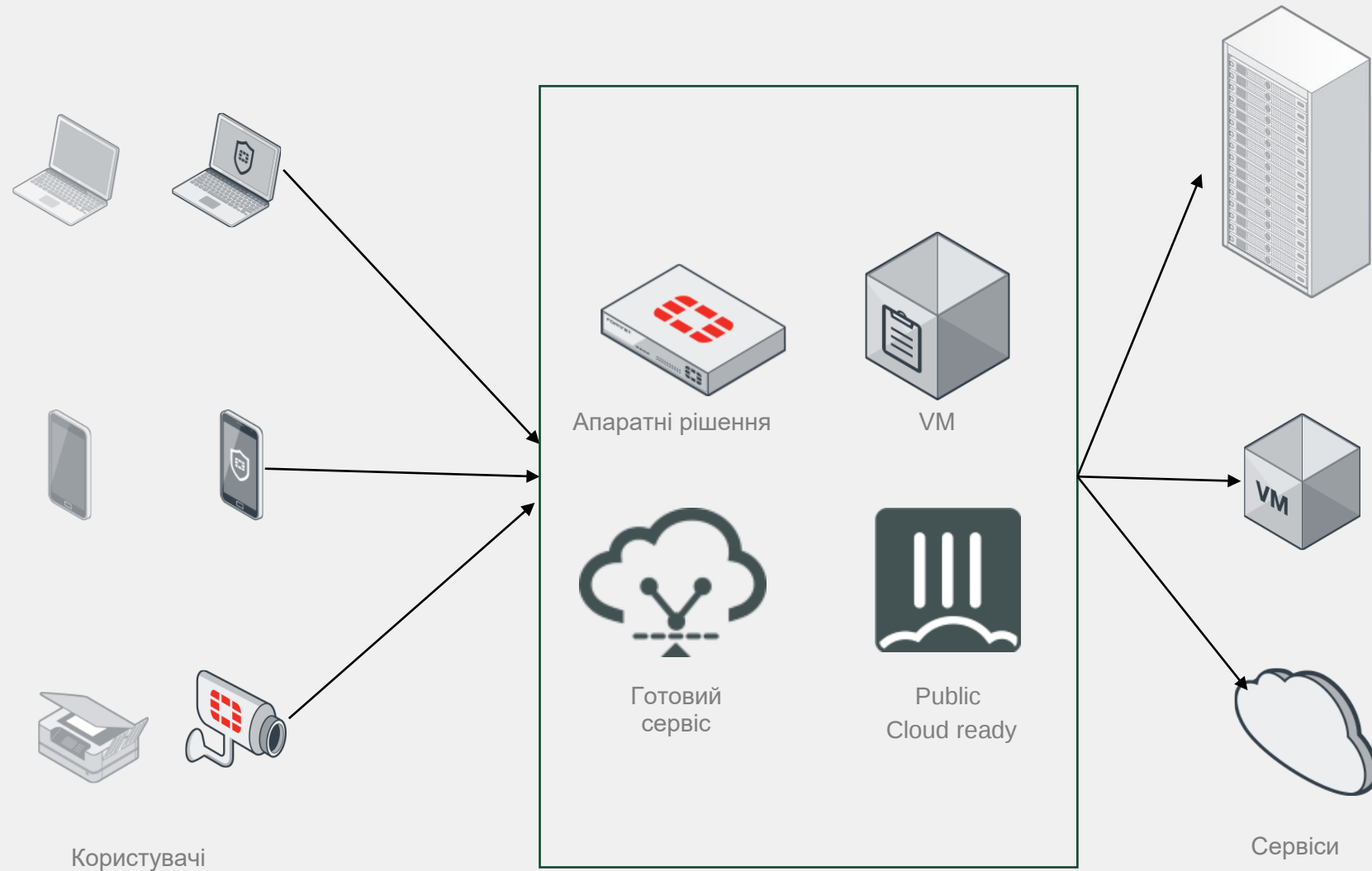
Сценарій 3. Комплекс



Сценарій 3. Комплекс



Гібридні мережі



Вимоги

- Уніфікований захист
- Уніфікована видимість
- ДЦ (хмари та класичні) та SaaS
- Відповідне ліцензування та формфактори рішень
 - Perpetual
 - BYOL
 - Subscription
 - PAYG

Гібридні мережі



Сучасні реалії

- Додатки різних типів
- Співробітники працюють звідусіль
- Непідконтрольні власні пристрої співробітників
- Все більше різних пристроїв
- Автоматизовані атаки
- Багато виробників
- Брак спеціалістів



Security Fabric

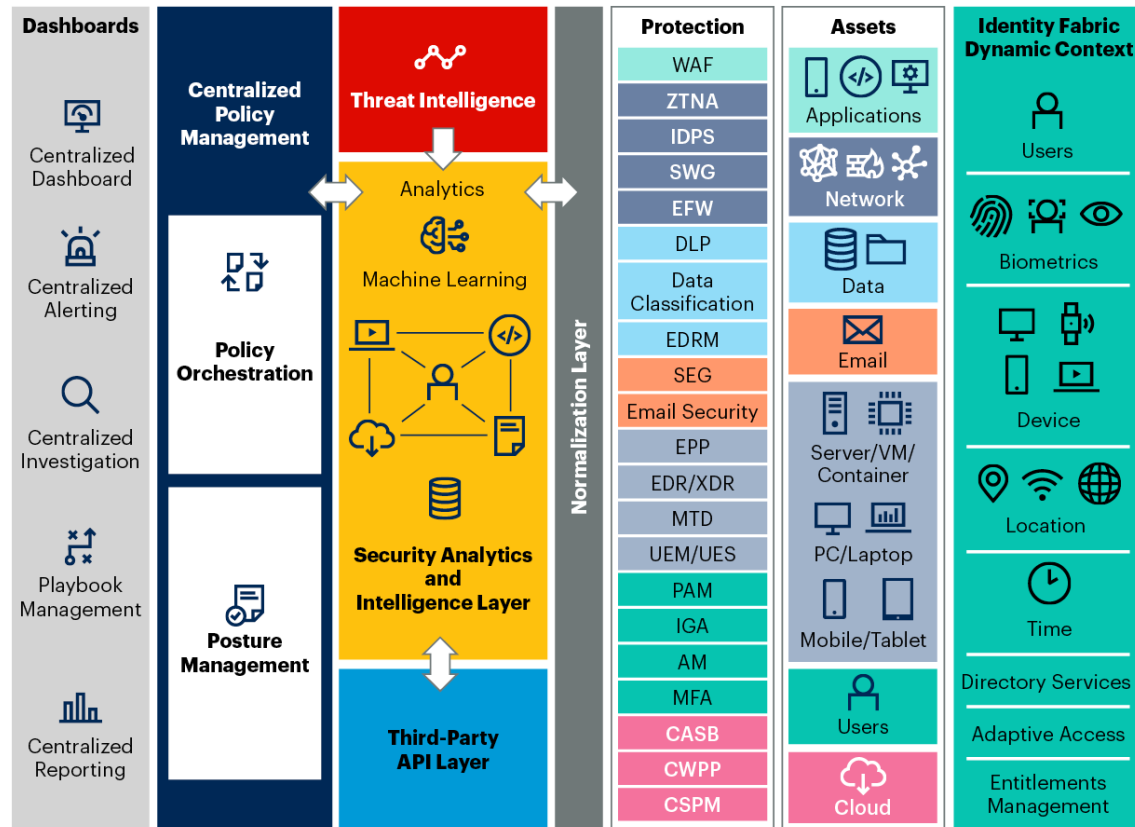
В чому складність керування?



Що з цього приводу каже Gartner?

Gartner

Cybersecurity Mesh Architecture



Source: Gartner
756156_C

Source: Gartner "Guide to Cloud Security Concepts", Patrick Hevesi, Richard Bartley, Dennis Xu. 21 September, 2021

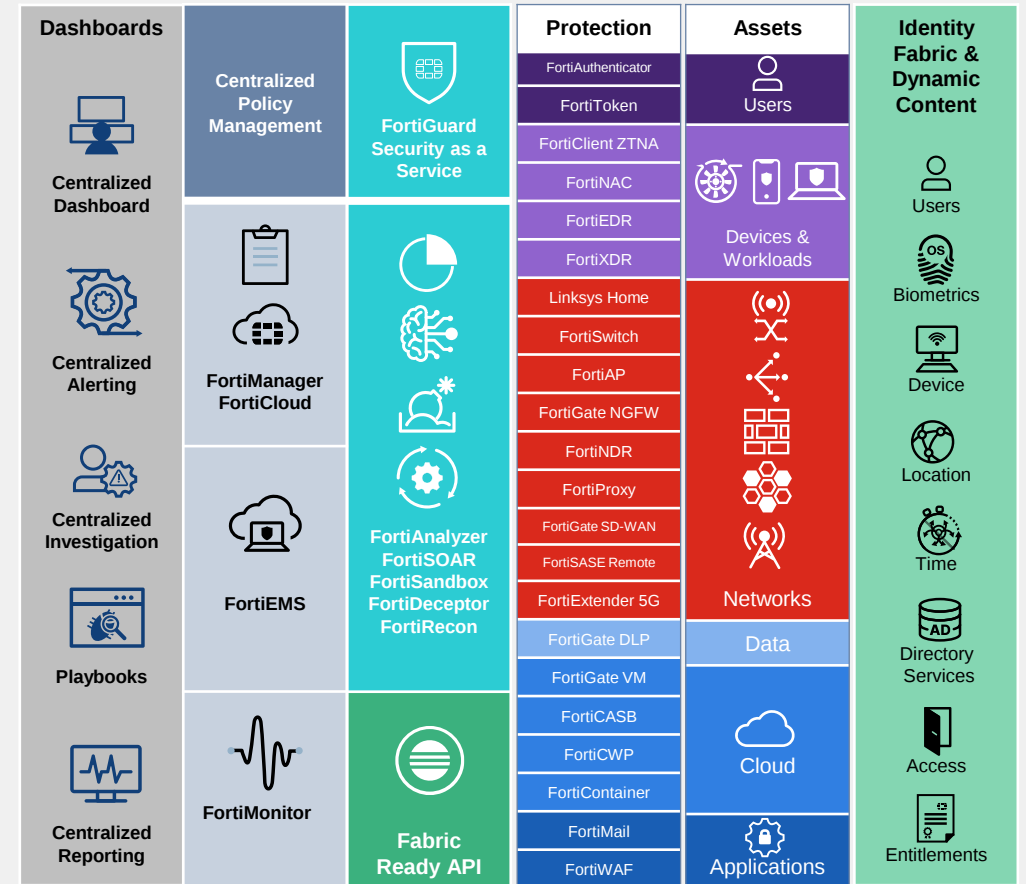
Gartner

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



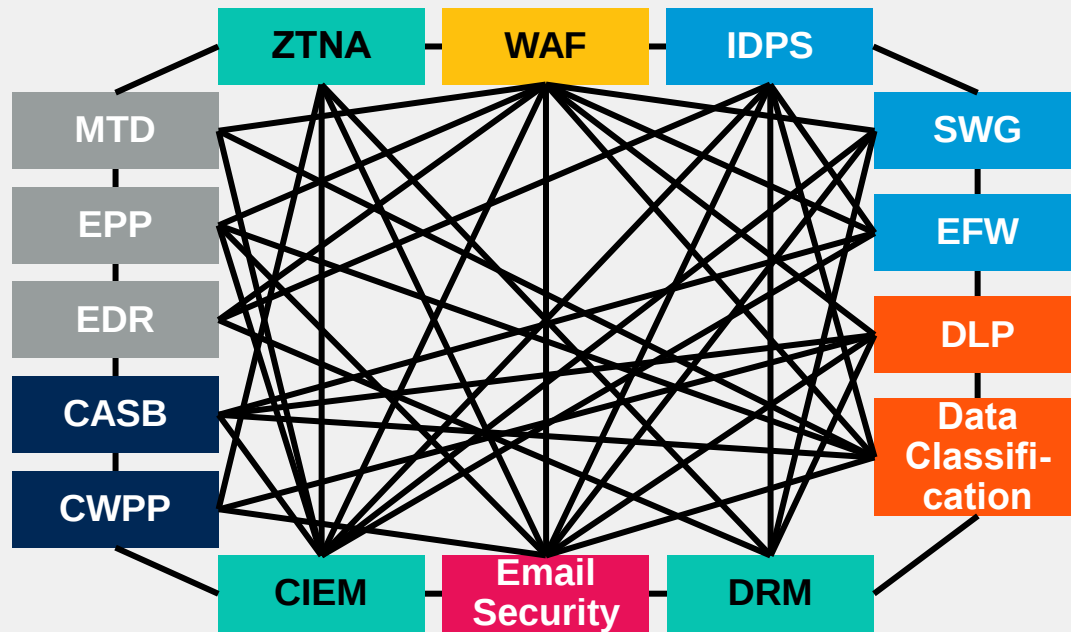
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET



Архитектура Gartner Cybersecurity Mesh

Gartner®



Executive Guide to Cybersecurity Mesh, 2022

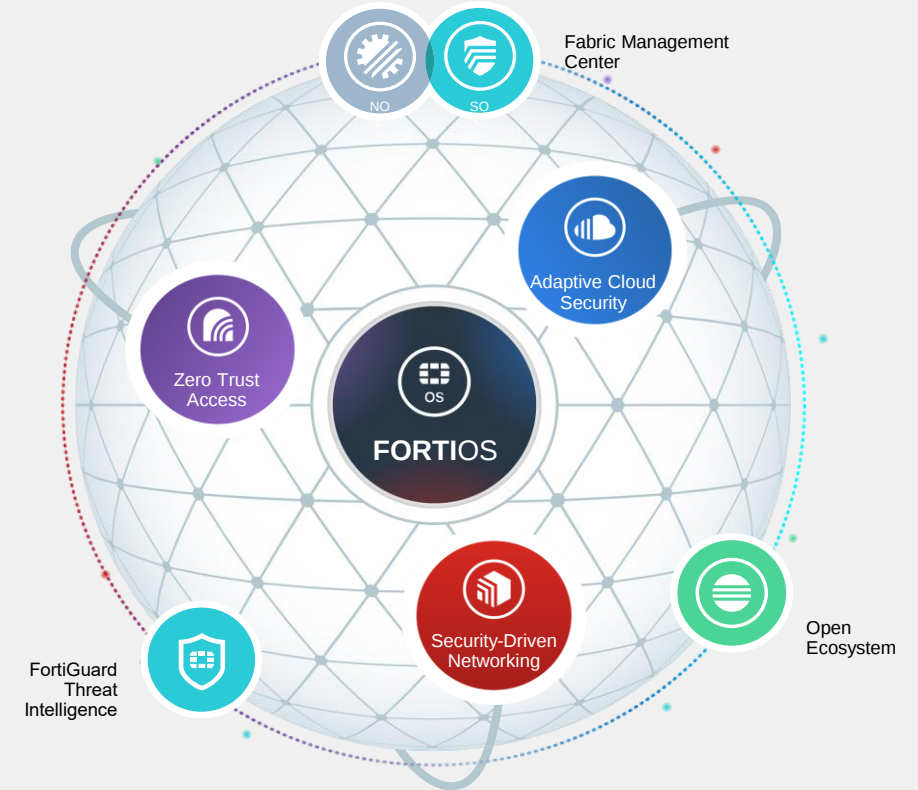
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET®



Fortinet Security Fabric

Всебічне охоплення

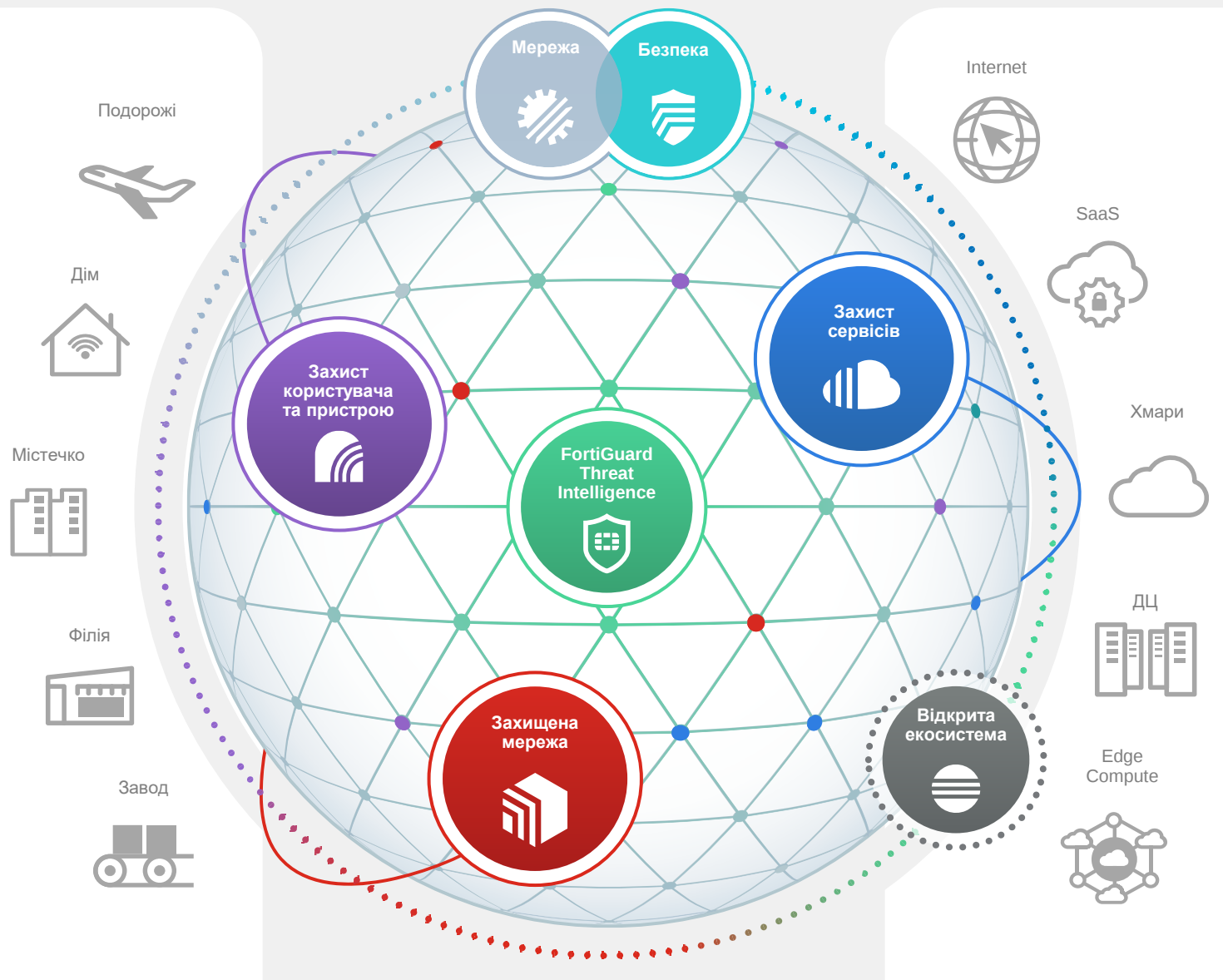
Багатовекторна видимість і захист для повного охоплення кібербезпеки

Інтеграція

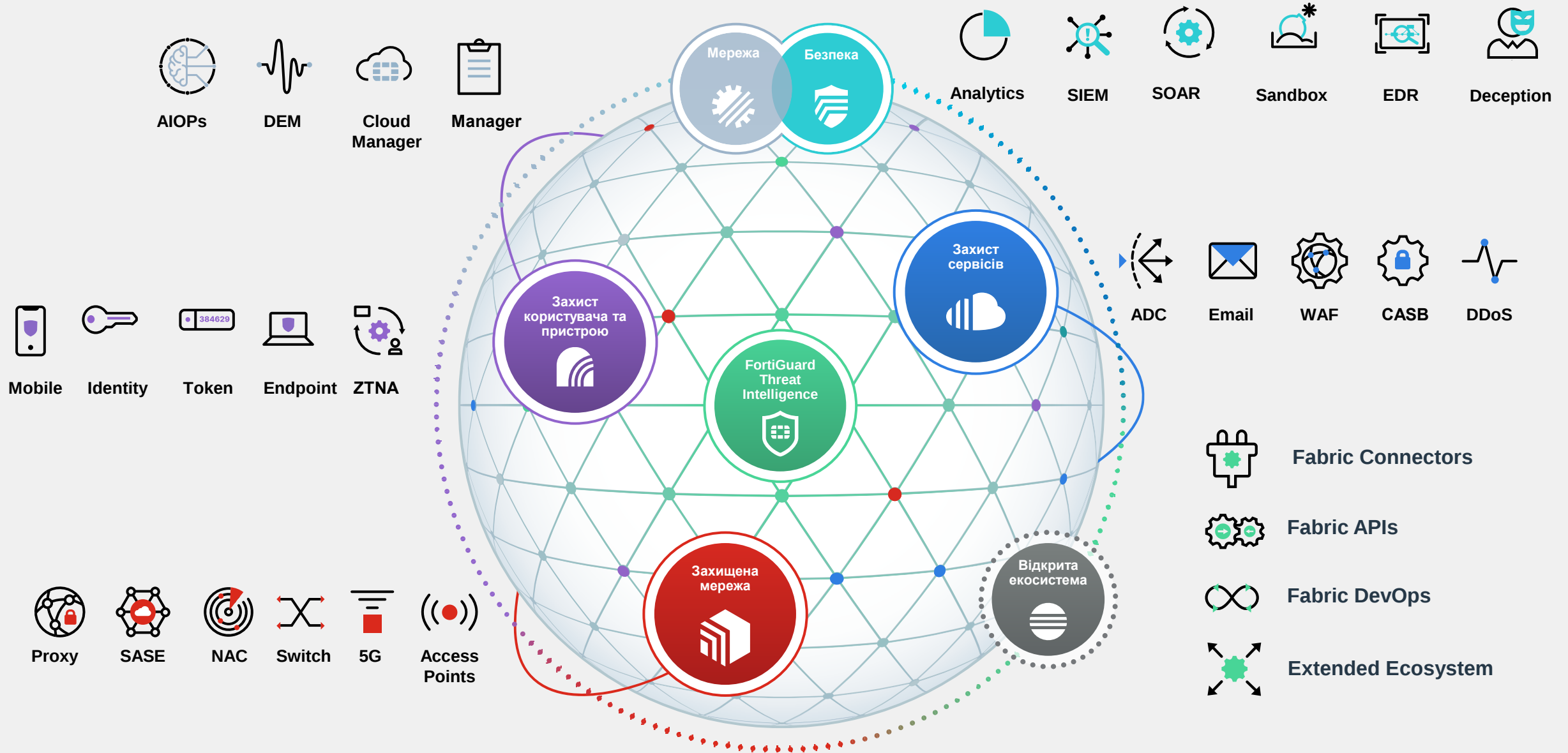
зменшує складність управління та обмін інформацією щодо загроз

Автоматизація

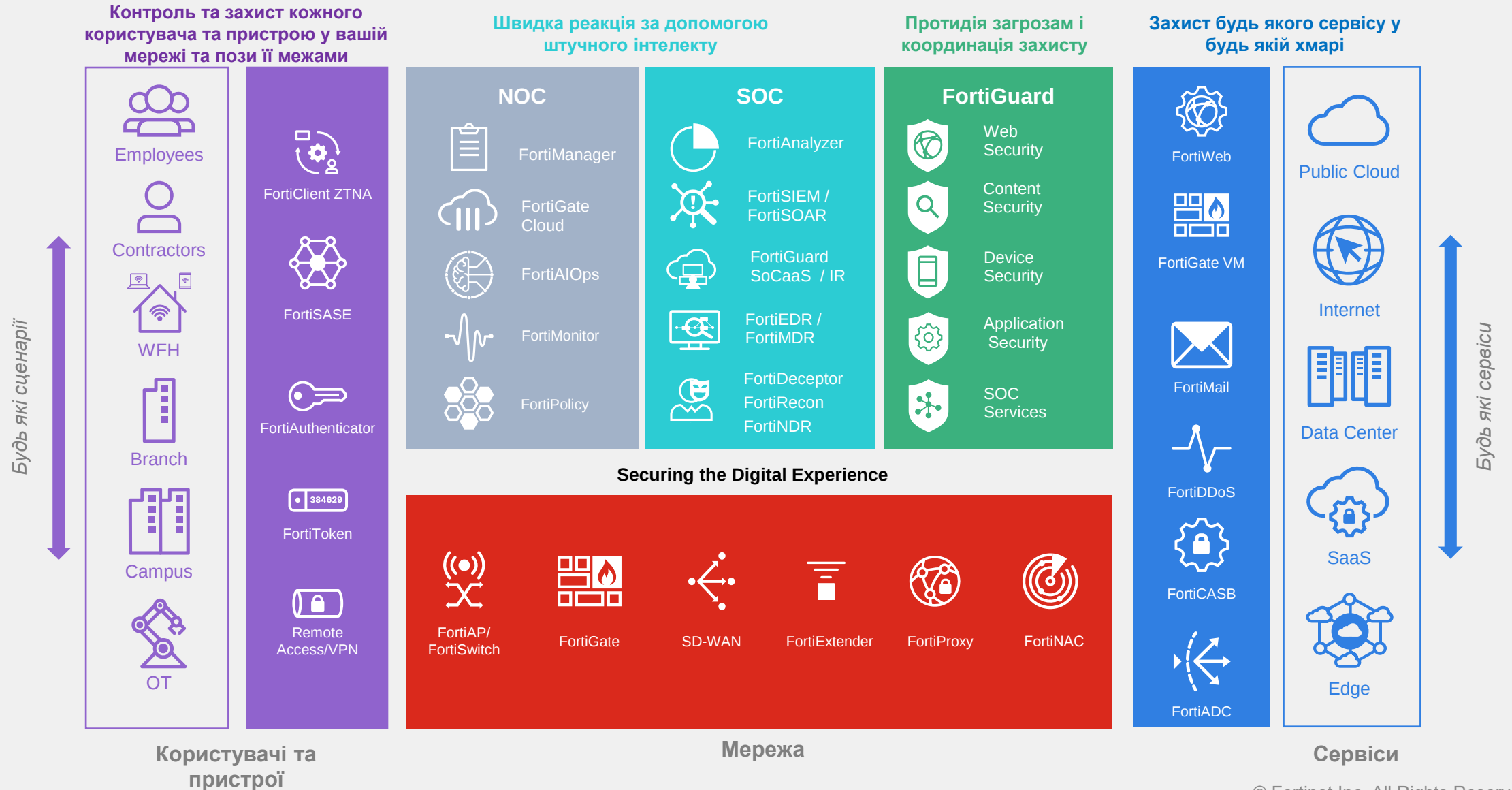
Автоматизація дій безпеки з використанням штучного інтелекту для підвищення швидкості та ефективності



Fortinet Security Fabric



Коротко про портфоліо Fortinet



Кращі в класі рішення вже інтегровані між собою

Network Firewall

Dec. 2022 Magic Quadrant for Network Firewalls

Fortinet Recognized as a Leader



SD-WAN

Sept. 2022 Magic Quadrant for SD-WAN

Fortinet Recognized as a Leader



Wired and Wireless LAN

Nov. 2022 Magic Quadrant for Wired and Wireless LAN

Fortinet Recognized as a Visionary



FortiOS Operating System



Одна платформа

Кращі в класі рішення вже інтегровані між собою

Endpoint Protection

Gartner Magic Quadrant for Endpoint Protection Platforms, 2023

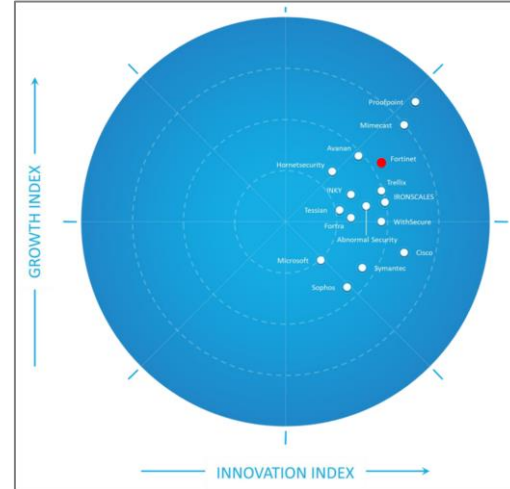
Fortinet Recognized as a Visionary Vendor



Email Security

Frost & Sullivan...Frost Radar™: Email Security, 2022

Fortinet Recognized as a Top Vendor



SIEM

Gartner Magic Quadrant for SIEM 2023

Fortinet Recognized as a Challenger



SOAR

KuppingerCole Leadership Compass for SOAR, 2023

Fortinet Recognized as a Leader



The Fortinet Security Fabric

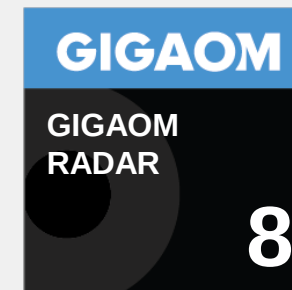
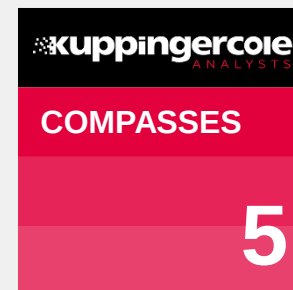
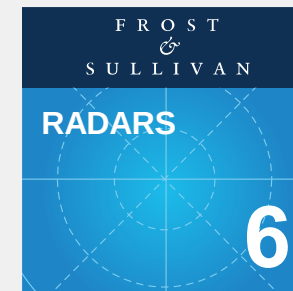


37

Звітів щодо Fortinet в корпоративному світі

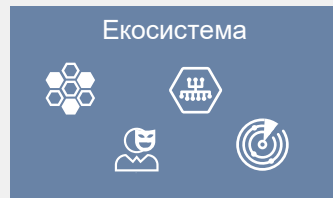
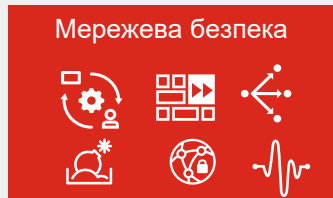
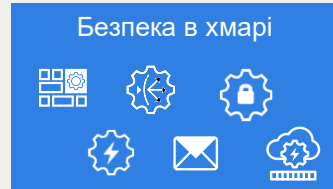
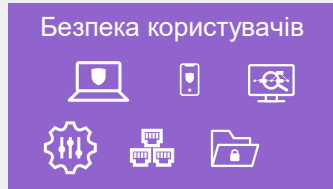
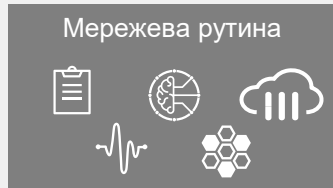
Fortinet є однією з найбільш перевірених корпоративних компаній з кібербезпеки в світі, що займає лідерські позиції в десятках аналітичних звітів, що підкреслюють широке застосування Fortinet Security Fabric.

*Analyst validation includes reports where expert and independent 3rd party analysts rank and evaluate vendors: Gartner Magic Quadrants, IDC Marketscapes, Frost & Sullivan Radars, Forrester Waves, Westlands Advisory Platform Navigator, Kuppingercole Compasses, Gigaom Radar.

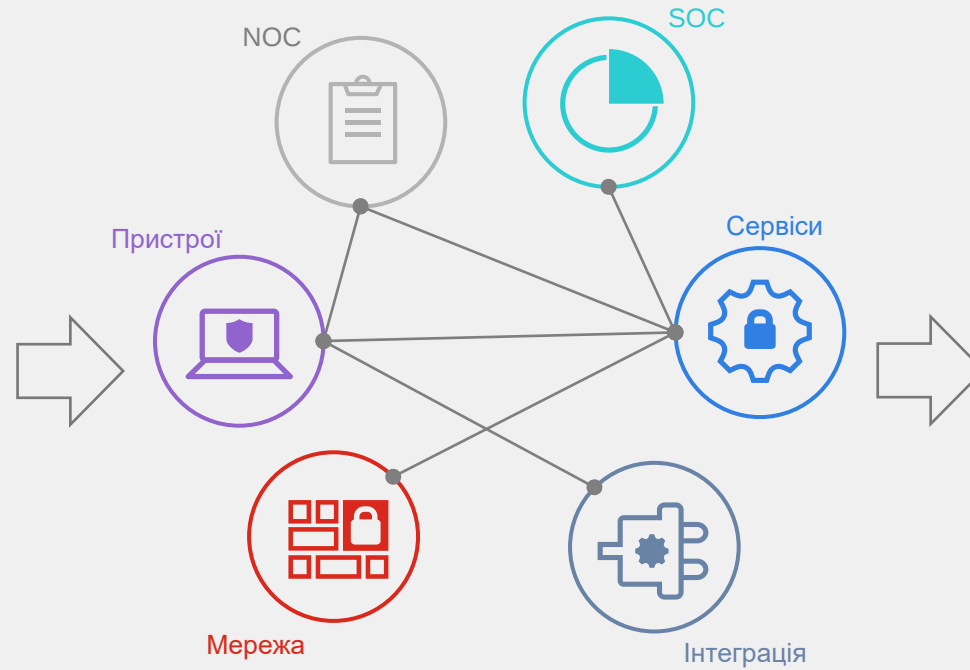


Основна складність

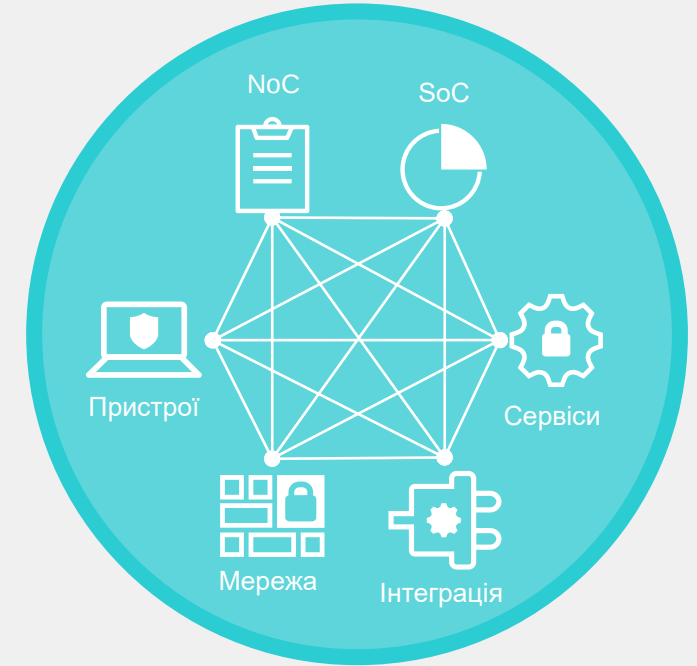
30+ виробників



10 виробників



2-3 платформи



Еволюція





Fortinet Fabric Management Center

Командна робота FortiManager та FortiAnalyzer та їх задачі



1. Просте налаштування

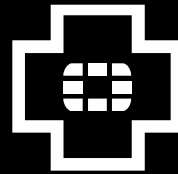
Економить час та запобігає помилкам

Ключове

- Швидкий запуск in <6 хв (перевірено NSS labs)
- SD-WAN & NGFW шаблони
- Консоль централізованого керування
- DevOps Playbooks & Scripts
- Резервне копіювання з історією

1

Реєстрація
пристрою



2

Налаштування
централізованого
керування



3

Конфігурація
100К+ пристроїв

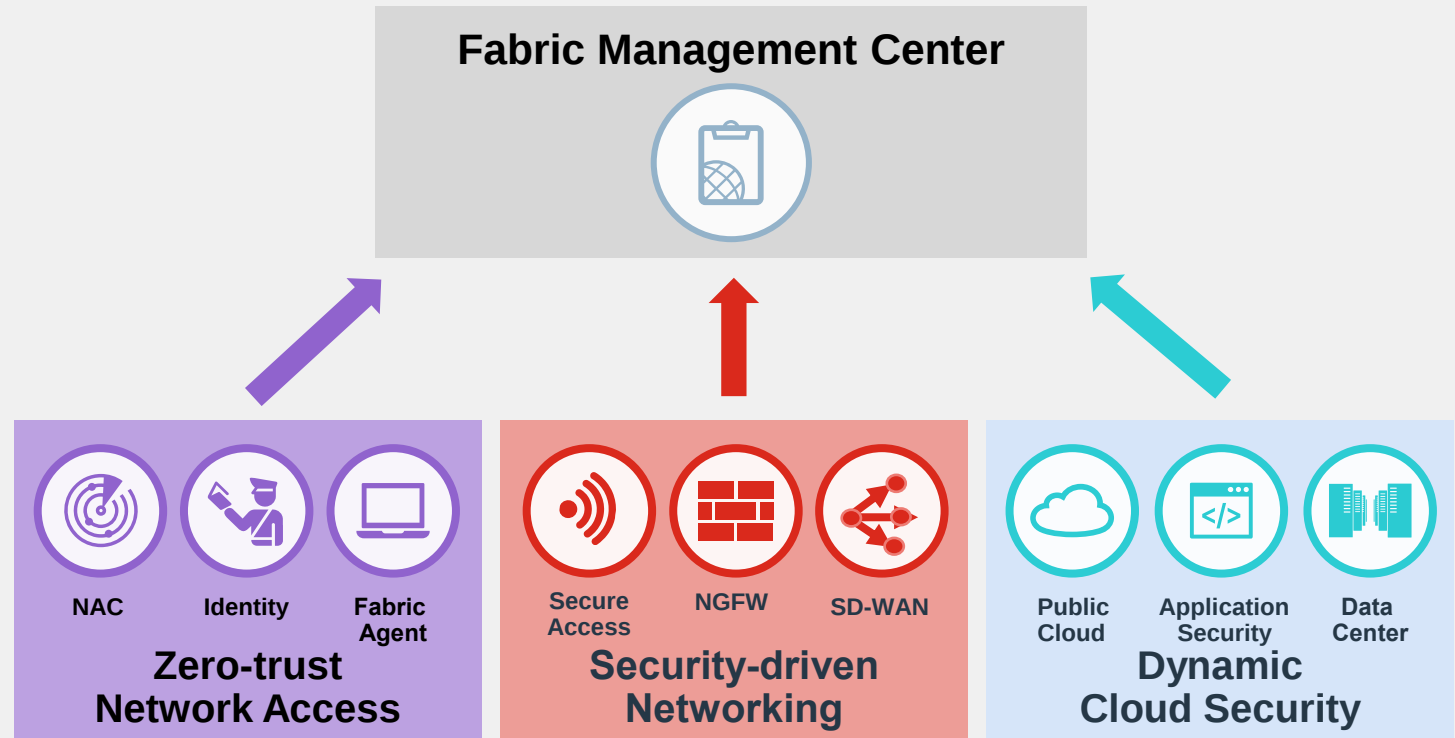


2. Централізоване керування

Спрощуємо складне та велике

Ключове

- Масштабування до **100k+** FortiGate(s)
- Fabric Management інтеграція
- SD-WAN, NGFW шаблони
- Централізовані журнали
- Role-based Access Control

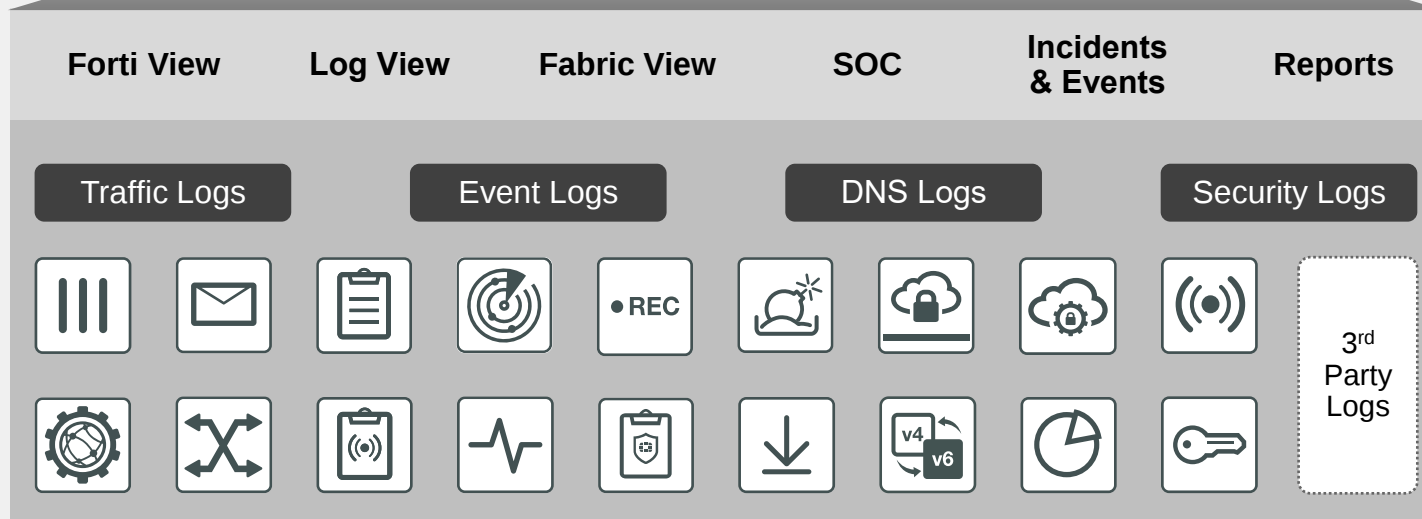
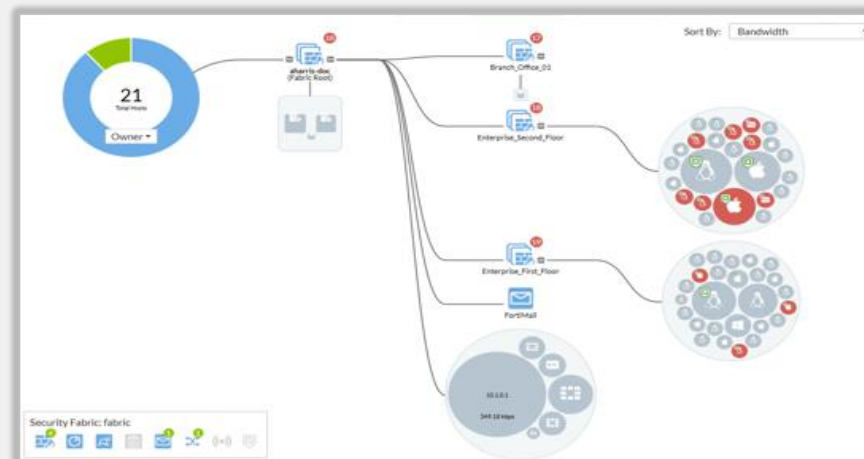


3. Аналітика

Мережа в реальному часі

Ключове

- Огляд стану мережі
- Звіт SLA в реальному часу
- Історичний SLA звіт
- Звіт використання сервісів
- Адаптивне реагування

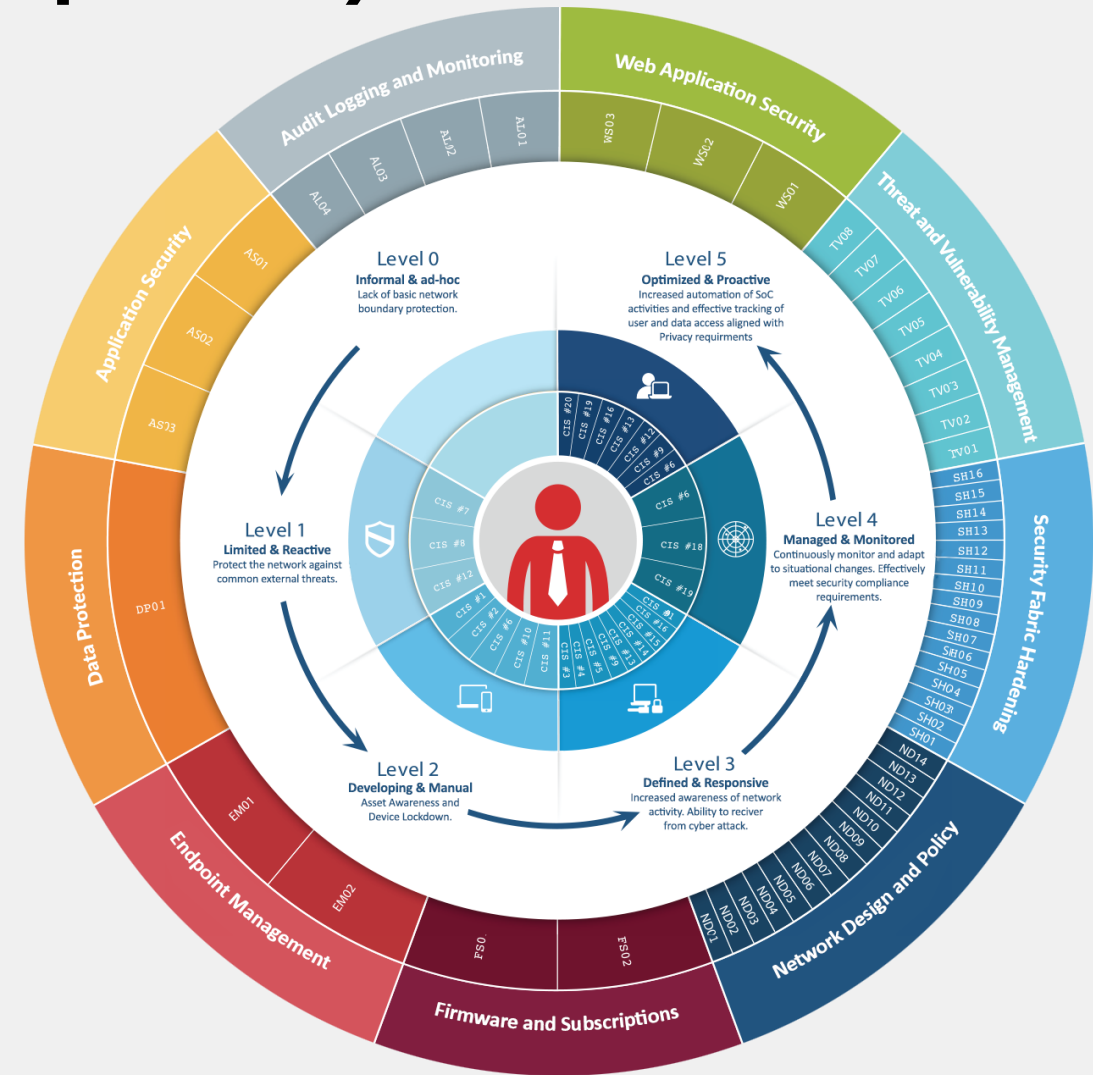


4. Звіти відповідності (Compliance)

Світові вимоги та best practice

Ключове

- PCI
- FSBP
- Звіти регуляторів можна змінювати
- Багатофакторна аутентифікація
- Інтеграція з SIEM / аналітикою / Compliance Tools

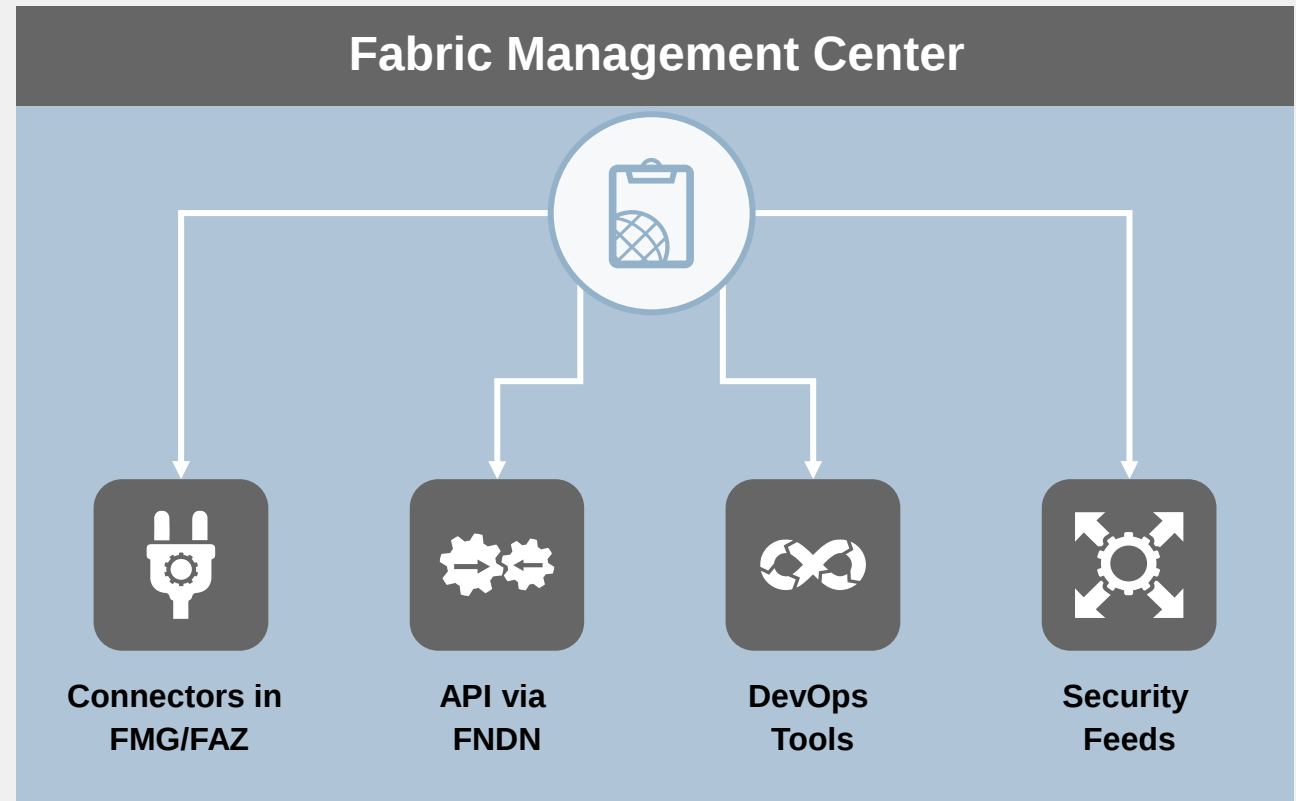


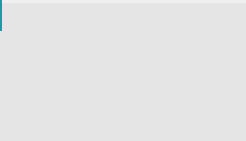
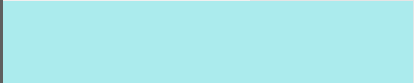
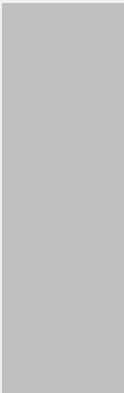
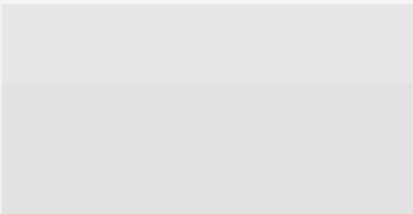
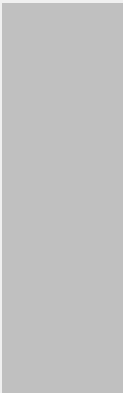
5. Автоматизація

Вбудовані механізми реагування

Ключове

- Вбудована інтеграція з SDN та Public Cloud
- ITSM інтеграція з ServiceNow
- REST API за допомогою fndn.fortinet.com
- DevOps Tools нахталт Ansible, Terraform тощо.





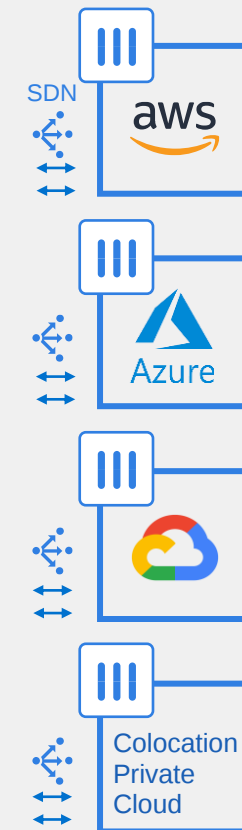
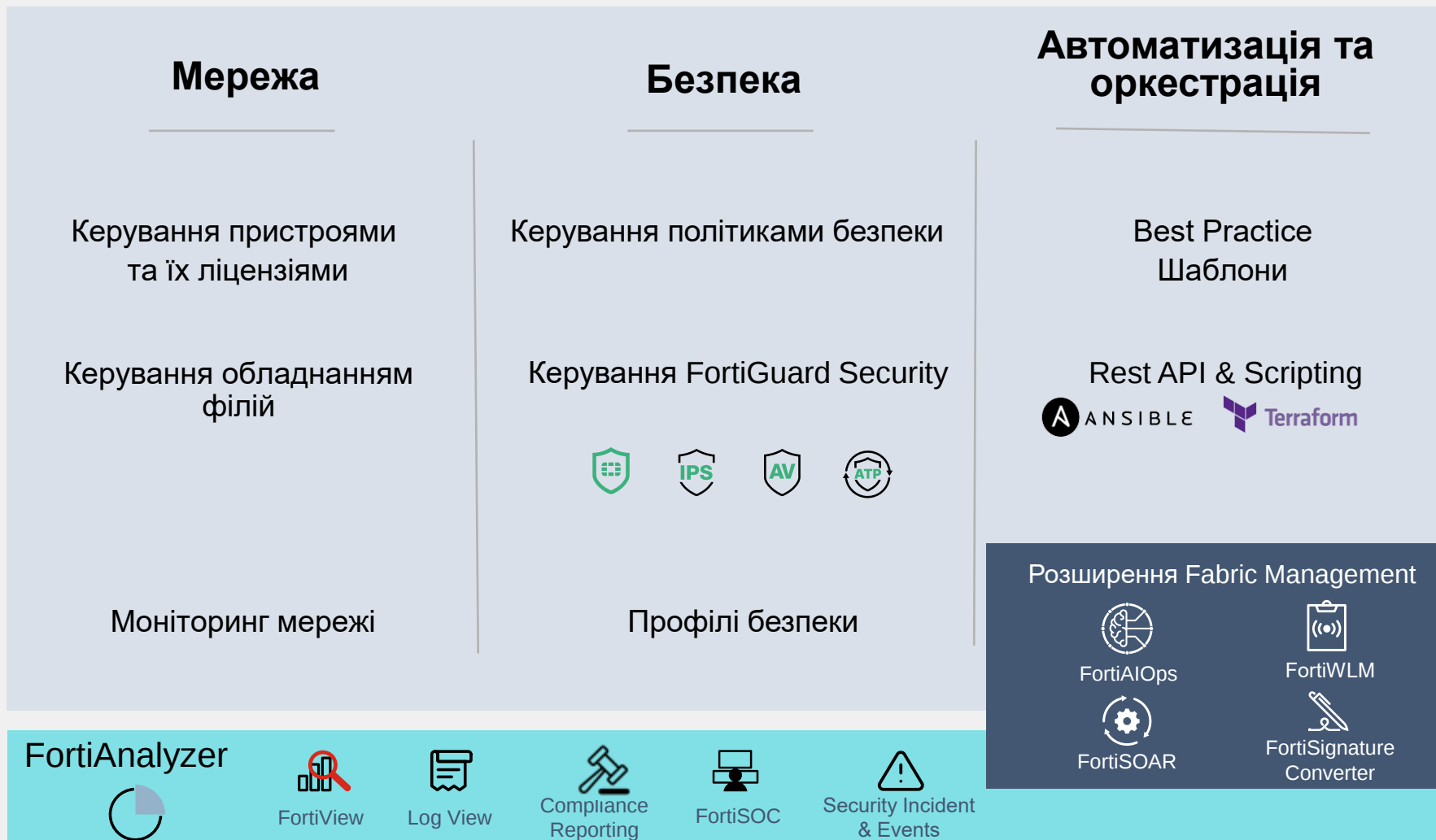
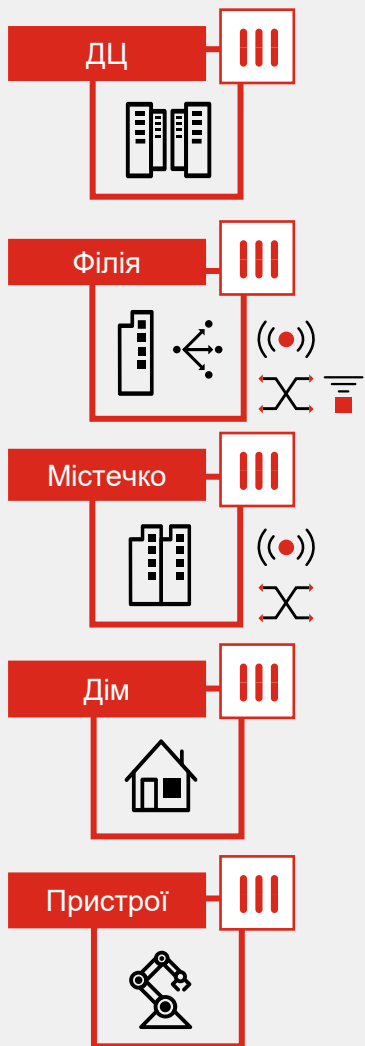
FortiManager

Детальніше



FortiManager

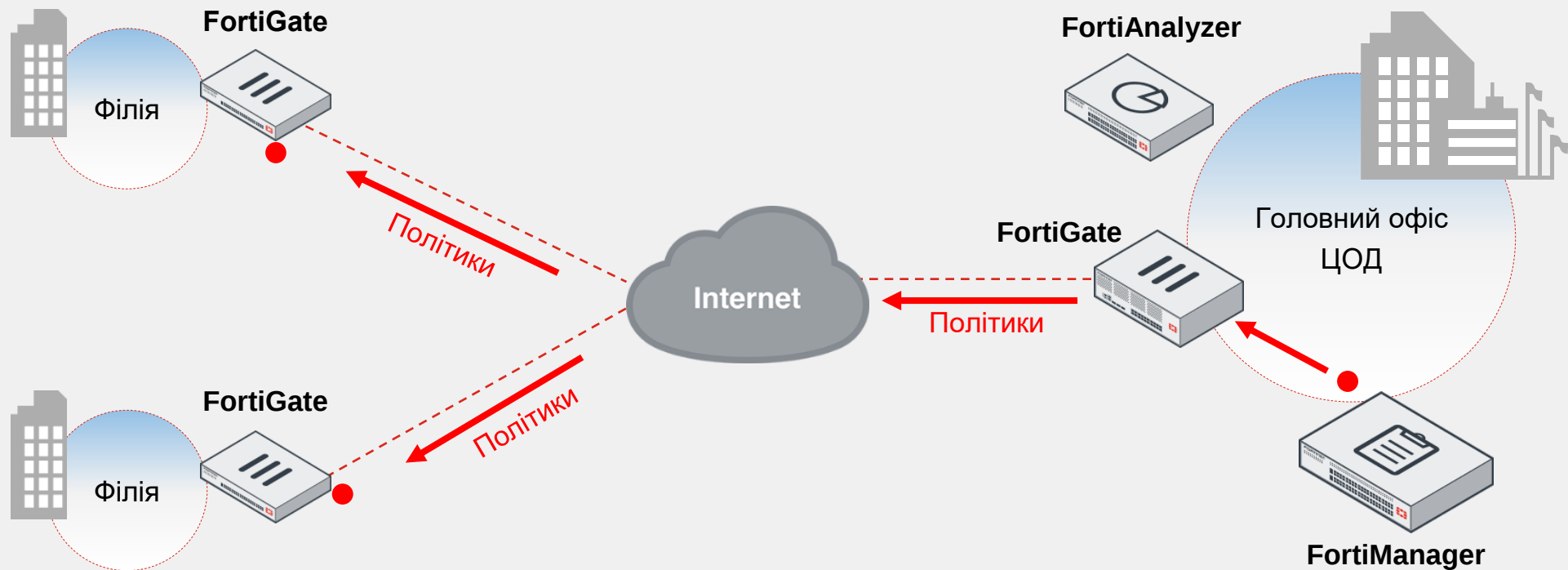
Єдина консоль керування



Ключове в Centralized Management

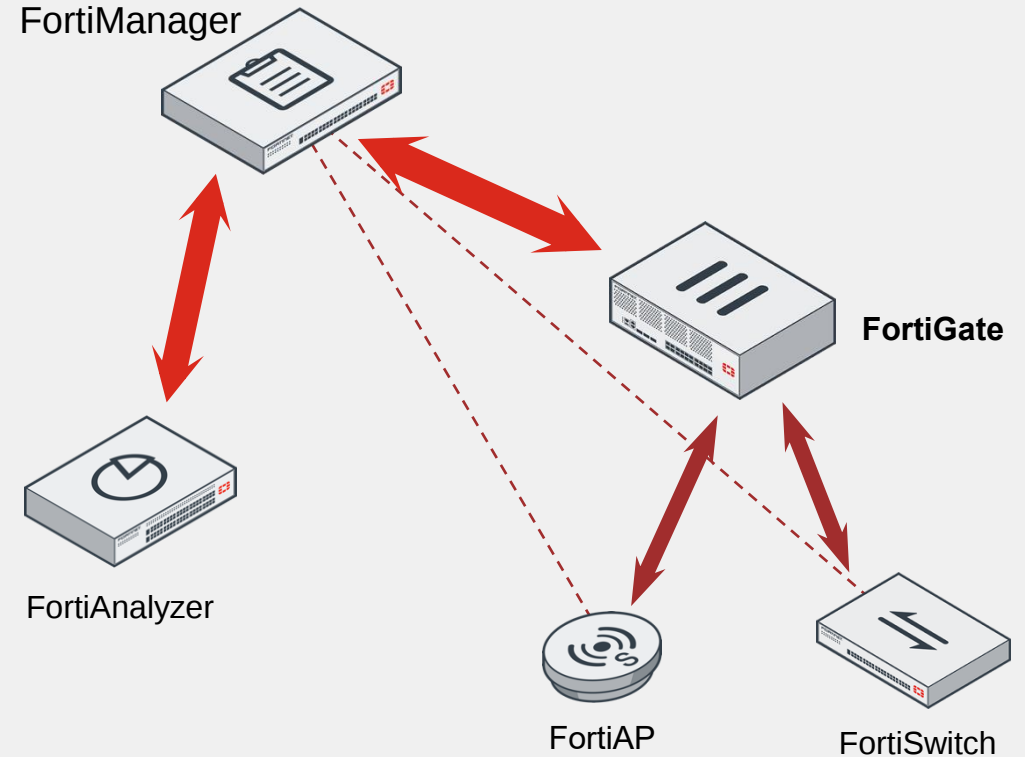
Централізоване керування:

- Налаштування та історія налаштувань
- Керування ПЗ
- Скрипти
- Журнали та звітність
- Ліцензії
- SD-WAN



Security Fabric Management. Роль FortiManager

- Спрощення керування економить час та зменшує помилки
- FortiGate
 - Налаштування за допомогою шаблонів FortiManager
 - Керування VPN
 - Моніторинг здоров'я
- FortiAnalyzer
 - FortiAnalyzer взаємно інтегровані між собою. FortiManager може керувати FortiAnalyzer а FortiAnalyzer надавати дані для FortiManager
- FortiSwitch, FortiAP
 - FortiManager налаштовує обладнання через FortiGate
 - Налаштування за допомогою шаблонів FortiManager



Централізоване керування





Fabric View



Management Extensions

Device Manager ▾

Device & Groups ▾

Provisioning Templates

Scripts

SD-WAN

ADOM: FortiGate-Cluster

S

satisfy ▾

Add Device ▾

Device Group ▾

Install Wizard

Tools ▾

Managed FortiGate 16

Managed FortiAnalyzer 1

16 Devices
Total

0 Devices
Connection Down

0 Devices
Device Config Modified

1 Devices
Policy Package Modified

Edit

Delete

Import Policy

Install ▾

More ▾

Column Settings ▾

Device Name

Config Status

Policy Package Status

Host Name

IP Address

Platform

Description

FGT-BR-Atlanta

Synchronized

FGT-BR-Atlanta

FGT-BR-Atlanta

10.88.210.162

FortiGate-VM64

FGT-BR-Cairo

Synchronized

FGT-BR-Cairo

FGT-BR-Cairo

10.88.210.168

FortiGate-VM64

FGT-BR-Dublin

Synchronized

FGT-BR-Dublin

FGT-BR-Dublin

10.88.210.172

FortiGate-VM64

FGT-BR-Honolulu

Synchronized

FGT-BR-Honolulu

FGT-BR-Honolulu

10.88.210.169

FortiGate-VM64

FGT-BR-Kuala-Lumpur

Synchronized

FGT-BR-Kuala-Lumpur

FGT-BR-Kuala-Lumpur

10.88.210.165

FortiGate-VM64

FGT-BR-Mexico-City

Synchronized

FGT-BR-Mexico-City

FGT-BR-Mexico-City

10.88.210.167

FortiGate-VM64

FGT-BR-Sao-Paulo

Synchronized

FGT-BR-Sao-Paulo

FGT-BR-Sao-Paulo

10.88.210.170

FortiGate-VM64

FGT-BR-St-Petersburg

Synchronized

FGT-BR-St-Petersburg

FGT-BR-St-Petersburg

10.88.210.166

FortiGate-VM64

FGT-BR-Tokyo

Synchronized

FGT-BR-Tokyo

FGT-BR-Tokyo

10.88.210.164

FortiGate-VM64

FGT-BR-Vancouver

Synchronized

FGT-BR-Vancouver

FGT-BR-Vancouver

10.88.210.161

FortiGate-VM64

FGT-HQ-Sunnyvale

Synchronized

FGT-HQ-Sunnyvale

FGT-HQ-Sunnyvale

10.88.210.160

FortiGate-VM64

FortiGate-Demo-01

Synchronized

FortiGate-Demo-01

FortiGate-Demo-01

10.88.210.125

FortiGate-VM64

root [NAT] (Management)

Synchronized

FortiGate-Demo-01_root

vdom

FortiGate-Demo-02

Auto-update

FortiGate-Demo-02_root

FortiGate-Demo-02

10.88.210.126

FortiGate-VM64

root [NAT] (Management)

Auto-update

FortiGate-Demo-02_root

vdom

FortiGate-Demo-03

Auto-update

FortiGate-Demo-03_root

FortiGate-Demo-03

10.88.210.127

FortiGate-VM64

root [NAT] (Management)

Synchronized

FortiGate-Demo-03_root

vdom

FortiGate-Demo-04

Auto-update

FortiGate-Demo-04_root

FortiGate-Demo-04

10.88.210.128

FortiGate-VM64

root [NAT] (Management)

Synchronized

FortiGate-Demo-04_root

vdom

FortiGate-Demo-05

Auto-update

FortiGate-Demo-05_root

FortiGate-Demo-05

10.88.210.130

FortiGate-VM64

root [NAT] (Management)

Synchronized

FortiGate-Demo-05_root

vdom

Search...

Q

FGT-BR-Atlanta

FGT-BR-Cairo

FGT-BR-Dublin

FGT-BR-Honolulu

FGT-BR-Kuala-Lumpur

FGT-BR-Mexico-City

FGT-BR-Sao-Paulo

FGT-BR-St-Petersburg

FGT-BR-Tokyo

FGT-BR-Vancouver

FGT-HQ-Sunnyvale

FortiGate-Demo-01

FortiGate-Demo-02

FortiGate-Demo-03

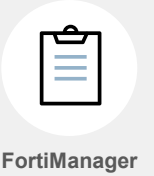
FortiGate-Demo-04

FortiGate-Demo-05

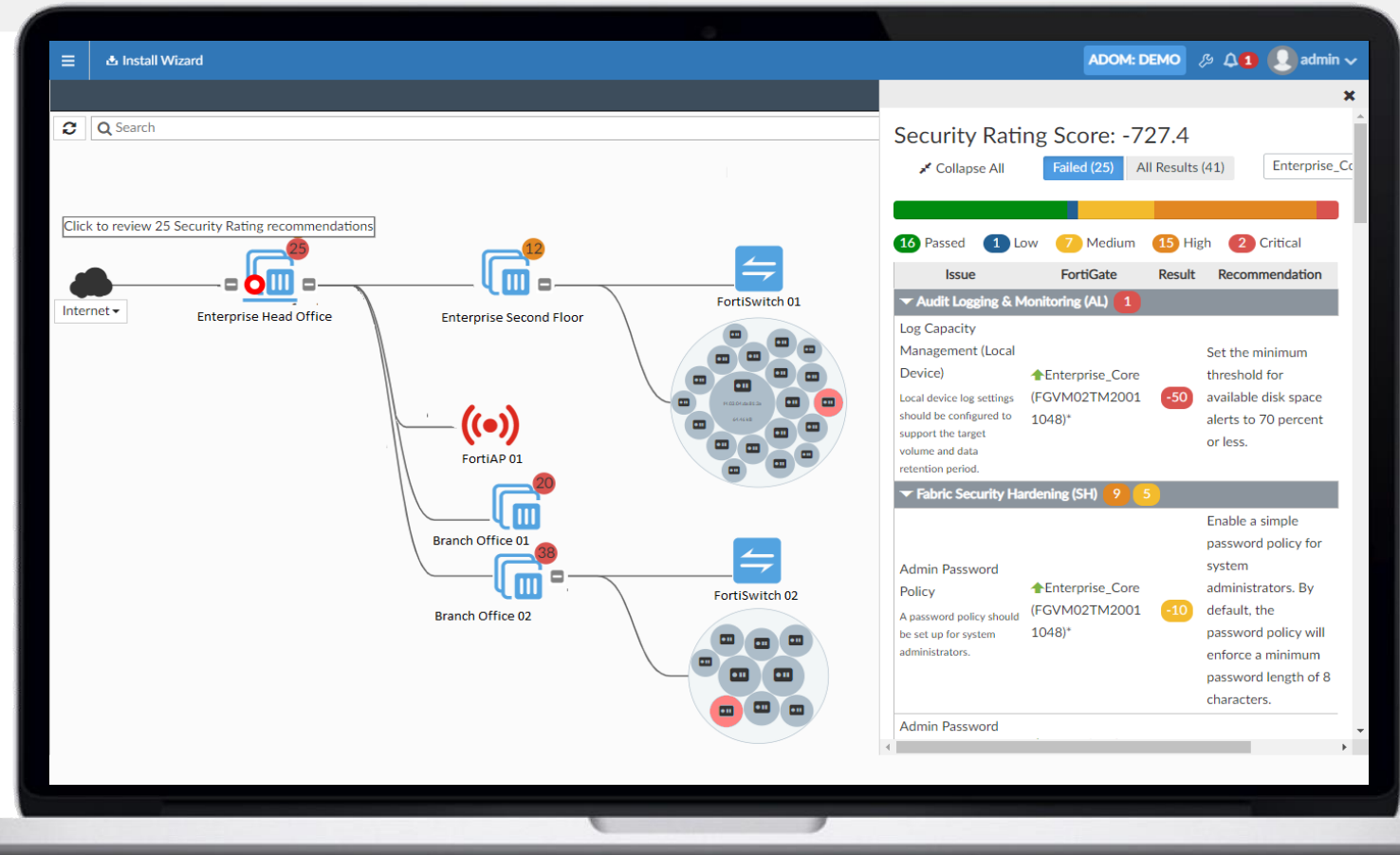


Мережа

Одна консоль для керування та звітності всієї мережі

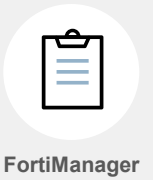


- **Керування мережею.** Вся мережа та безпека у вас на долоні
- **Відмовстійкість** всіх FortiGate та їх оновлення
- **Моніторинг** роботи Fortinet security fabric
- **Спрощення налаштувань** для FortiGate, Secure SD-WAN та SD-Branch для тисячі об'єктів.
- **Автоматизація** застосування налаштувань NGFW та ZTNA
- **SD-WAN** майстер налаштувань з вбудованими порадами (best practices)

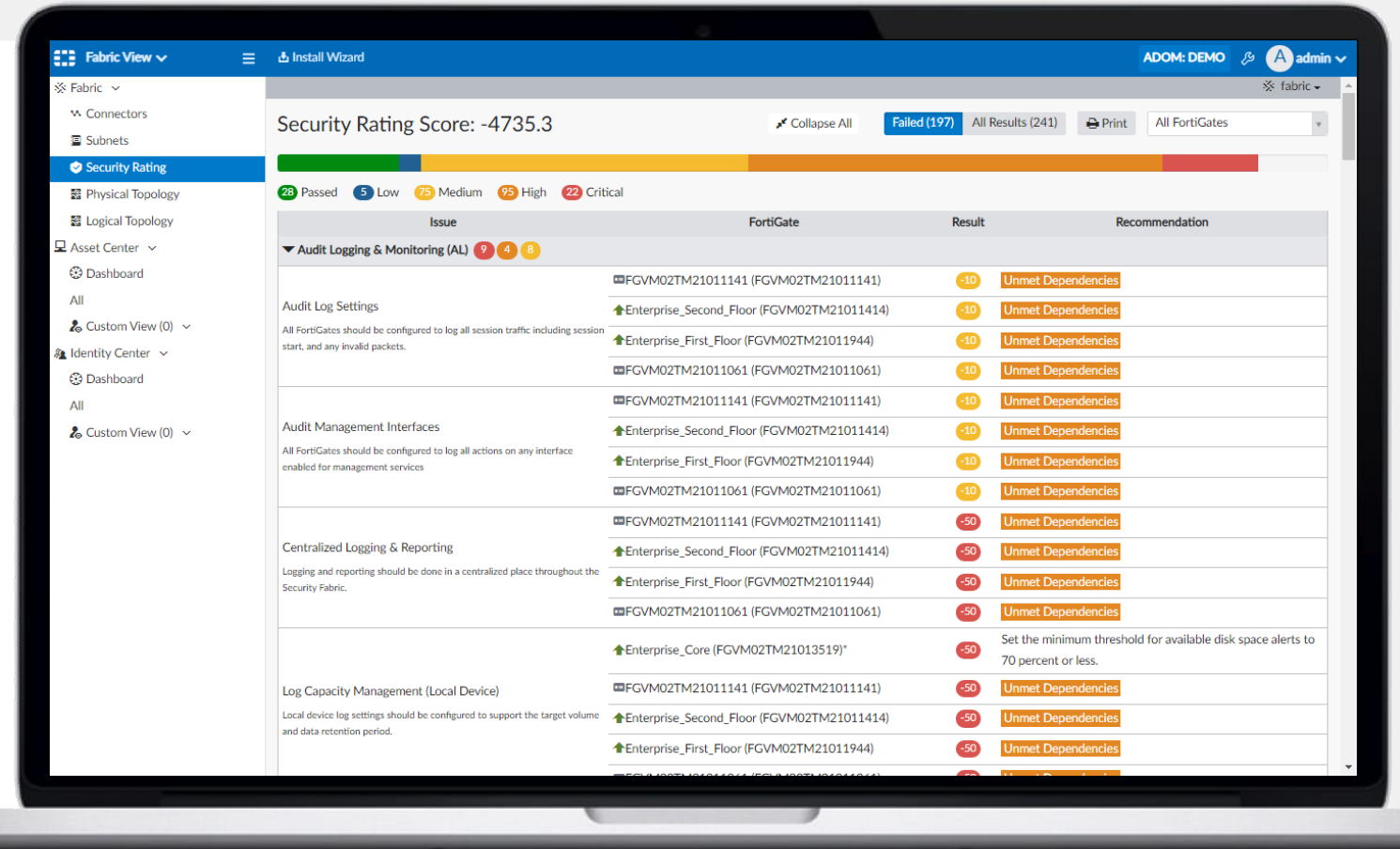


Безпека згідно світових стандартів

Звітність та відповідність вимогам



- Керування політиками безпеки
- Оцінка безпеки налаштувань мережі
- Відповідність вимогам за допомогою вбудованих шаблонів, аудитів та звітності різних типів.



Автоматизація робочих процесів

Автоматизація та інтеграція



FortiManager

- **NOC/SOC рішення** – використовуйте заготовлені дії (playbooks) щодо подій NOC
- Інтеграція з існуючими механізмами автоматизації (Service Now, AWS тощо)
- Автоматизація детектування загрози та продії

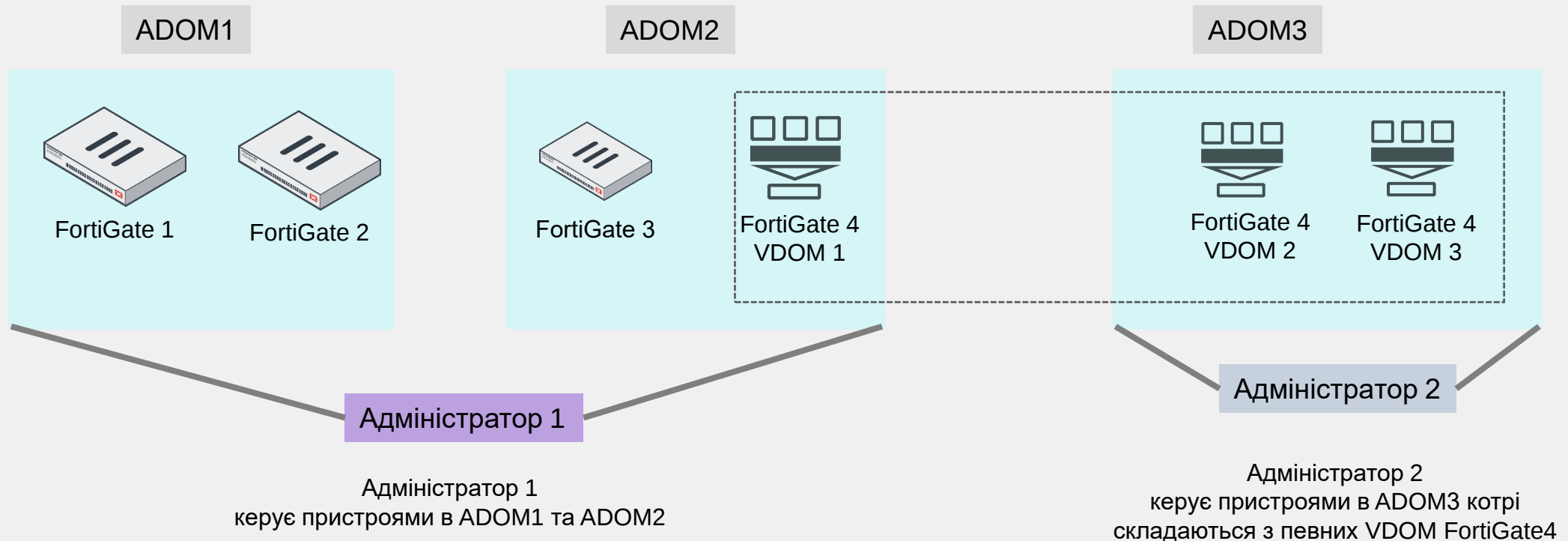
The screenshot displays the FortiManager Event Monitor interface. The left sidebar shows navigation options like Dashboards, Playbooks, Incidents, Automation, Connectors, Playbook Monitor, Event Monitor (selected), All Events, By Endpoint, By Threat, System Events, Custom View, Handlers, and Incidents. The main panel shows a table of events for the handler 'Default_NOC'. The table includes columns for Event ID, Event Name, Event Status, Event Type, Correlation ID, Severity, Handler, Additional Info, First Occurrence, and Last Update.

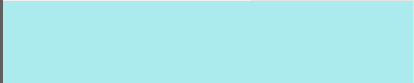
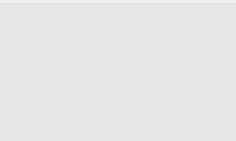
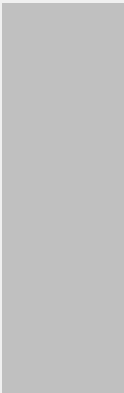
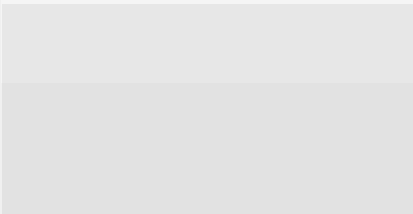
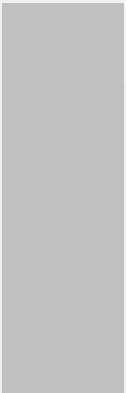
#	Event	Event Stat	Event Type	Corr.	Severity	Handler	Additional Info	First Occurrence	Last Update
1	> FGT_SVN_JENKINS (362)	...	...	8...	Critical	...	...	7 days ago	In a few sec...
2	> Van_DC_Srv221 (38)	...	...	1...	High	...	...	7 days ago	In a few sec...
3	Van_Office_FW2 (439)	...	...	...	...	...	...	...	...
	Van_Office_FW2 primary switch port port31 has come up	...	Others	97	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:40:10	2021-02-10
	Van_Office_FW2 IPsec phase 1 error detected	...	VPN	9...	High	Default_NOC_VPN_Events	IPsec phase 1 error due to: negotiate_error with reason: ...	2021-02-10 16:00:00	2021-02-10
	Van_Office_FW2 primary switch port port31 has gone down	...	Others	96	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:40:22	2021-02-10
	Van_Office_FW2 FortiSwitch system vlan interface change has occurred	...	Others	52	Medium	Default_NOC_Switch_Events	Device Van_Office_FW2 interface vlan change with messa...	2021-02-10 16:00:11	2021-02-10
	Van_Office_FW2 Disconnected from FortiAnalyzer 172.18.3.226	...	System	2...	High	Default_NOC_Fabric_Events	Disconnected from FortiAnalyzer 172.18.3.226	2021-02-10 16:00:11	2021-02-10
	Van_Office_FW2 primary switch port port26 has come up	...	Others	2...	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:00:12	2021-02-10
	Van_Office_FW2 primary switch port port26 has gone down	...	Others	2...	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:00:12	2021-02-10
	Van_Office_FW2 primary switch port port4 has come up	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:00:28	2021-02-10
	Van_Office_FW2 primary switch port port4 has gone down	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:00:23	2021-02-10
	Van_Office_FW2 primary switch port port17 has come up	...	Others	4	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 18:02:13	2021-02-10
	Van_Office_FW2 primary switch port port7 has gone down	...	Others	4	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 18:02:09	2021-02-10
	Van_Office_FW2 primary switch port port16 has come up	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:58:17	2021-02-10
	Van_Office_FW2 primary switch port port16 has gone down	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:58:14	2021-02-10
	Van_Office_FW2 primary switch port port38 has come up	...	Others	2	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:48:36	2021-02-10
	Van_Office_FW2 primary switch port port38 has gone down	...	Others	2	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:48:33	2021-02-10
	Van_Office_FW2 IPsec phase 2 status change	...	VPN	8	Medium	Default_NOC_VPN_Events	IPsec phase 2 status changed due to: phase2-down...	2021-02-10 16:13:57	2021-02-10
	Van_Office_FW2 security fabric settings change: Connection with CSF...	...	System	1	Medium	Default_NOC_Fabric_Events	Device: Van_Office_FW2 change with message: Connect...	2021-02-10 17:17:48	2021-02-10
	Van_Office_FW2 security fabric settings change: Connection with aut...	...	System	1	Medium	Default_NOC_Fabric_Events	Device: Van_Office_FW2 change with message: Disconn...	2021-02-10 17:17:36	2021-02-10
	Van_Office_FW2 Disconnected from Cooperative Security Fabric me...	...	System	1	High	Default_NOC_Fabric_Events	Connection with authorized CSF member terminated on...	2021-02-10 17:17:36	2021-02-10
	Van_Office_FW2 primary switch port port1 has gone down	...	Others	1	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:15:20	2021-02-10
	Van_Office_FW2 primary switch port port25 has come up	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:13:57	2021-02-10
	Van_Office_FW2 primary switch port port25 has gone down	...	Others	3	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:13:55	2021-02-10
	Van_Office_FW2 primary switch port port41 has gone down	...	Others	1	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 17:02:33	2021-02-10
	Van_Office_FW2 primary switch port port48 has come up	...	Others	7	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:43:13	2021-02-10
	Van_Office_FW2 primary switch port port48 has gone down	...	Others	7	Medium	Default_NOC_Switch_Events	FortiSwitch link on Device: Van_Office_FW2 with messa...	2021-02-10 16:43:10	2021-02-10



Підтримка розділення (ADOMs)

- ADOMs створює групи пристроїв для керування ними
- Призначте пристрою один або кілька ADOM
- Призначений для розподілення доступу адміністраторам між пристроями





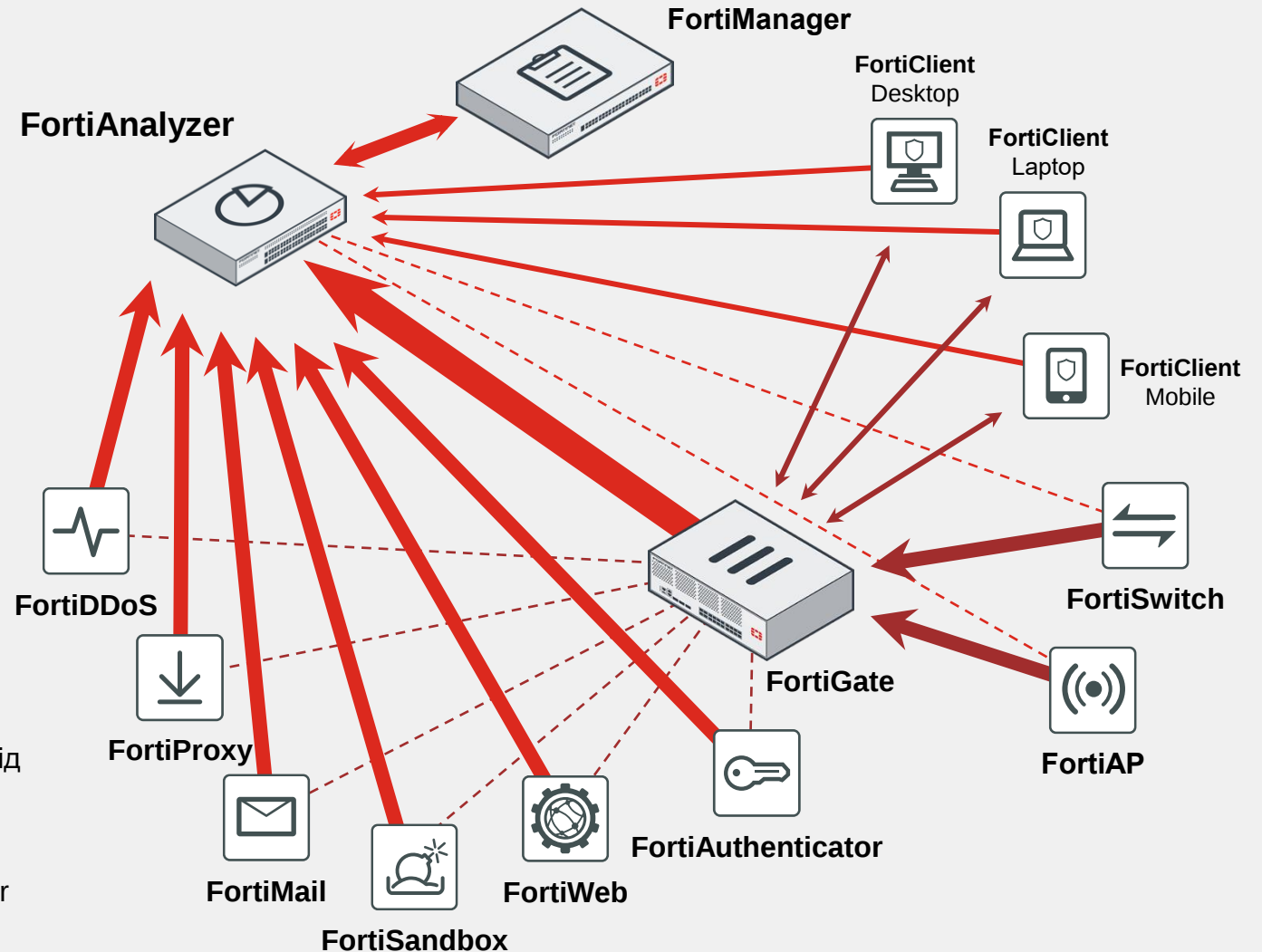
FortiAnalyzer

Детальніше



Security Fabric Management. Роль FortiAnalyzer

- Видимість всього що відбувається
- FortiGate
 - Одне з пріоритетних джерел інформації
 - FortiAnalyzer отримує повні журнали безпеки, трафіку та здоров'я
 - FortiGate збирає та записує журнали від інших пристроїв в рамках своєї Security Fabric
- FortiSwitch та FortiAP
 - FortiAnalyzer отримає сповіщення щодо трафіку який вони обробили та записані в журнали FortiGate logs
- FortiClient
 - FortiAnalyzer отримує сповіщення індивідуально від кожного клієнта
- FortiMail, FortiSandbox, FortiWeb, FortiAuthenticator, FortiDDoS
 - FortiAnalyzer отримує сповіщення безпеки та статусу прямо від цих компонентів
- FortiManager
 - FortiAnalyzer може бути керованим за допомогою FortiManager та надавати йому дані для роботи.



FortiAnalyzer

Погляд з іншої сторони

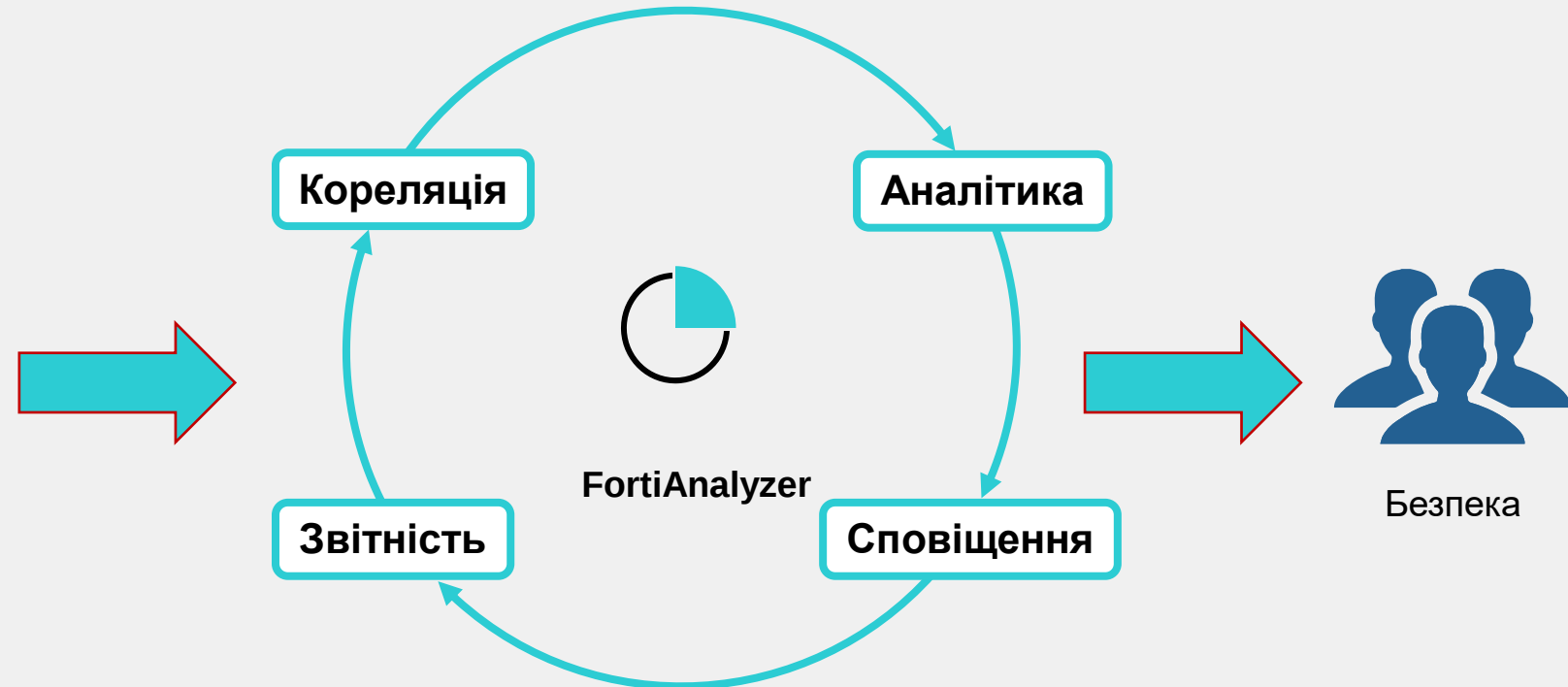
Мережеві пристрої

Firewall & IPS
Router & Switch
Wireless LAN
NetFlow

Сервіси та сервери

Windows & Linux
Database
DHCP & DNS
AAA, RADIUS & AD
Database
Web Application

...and more

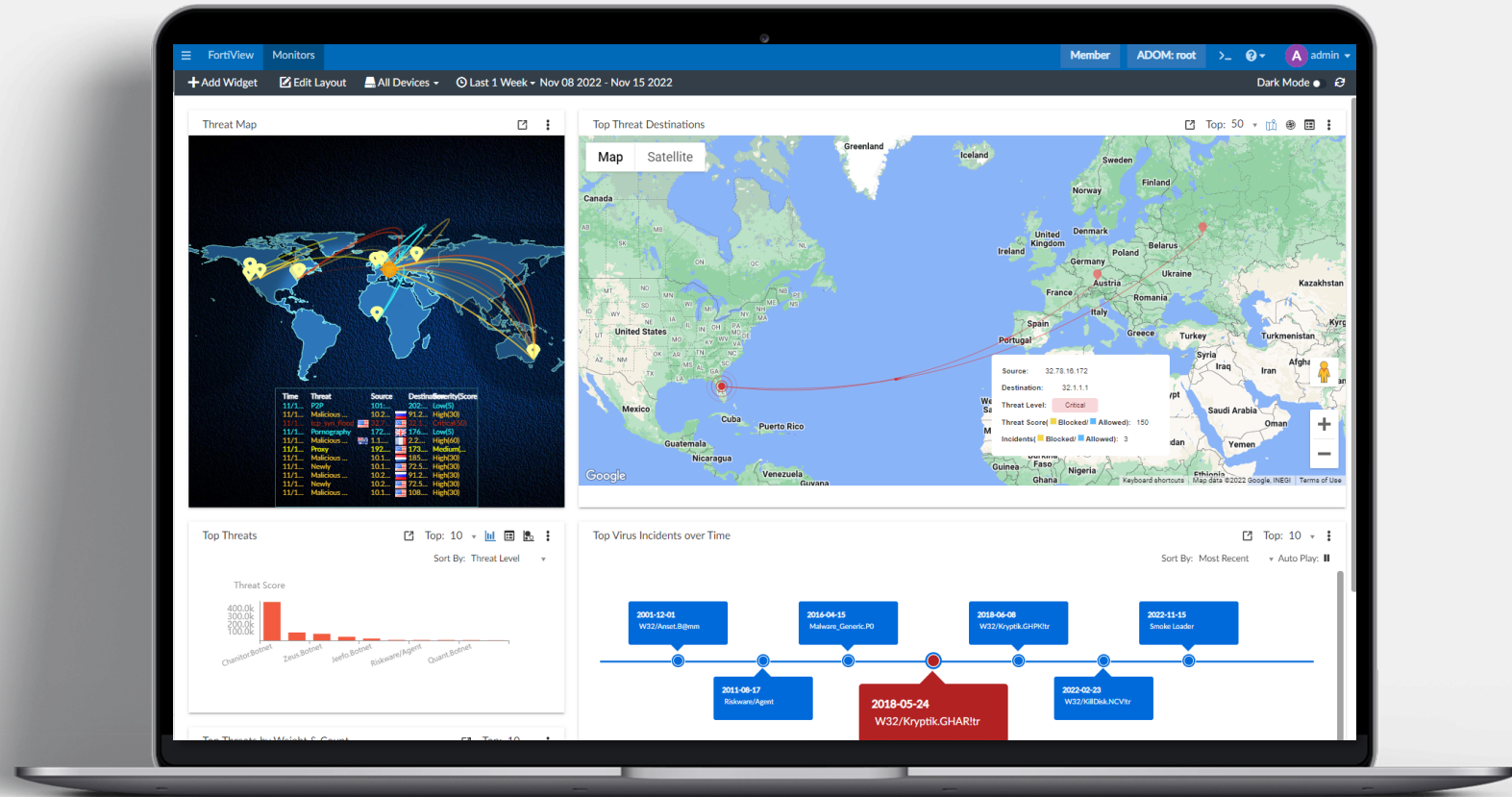


Моніторинг в реальному часі

FortiView

Бачити все

- Дозволяє швидко зрозуміти «що відбувається»
- Надає повну видимість від клієнта до сервера додатку
- Виявляє основні загрози та аналізує їх активність

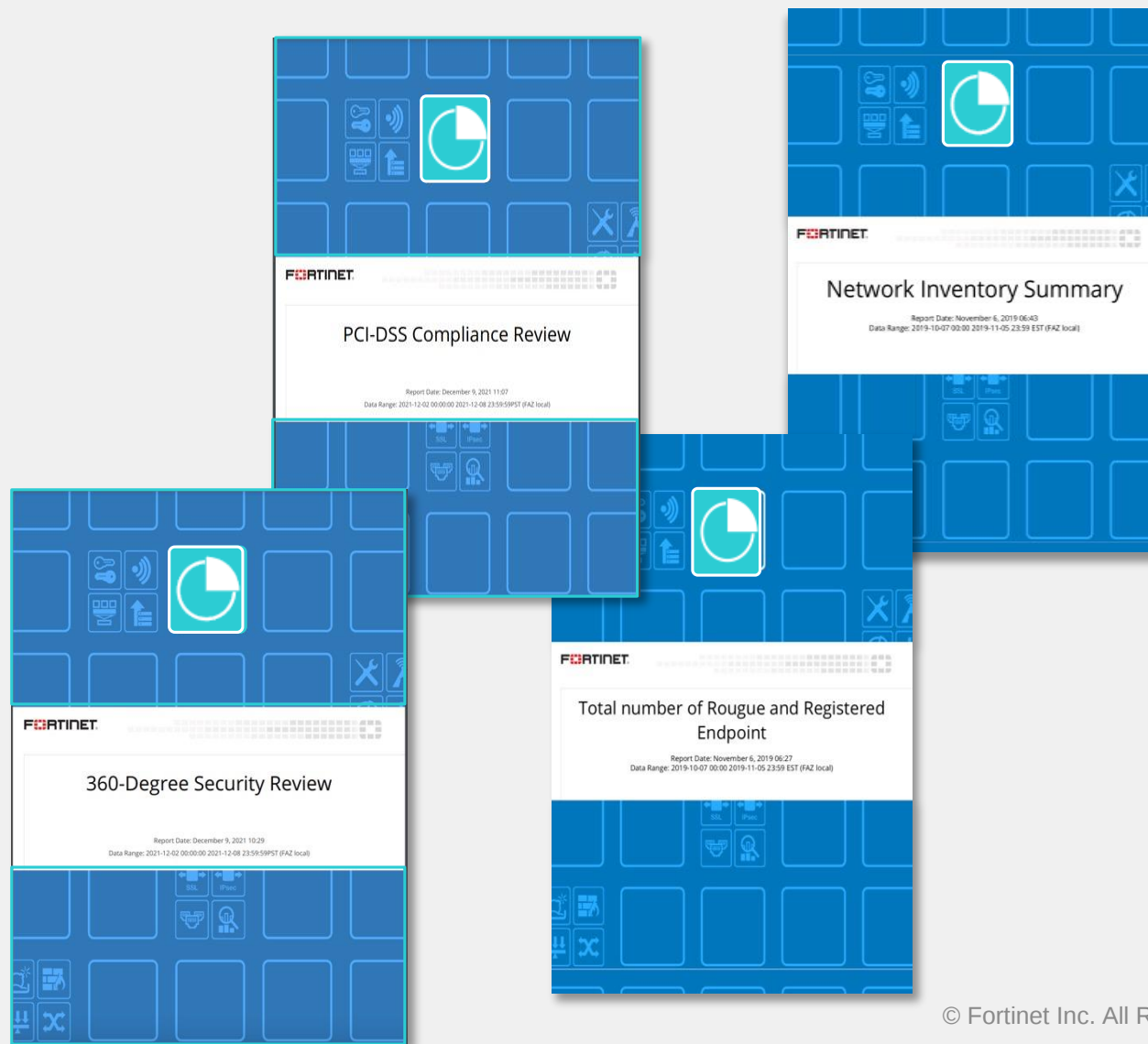


Звіт в пару кліків

Сотні готових звітів

Готові звіти

- Звіти в комплекті які можна змінювати «під себе»
- Автоматизація виправлення недоліків згідно та усунення помилок налаштувань
- PCI / SAR звіти



Моніторинг сервісів та їх безпеки

Кореляція журналів (logs)

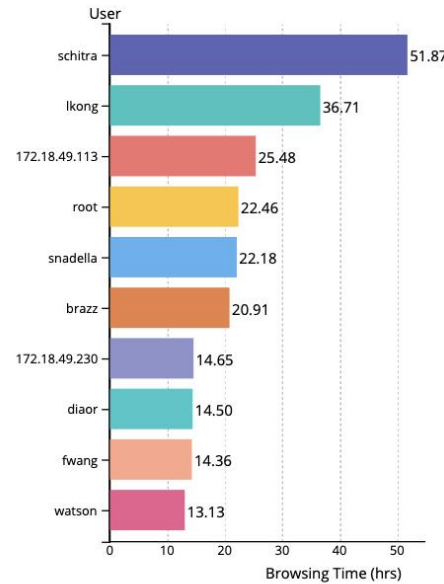
Test 16 - Web Usage Summary Report

Data Range: 2022-01-18 00:00:00 2022-02-16 23:59:59PST (FAZ local)

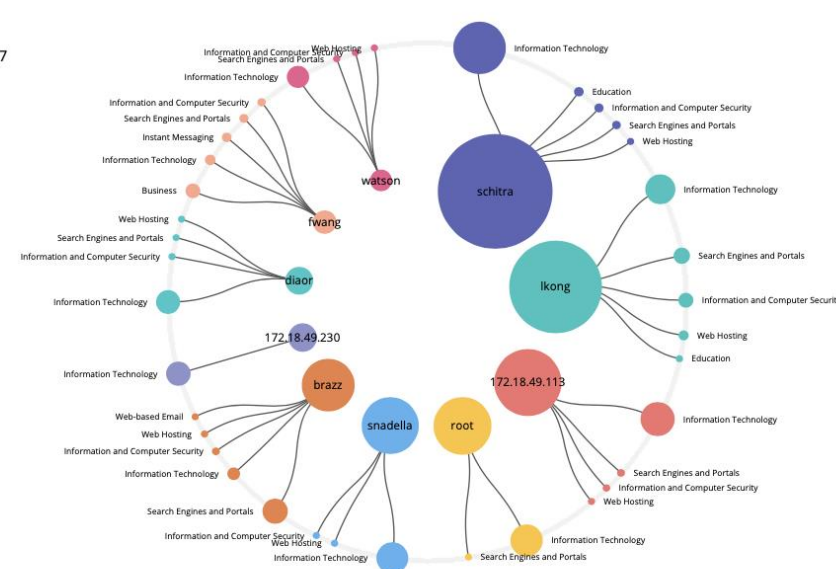
FORTINET

Web Browsing

Top 10 Online Users by Browsing Time



Top 10 Online Users by Categories



page 1 of 9

Improve Operations

- Моніторинг веб трафіку, сервісів, користувачів та загроз
- Занурення до поведінки інфікованих машин
- Звіт «безпека 360»
- Виявлені загрози та протидія ним

Керування інцидентами

Інцидент є невід'ємною складовою роботи інформаційної безпеки. Рішення допомагає швидко зрозуміти його статус одним поглядом завдяки:

- Відображення деталей інциденту
 - Пристрій та користувач
 - Хронологія
 - Автоматичні дії
 - Історія аудиту
 - Додаткові дані, наприклад, звіти
- Коментарі по результату виправлення
- Призначене розслідування
- Сповіщення

The screenshot displays the 'Edit Incident' modal in the Fortinet Security Fabric interface. The modal is overlaid on a background showing incident details for ID IN00002541. The modal fields are as follows:

- Incident Date / Time: 2020-03-24 20:11:22
- Incident Category: Uncategorized
- Severity: High
- Status: Analysis
- Affected Endpoint: Alder
- Description: IoC incident created for endpoint
- Assigned To: (empty dropdown)

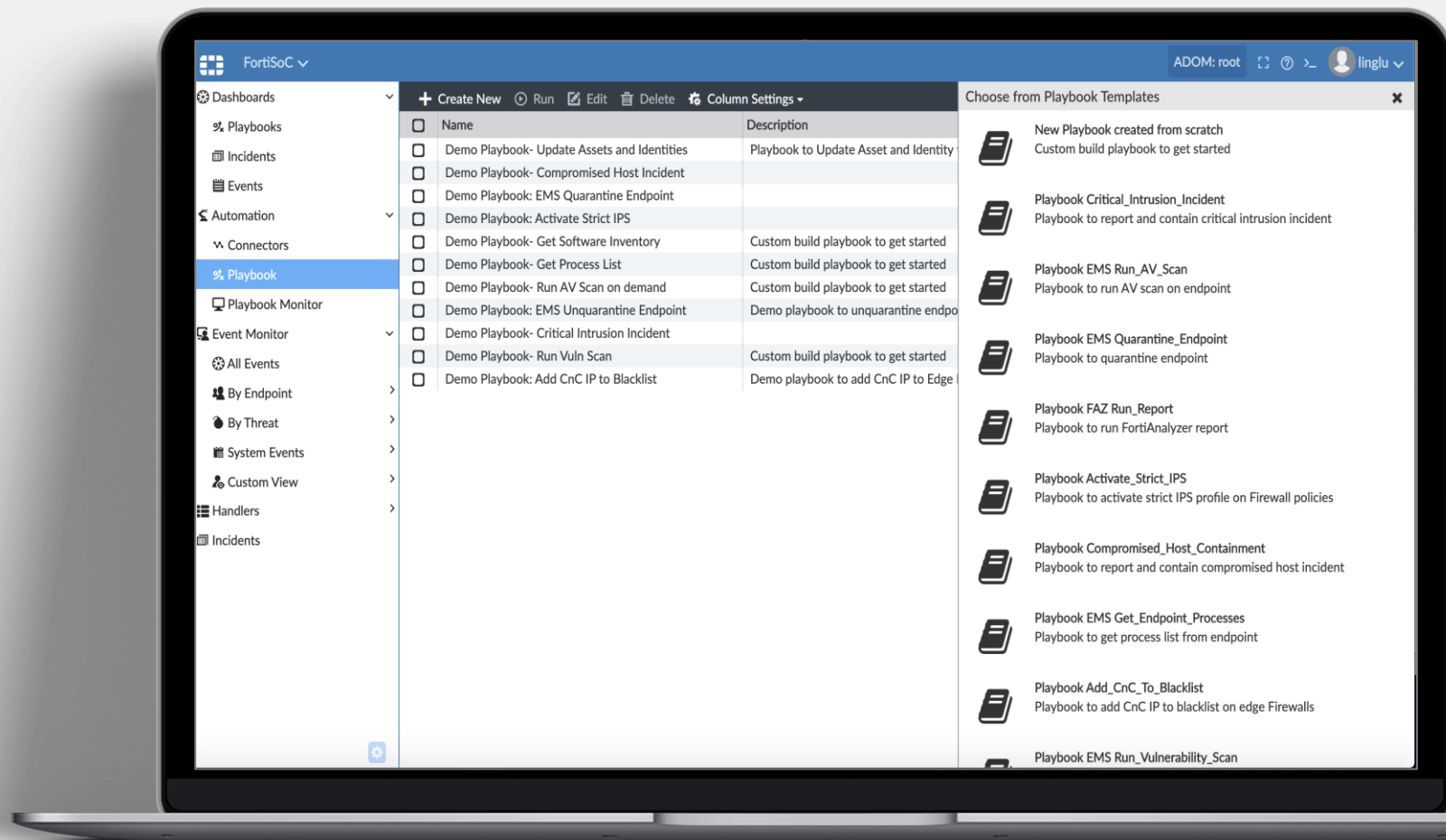
Buttons at the bottom of the modal are 'OK' and 'Cancel'. The background interface shows the incident is 'High' severity, 'Uncategorized', 'Not Assigned', and in 'Analysis' status. It lists affected endpoints, topology, addresses, and operating systems. A sidebar on the right shows 'Note Attach to Incident' and 'Events Attached to Incident'.

Готові до автоматизації

Шаблони

«3 коробки» надані шаблони
що дозволяють спеціалісту
SOC створити власні

- Розслідування інцидентів щодо пристрою в мережі або ж вторгнення
- Збір додаткової інформації в ході розслідування
- Шаблони протидії (блокування IP, тощо)

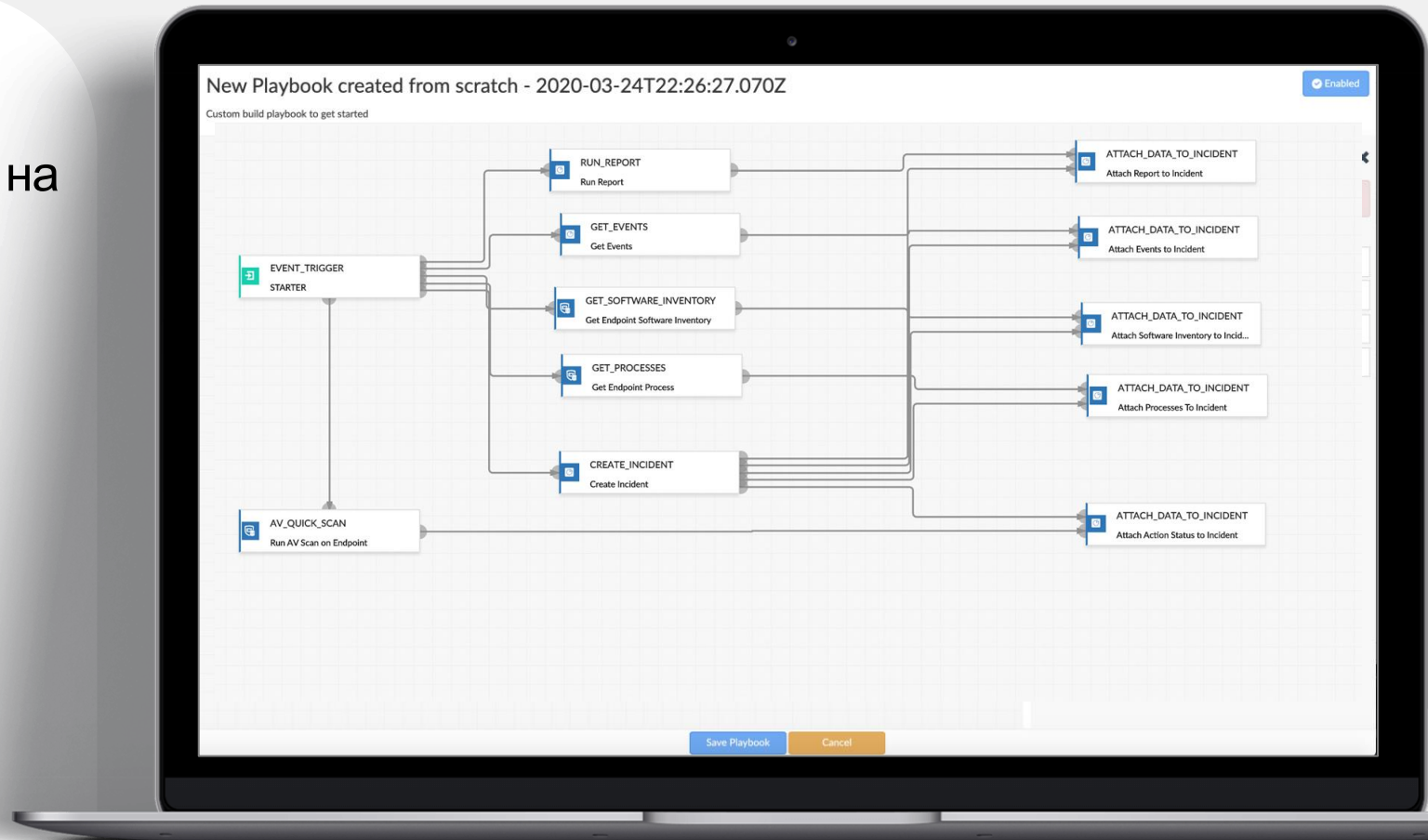


Автоматизація

Візуальне створення алгоритму дій

Інтуїтивний та зрозумілий інтерфейс дозволяє зручно створювати реакції на події та автоматизувати їх.

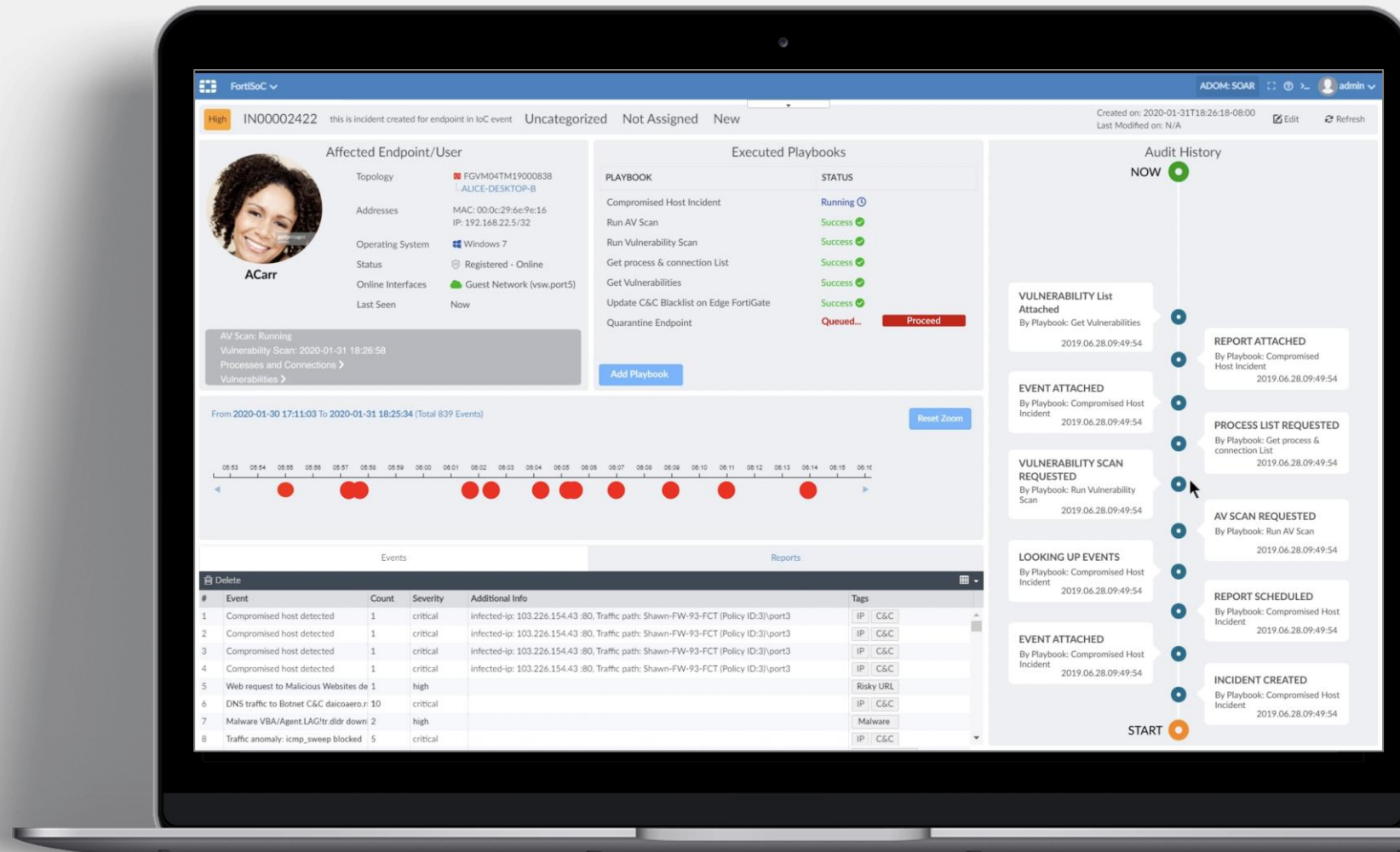
- Редагування/копія вбудованих сценаріїв чи створення власних
- Діаграма створеного сценарію дій
- Умова для старту сценарію
 - Подія
 - Інцидент
 - За розкладом
 - Ручний запуск



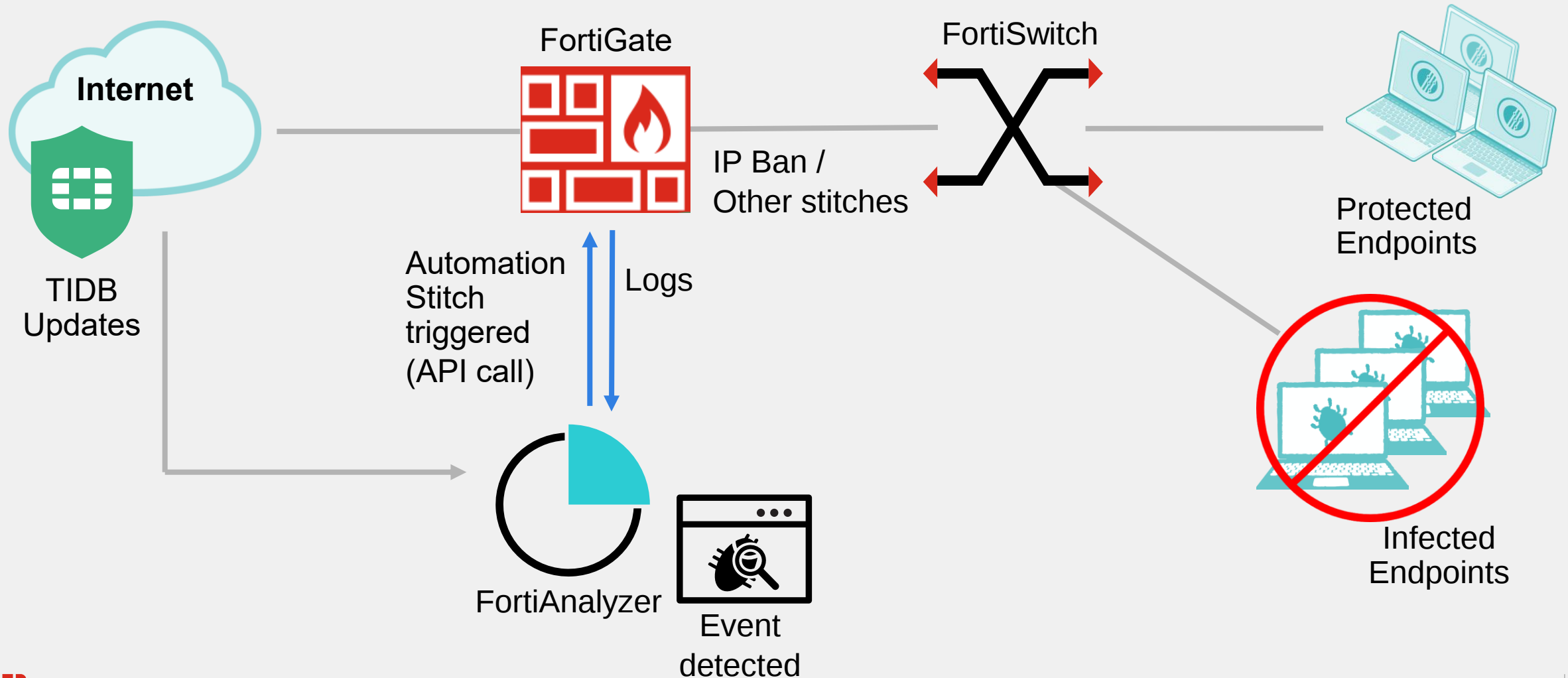
Автоматизація вирішення інцидентів

Автоматичні реакції на інциденти

- Ескалація
- Збір сповіщень
- Звіти
- Коментарі
- Збір інформації
- Дії щодо стримування
- Призначення відповідального
- Сповіщення
- Виправлення



Fortinet Security Fabric Automation



Аналіз та автоматична реакція

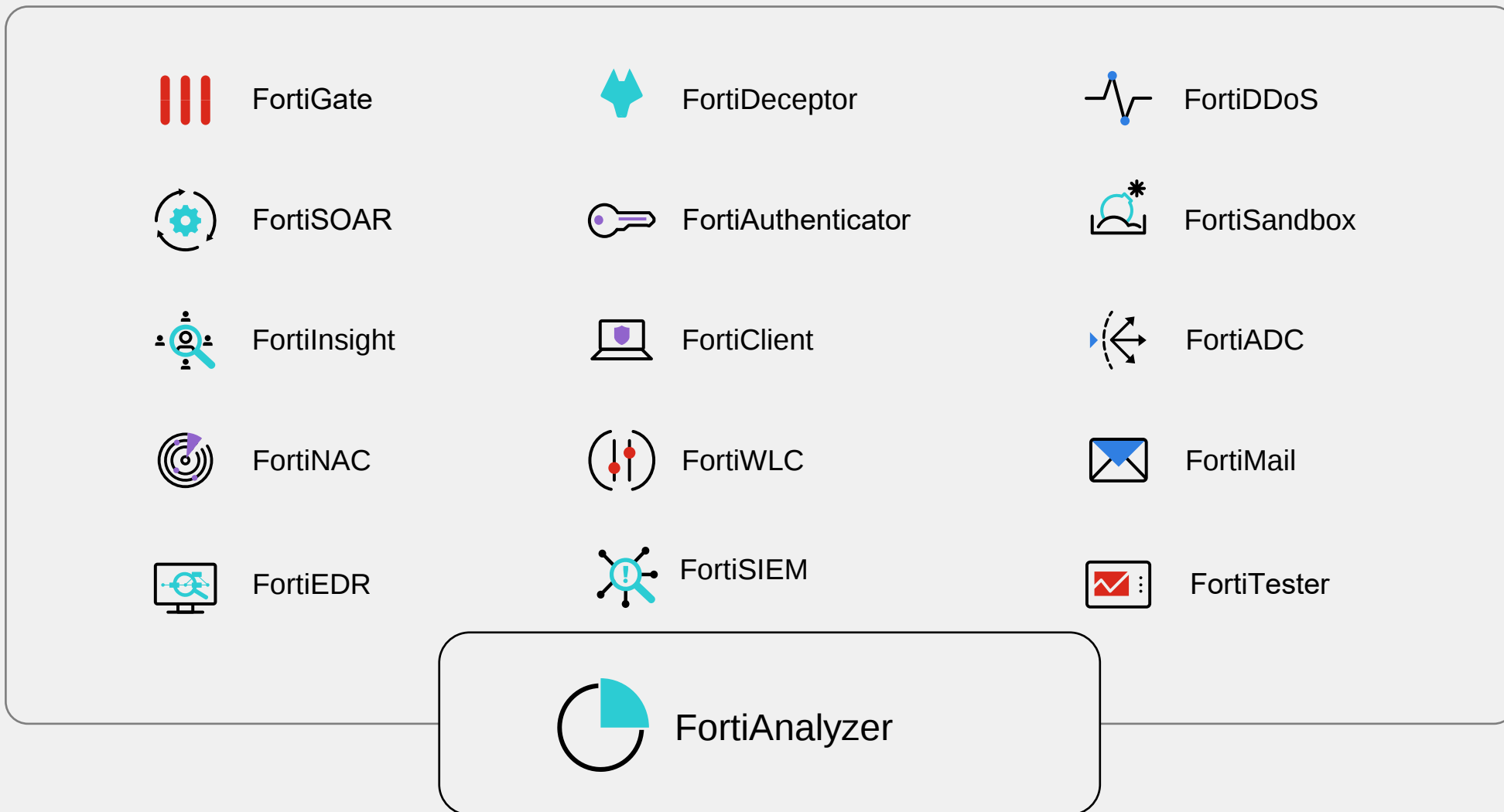
Створюйте свої події
та реакції на них

The screenshot displays the 'Create New Handler' configuration page in the FortiGate web interface. The left sidebar shows the navigation menu with 'FortiGate Event Handlers' selected. The main configuration area includes the following sections:

- Status:** A toggle switch set to 'ON'.
- Name:** 'Botnet Communication detected'.
- Description:** 'For FGT Automation Stitch'.
- Devices:** Radio buttons for 'All Devices' (selected) and 'Specify'.
- Subnets:** Radio buttons for 'All Subnets' (selected) and 'Specify'.
- Filters:** A section with a '+', containing 'Filter 1' which is also 'ON'.
 - Log Device Type:** 'FortiGate'.
 - Log Type:** 'IPS (ips)'.
 - Group By:** A list containing 'Attack Name (attack)' and 'Destination Endpoint (dstendpoint)'.
 - Logs match:** Radio buttons for 'All' and 'Any of the following conditions' (selected).
 - Log Field, Match Criteria, Value table:**

Log Field	Match Criteria	Value
Level (pri)	Equal To	Emergency
 - Generic Text Filter:** A text box containing the expression 'attack ~ Botnet and direction=outgoing and (action=='detected' or action=='pass session')'.
- Generate alert when at least:** '1' matches occurred over a period of '30' minutes.
- Event Message:** 'Traffic from Botnet C&C to \$groupby2 detected'.
- Event Status:** '(Blank)'.
- Event Severity:** 'Medium'.
- Tags:** An empty text box.
- Additional Info:** Radio buttons for 'Use system default' and 'Use custom message' (selected). The custom message text box contains: 'Traffic from Botnet C&C \${attack}, Reference: \${ref}, Traffic path: PolicyID: \${policyid}, \${srcintf}, \${srcip}: \${srcport}'.

Інтеграція FortiAnalyzer



Інтеграція за межами Fortinet

Fortinet інтегрується з 500+ рішеннями інших виробників



Fabric Connectors

Розроблена Fortinet інтеграція автоматизує операції та політики безпеки



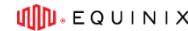
Fabric APIs

Партнерська інтеграція з використанням Fabric API забезпечує широкую видимість із комплексними рішеннями

OT/ IoT



FinServ



Healthcare/
Life Sciences & Pharma



Retail



SLED



+300 other Fabric-Ready Partners



Fabric DevOps

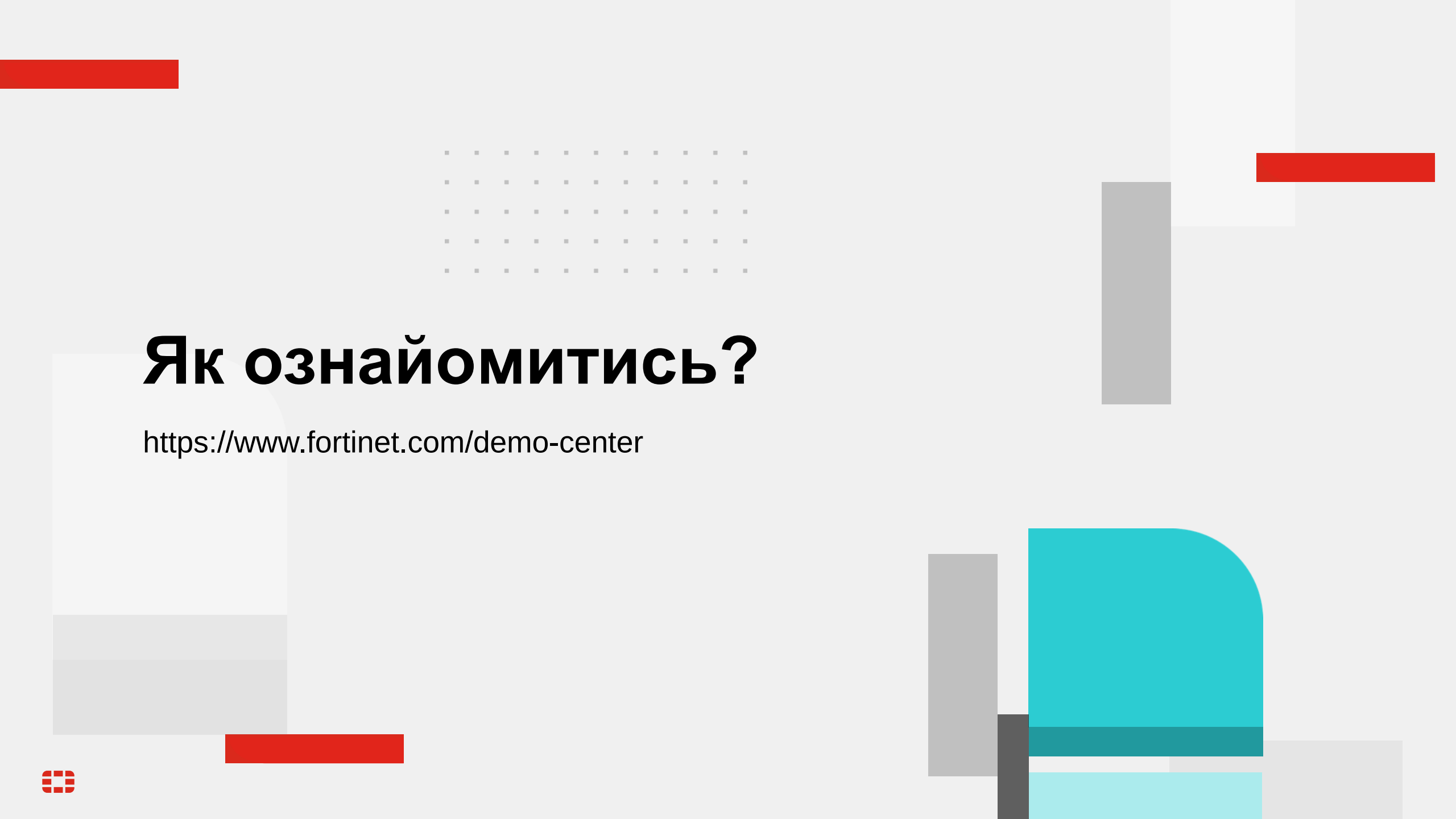
Керовані спільнотою DevOps-скрипти автоматизують надання, конфігурацію та керування мережі та безпеки



Extended Ecosystem

Інтеграція з іншими технологіями та відкритими системами

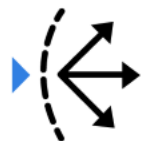




Як ознайомитись?

<https://www.fortinet.com/demo-center>





FortiADC Demo



FortiAnalyzer Den



FortiGate Secure Web Gateway Demo



FortiGate-VM Demo



FortiMail Demo



FortiManager Demo



FortiAuthenticator Demo



FortiClient EMS De



FortiNAC I



FortiWeb Demo



FortiWLM Demo



FortiSOAR Demo



FortiNDR Demo



FortiSandbo



FortiEDR Demo



FortiTester Demo



FortiExtender Demo



LAN Edge Demo



FortiGate-CGN Demo



FortiGate IPS Demo



FortiCNP Demo



FortiAIOps Demo



FortiAnalyzer

Free Product Demo

This full working demo lets you explore the many features of FortiAnalyzer.



FortiAnalyzer offers centralized network security logging and reporting for the Fortinet Security Fabric. FortiAnalyzer accepts inbound logs from multiple downstream Fortinet devices such as FortiGate, FortiMail, and FortiWeb devices etc. Functions such as viewing/filtering individual event logs, generating security reports, alerting based on behaviors, and investigating activity via drill-downs are all key features of FortiAnalyzer. In this demo, see how it presents the visibility of your networks such as an aggregate view of applications, web usage, and potentially malicious behavior affect your network.

Get Started

First Name *

Last Name *

Job Function *

Job Level *

Дякую за увагу!





FORTINET®