



FortiAnalyzer як засіб забезпечення видимості та автоматизації

Євгеній Таран, Systems Engineer

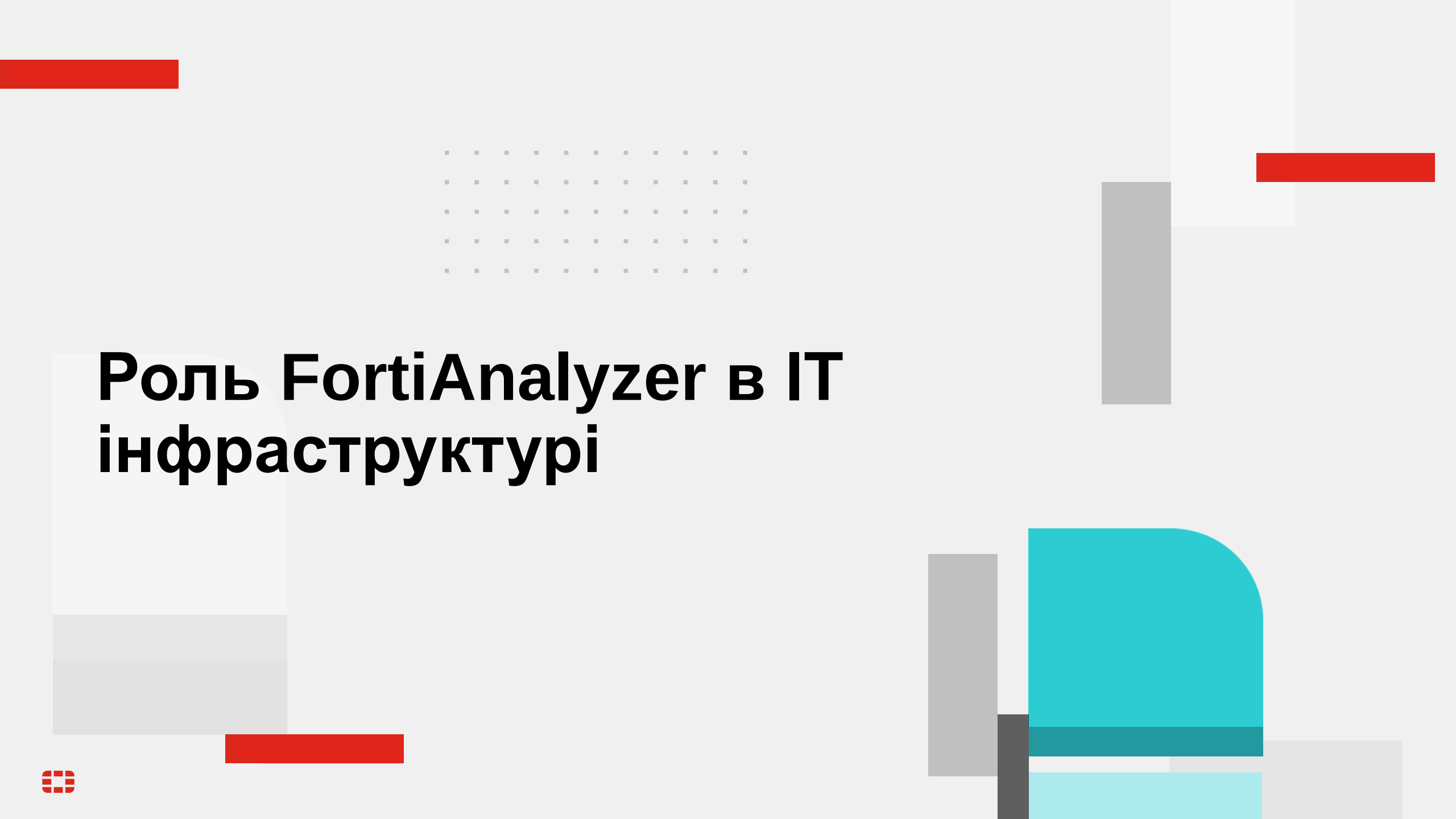
ytaran@fortinet.com

Таран Євгеній

- 15 років в IT
- останні 8 років будую/модернізую IT інфраструктури та змушую веб сервіси працювати «як має бути» 😊
- IT системи міжнародних заходів (спортивні змагання, вибори тощо)
- Досвід роботи в 10 країнах регіону
- Fortinet NSE 7

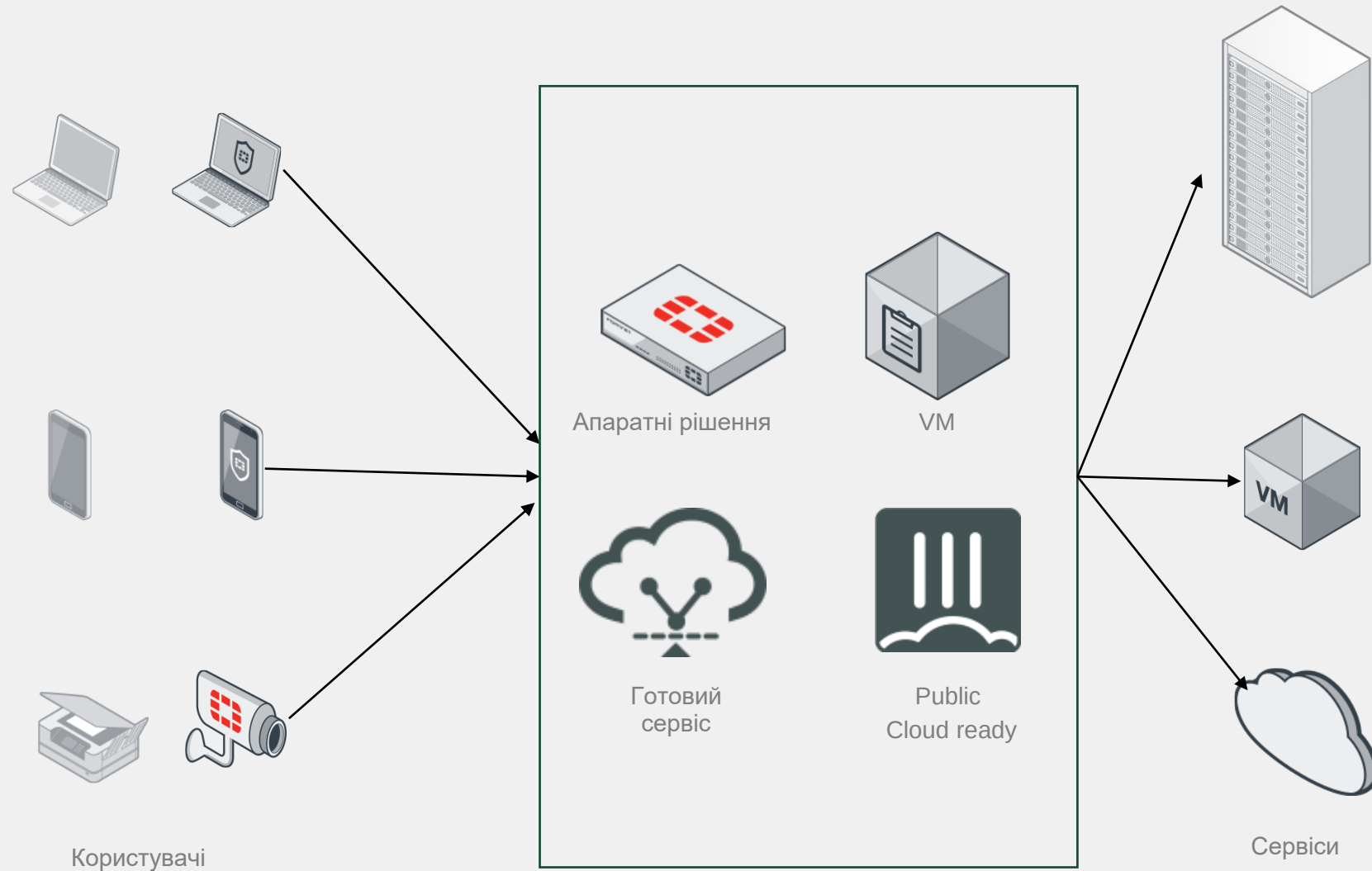
P.S. Це моя друга кібервійна...





Роль FortiAnalyzer в IT інфраструктурі

Гібридні мережі



Вимоги

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

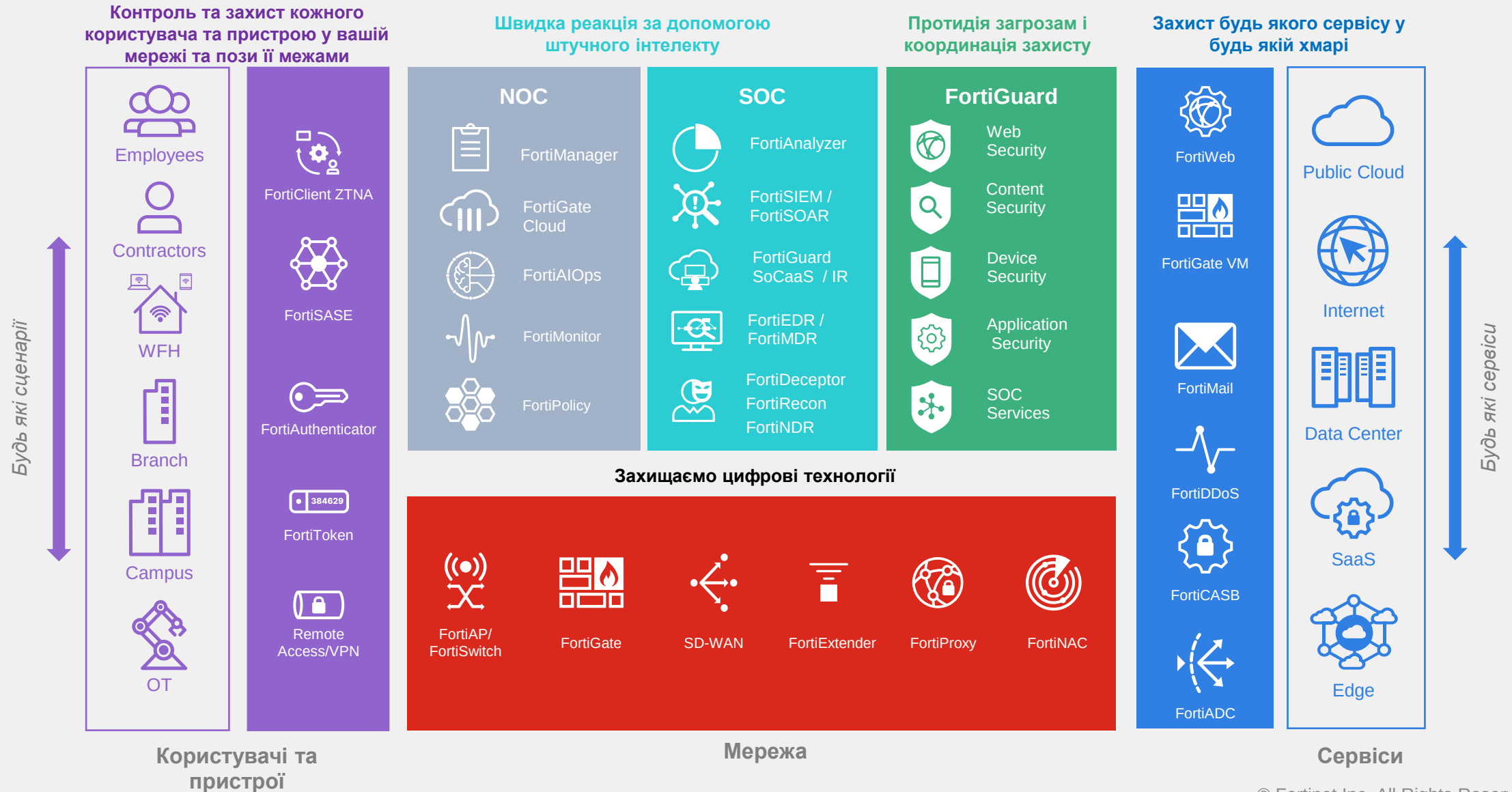
Гібридні мережі



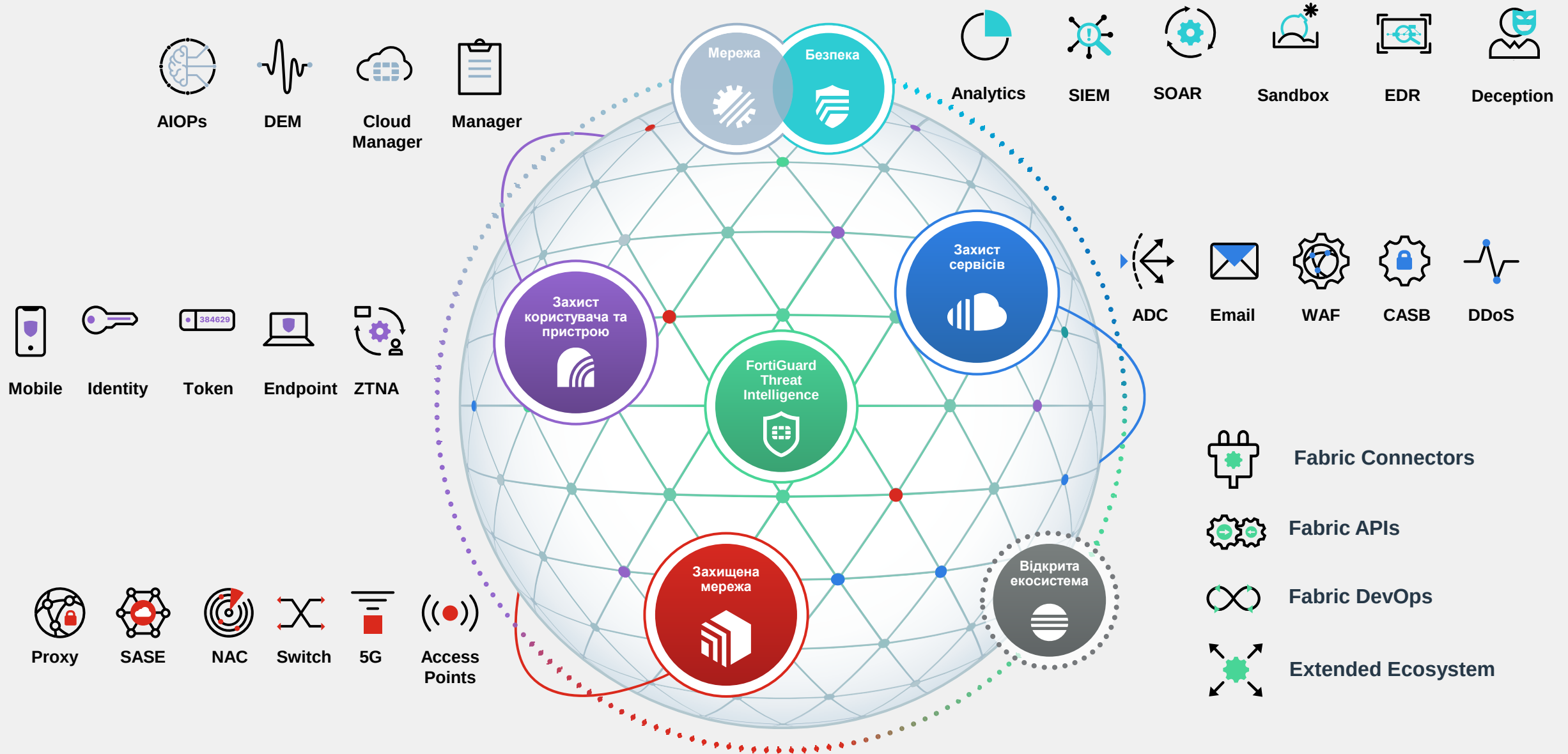
Сучасні реалії

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

Коротко про портфоліо Fortinet

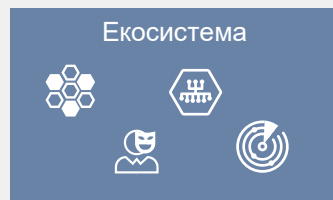
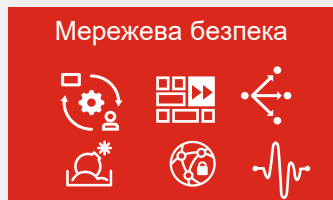
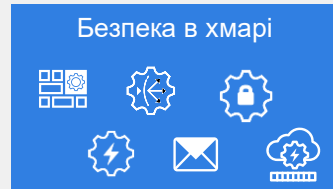
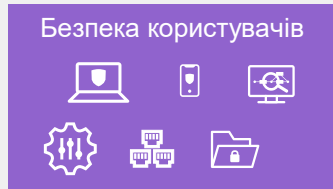
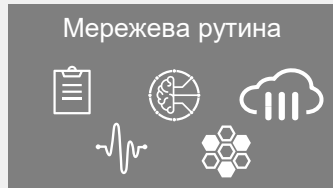


Fortinet Security Fabric

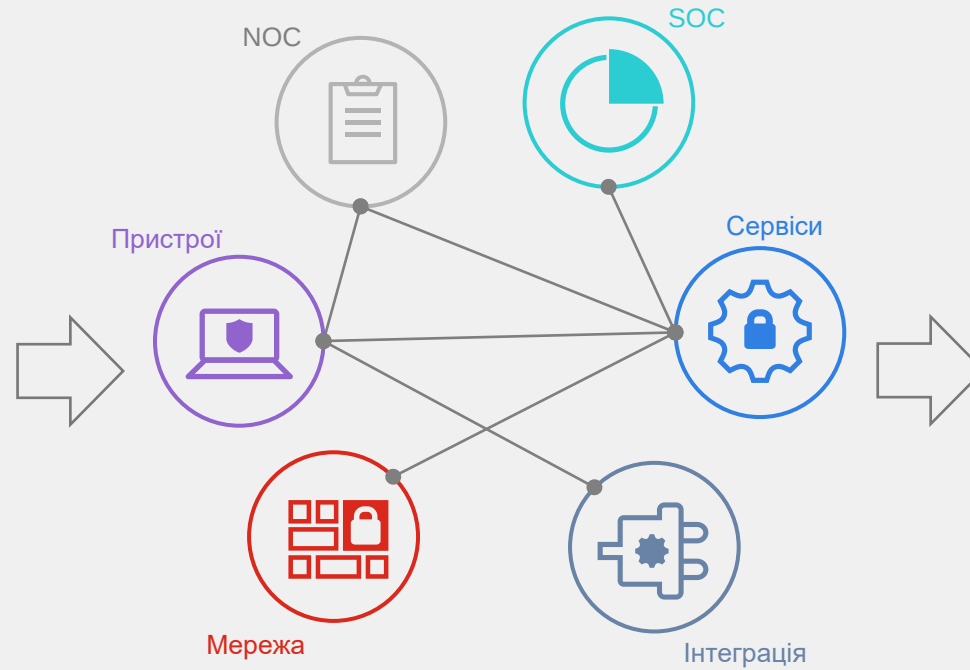


Основна складність

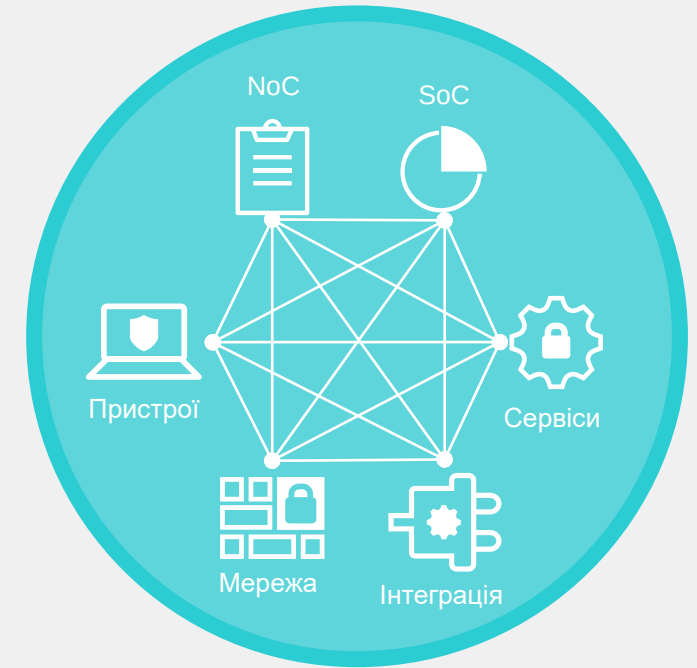
30+ виробників



10 виробників



2-3 платформи

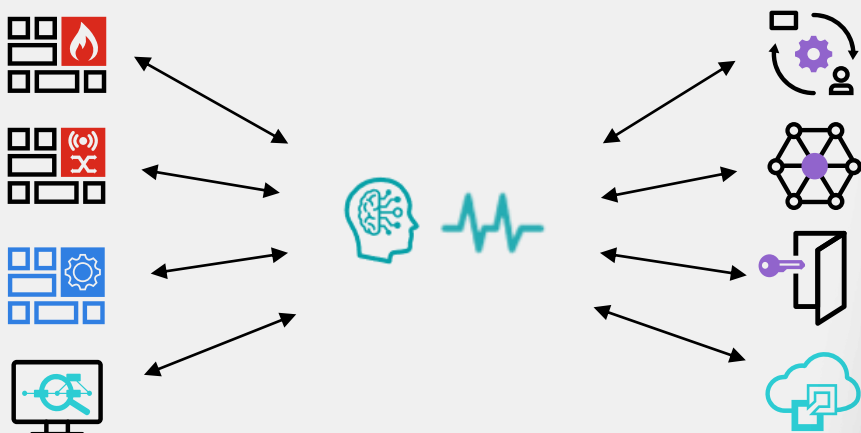


Еволюція



Аналітика та автоматизація з FortiAnalyzer

Нормалізована аналітика даних з використанням AI для виявлення інцидентів

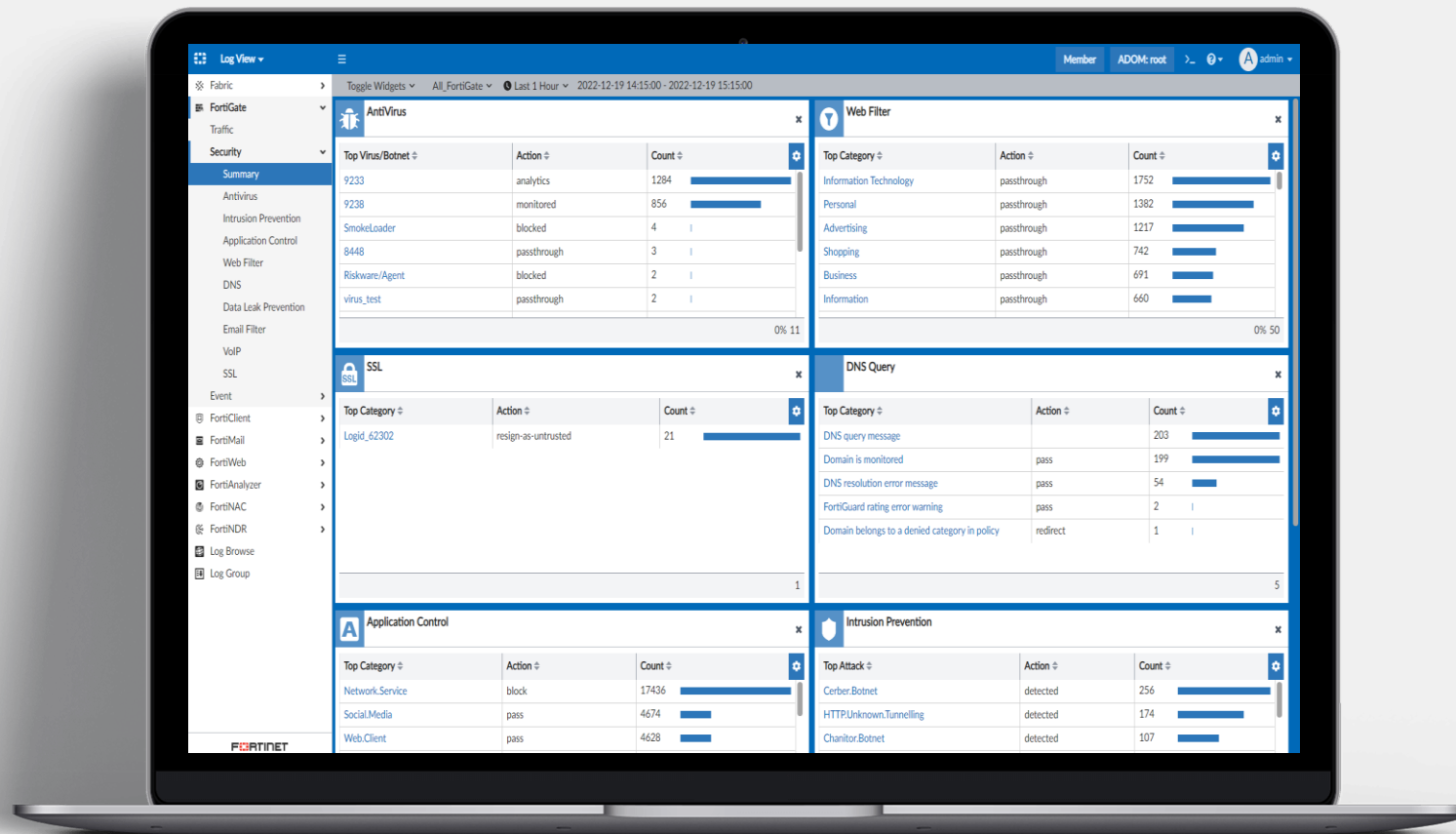


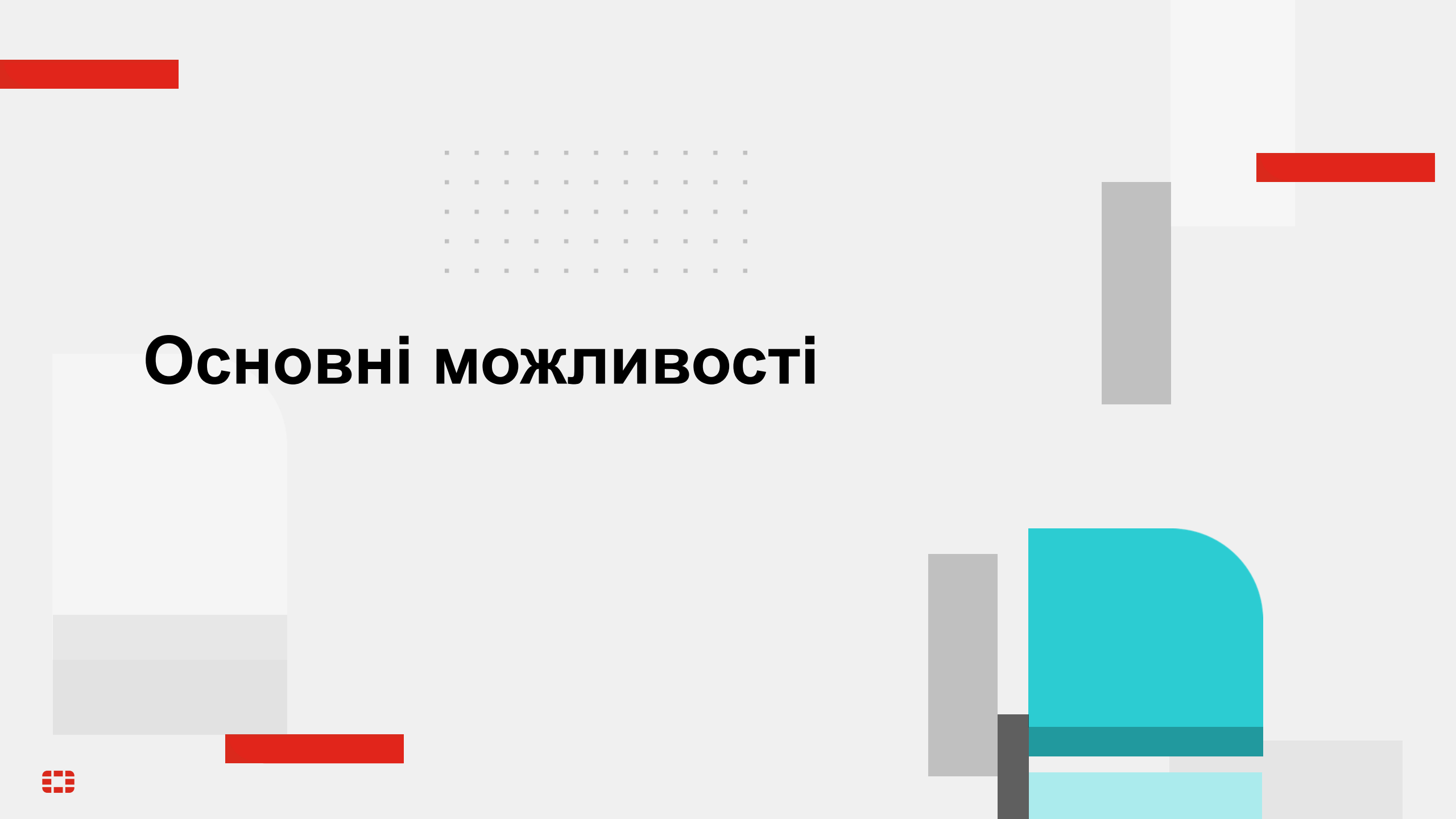
Видимість подій

Автоматична реакція

Детектування відомих атак

Компонент побудови SOC





Основні можливості

FortiAnalyzer

Погляд з іншої сторони

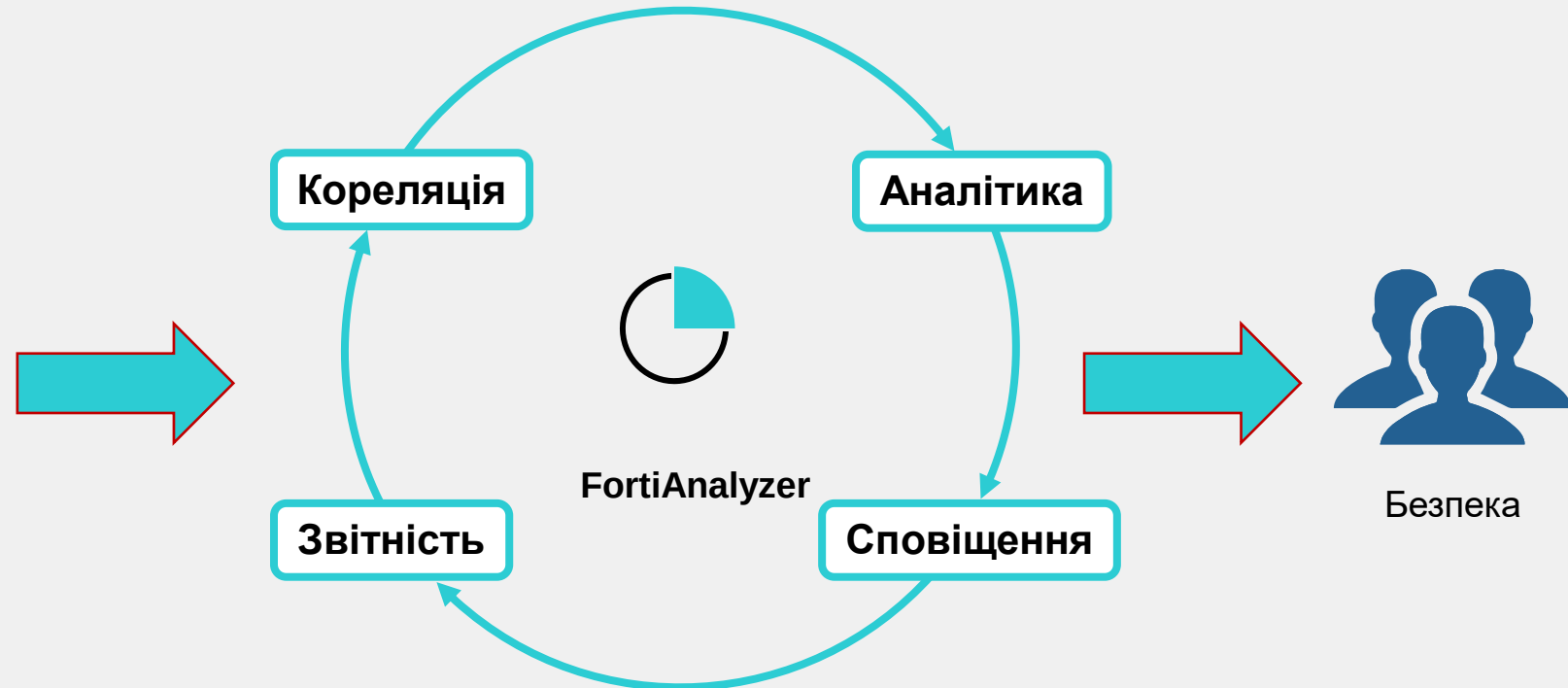
Мережеві пристрої

Firewall & IPS
Router & Switch
Wireless LAN
NetFlow

Сервіси та сервери

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

...і багато іншого

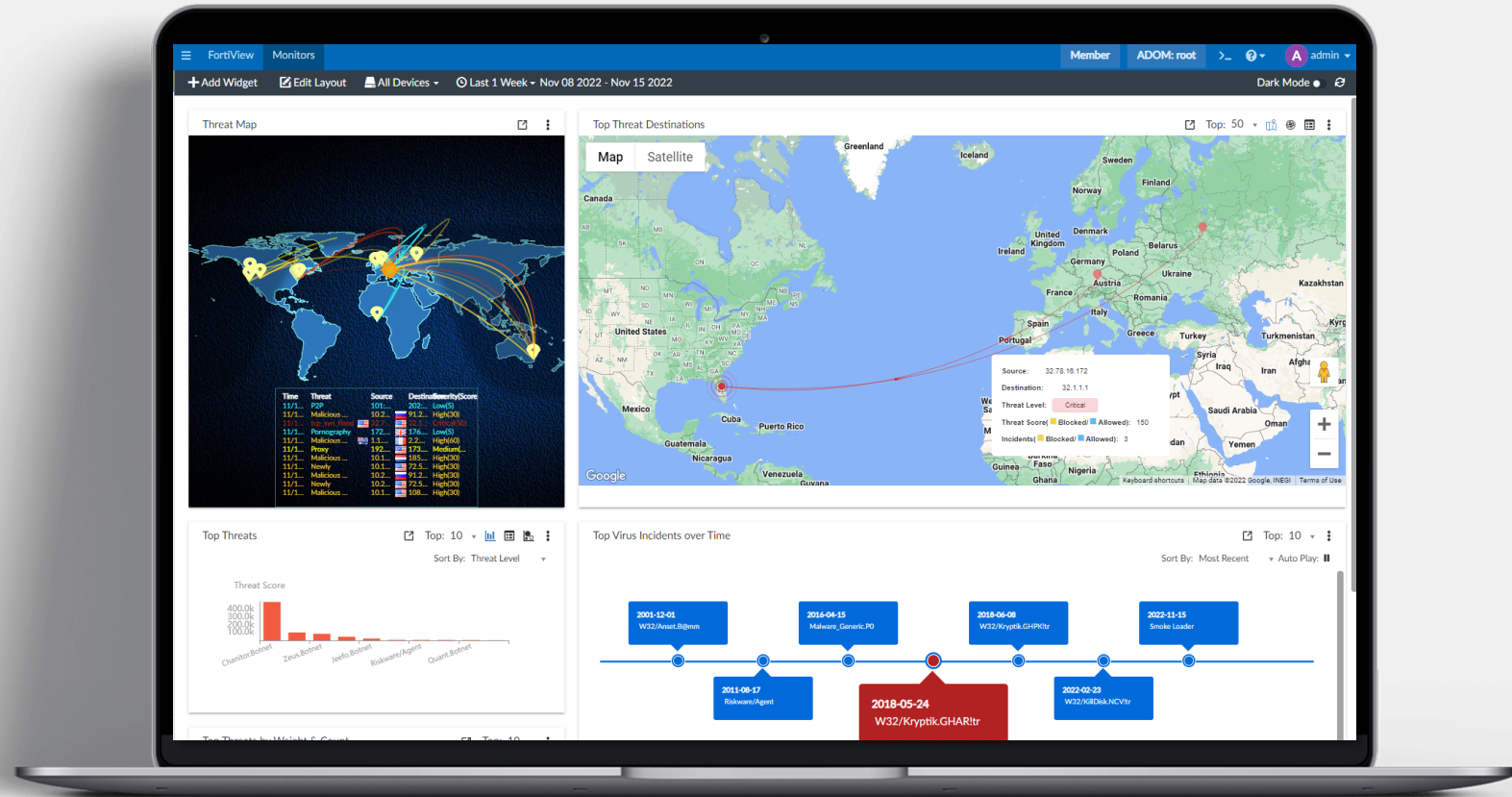


Моніторинг в реальному часі

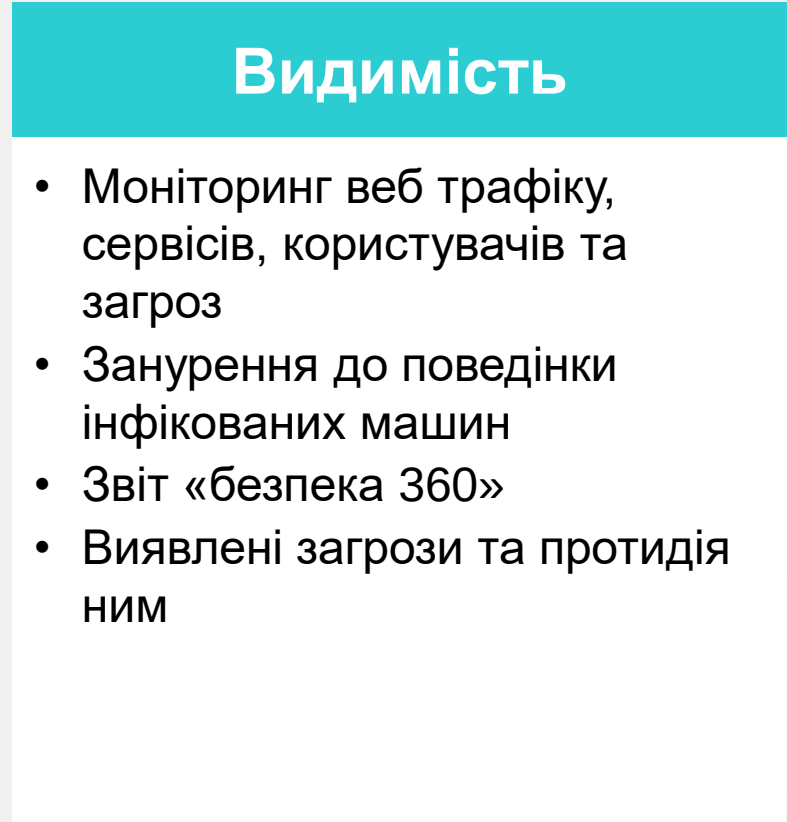
FortiView

Бачити все

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



Кореляція журналів (logs)



Звіт в пару кліків

Сотні готових звітів

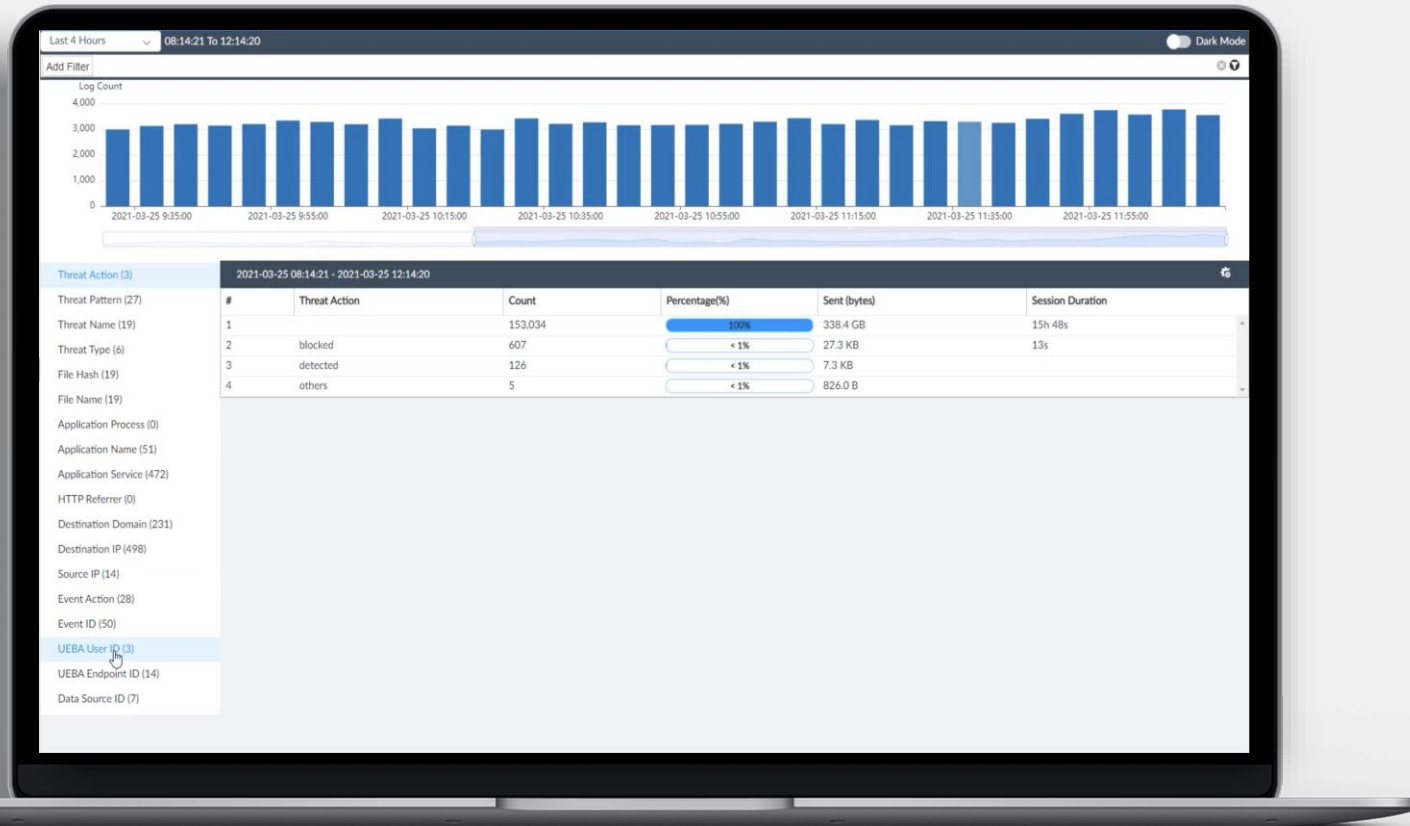
Готові звіти

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



Пошук загроз у реальному часі

Кореляція логів



Проактивний підхід

Полювання на загрози

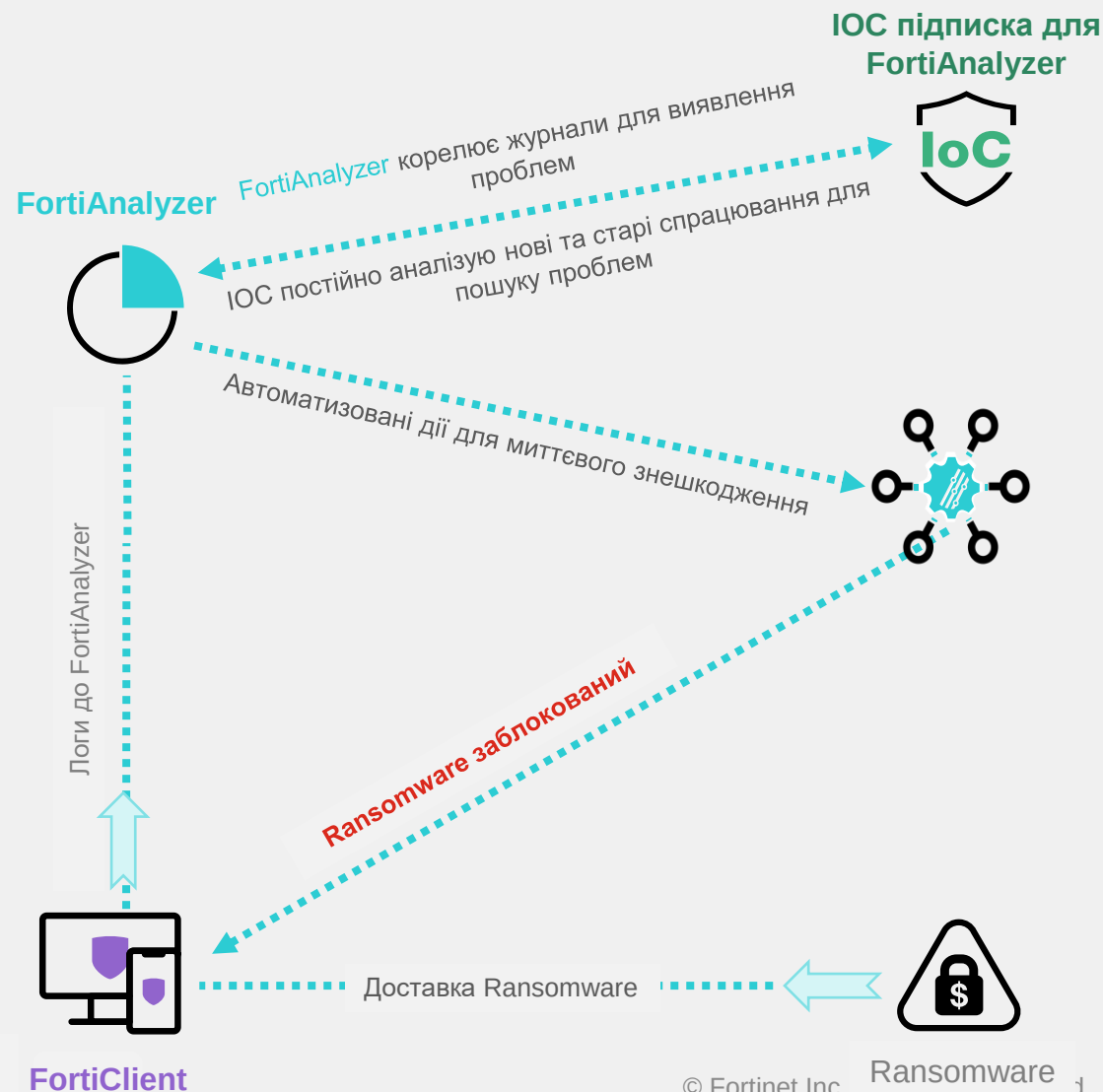
- 16 критично важливих елементів для SOC,
- Гнучкий пошук
 - Глобальний фільтр для швидкого пошуку індикатору компрометації (IOC)
 - Інтерактивний журнал трафіку

Виявлення загроз

Індикатори компрометації & взлому допомагає закрити питання безпеки компанії

ІоС підписка

- з 3М+ сенсорів Fortinet розташованих по світу дозволяють раніше реагувати на загрози
- FortiAnalyzer оновлює механізми/сигнатури щоденно з врахуванням історії минулих спрацювань для постійного контролю рівні захисту

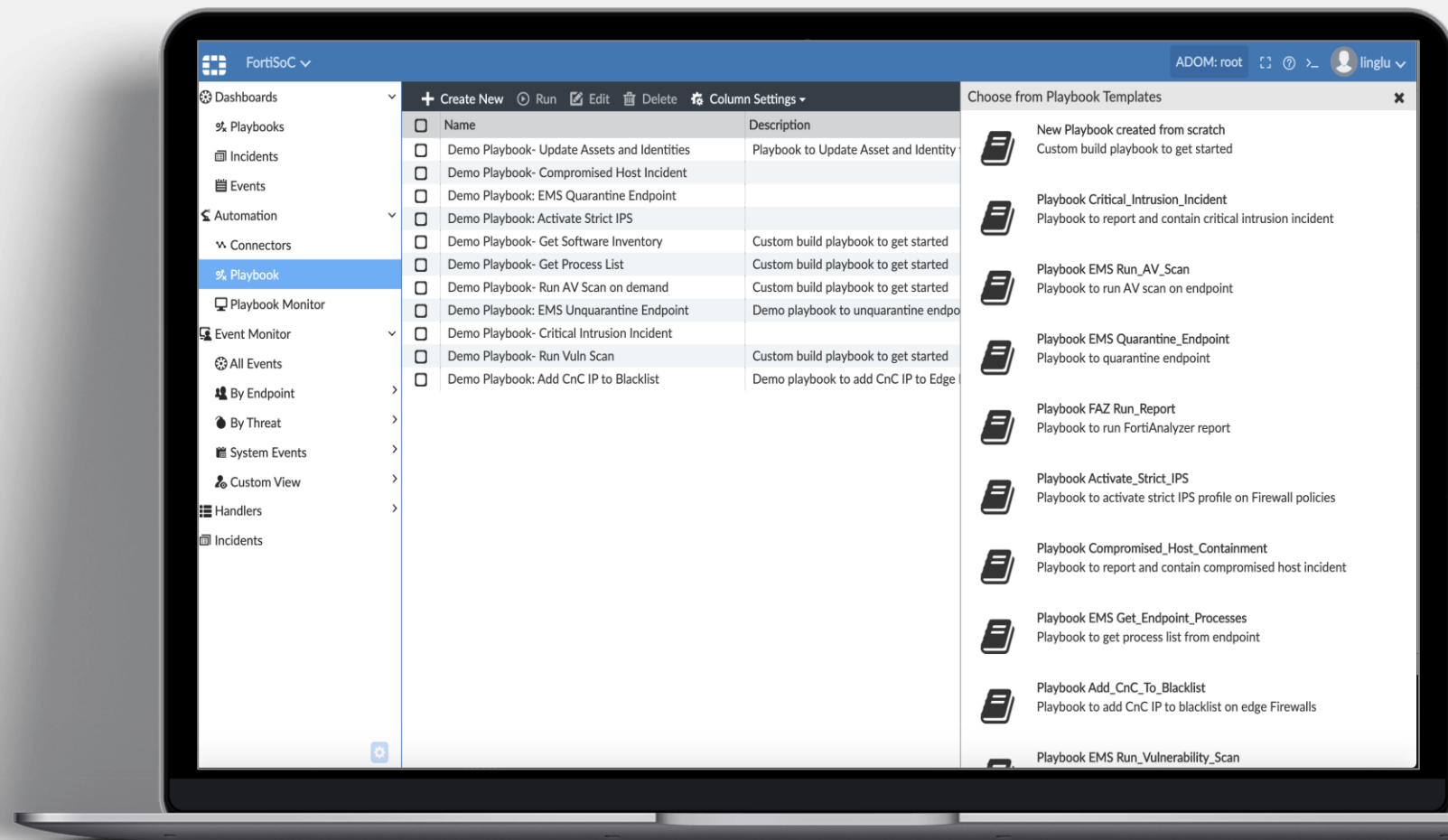


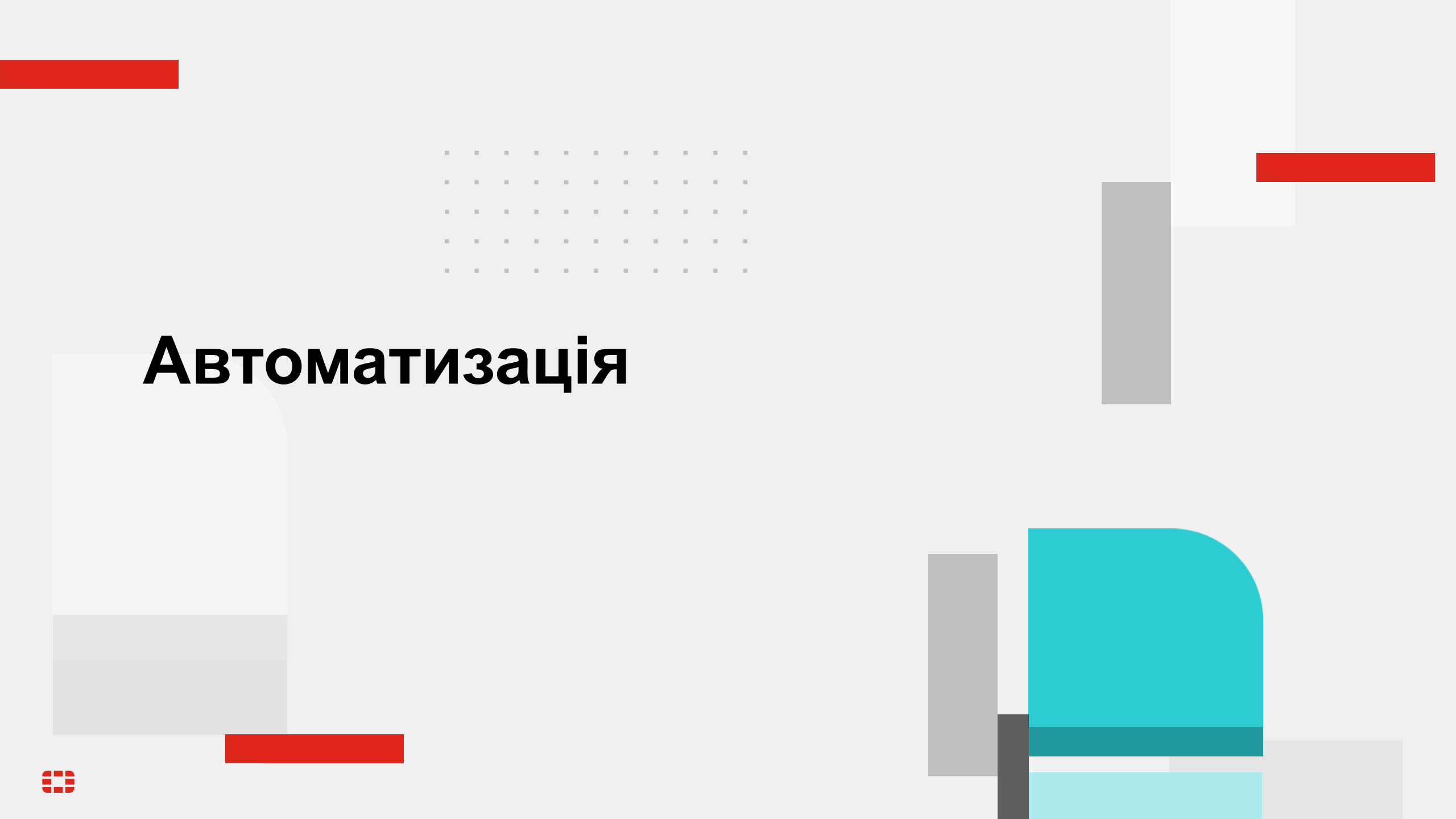
Готові до автоматизації

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)





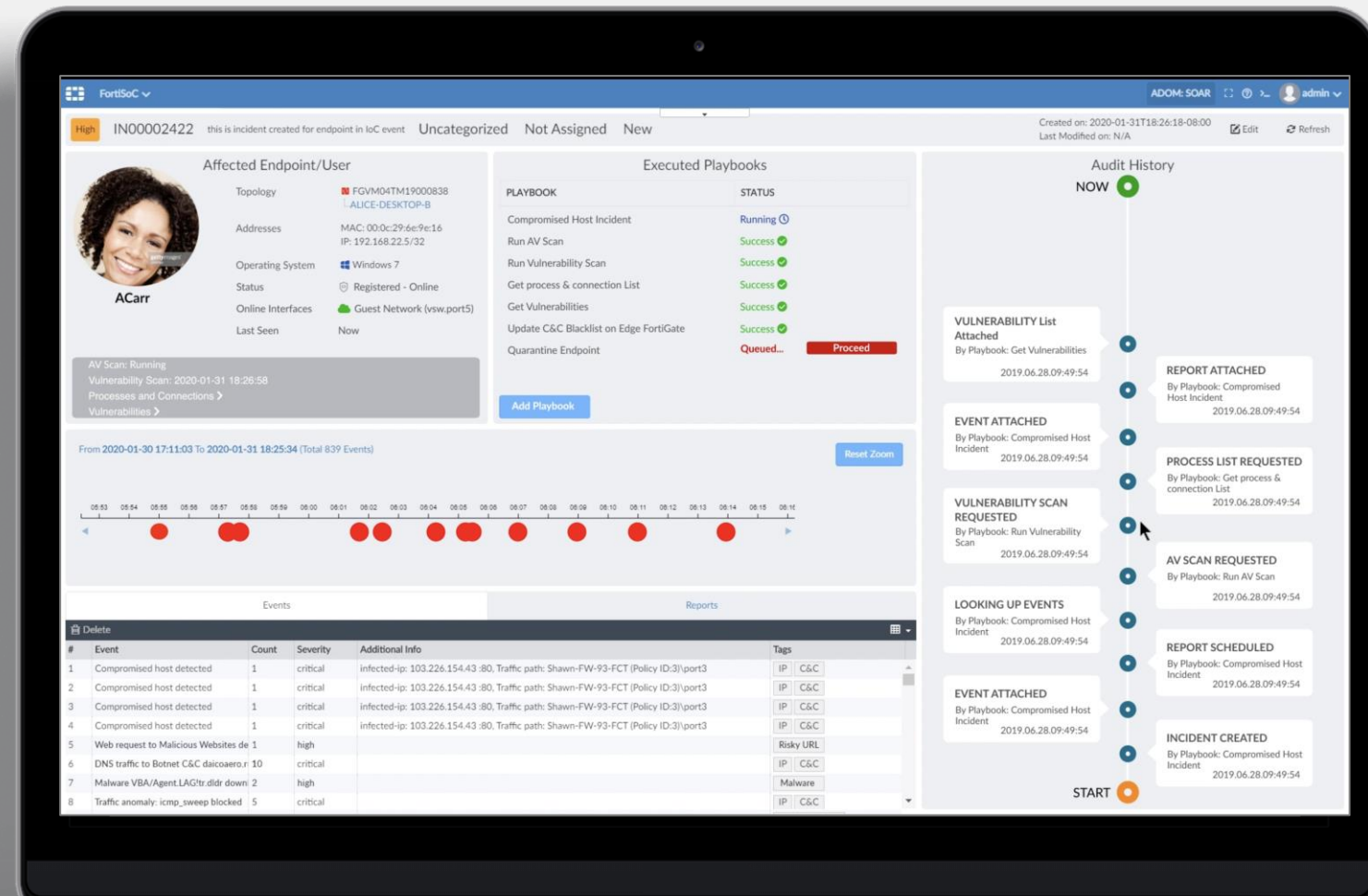
Автоматизація



Автоматизація вирішення інцидентів

Автоматичні реакції на інциденти

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



Керування інцидентами

Компонент дозволяє команді з безпеки керувати життєвим циклом інциденту з єдиного подання:

- Перегляд деталей інциденту
 - Уражений ПК та користувач
 - Хронологія інциденту
 - Деталі виконання автоматизації
 - Показати/Сховати історію аудиту
 - Додатки до інцидентів (події, звіти тощо)
- Коментарі щодо спільної роботи
- Призначення відповідального за інцидент
- Сповіщення

The screenshot displays the 'Edit Incident' modal window for incident IN00002541. The modal is overlaid on a background showing the incident details page. The incident is categorized as 'High', 'Uncategorized', 'Not Assigned', and 'Analysis'. The 'Affected Endpoint' is 'Alder'. The 'Description' field contains the text 'IoC incident created for endpoint'. The 'Assigned To' field is currently empty. The modal includes 'OK' and 'Cancel' buttons at the bottom right. The background interface shows various sections like 'Topology', 'Addresses', 'Operating System', 'Vulnerabilities', 'Processes', 'Software Inventory', 'Comments', and 'Events'.

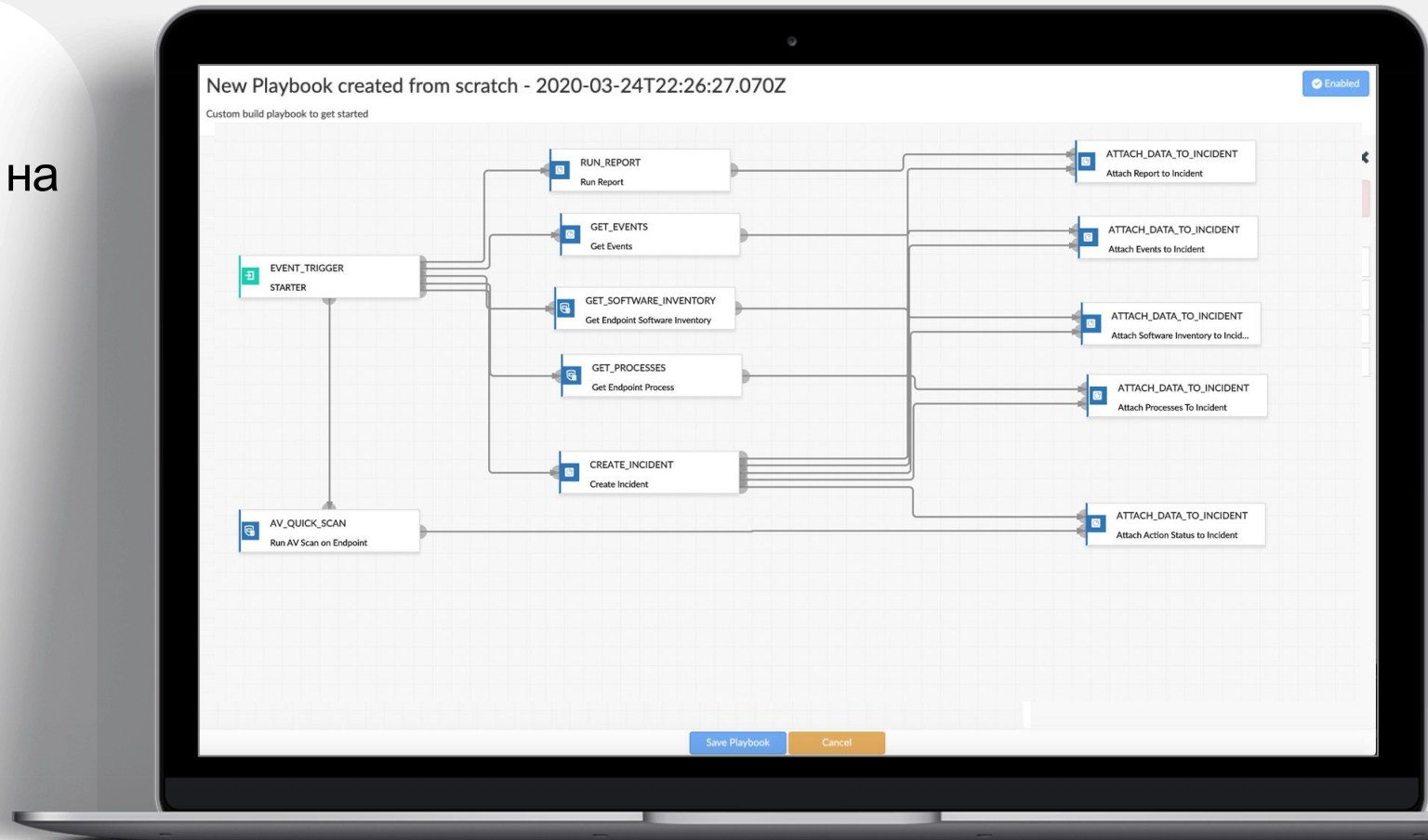
Field	Value
Incident Date / Time	2020-03-24 20:11:22
Incident Category	Uncategorized
Severity	High
Status	Analysis
Affected Endpoint	Alder
Description	IoC incident created for endpoint
Assigned To	

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

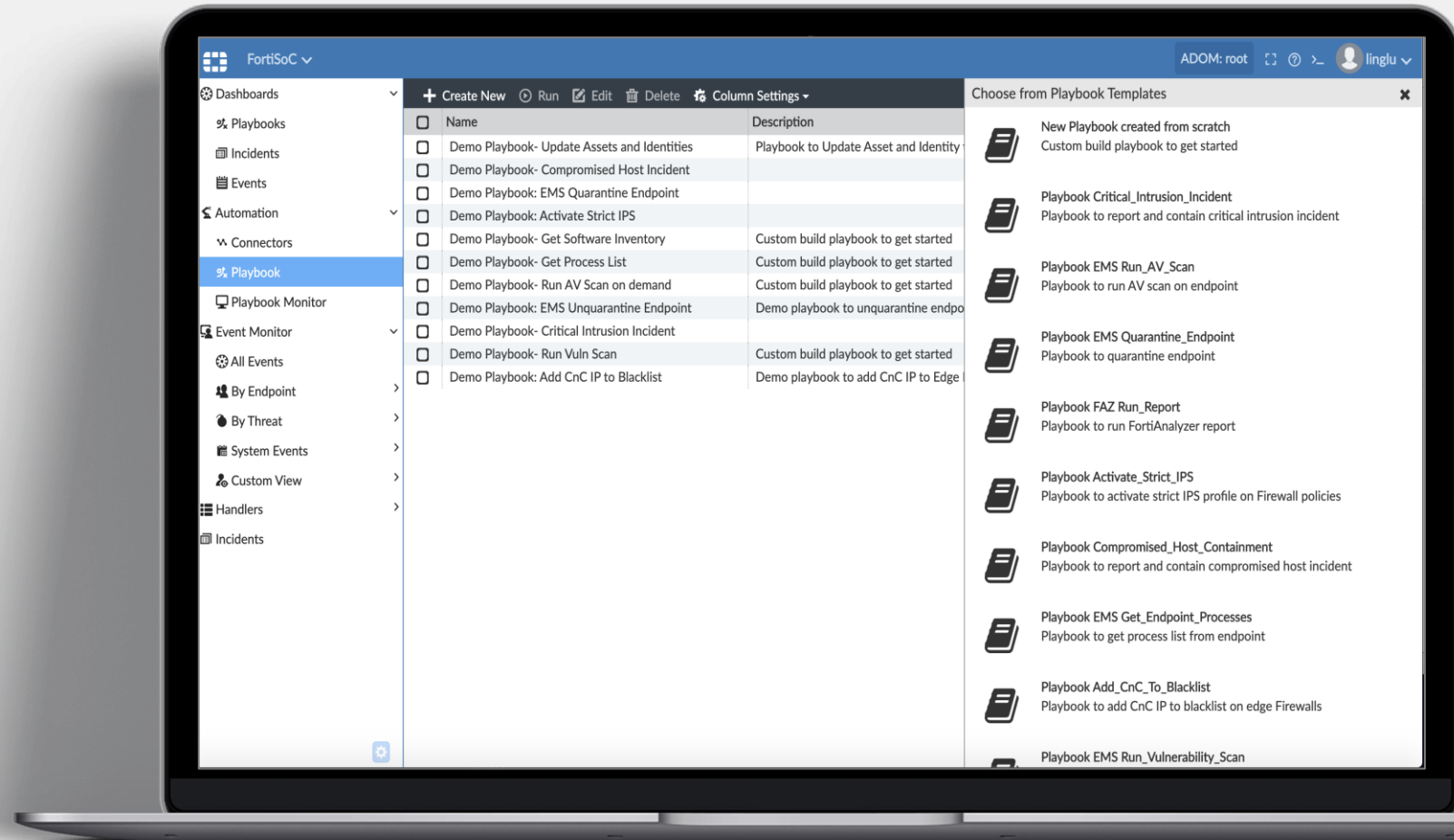


Вбудовані шаблони автоматизації

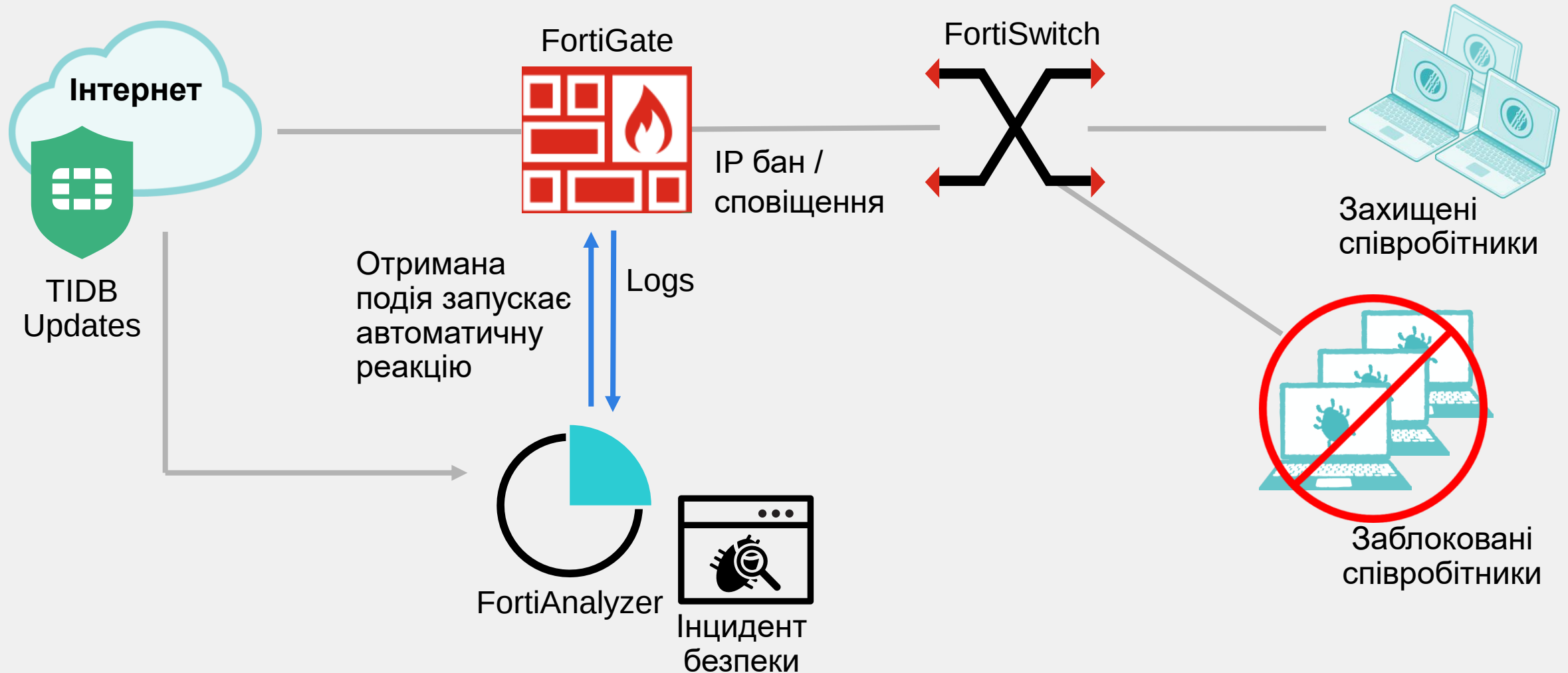
Playbooks

Готові шаблони дають змогу аналітикам SOC швидко налаштувати їх відповідно до своїх випадків використання

- Playbooks розслідування зараження
- Playbooks для збору даних
- Playbooks протидії та блокування загрози



Приклад автоматизації



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 a navigation menu with categories like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Custom View, Handlers, Event Handler List, FortiGate Event Handlers (selected), Subnet List, and Incidents.

The main configuration area is titled 'Create New Handler' and includes the following sections:

- Status:** A toggle switch set to 'ON'.
- Name:** A text field containing 'Botnet Communication detected'.
- Description:** A text field containing '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 '+' icon to add filters.
- Filter 1:** A toggle switch set to 'ON'.
- Log Device Type:** A dropdown menu set to 'FortiGate'.
- Log Type:** A dropdown menu set to 'IPS (ips)'.
- Group By:** A dropdown menu set to 'Attack Name (attack)'.
- Destination Endpoint (dstendpoint):** A dropdown menu with a trash icon.
- Logs match:** Radio buttons for 'All' and 'Any of the following conditions' (selected).
- Log Field, Match Criteria, Value:** A table with one row: 'Level (pri)' | 'Equal To' | 'Emergency'.
- Generic Text Filter:** A text field containing the expression 'attack ~ Botnet and direction=outgoing and (action=='detected' or action=='pass session')'.
- Generate alert when at least:** A text field containing '1'.
- matches occurred over a period of:** A text field containing '30'.
- minutes:** A text field containing '30'.
- Event Message:** A text field containing 'Traffic from Botnet C&C to \$groupby2 detected'.
- Event Status:** A dropdown menu set to '(Blank)'.
- Allow FortiAnalyzer to choose:** A checkbox that is unchecked.
- Event Severity:** A dropdown menu set to 'Medium'.
- Tags:** A text field.
- Additional Info:** Radio buttons for 'Use system default' and 'Use custom message' (selected).
- Custom message:** A text field containing the expression 'Traffic from Botnet C&C \${attack}, Reference: \${ref}, Traffic path: PolicyID \${policyid}_\${srcintf}_\${srcip}:\${srcport}'.

Автоматизована реакція на інцидент

Enterprise_FortiAnalyzer

>

?

2

A

Admin

Custom Playbook

Enabled

EVENT_TRIGGER
STARTER

LOCALHOST_CREATE_INCIDENT
CREATE_INCIDENT

LOCALHOST_ATTACH_DATA_TO_I
ATTACH_DATA_TO_INCIDENT

LOCALHOST_RUN_REPORT
RUN_REPORT

Save Playbook

Cancel

LOCALHOST_ATTACH_DATA_TO_INCIDENT

Name

ATTACH_DATA_TO_INCIDENT

Description

Attach report to incident

Connector

Local Connector

Action

Attach Data to Incident

Incident ID ?

CREATE_INCIDENT (id_243_e8...

incident_id

Attachment ?

RUN_REPORT (id_a52_af3_c9a...

report_uuid

OK

Cancel



Основи роботи автоматичних сценаріїв (playbook)

Triggers

- Device type
- Endpoint ID
- Endpoint IP
- Endpoint MAC
- Endpoint name
- End user ID
- End user name
- Event ID
- Event status
- Event time
- Event type
- Severity
- Tag
- Threat type



Основні варіанти дій автоматичних сценаріїв (playbook)

Actions

- EPEU is a JSON data structure with all related endpoint and enduser info in it: epid, epname, epip, epmac, fluid, etc.
- Run report
- Attach data to incident
- Create/Update incident
- Get events matching filter conditions
- Threat intelligence indicators
- Get sender reputation statistics for a given email address
- Add sender to blocklist (system and domain level)
- Webhook call towards FortiOS
- Send message in Microsoft Teams
- Threat intelligence indicators
- Tag endpoints
- Retrieve list of vulnerabilities on an endpoint
- Retrieve list of running processes on an endpoint
- Retrieve software list installed on an endpoint
- Request AV full scan on an endpoint
- Request AV quick scan on an endpoint
- Request vulnerability scan on an endpoint
- Request to unquarantine an endpoint
- Request to quarantine an endpoint
- Untag endpoints



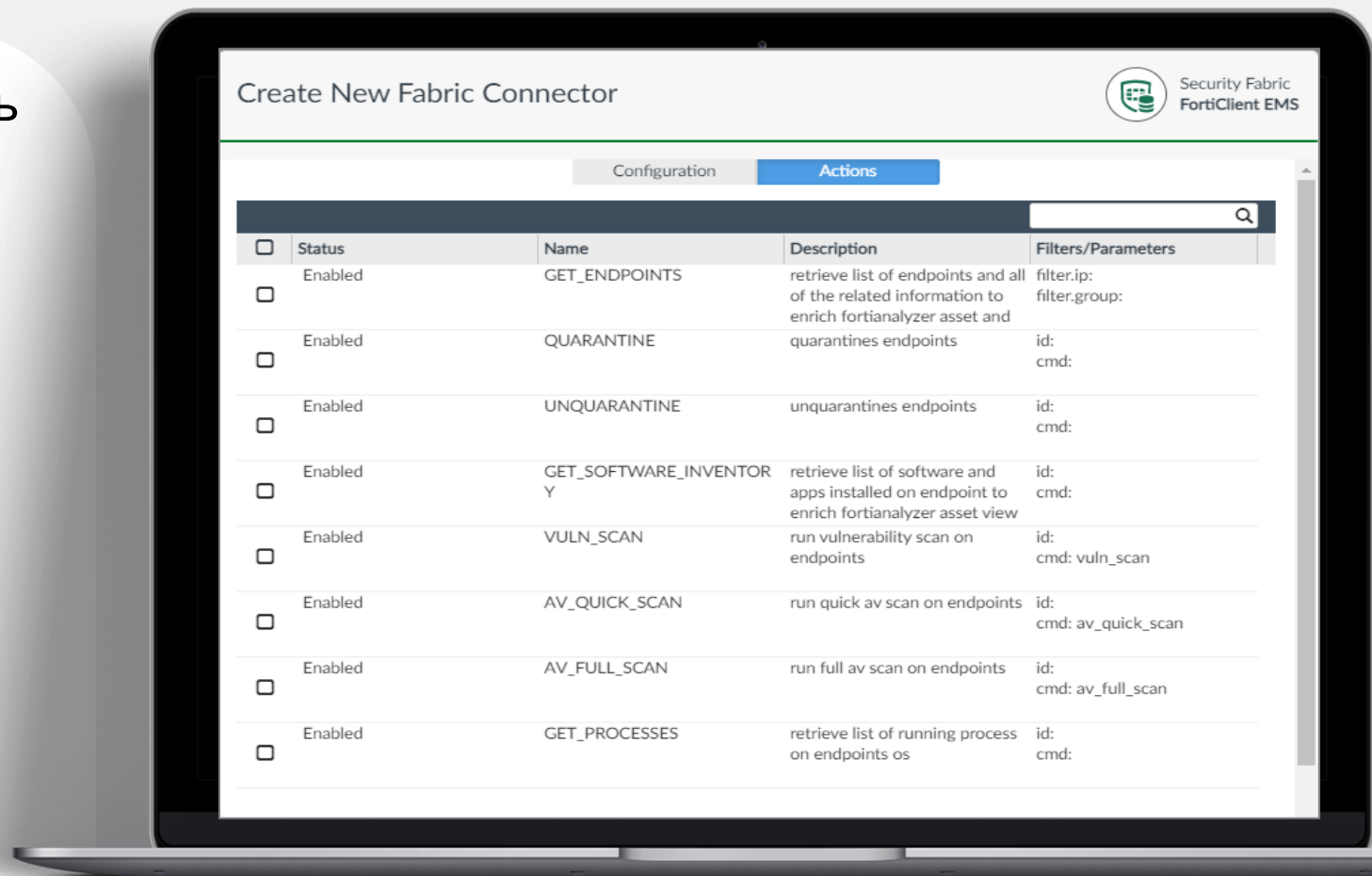
Інтеграція з іншими пристроями

Playbook конектори

Вбудовані засоби взаємодія дозволяють значно спростити роботу з інцидентами та сильно розширити можливі заходи пародії

Підтримуються:

- EMS (Enterprise Management Server) конектор
- FortiOS конектор
- FortiMail конектор
- FCASB конектор
- FAZ built-in Connectors
- FortiGuard Connector



Комплексна робота з загрозами

Behavior Detection

Behavior Detection Engine detects "ELF/Zerobot.A!tr" as High Risk



FortiSandbox

v4.0+

Exploitation

IPS

Detect and block Zerobot related attack



FortiGate

DB 22.464



FortiSASE

DB 22.464



FortiSASE

DB 22.464

DETECT

Find and correlate important information to identify an outbreak
updates are available to raise alert and generate reports:

IOC



FortiAnalyzer

DB 1.002442



FortiSIEM

DB 1.002442



FortiSOCaaS

DB 1.002442

RESPOND

Develop containment techniques to mitigate impacts of security

Automated Response

Services that can automatically respond to threats



FortiXDR

Assisted Response Services

RECOVER

Improve security posture and processes by implementing security
and training, in preparation for (and recovery from) security incidents

InfoSec Services

Security readiness and awareness
employees.



Response
Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering
external attack vectors, including those introduced internally via supply
chain.



Комплексна робота з загрозами



DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC



FortiAnalyzer



FortiSIEM



FortiSOCaaS

Outbreak Detection



FortiAnalyzer

DB 2.00012

Threat Hunting



FortiAnalyzer

IOC



FortiAnalyzer



FortiSIEM



FortiSOCaaS

Outbreak Detection



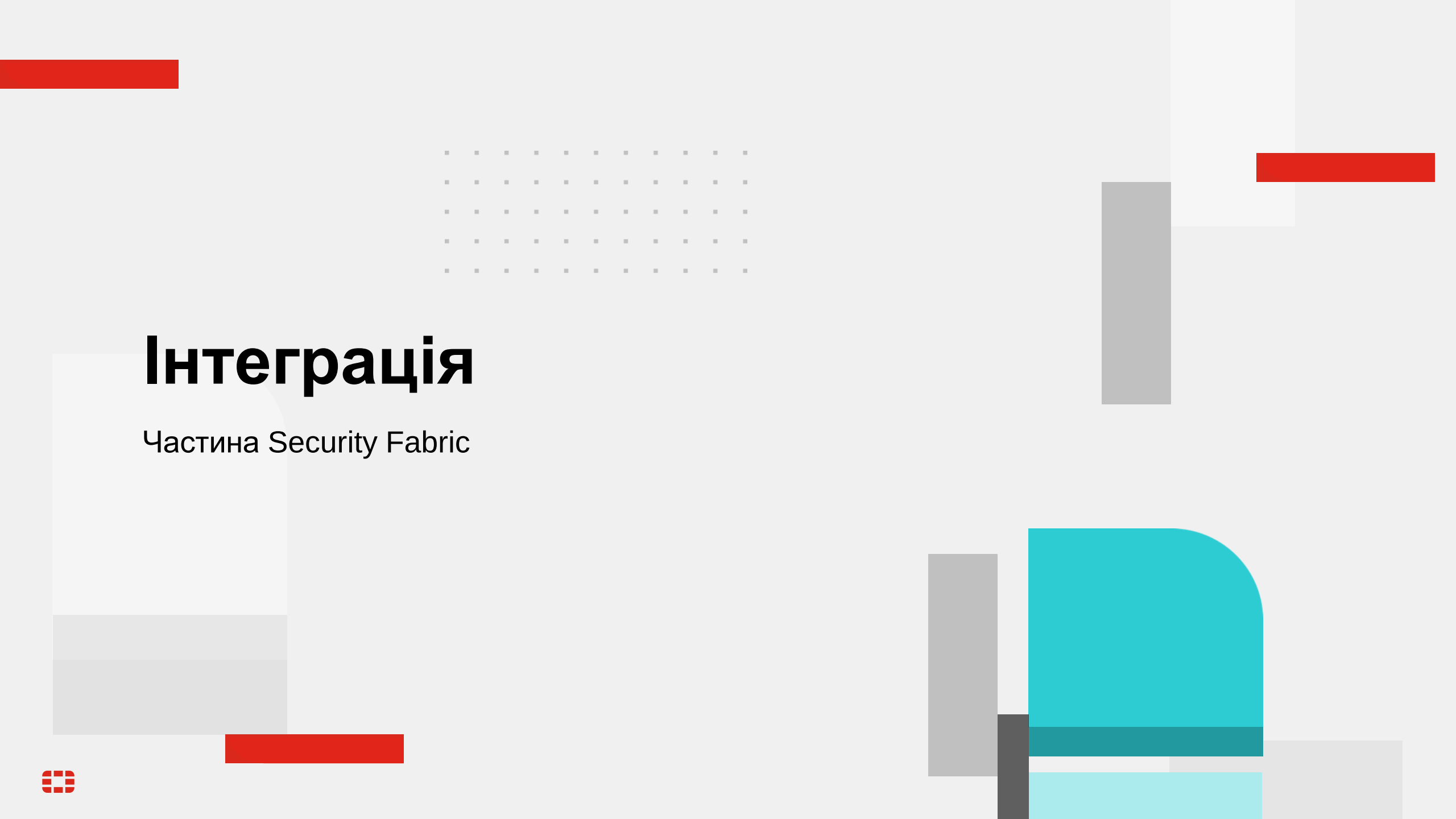
FortiAnalyzer

DB 2.00012

Threat Hunting

Виявлення





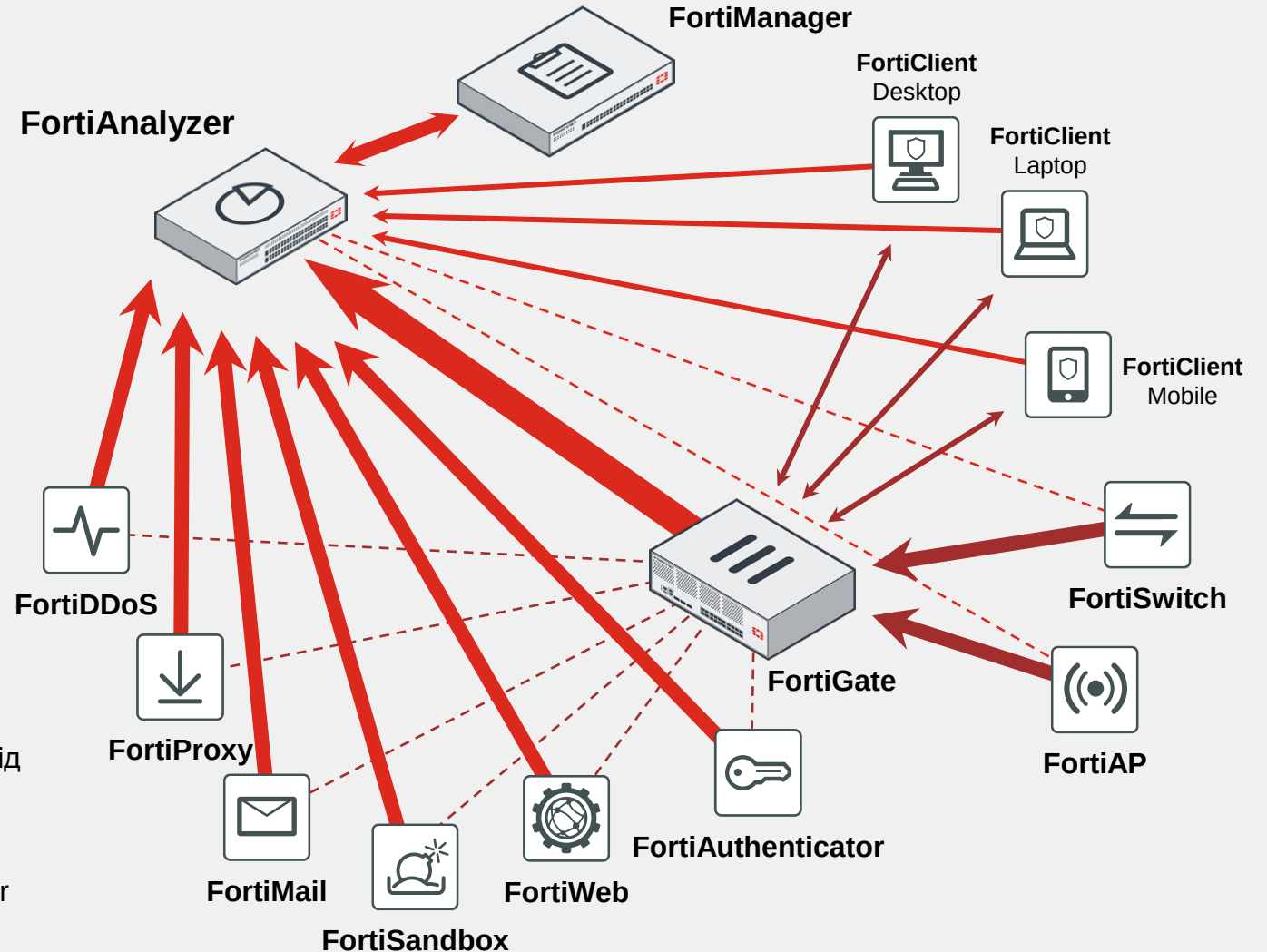
Інтеграція

Частина Security Fabric

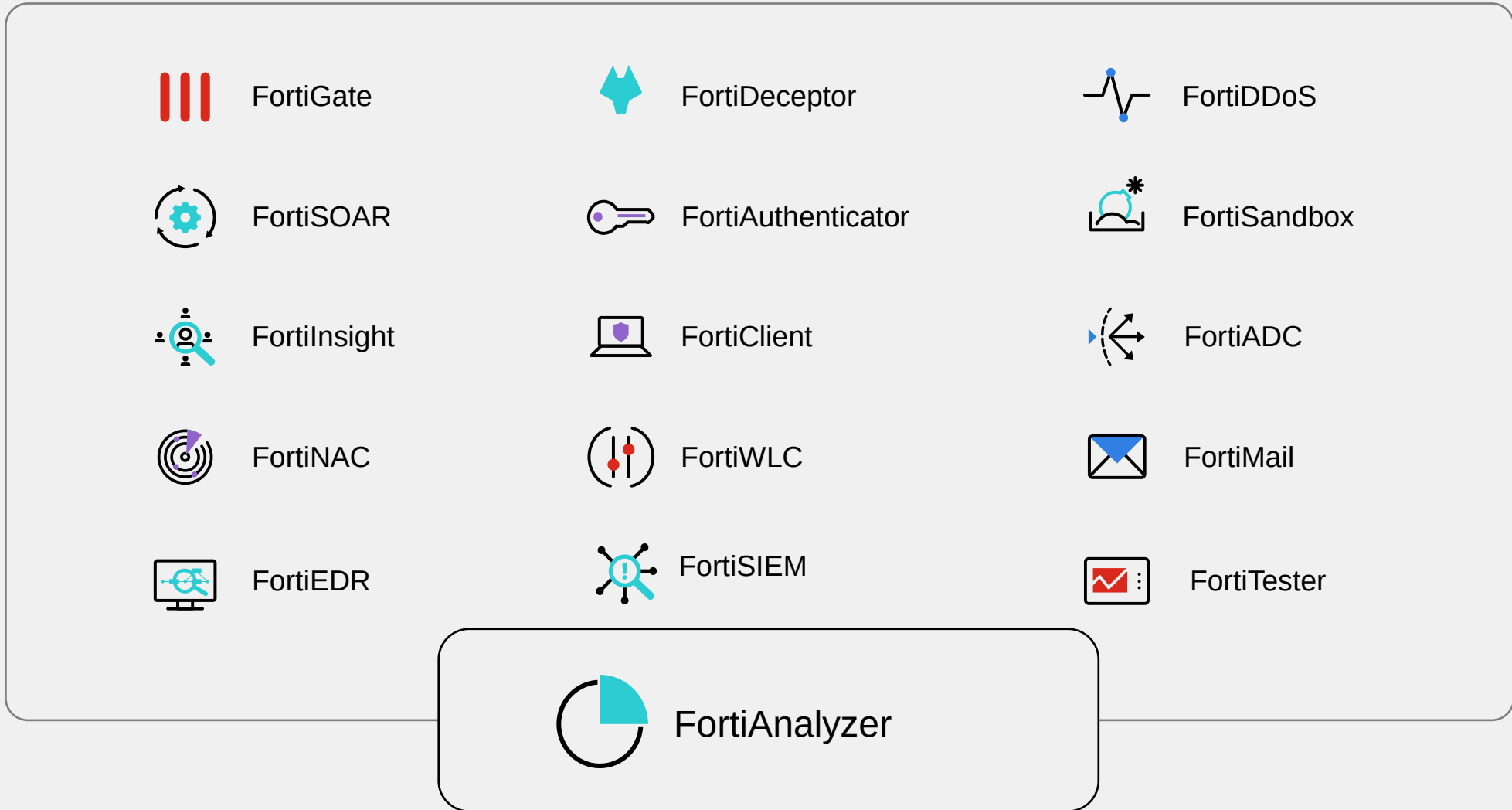


Security Fabric Management. Роль FortiAnalyzer

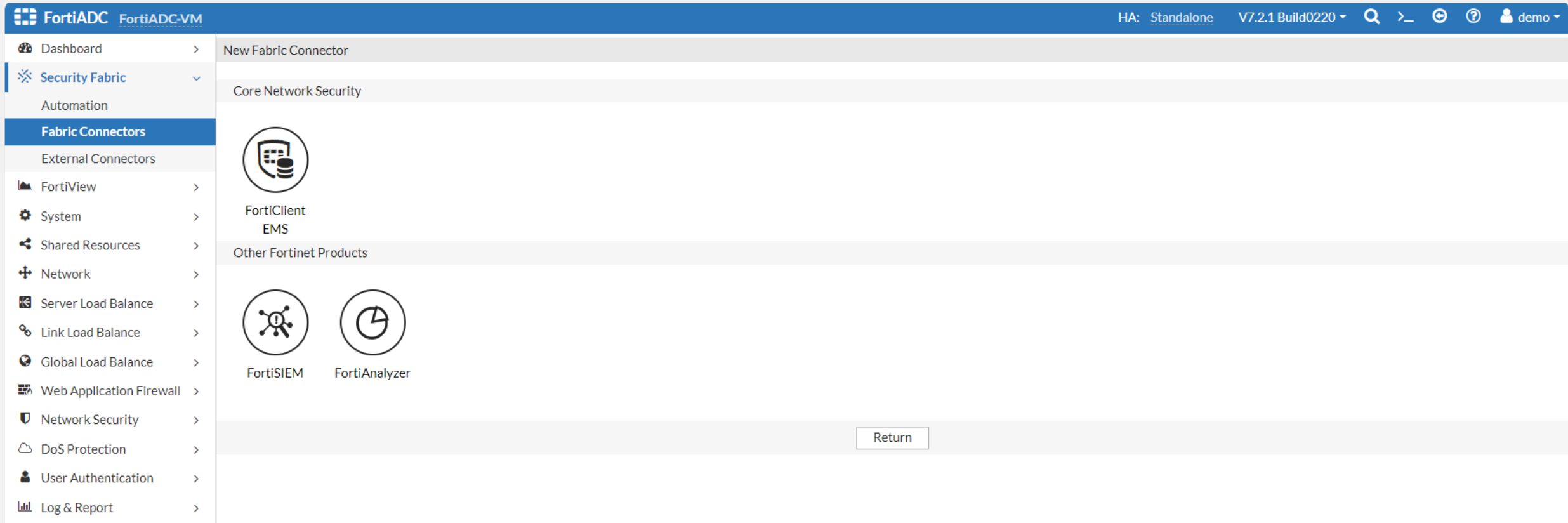
- Видимість всього що відбувається
- FortiGate
 - Одне з пріоритетних джерел інформації
 - FortiAnalyzer отримує повні журнали безпеки, трафіку та здоров'я
 - FortiGate збирає та записує журнали від інших пристроїв в рамках своєї Security Fabric
- FortiSwitch та FortiAP
 - FortiAnalyzer отримає сповіщення 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.



Інтеграція FortiAnalyzer



Як це виглядаю, на прикладі ADC



Інтеграція & Автоматизація

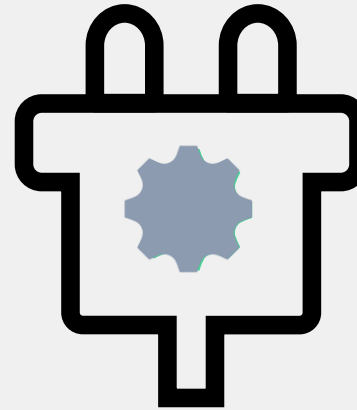
Вбудовані сценарії

Простота та швидкість

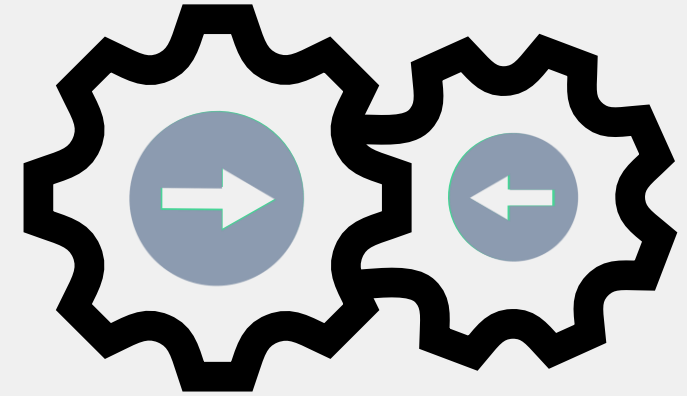
Зменшуємо час інтеграції з наявними рішеннями для мінімального впливу на наявну інфраструктуру

Готова інтеграція з

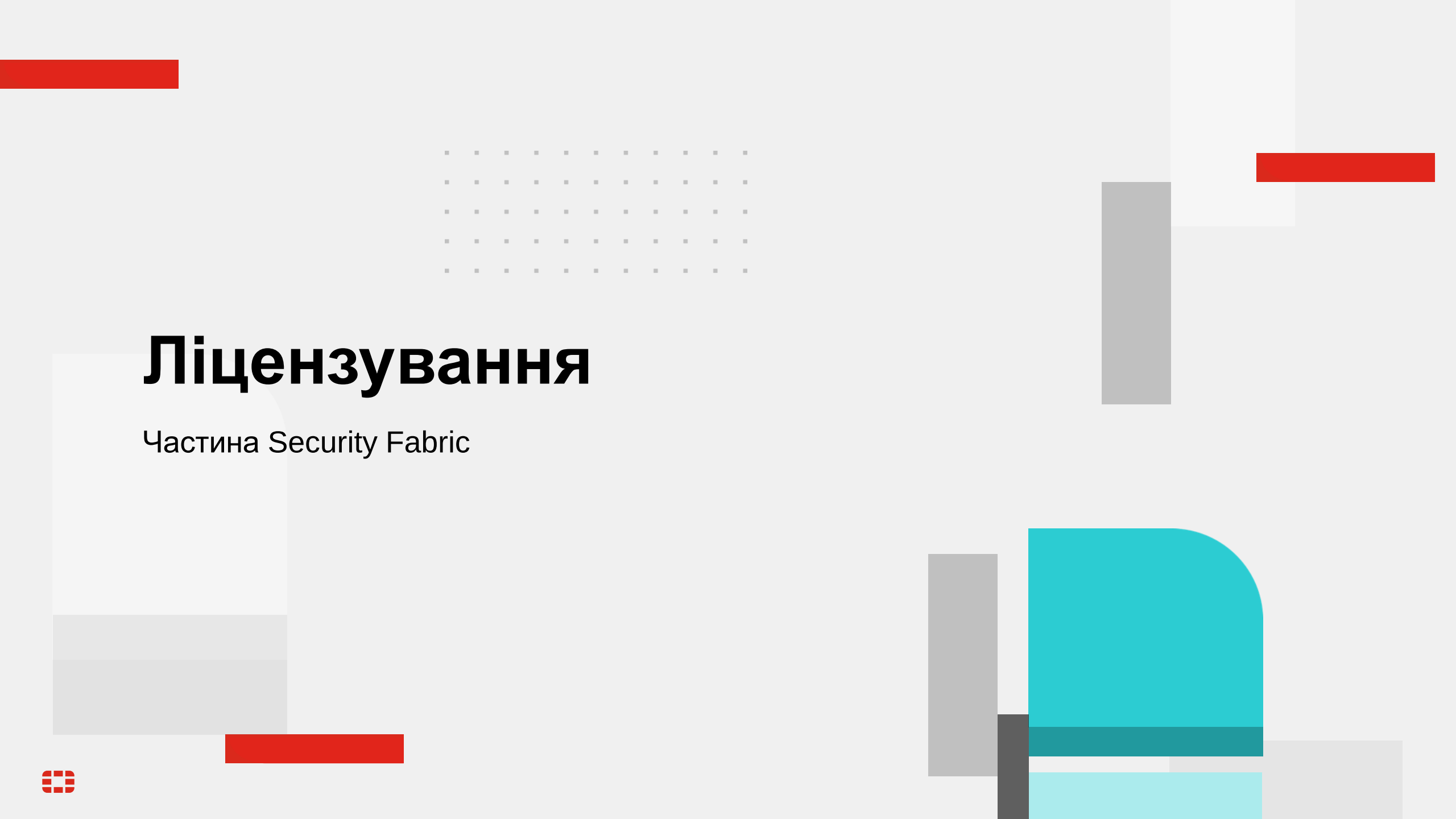
- SIEM, наприклад, Splunk
- ITSM, наприклад, ServiceNow
- Devops інструменти (Ansible, Terraform).
- REST API (fndn.fortinet.com)



Конектори



REST API



Ліцензування

Частина Security Fabric



Варіанти рішення та сайзинг

Власний пристрій

Рішення для організацій які бажають отримати повний контроль



Апаратні пристрої

- 8 моделей
- До 20 ТБ/добу
- До 300к LPS



Віртуальні машини

- 6 градацій що комбінуються
- Ліцензування на основі ТБ/добу
- Постійна ліцензія чи підписка



Послуга в хмарі

Компанії які бажають отримати видимість в форм факторі SaaS



SaaS

- Керується Fortinet
- Ліцензування по пристроях
- Весь функціонал в одній підписці (без додаткових модулів)

Типова специфікація

Стандарт

SKU	Description
FAZ-VM-GB1	FortiAnalyzer-VM Upgrade license for adding 1 GB/Day of Logs.
FC1-10-LV0VM-248-02-12	FortiAnalyzer-VM FortiCare Premium Support 1 Year FortiCare Premium Support (for 1-6 GB/Day of Logs)



Ліцензія автоматизації

Важливе доповнення

SKU	Description
FC1-10-LV0VM-335-02-12	FortiAnalyzer-VM Security Automation Service 1 Year FortiAnalyzer Security Automation Service including premium reports , event handlers, SIEM correlation rules for advanced threat detection and SOAR playbooks. (1-6 GB/Day of Logs)



Підписки безпеки

Важливе доповнення

SKU	Description
FC1-10-LV0VM-661-02-12	FortiAnalyzer-VM IOC and Outbreak Detection Service 1 Year FortiGuard IOC and Outbreak Detection Service for FAZVM Perpetual (1-6 GB/Day of Logs)
FC1-10-LV0VM-175-02-12	FortiAnalyzer-VM Surface Security Rating and Compliance Service 1 Year FortiAnalyzer Attack Surface Security Rating and Compliance (for 1-6 GB/Day of Logs)



Промислові протоколи

Важливе доповнення

SKU	Description
FC1-10-LV0VM-159-02-12	FortiAnalyzer-VM OT Security Service 1 Year OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules (for 1-6 GB/Day of Logs)



Співставлення функцій на прикладі FortiGate 90G

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service ¹	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) ¹	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license ²	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) ¹	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			



FortiAnalyzer Cloud

SKU	Description
FC-10-0090G-585-02-12	FortiGate-90G 1 Year FortiAnalyzer Cloud : cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service.

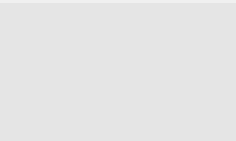
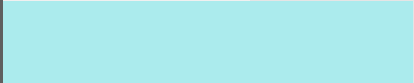
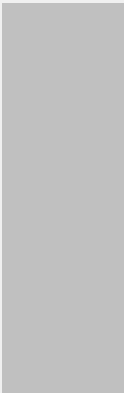
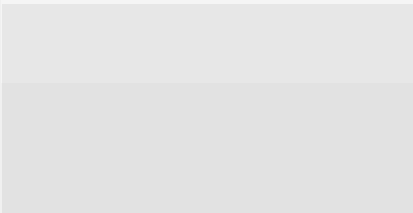
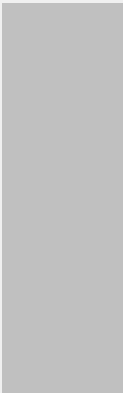


Безкоштовний FAZ-VM

Швидкий старт

- 1 Гб/добу логів
- 3 пристрої
- 3 ADOM
- Немає підтримки
- Одна активна ліцензія на обліковий запис
- Перевиписувати можна





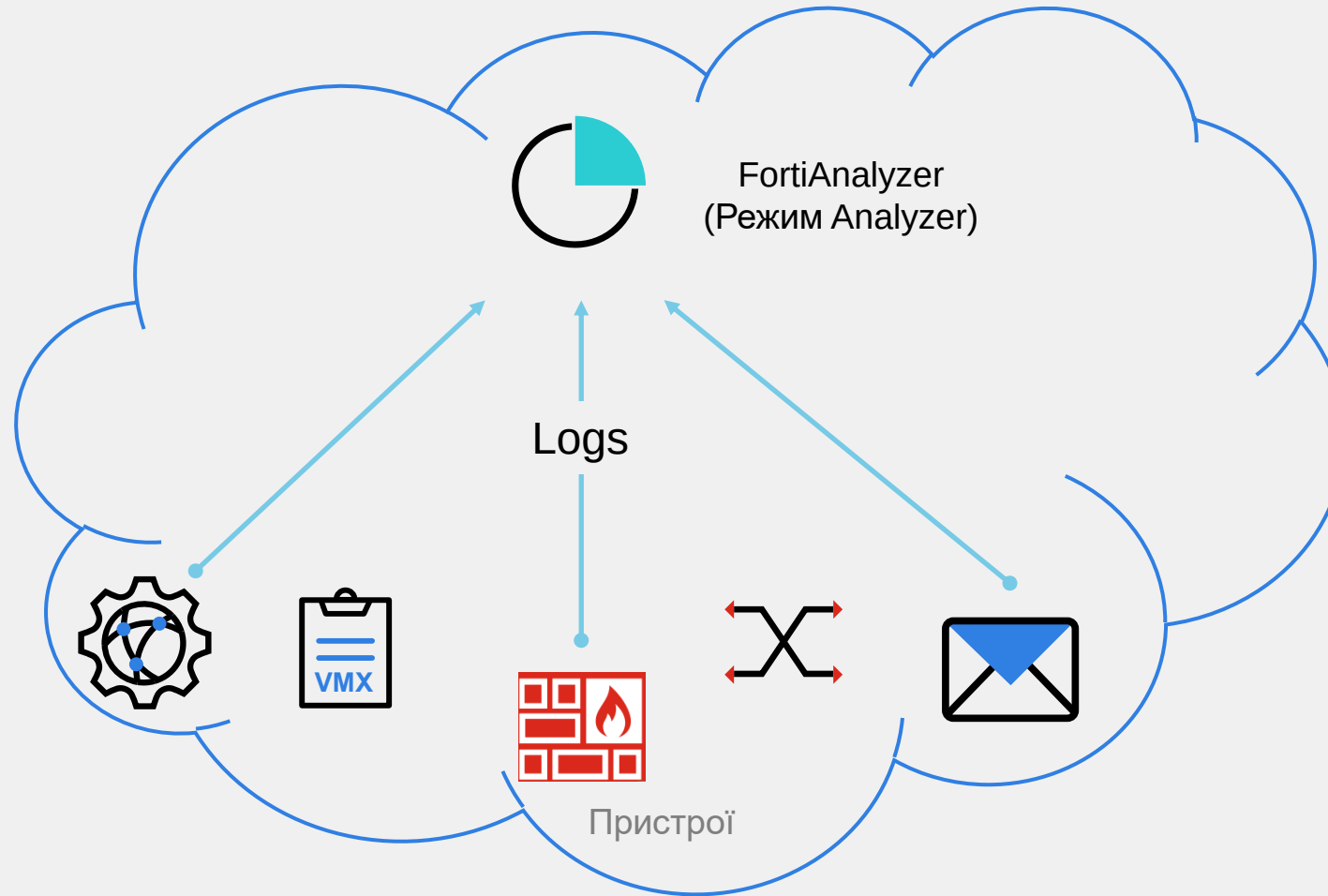
Цікавинки

На десерт



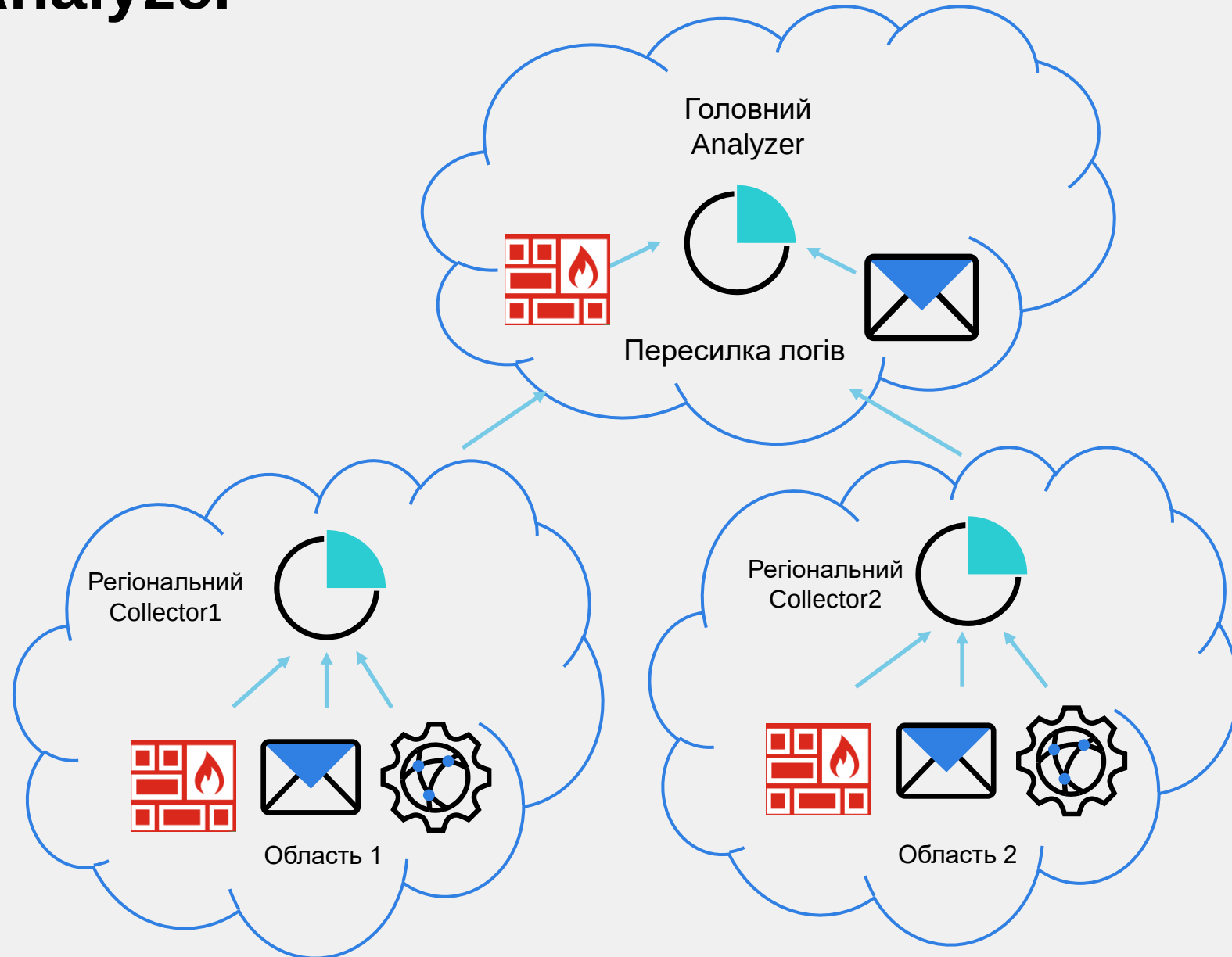
Традиційне використання FortiAnalyzer

Єдиний FortiAnalyzer



Корисна опція FortiAnalyzer

З використанням Collector



Обмеження Collector

Особливості функціоналу

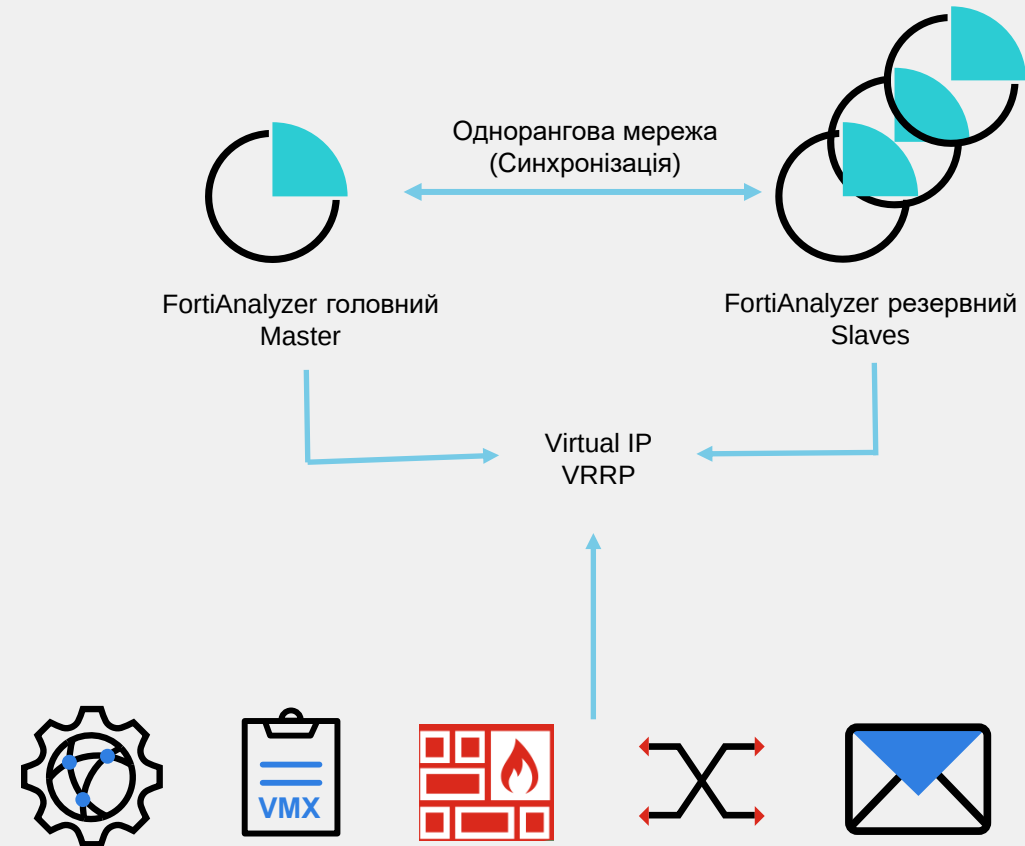
Feature	Analyzer Mode	Collector Mode
Device Manager	Yes	Yes
FortiView	Yes	No
Log View	Yes	Raw archive logs only
Incidents & Events	Yes	No
Monitoring devices	Yes	No
Reporting	Yes	No
System Settings	Yes	Yes
Log Forwarding	Yes	Yes



FortiAnalyzer

Кластеризація (HA)

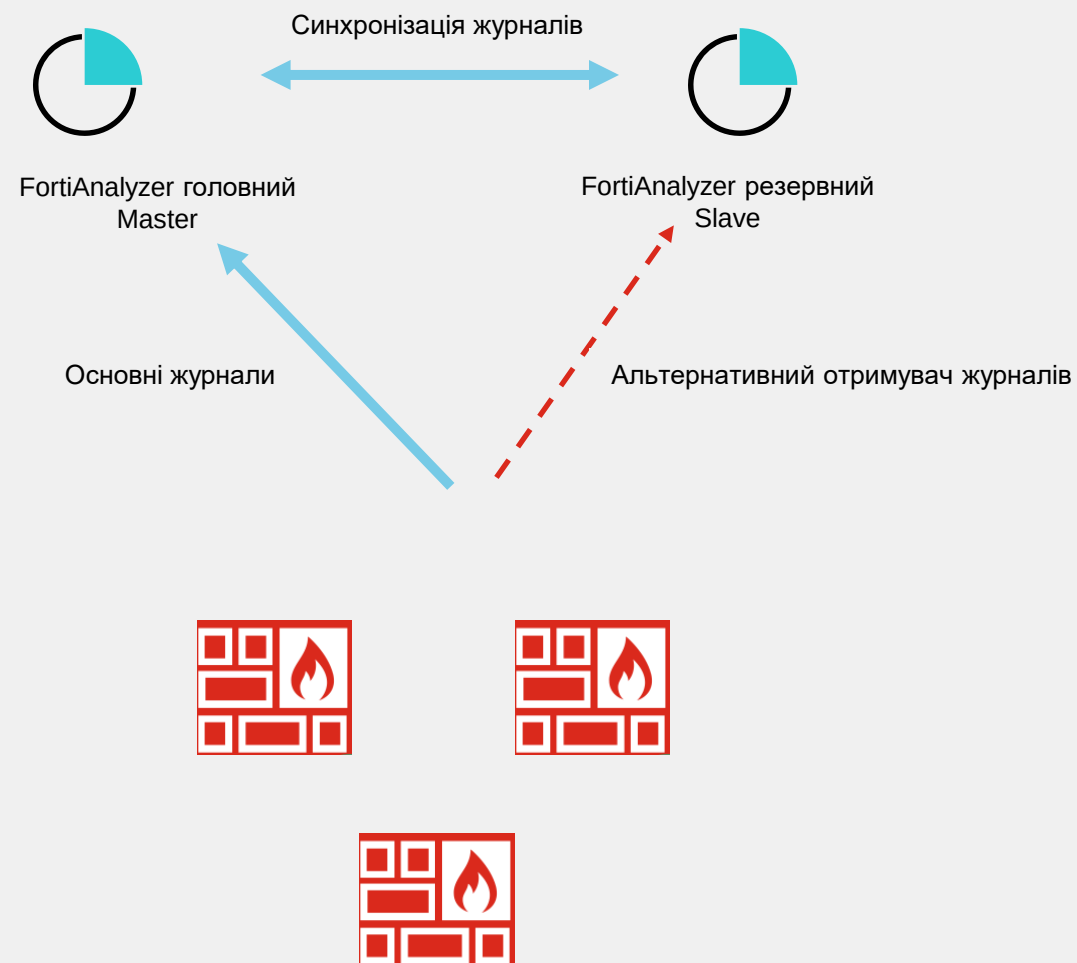
- Перемикання в режимі реального часу
 - IP failover
 - Пересилка та синхронізація логів
- До 4-х пристроїв в кластері (1 головний + 3 другорядних)
- Використовуйте можливості резервних FortiAnalyzer (звіти, FortiView тощо)



FortiAnalyzer

ГеоРозподілений кластер

- Real-Time failover
 - Пересилка журналів
 - Синхронізація даних
- Один головний та один другорядний
- Підтримується FortiGate



SQL report

Звіт можна зробити самому

The screenshot shows the 'Edit Dataset' interface in FortiAnalyzer. On the left is a sidebar with navigation options: Reports, Generated Reports, Report Definitions, All Reports, Templates, Chart Library, Macro Library, Datasets (selected), Advanced, Language, Output Profile, and Report Calendar. The main area is titled 'Edit Dataset' and contains the following fields:

- Name:** a33
- Log Type:** Traffic
- Query:**

```
select from_itime(itime)::date as datestamp, sum(rcvdbyte) as traffic_in, sum(sentbyte) as traffic_out, policyid, devid
from $log
where $filter
group by datestamp, policyid, devid
```
- Variables:** A table with columns 'Variable', 'Expression', and 'Description'. Below the table is a link 'Click here to add a new entry.' and a '+ icon' button.

On the right side, there are additional controls:

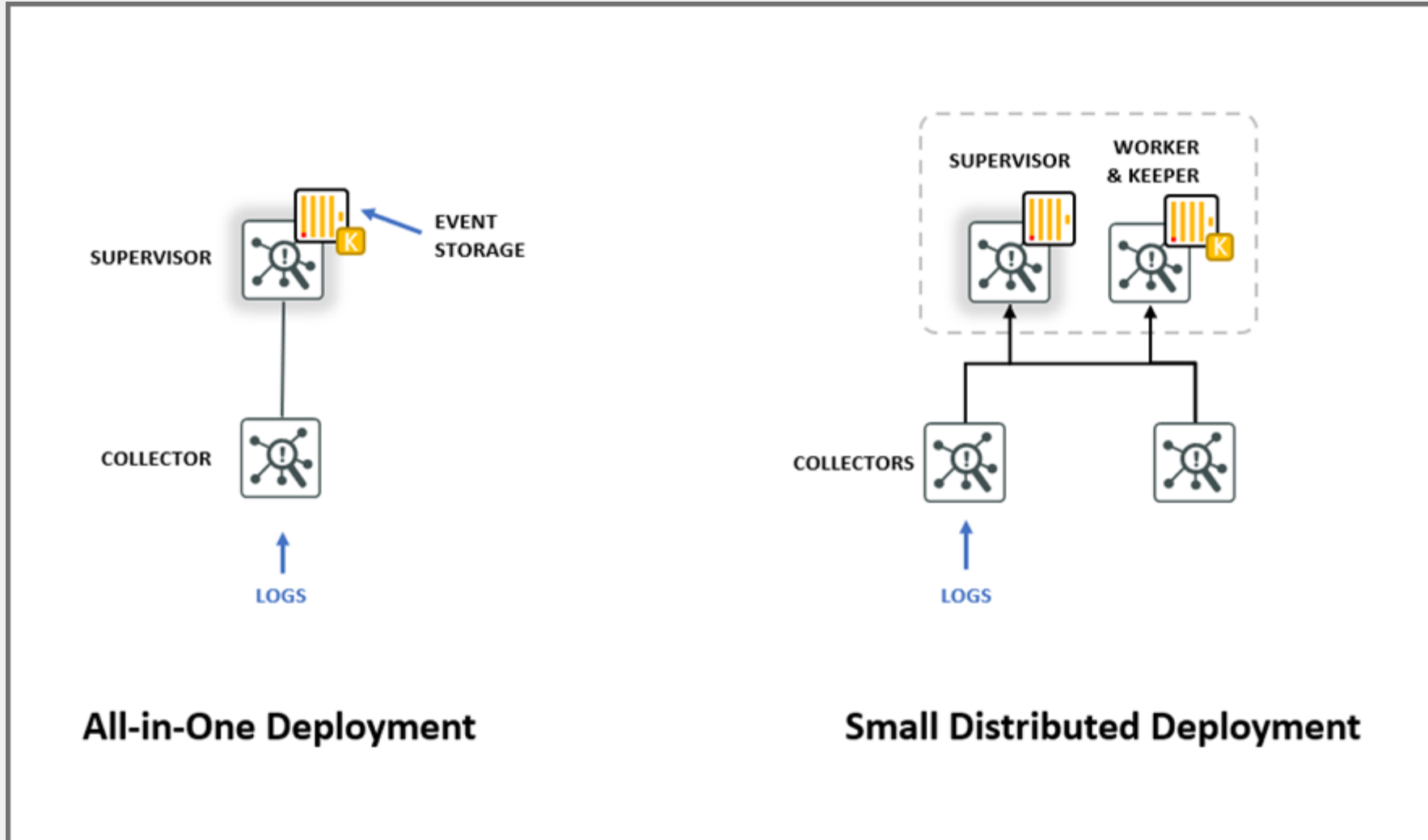
- Test query with specified devices and time period:** Includes a 'Test' button.
- Time Period:** Set to 'Last N Days' with 'N' equal to 250.
- Devices:** Radio buttons for 'All Devices' (selected) and 'Specify'.
- Test Result:** A section for displaying the results of the query test.

<https://docs.fortinet.com/document/fortianalyzer/7.4.0/sql-log-database-query-technote/861740/introduction>



SIEM колектор. Доповнення до FortiAnalyzer

MEA (Management Extensions)



SOAR. Доповнення до FortiAnalyzer

MEA (Management Extensions)

SKU	Description
FC-10-SRVMS-389-02	FortiSOAR Enterprise Subscription plus 24x7 FortiCare and FortiCare Best Practice Service - 2 User Logins included



Висновки

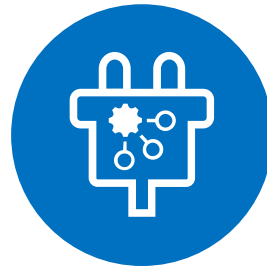
Видимість



Все в одній консолі

Економія часу необхідного для виявлення та розслідування проблеми

Безпека



Автоматизація

Пошук проблем безпеки
Автоматична та централізована протидія
Командна робота

Відповідність вимогам



Аудит

Звіти відповідності світовим стандартам

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®