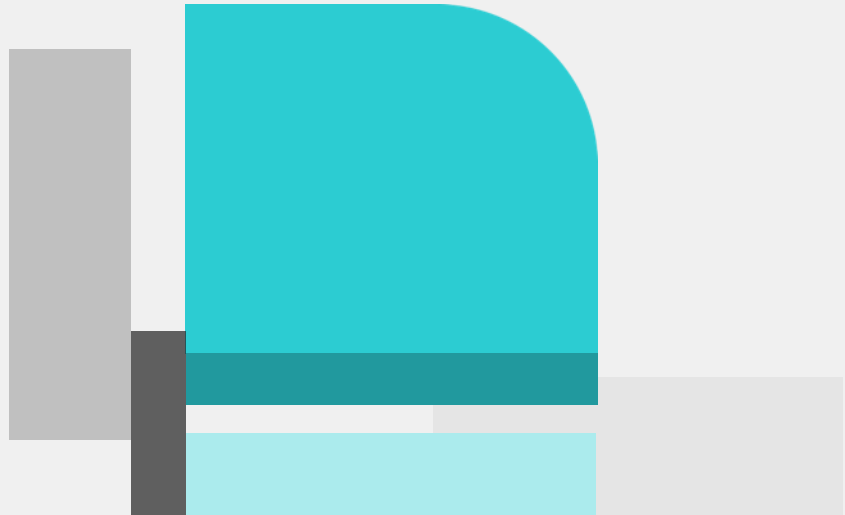
Гібридні мережі з Fortinet Fabric Management Center. Побудова, адміністрування та безпека.

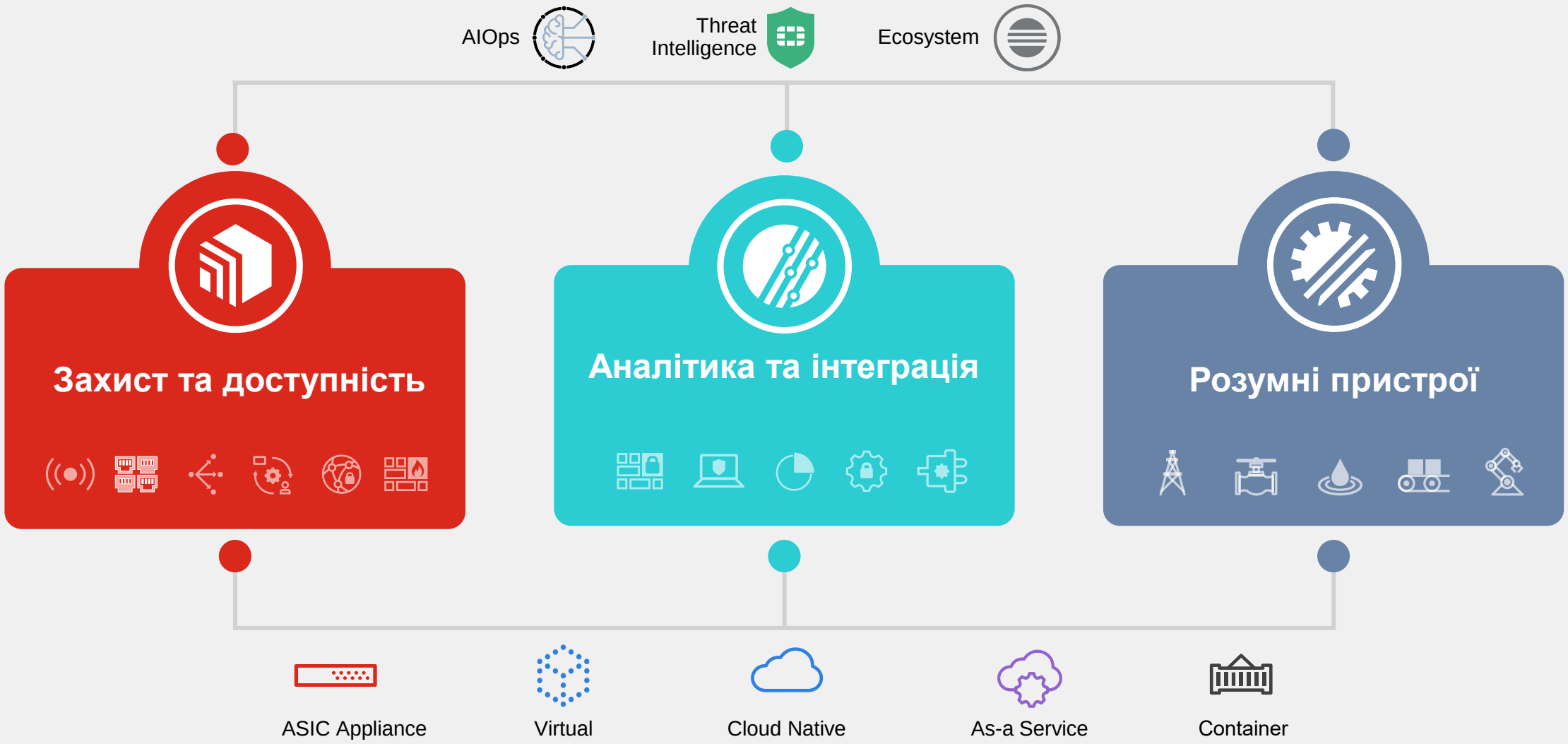
Євгеній Таран, Systems Engineer

А що тут складного?

Почнемо з основ



Безпека – це комплекс



Кожний напрям – свої рішення

AIOps | Threat Intelligence | Ecosystem

Захист та доступність

Досвід користувача

Secure LAN	Firewall
Secure WLAN	SD-WAN
5G	SASE
SWG	ZTNA
Cloud Networking	NAC

Аналітика та інтеграція

Ризики та керування ними

SIEM	SOAR
Analytics	Threat Intelligence
EDR/XDR	Identity
Email	WAF
Cloud Security	NDR

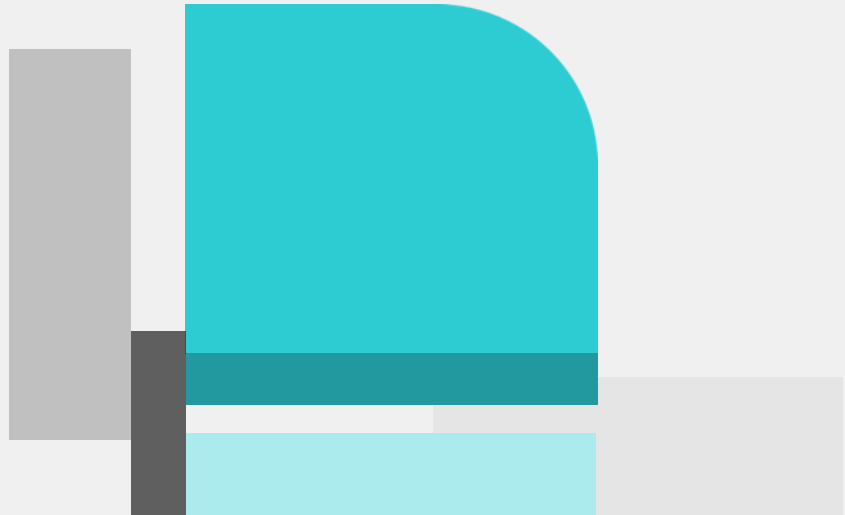
Розумні пристрої

«Новий» вектор

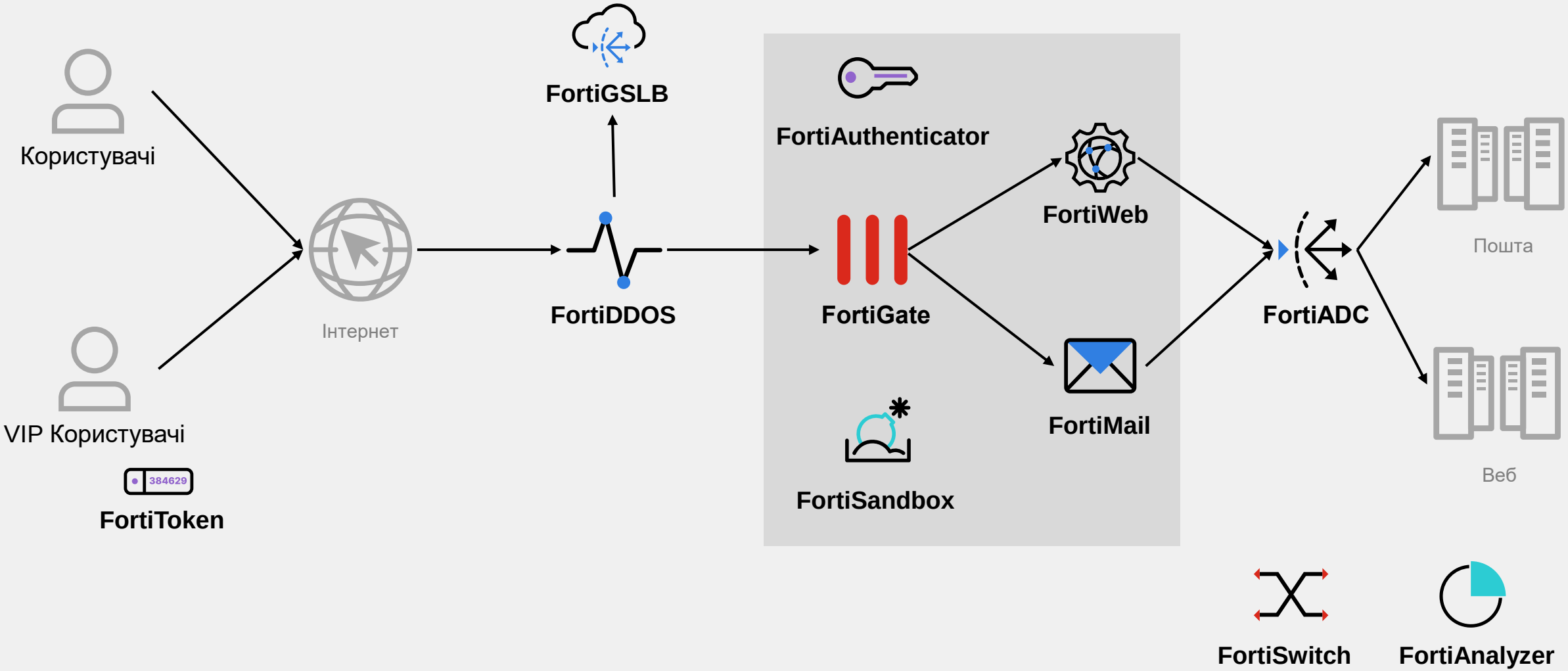
Rugged AP	NAC/PAM
Rugged FW	OT Services
Industrial Switch	OT SIEM/SOAR
SD-WAN/5G	OT EDR

Гібридні мережі

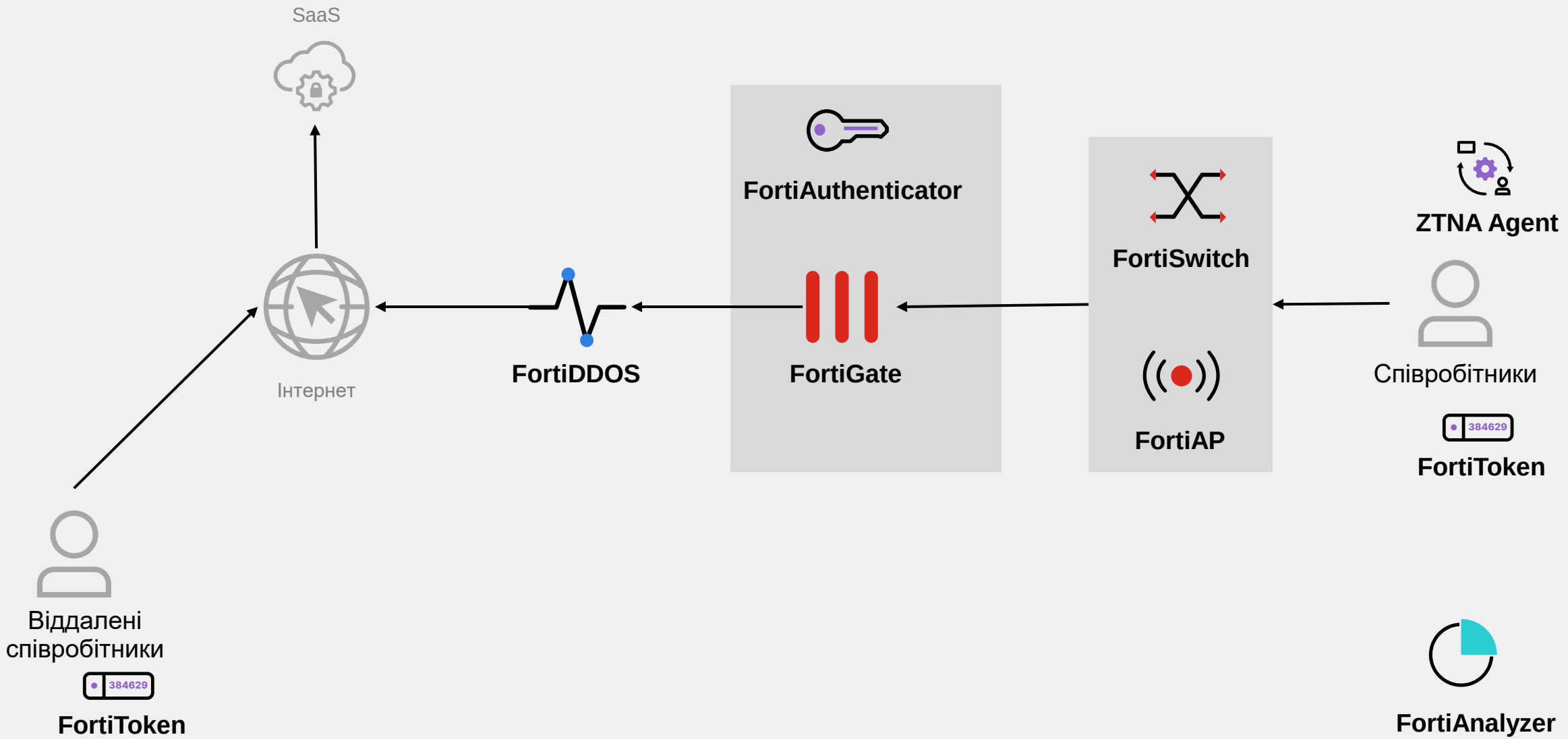
Кілька практичних прикладів і проблем що виникають при їх побудові



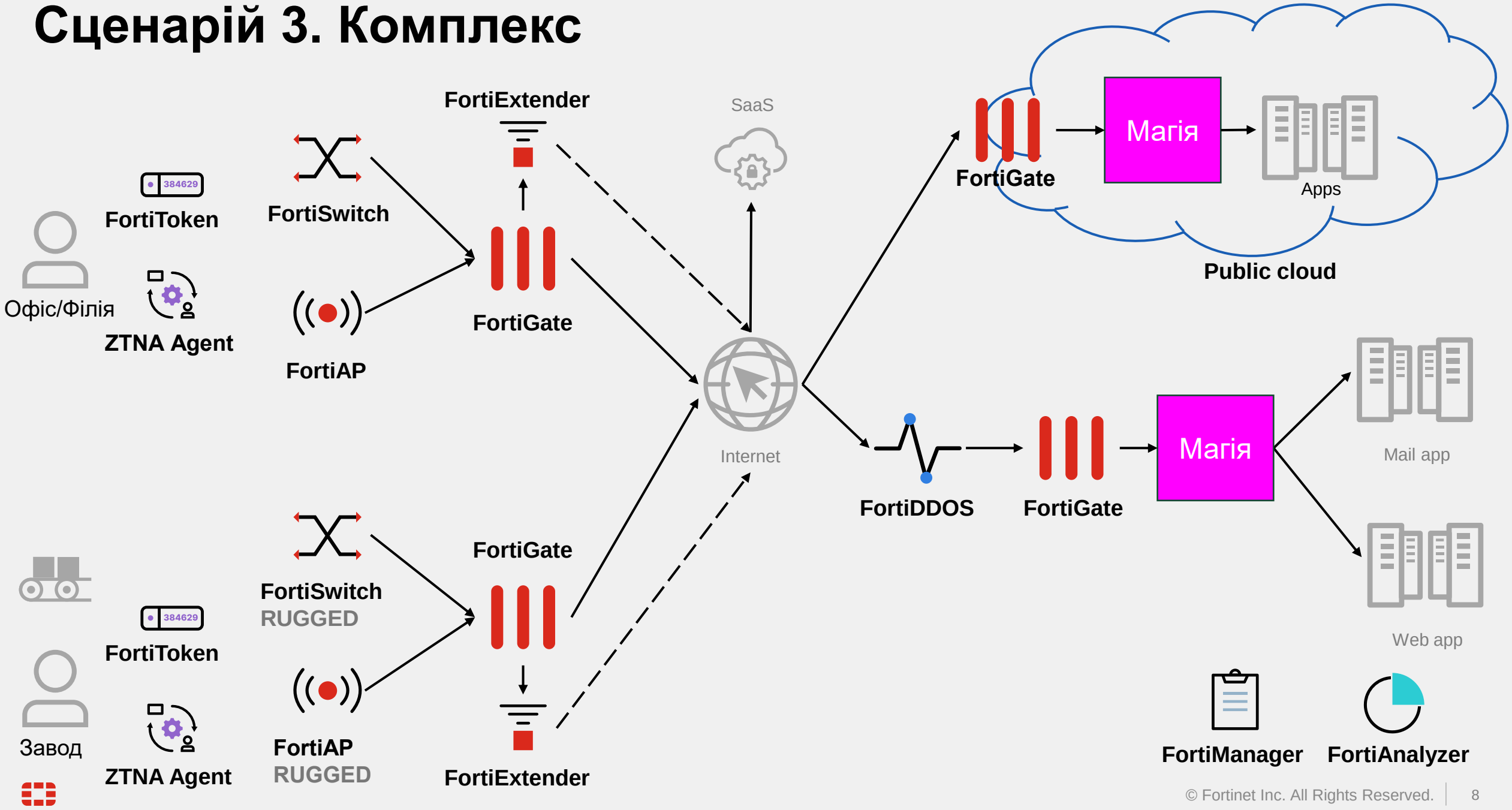
Сценарій 1. Публікація веб/поштового сервісу



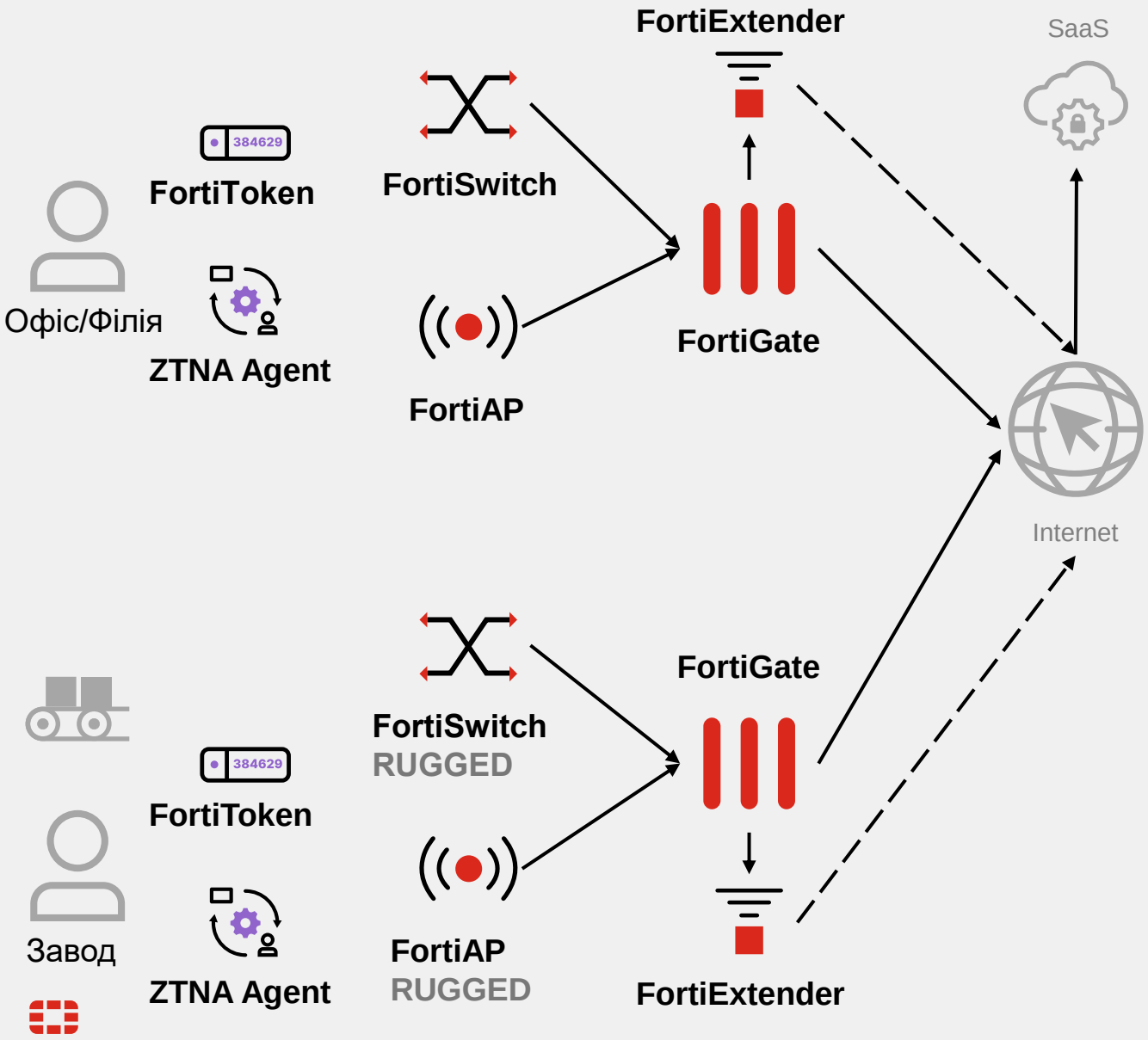
Сценарій 2. Безпека співробітників



Сценарій 3. Комплекс



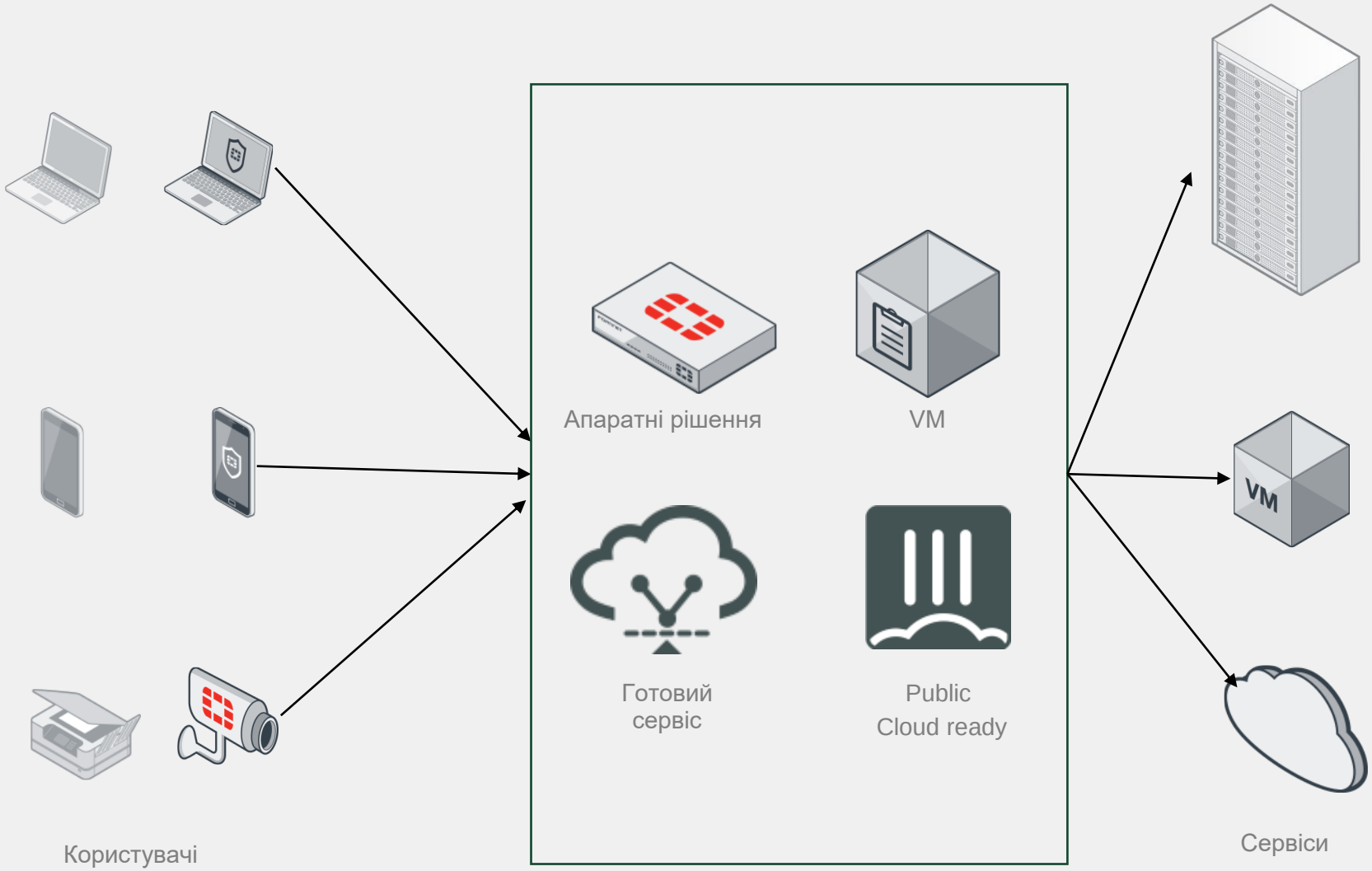
Сценарій 3. Комплекс



FortiManager

FortiAnalyzer

Гібридні мережі



Вимоги

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

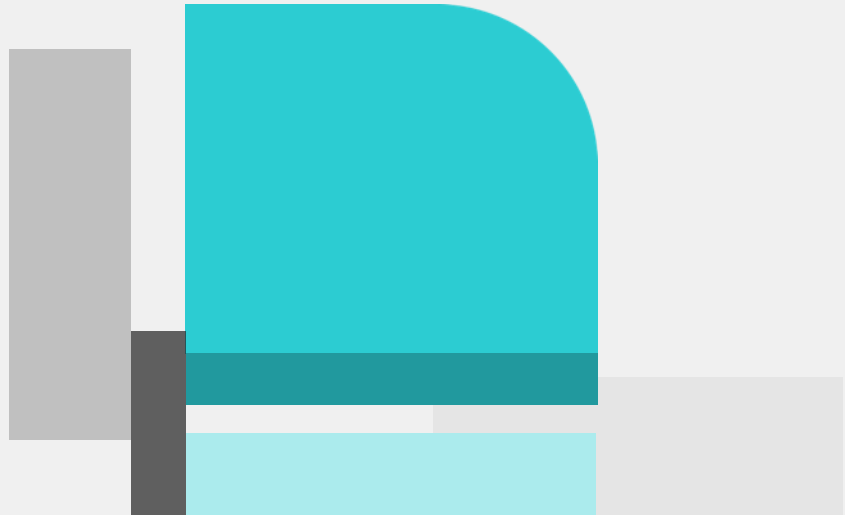
Гібридні мережі

Сучасні реалії

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

Security Fabric

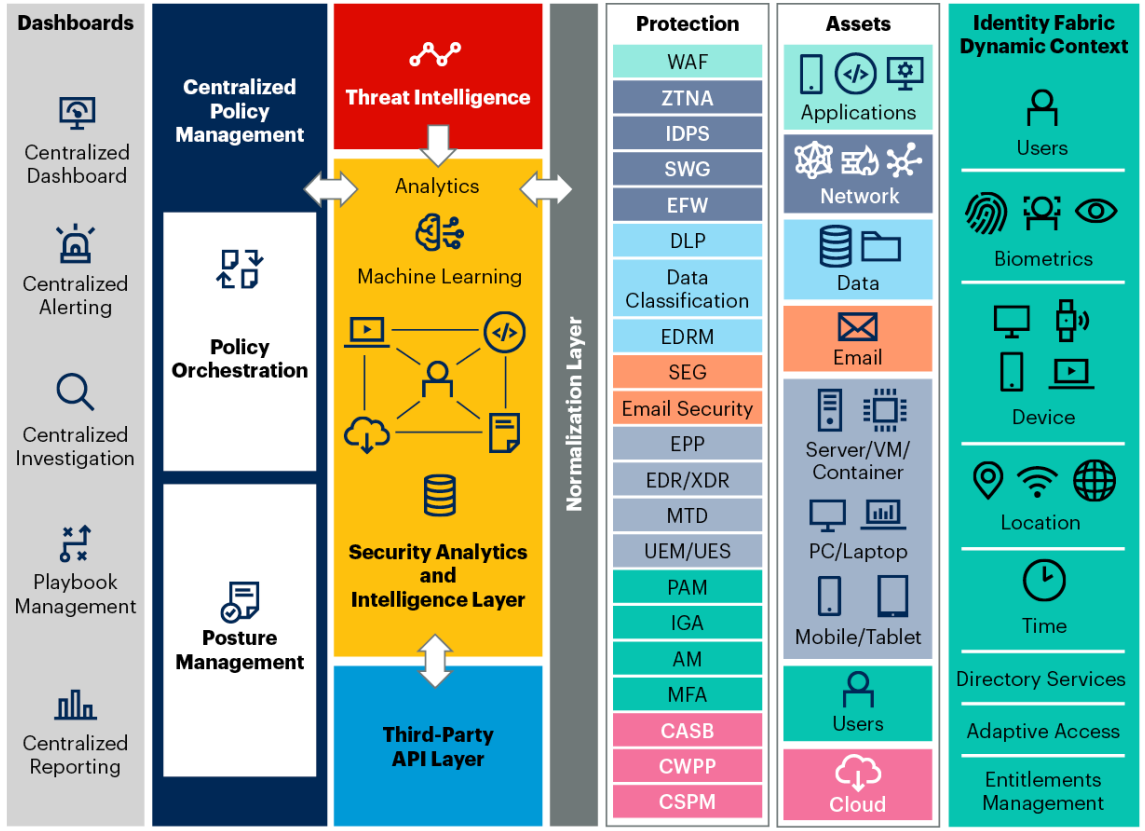
В чому складність керування?



Що з цього приводу каже Gartner?

Gartner

Cybersecurity Mesh Architecture



Source: Gartner
756156_C

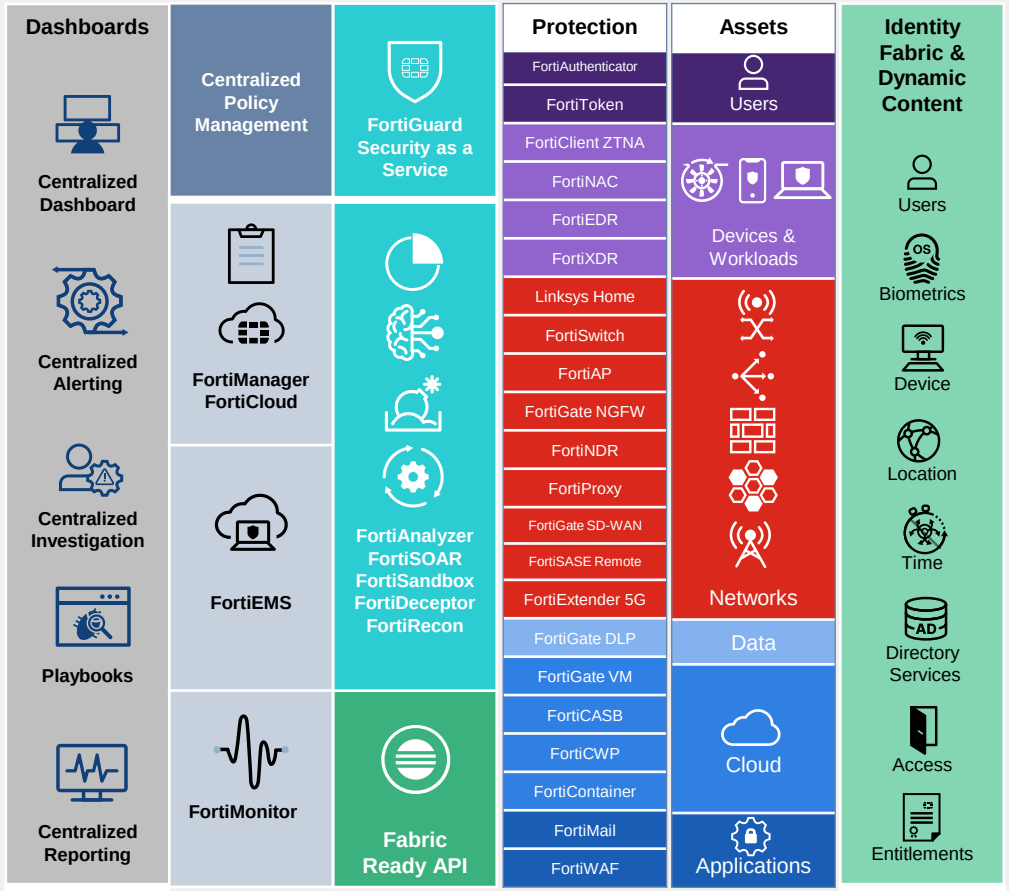
Source: *Gartner "Guide to Cloud Security Concepts"*, Patrick Hevesi, Richard Bartley, Dennis Xu. 21 September, 2021

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.

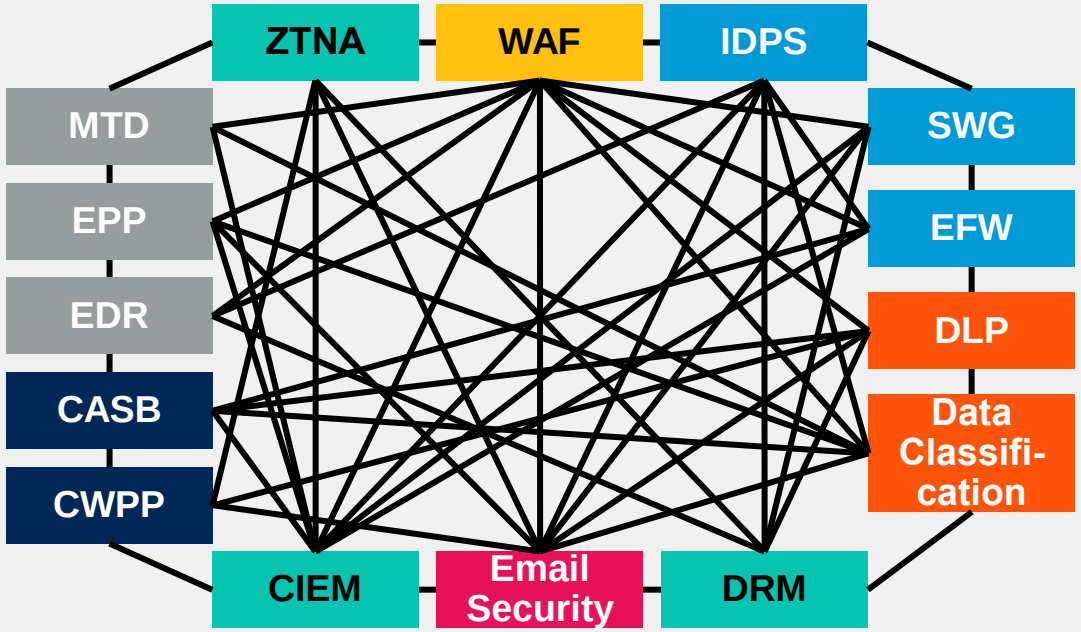
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET



Архітектура Gartner Cybersecurity Mesh

Gartner®



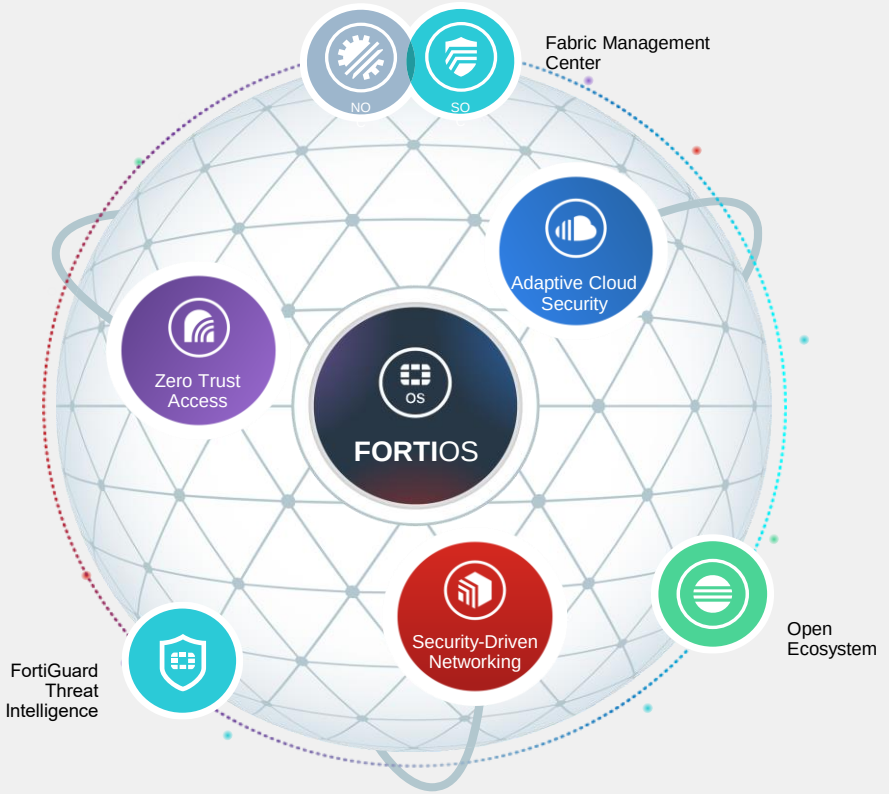
Executive Guide to Cybersecurity Mesh, 2022

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

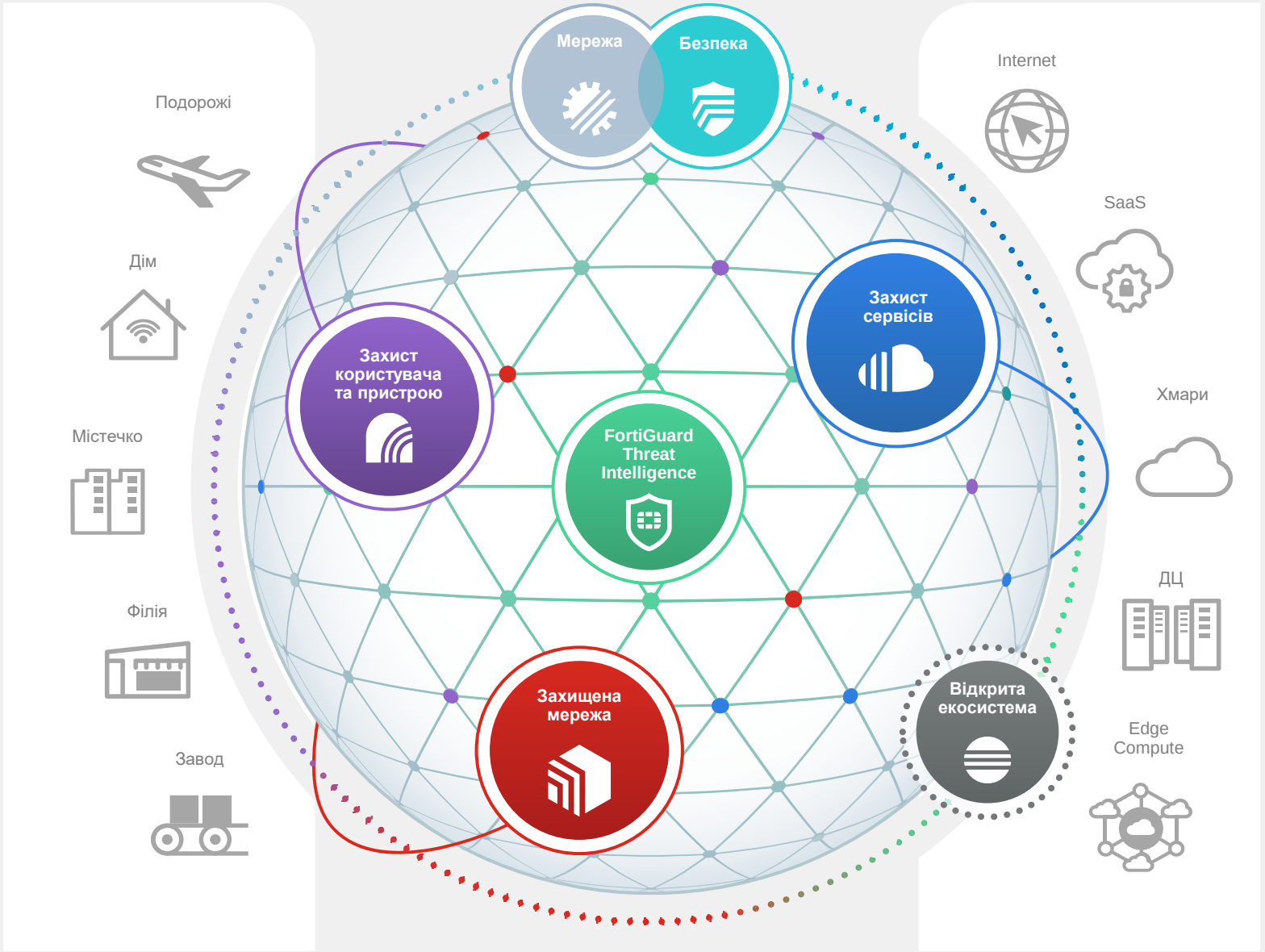
Багатовекторна видимість і захист для повного охоплення кібербезпеки

Інтеграція

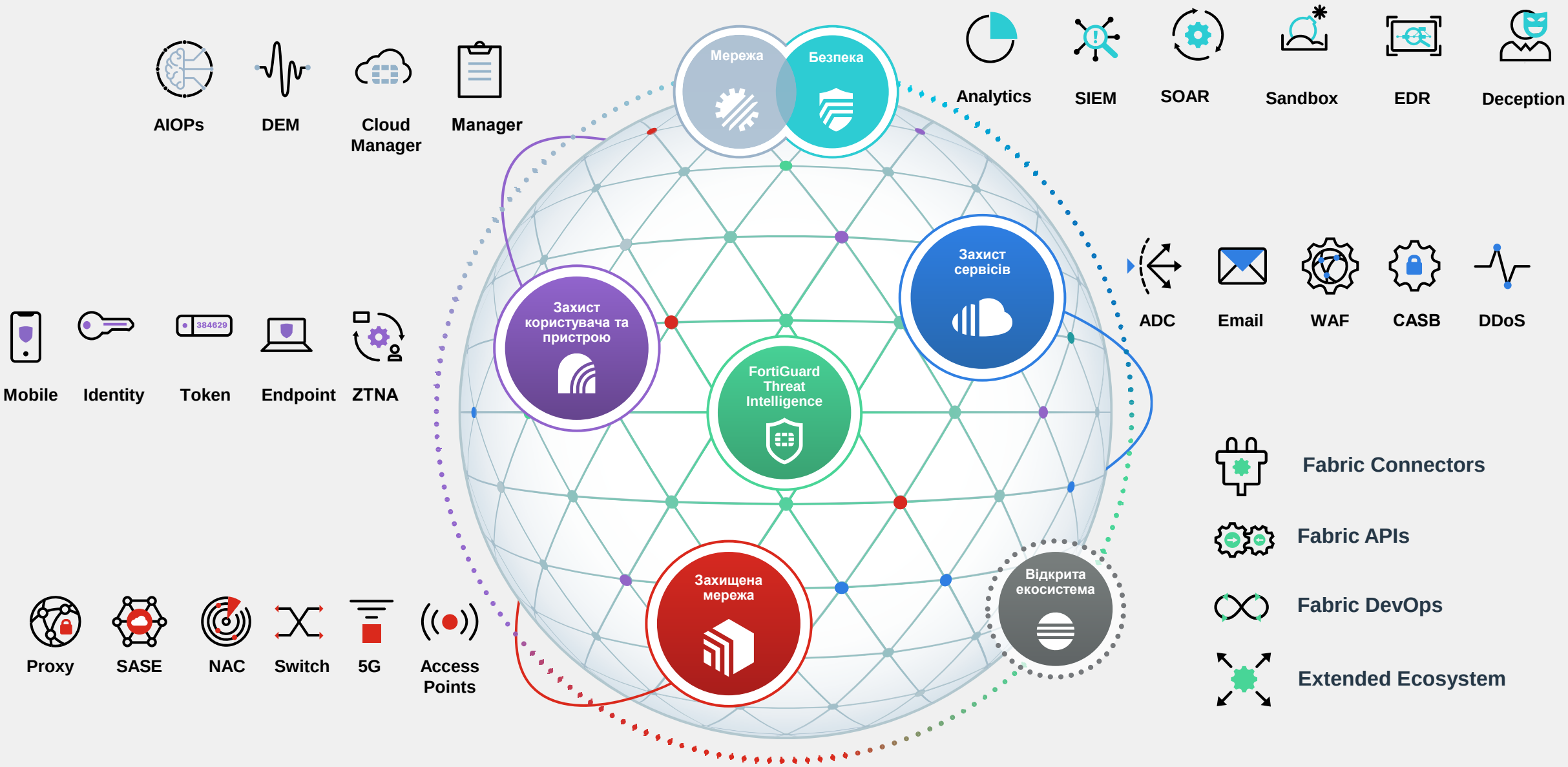
зменшує складність управління та обмін інформацією щодо загроз

Автоматизація

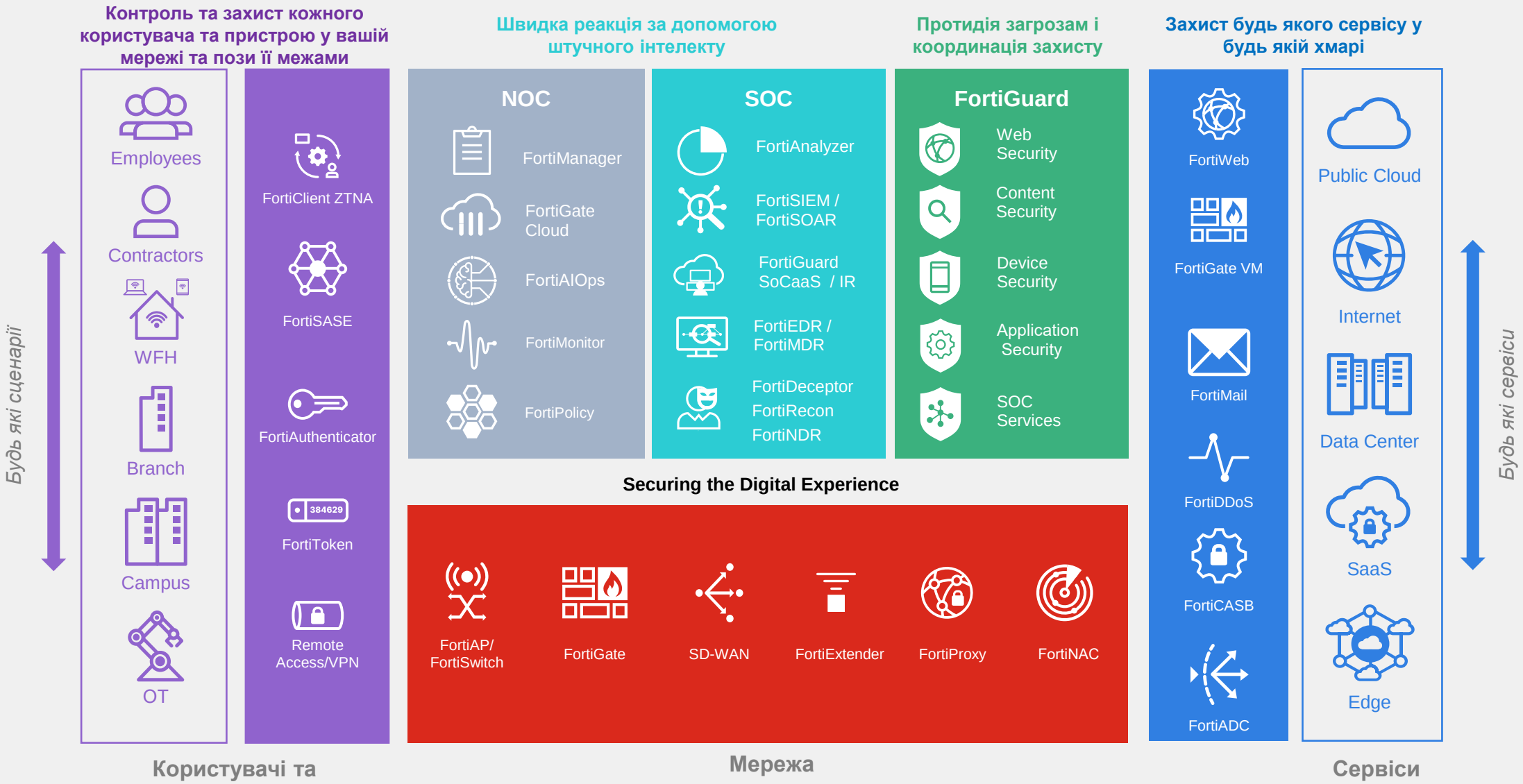
Автоматизація дій безпеки з використанням штучного інтелекту для підвищення швидкості та ефективності



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

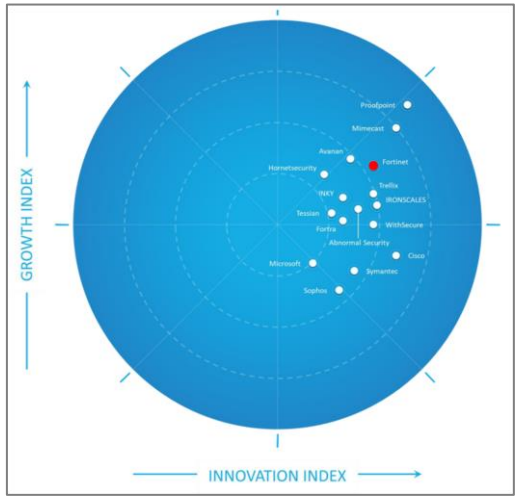
Gartner Magic Quadrant for Endpoint Protection Platforms, 2023

Fortinet Recognized as a Visionary Vendor

Email Security

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

Fortinet Recognized as a Top Vendor



SIEM

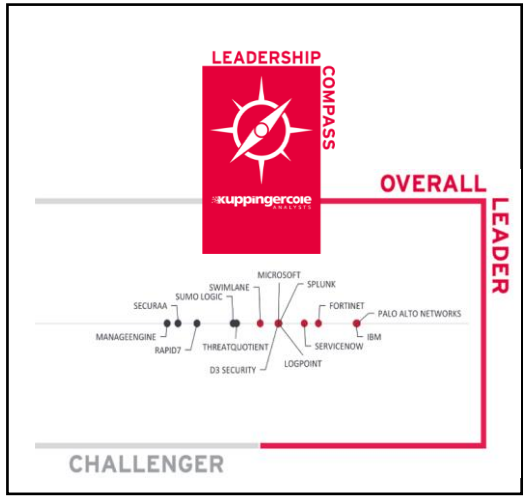
Gartner Magic Quadrant for SIEM 2023

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

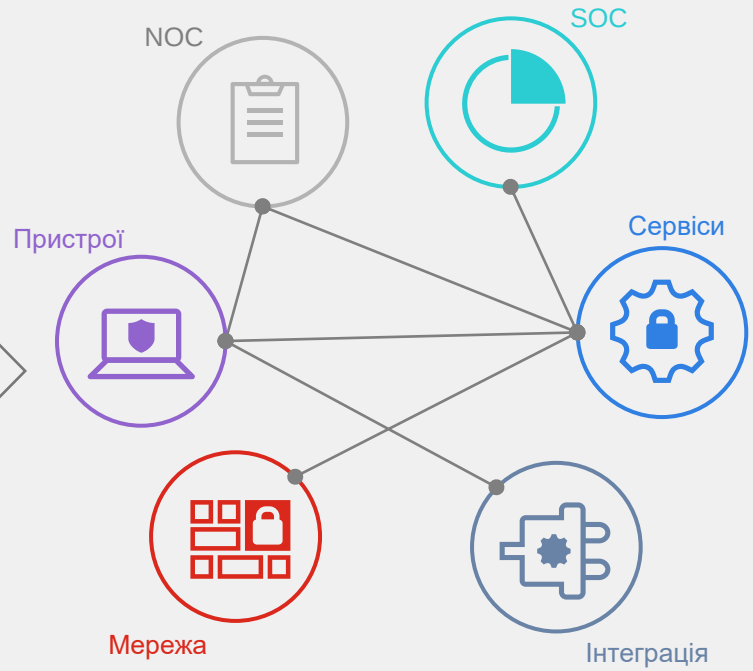
Fortinet є однією з найбільш перевірених корпоративних компаній з кібербезпеки в світі, що займає лідерські позиції в десятках аналітичних звітів, що підкреслюють широке застосування Fortinet Security Fabric.

*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 Plaform Navigator, Kuppingercole Compasses, Gigaom Radar.

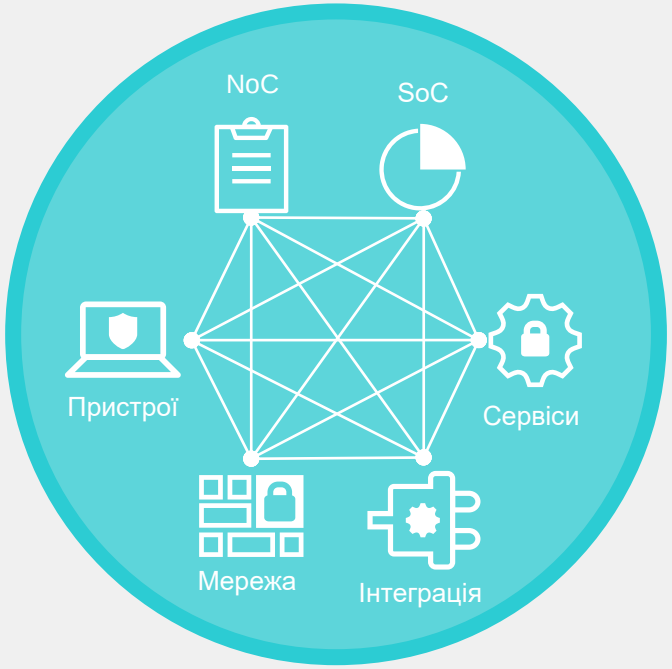
Основна складність

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

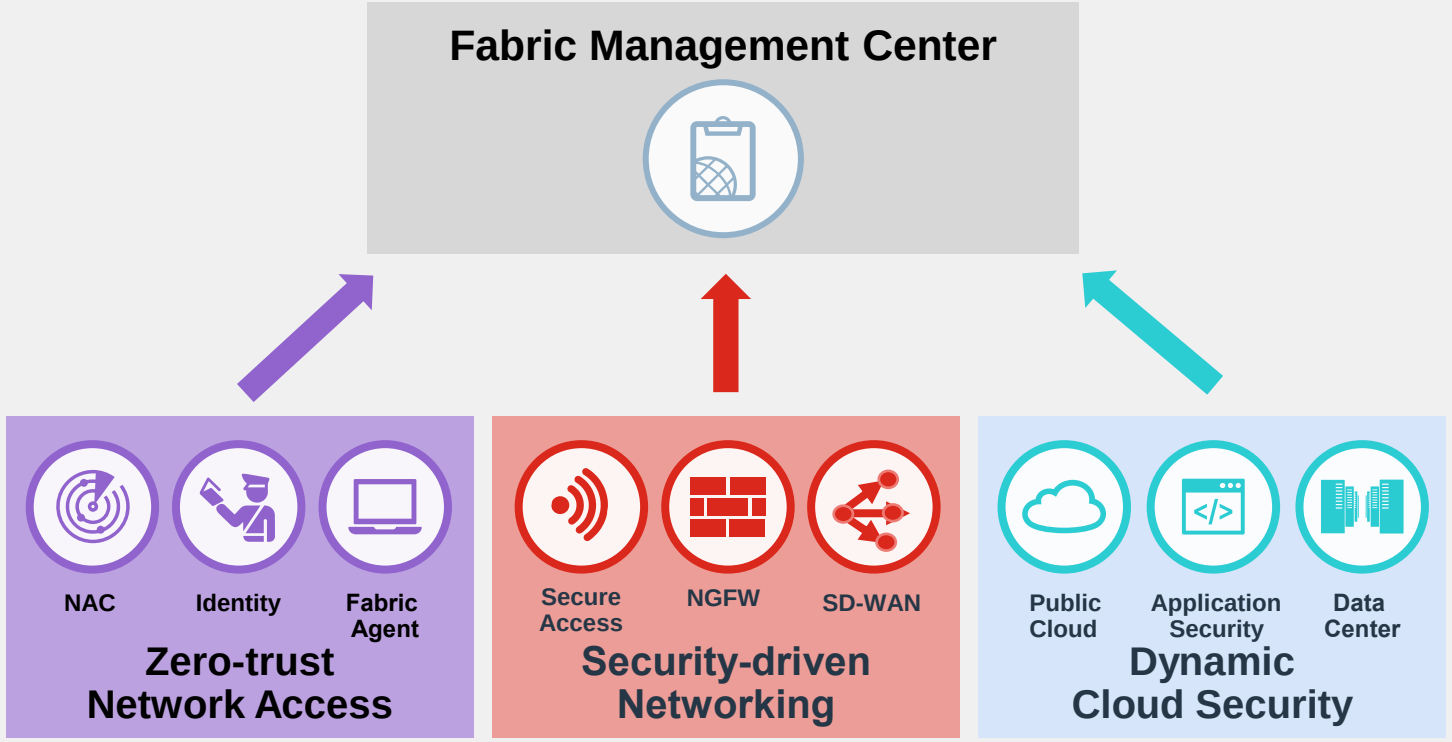
- Швидкий запуск in <6 хв (перевірено NSS labs)
- SD-WAN & NGFW шаблони
- Консоль централізованого керування
- DevOps Playbooks & Scripts
- Резервне копіювання з історією

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

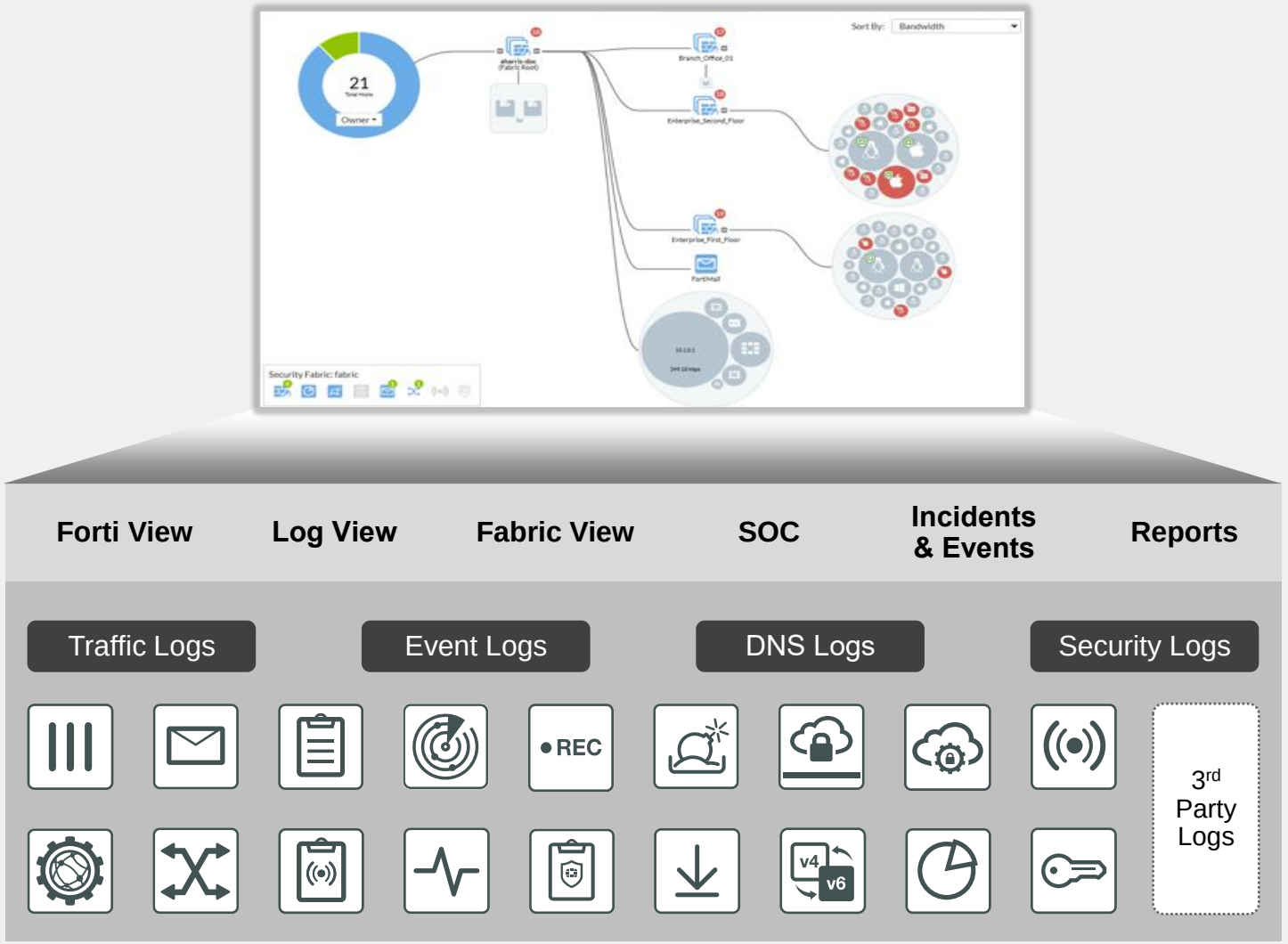


3. Аналітика

Мережа в реальному часі

Ключове

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

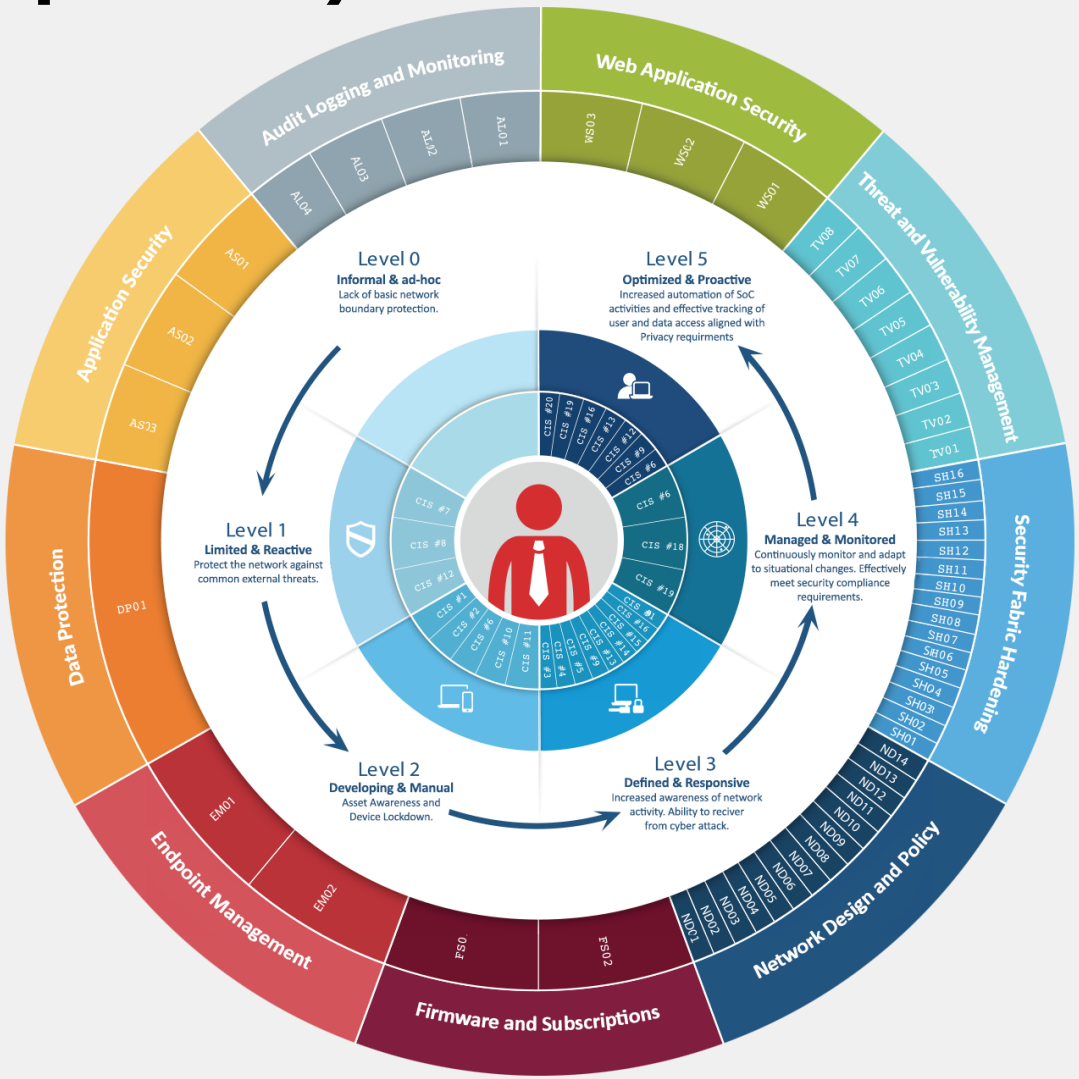


4. Звіти відповідності (Compliance)

Світові вимоги та best practice

Ключове

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

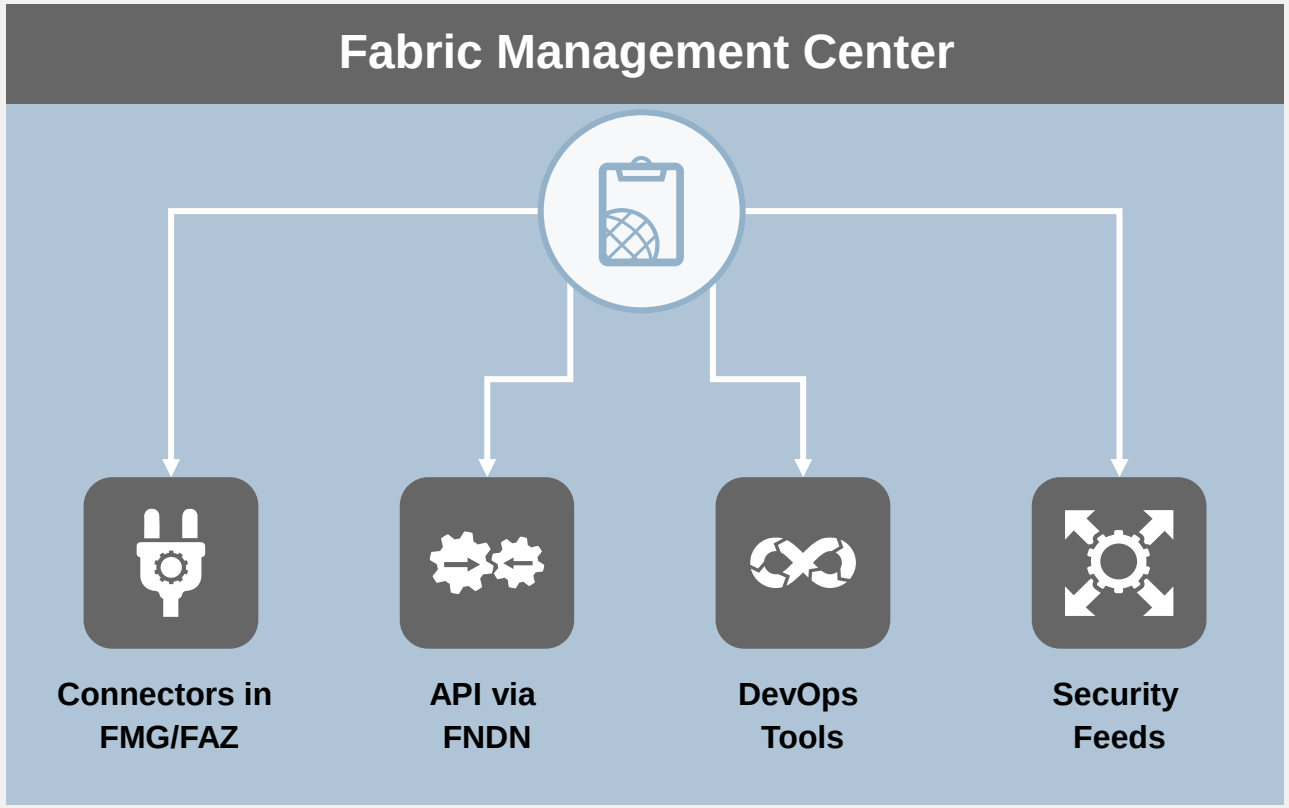


5. Автоматизація

Вбудовані механізми реагування

Ключове

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



FortiManager

Детальніше

FortiManager

Єдина консоль керування

Мережа

Керування пристроями та їх ліцензіями

Керування обладнанням філій

Моніторинг мережі

Безпека

Керування політиками безпеки

Керування FortiGuard Security

IPS AV ATP

Профілі безпеки

Автоматизація та оркестрація

Best Practice Шаблони

Rest API & Scripting

ANSIBLE Terraform

Розширення Fabric Management

FortiAIOps

FortiWLM

FortiSOAR

FortiSignature Converter

FortiAnalyzer

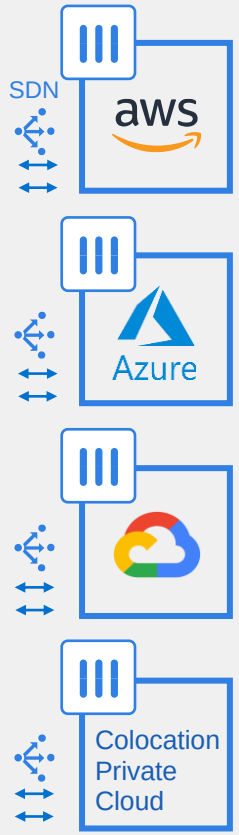
FortiView

Log View

Compliance Reporting

FortiSOC

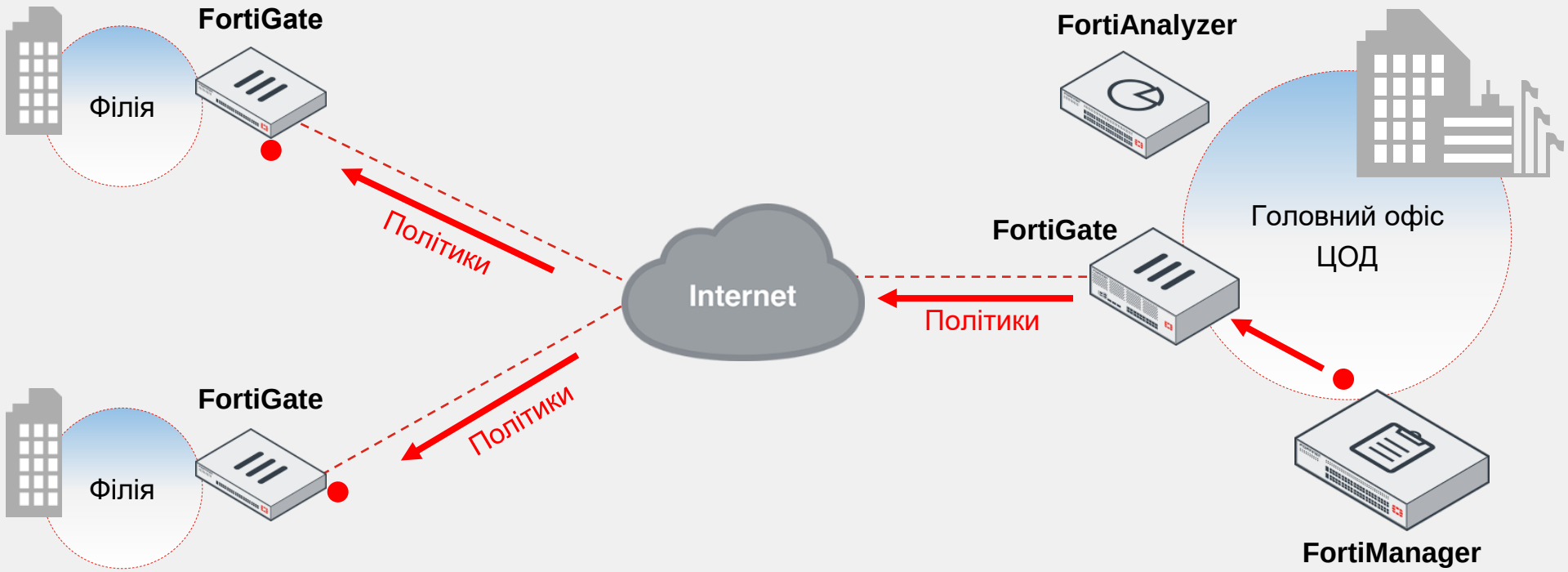
Security Incident & Events



Ключове в Centralized Management

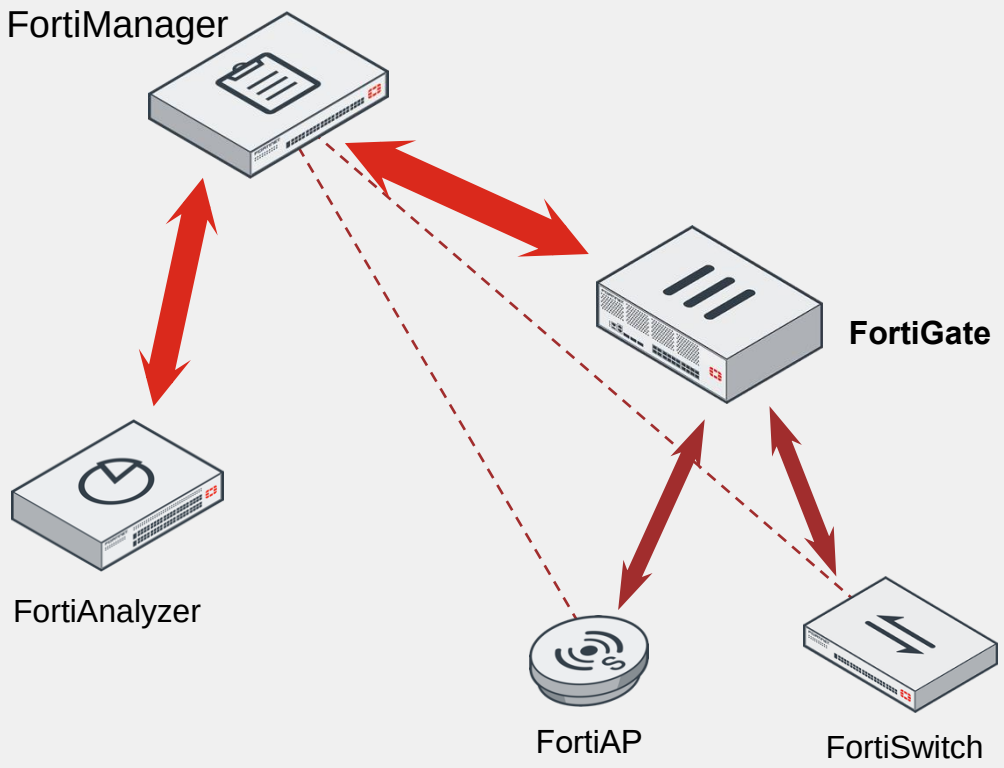
Централізоване керування:

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

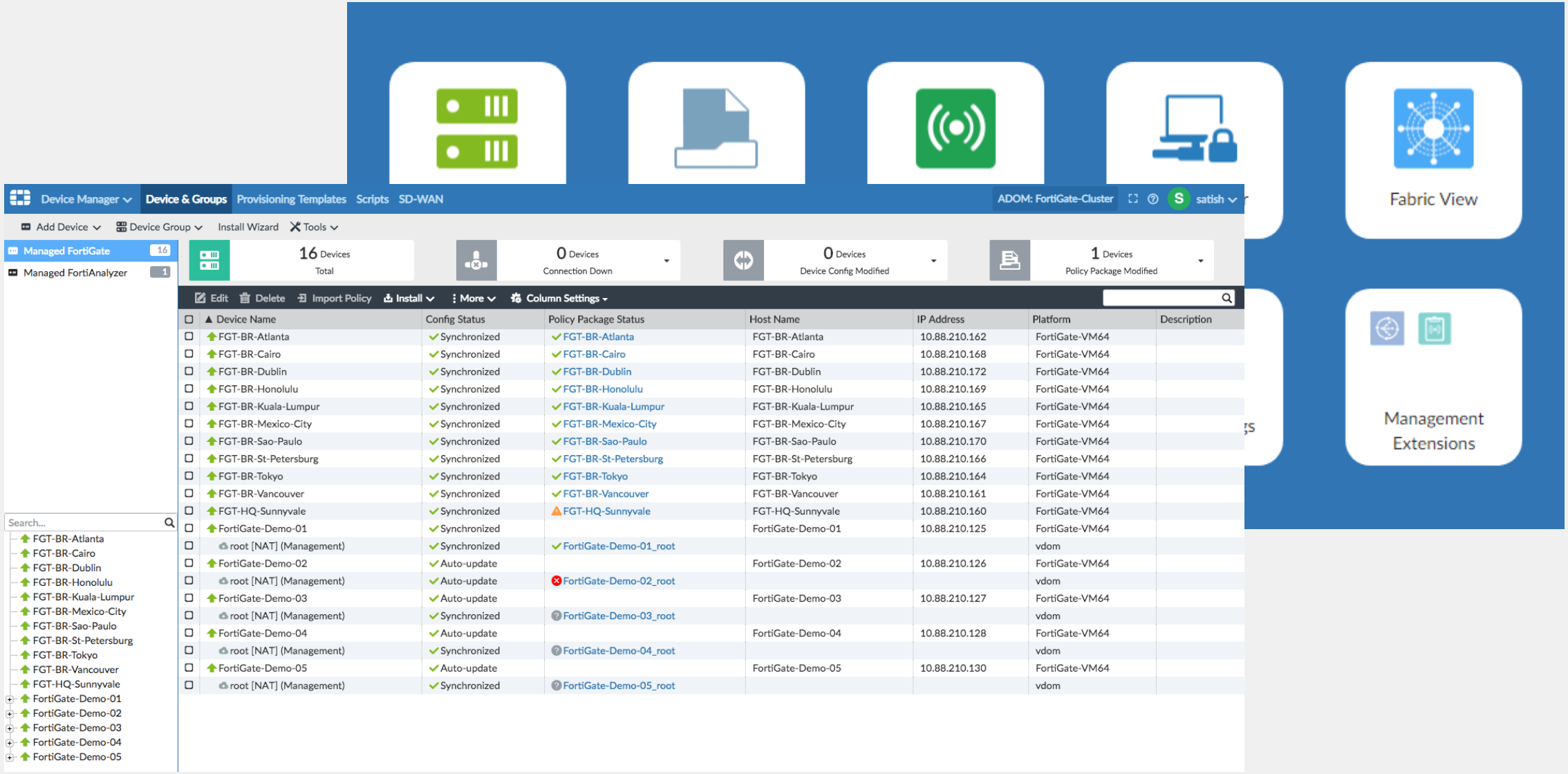


Security Fabric Management. Роль FortiManager

- Спрощення керування економить час та зменшує помилки
- ForitGate
  - 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 FortiAnalyzer
- FortiSwitch, FortiAP
  - FortiManager налаштовує обладнання через FortiGate
  - Налаштування за допомогою шаблонів FortiManager



Централізоване керування

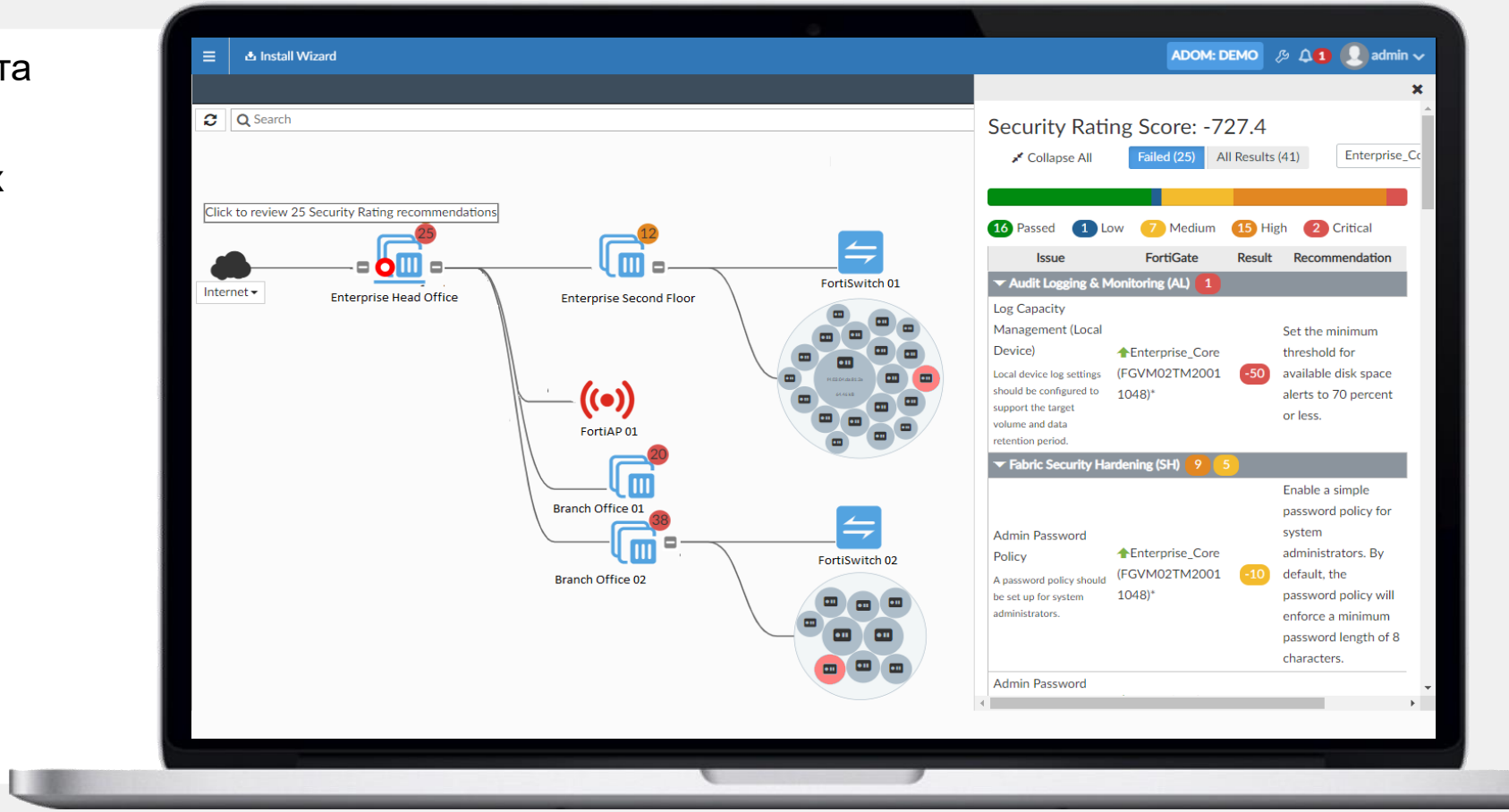


Мережа

Одна консоль для керування та звітності всієї мережі

FortiManager

- **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)

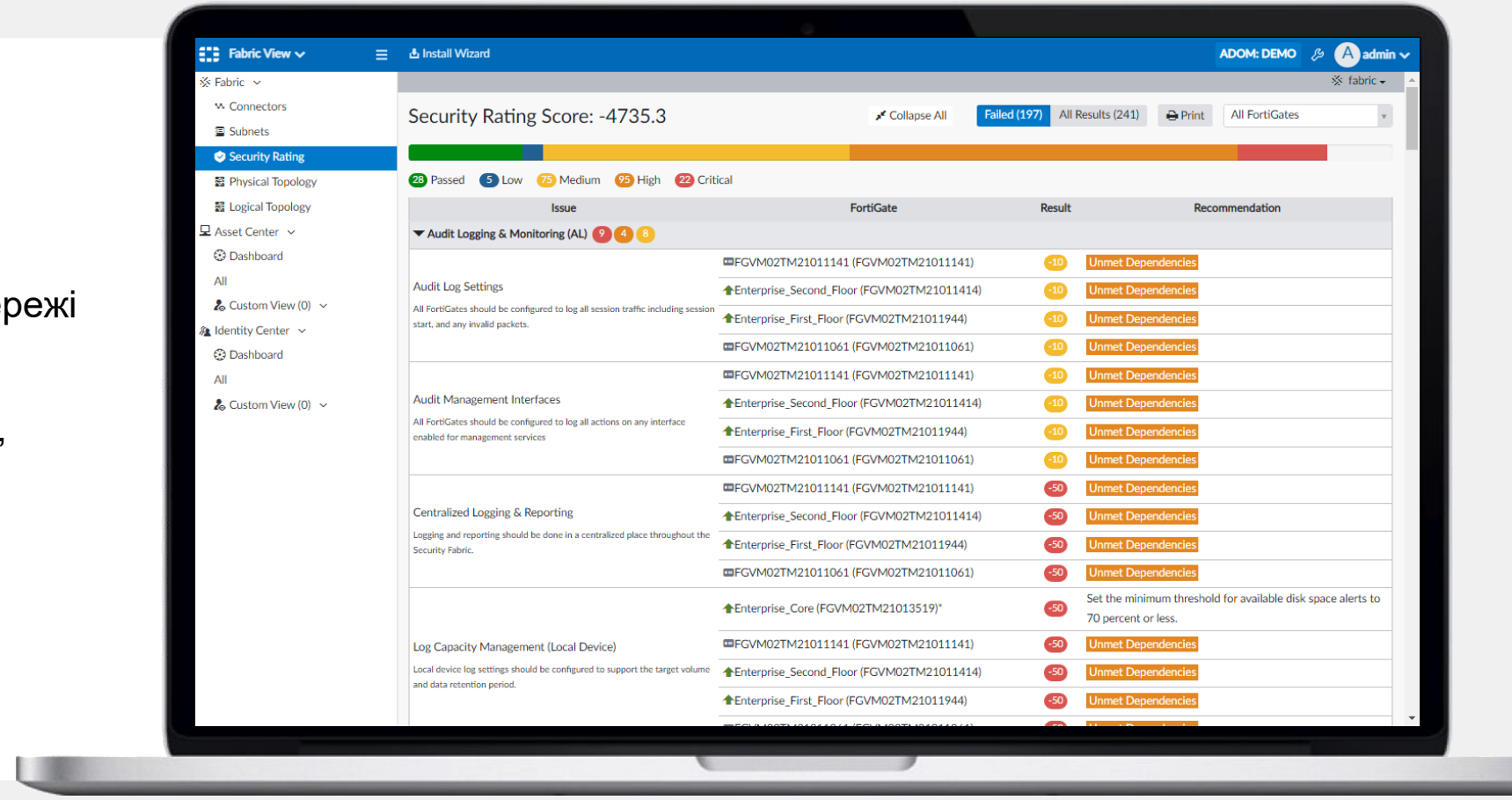


Безпека згідно світових стандартів

Звітність та відповідність вимогам

FortiManager

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

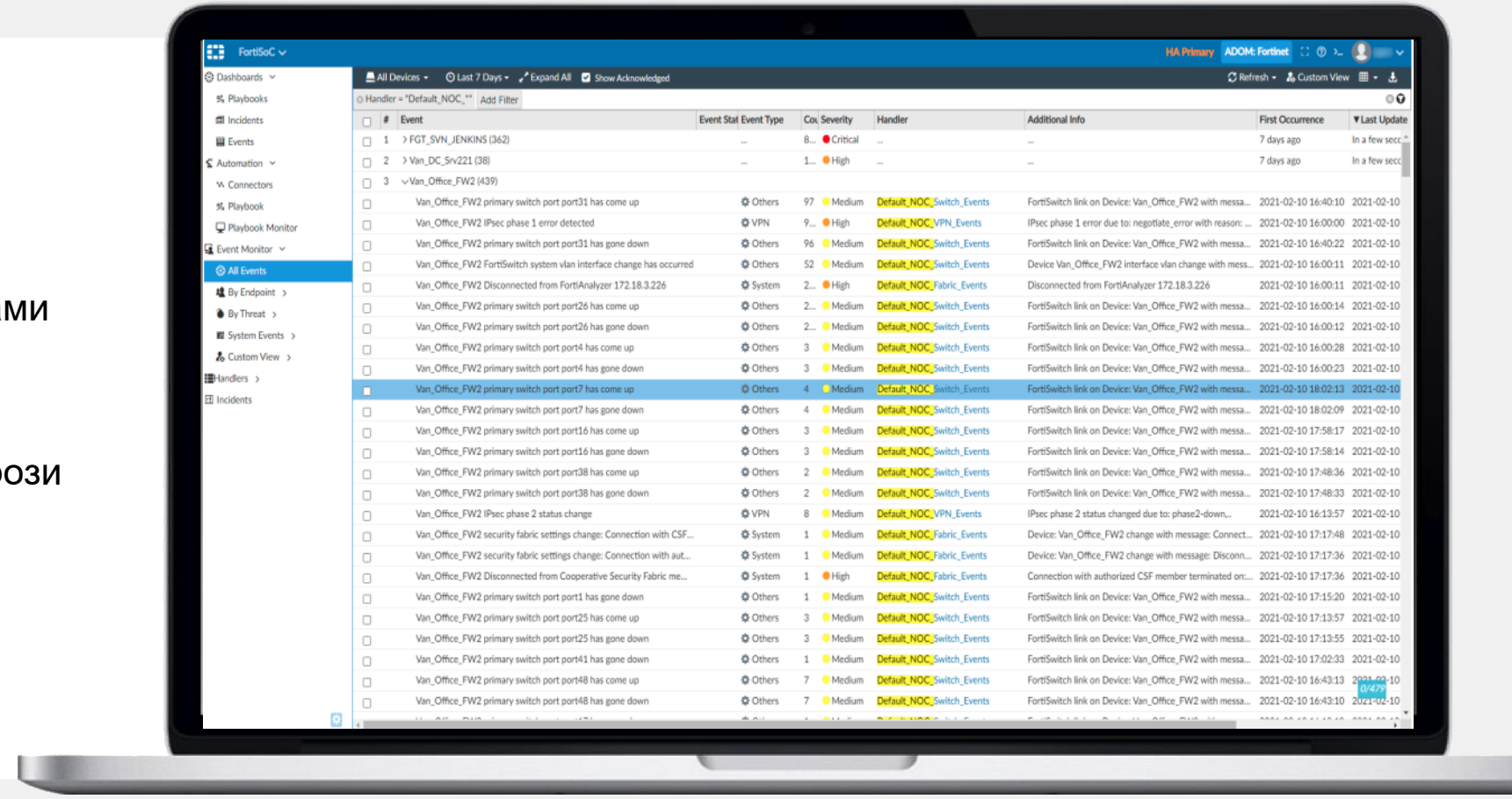


Автоматизація робочих процесів

Автоматизація та інтеграція

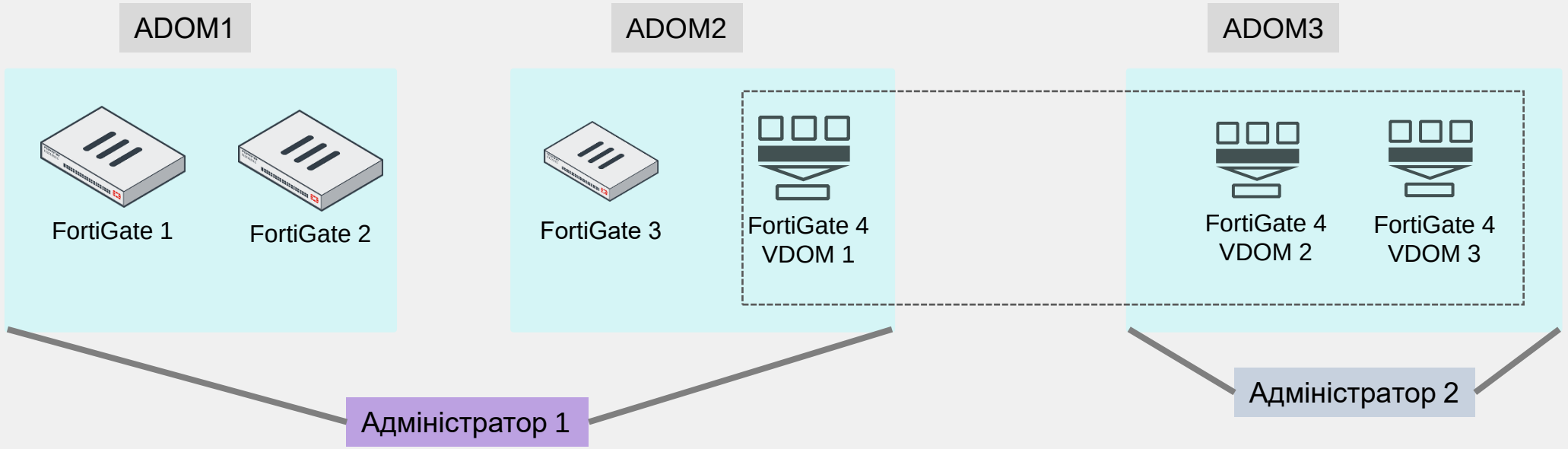
FortiManager

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



Підтримка розділення (ADOMs)

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



Адміністратор 1
керує пристроями в ADOM1 та ADOM2

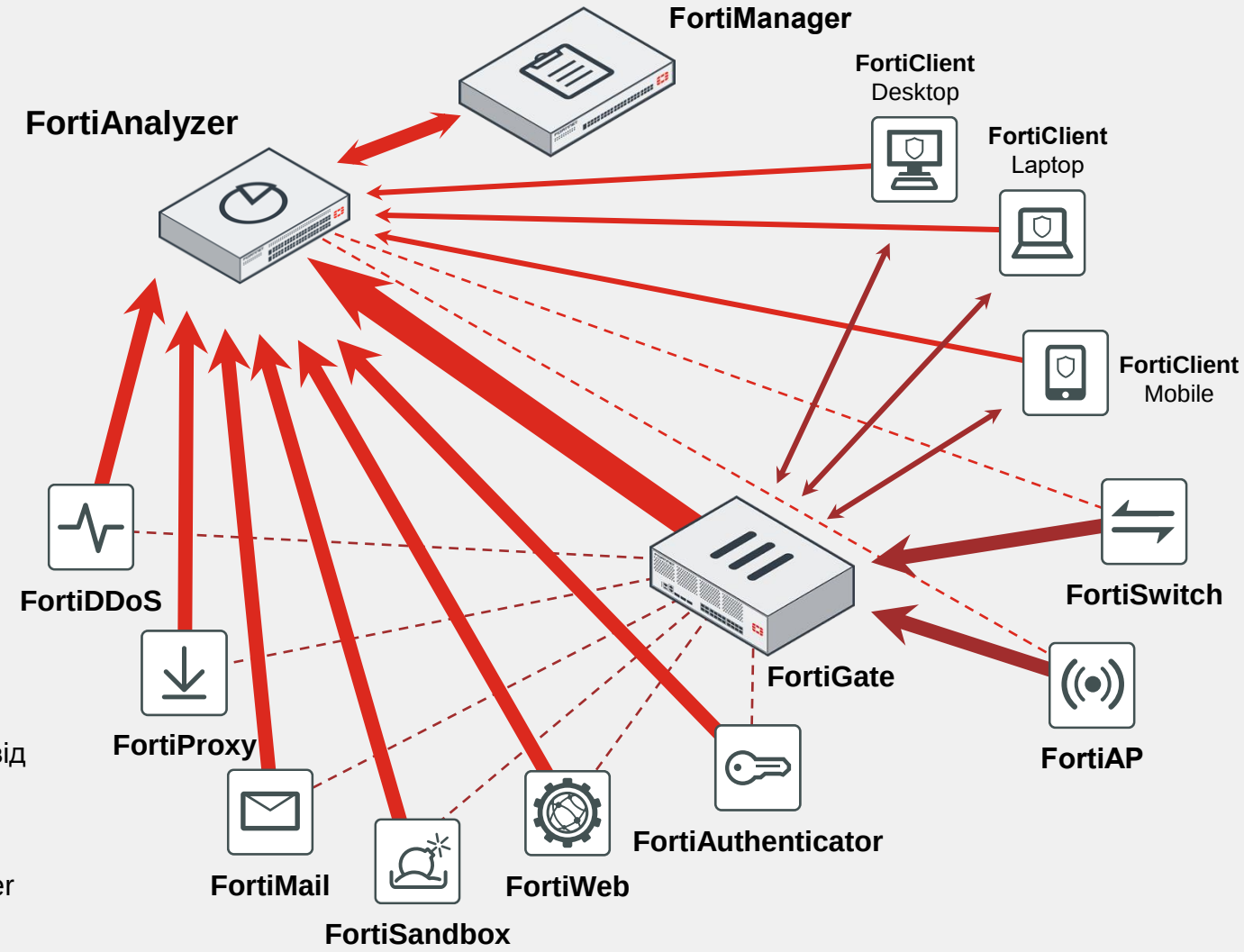
Адміністратор 2
керує пристроями в ADOM3 котрі
складаються з певних VDOM FortiGate4

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 отримає 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 допомогоюFortiManager 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

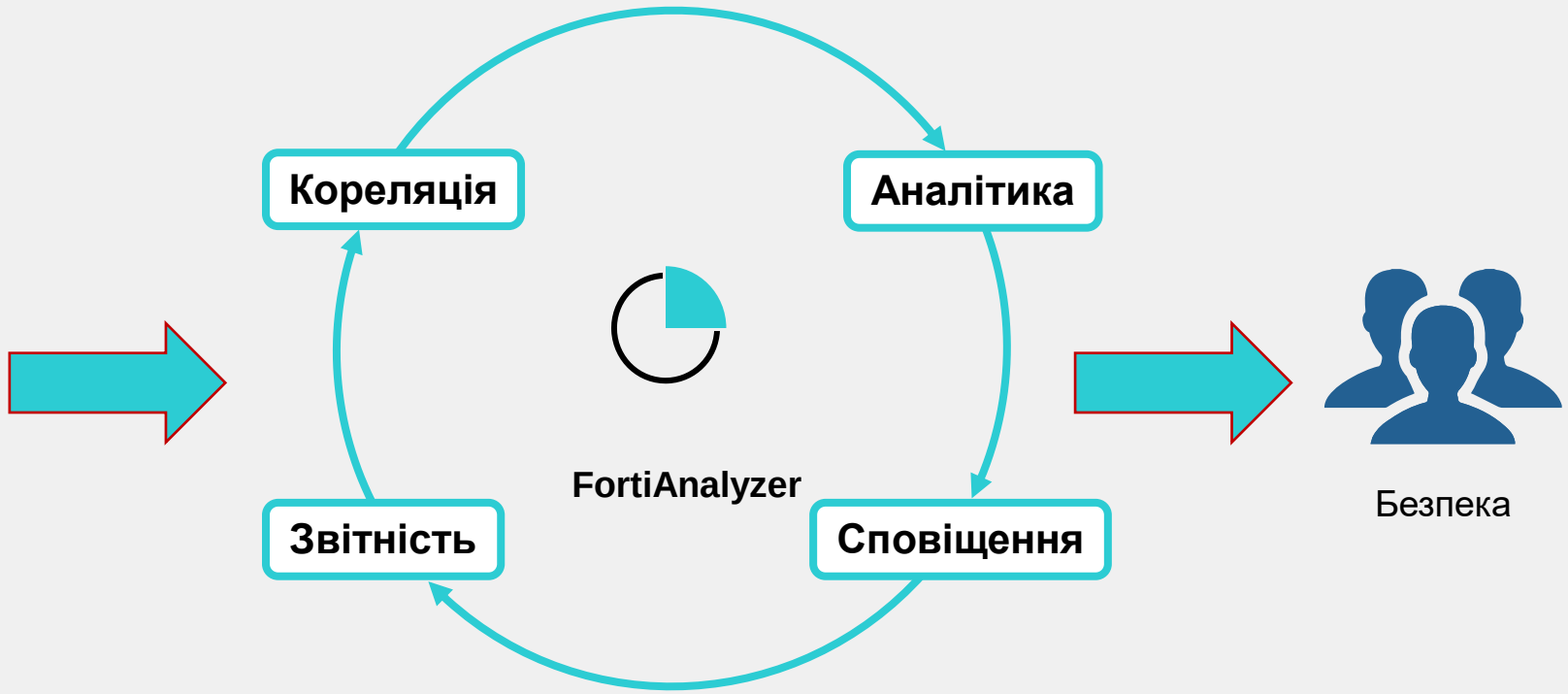
DHCP & DNS

AAA, RADIUS & AD

Database

Web Application

…and more

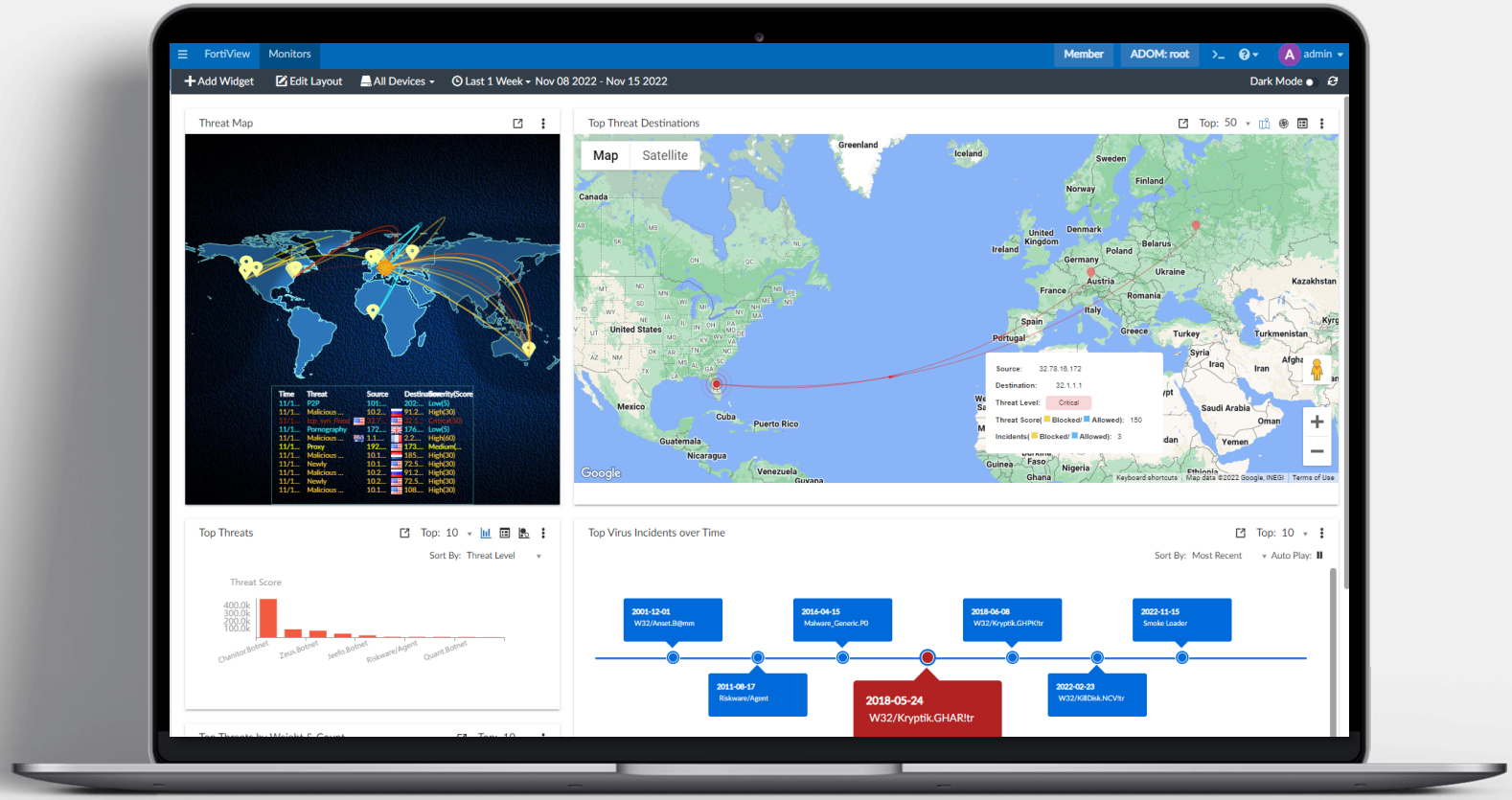


Моніторинг в реальному часі

FortiView

Бачити все

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

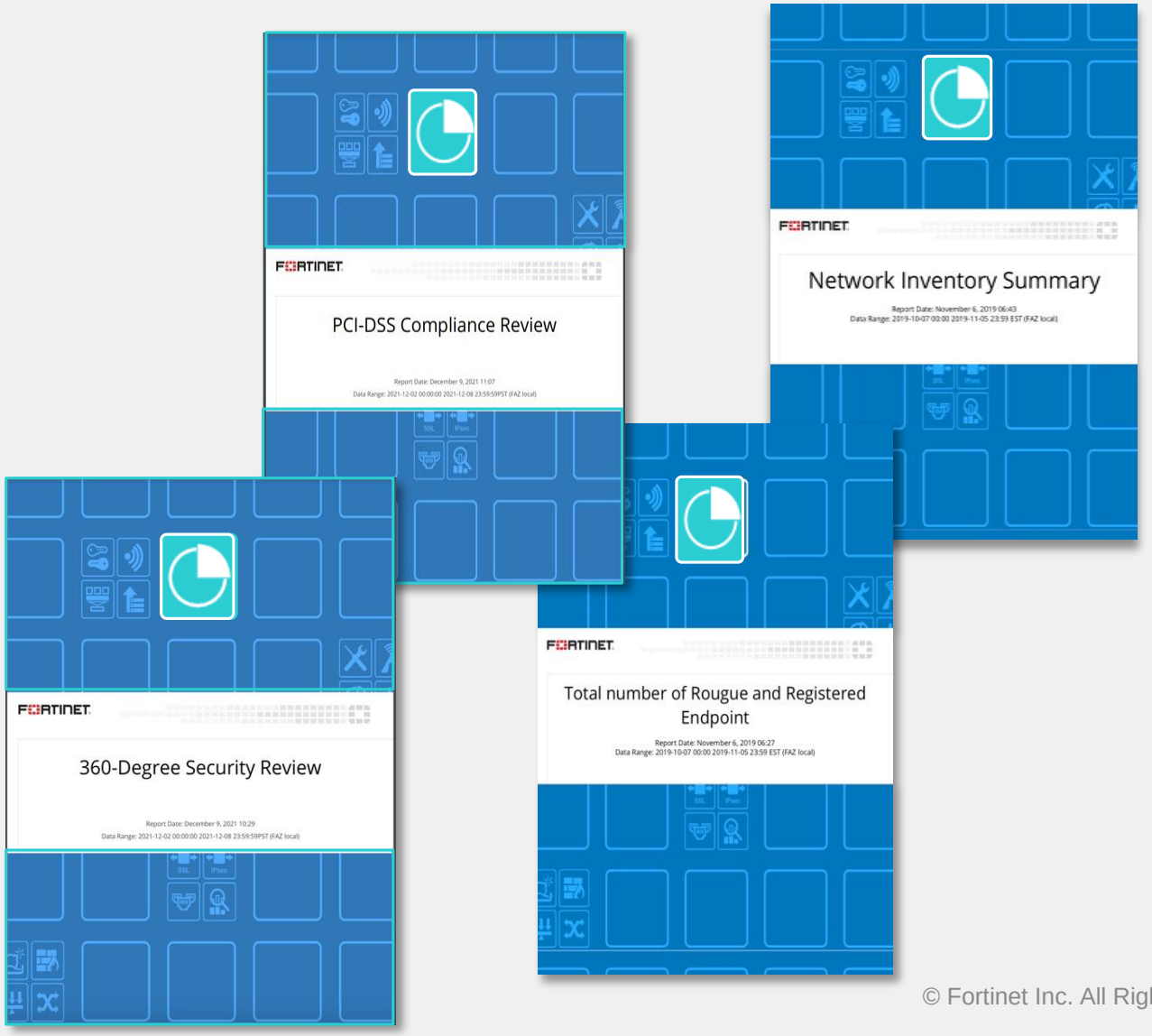


Звіт в пару кліків

Сотні готових звітів

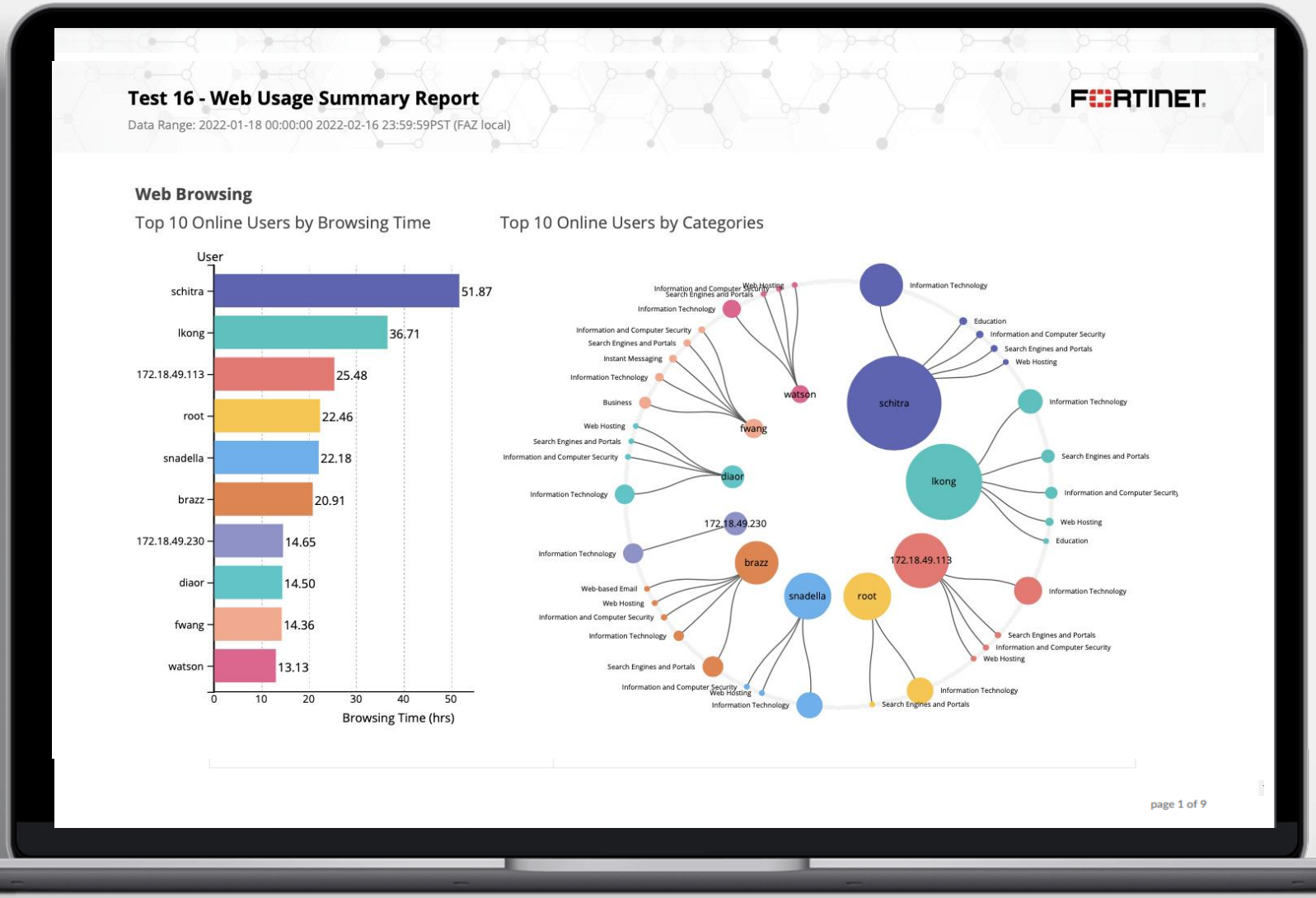
Готові звіти

- 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)



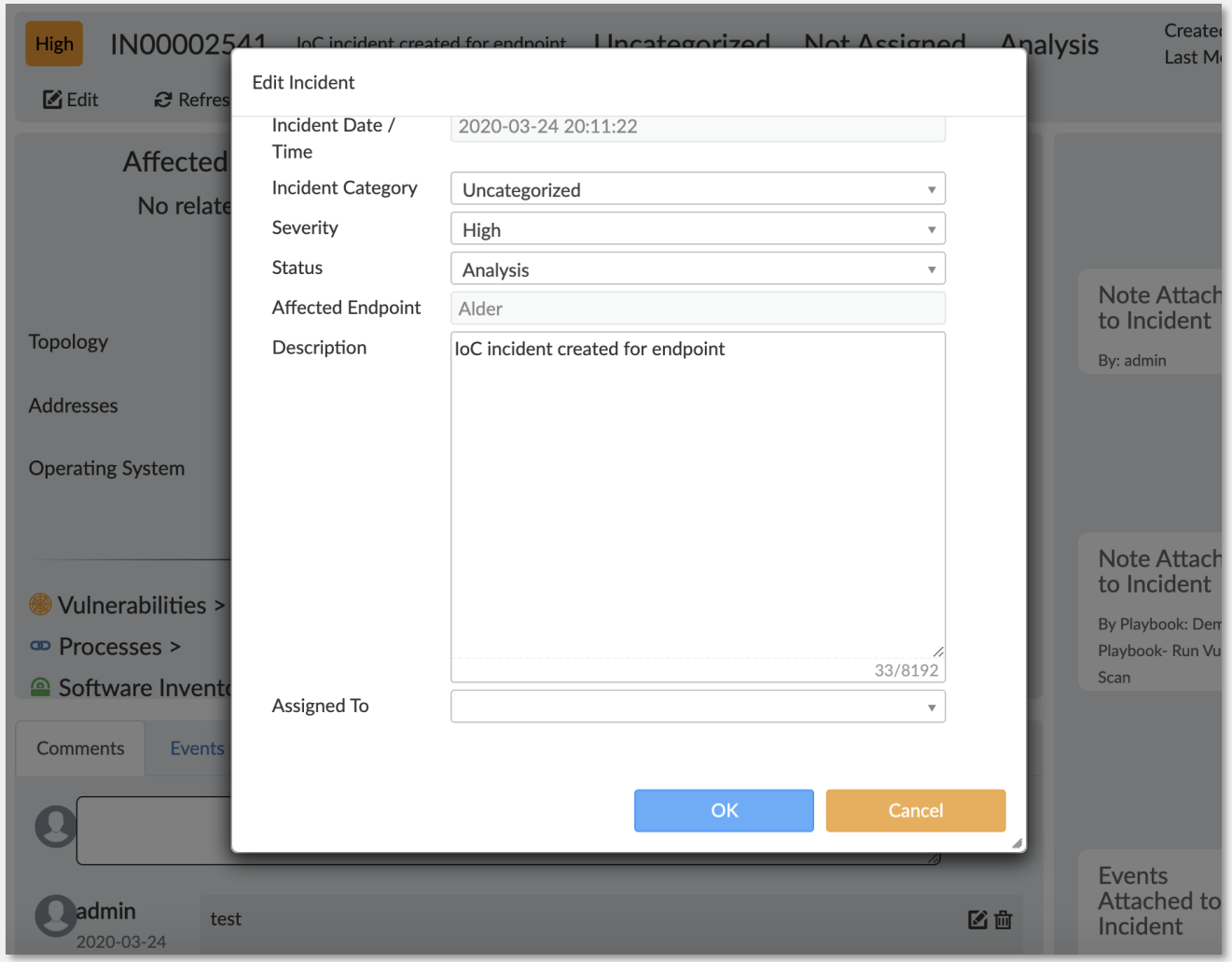
Improve Operations

- 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

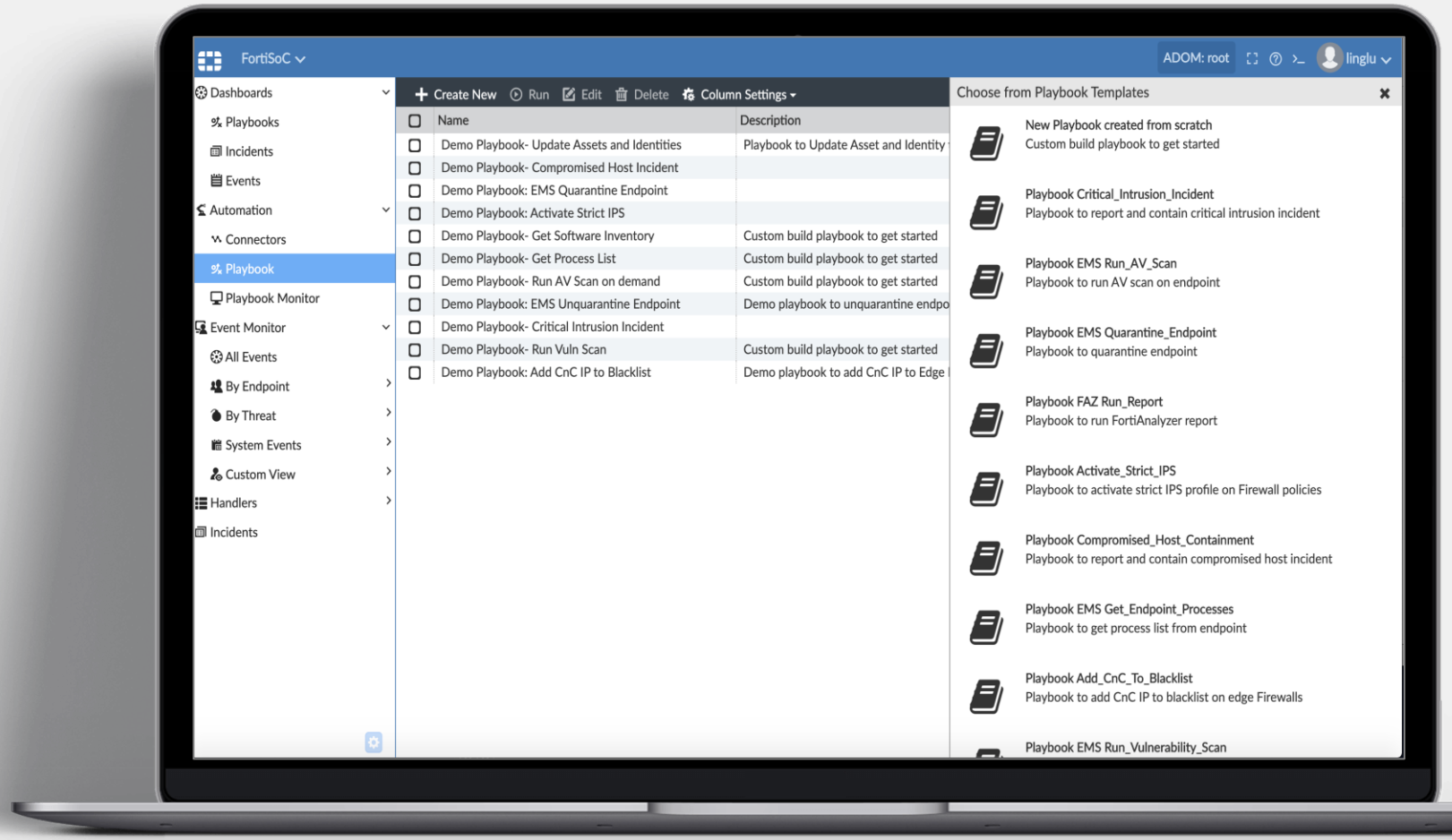


Готові до автоматизації

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)

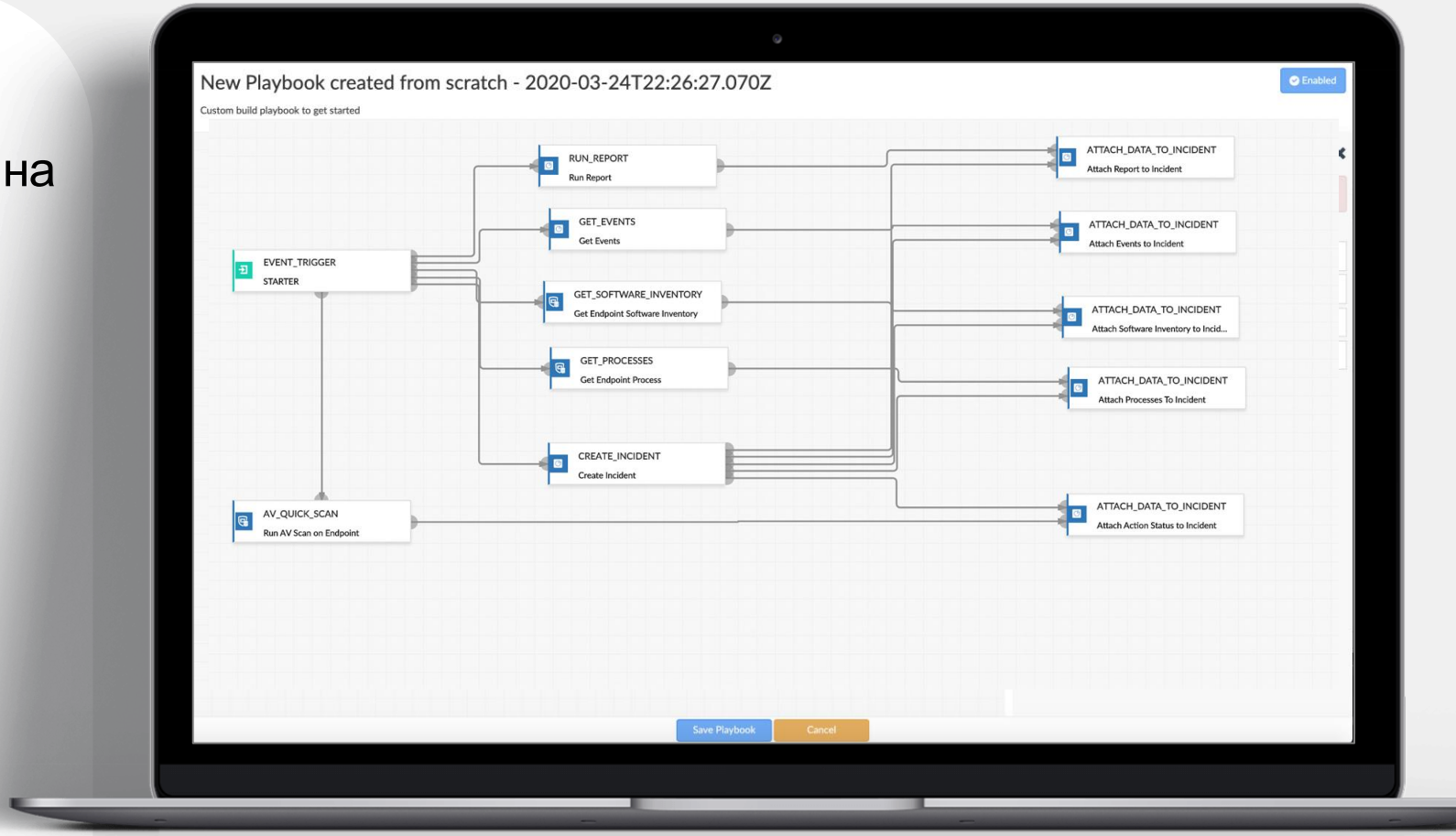


Автоматизація

Візуальне створення алгоритму дій

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

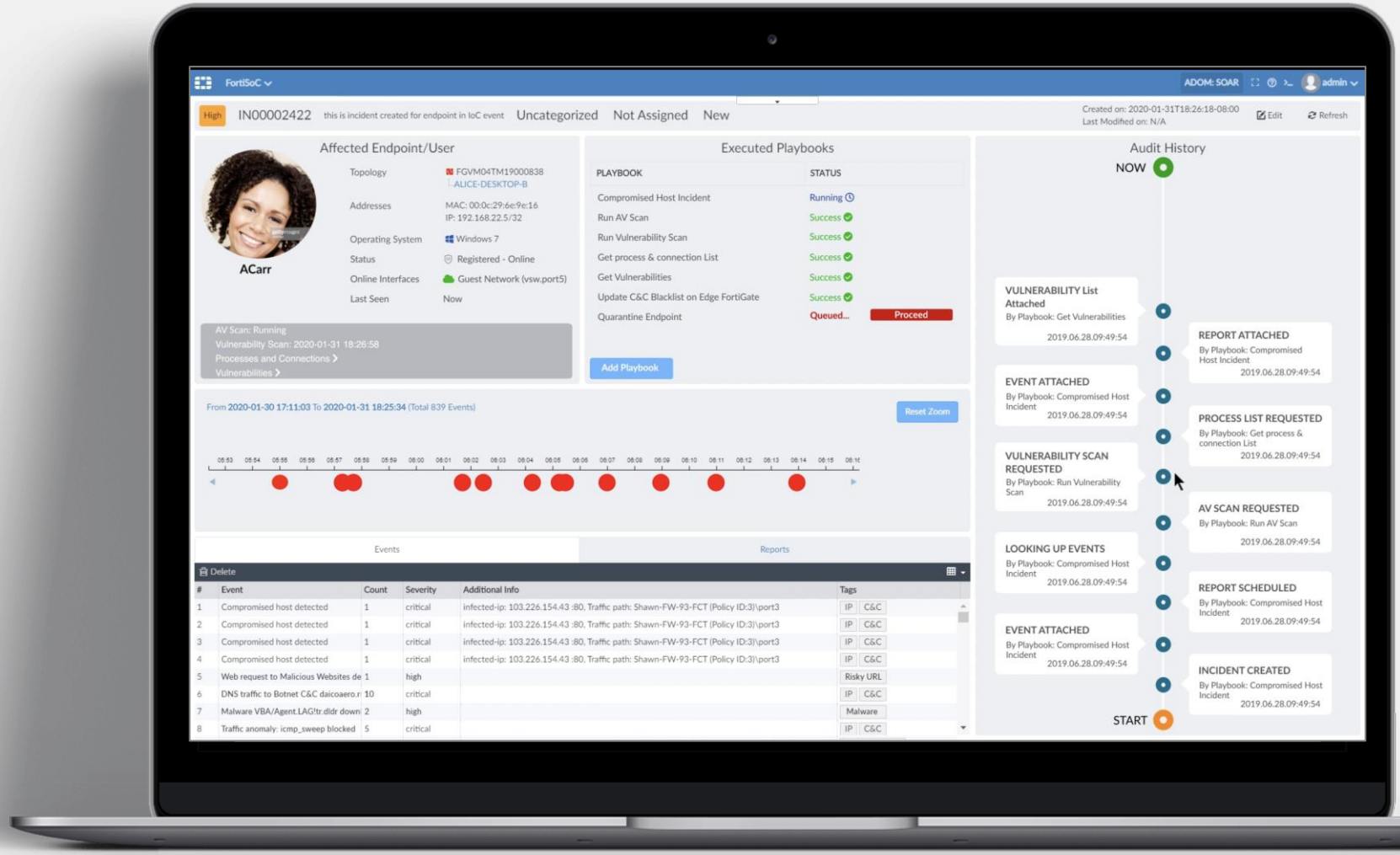
- Редагування/копія вбудованих сценаріїв чи створення власних
- Діаграма створеного сценарію дій
- Умова для старту сценарію
  - Подія
  - Інцидент
  - За розкладом
  - Ручний запуск



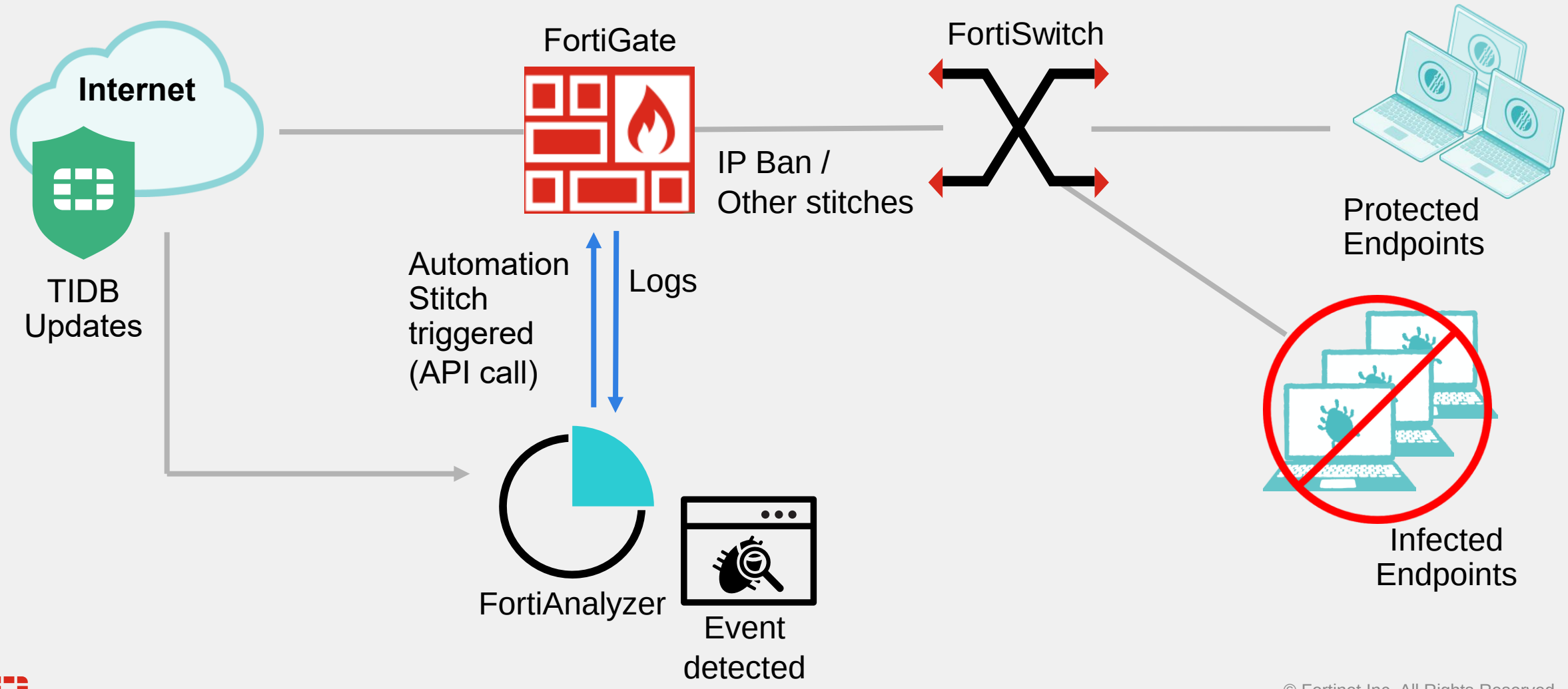
Автоматизація вирішення інцидентів

Автоматичні реакції на інциденти

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

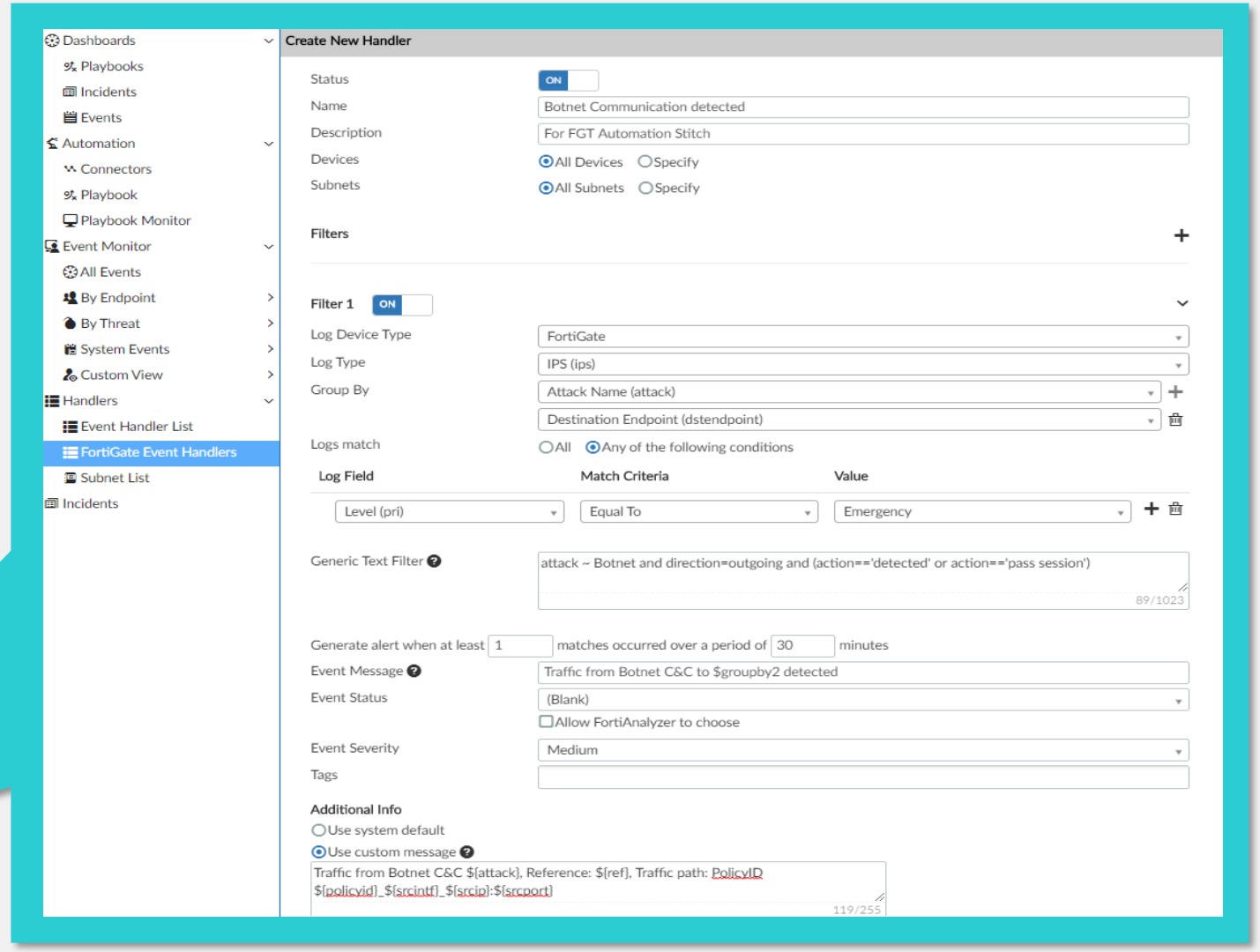


Fortinet Security Fabric Automation

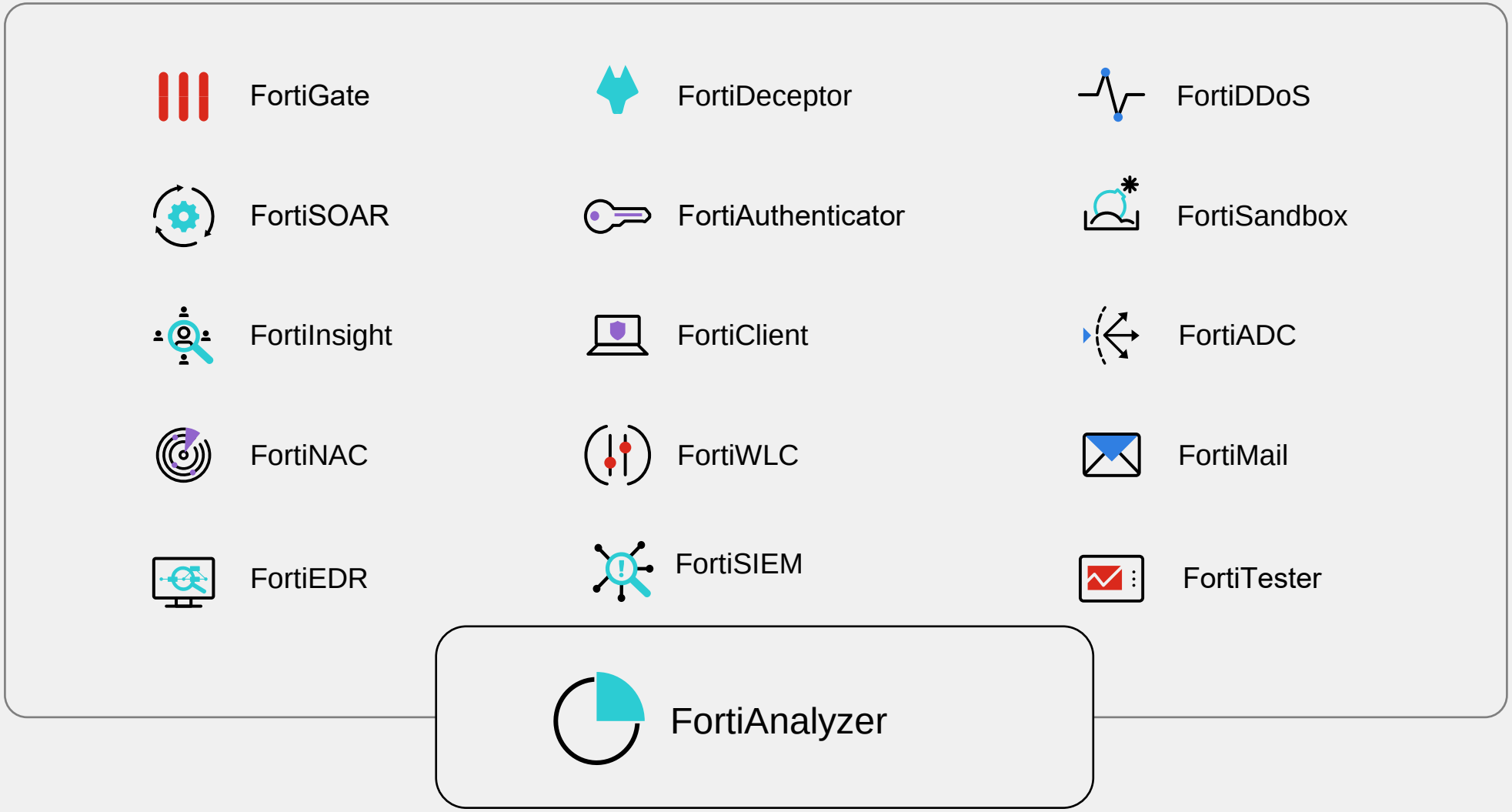


Аналіз та автоматична реакція

Створюйте свої події
та реакції на них



Інтеграція FortiAnalyzer



Інтеграція за межами Fortinet

Fortinet інтегрується з 500+ рішеннями інших виробників

Fabric Connectors

Розроблена Fortinet інтеграція автоматизує операції та політики безпеки

Microsoft Azure, Symantec, ORACLE, aws, nuagenetworks, openstack, vmware, servicenow, Google Cloud, cisco, IBM Cloud

Fabric APIs

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

OT/ IoT: NOZOMI NETWORKS, DRAGOS, CLAROTY

FinServ: splunk>, intel, EQUINIX, tufin, NVIDIA, servicenow

Healthcare/ Life Sciences & Pharma: ordr, asimily, ARMIS

Retail: ARISTA, AMD, Gigamon

SLED: vmware, NUTANIX, rubrik

+300 other Fabric-Ready Partners

Fabric DevOps

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

aws, ORACLE, HashiCorp, Microsoft Azure, Alibaba Cloud, Google Cloud, Red Hat, refactr, openstack, vmware

Extended Ecosystem

Інтеграція з іншими технологіями та відкритими системами

cisco, paloalto NETWORKS, Hewlett Packard Enterprise, CROWDSTRIKE, vmware

Як ознайомитись?

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

Fortinet Product Demos

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

FortiADC Demo

FortiAnalyzer Dem

FortiAuthenticator Demo

FortiClient EMS De

FortiGate-CGN Demo

FortiGate IPS Demo

FortiGate Secure Web Gateway Demo

FortiGate-VM Demo

FortiMail Demo

FortiManager Demo

FortiNAC D

FortiSandbo

FortiWeb Demo

FortiWLM Demo

FortiSOAR Demo

FortiNDR Demo

FortiEDR Demo

FortiTester Demo

FortiExtender Demo

LAN Edge Demo

FortiCNP Demo

FortiAIOps Demo

FortiAnalyzer Demo

https://www.fortinet.com/demo-center/fortianalyzer-demo

InPrivate (2)

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