FortiMail
Комплексний захист корпоративної пошти

Євгеній Таран, Systems Engineer

Електрона пошта – один з основних способів доставки загроз

Фішинг

36% ↑

Підробка адрес

15X ↑

Підробка листів

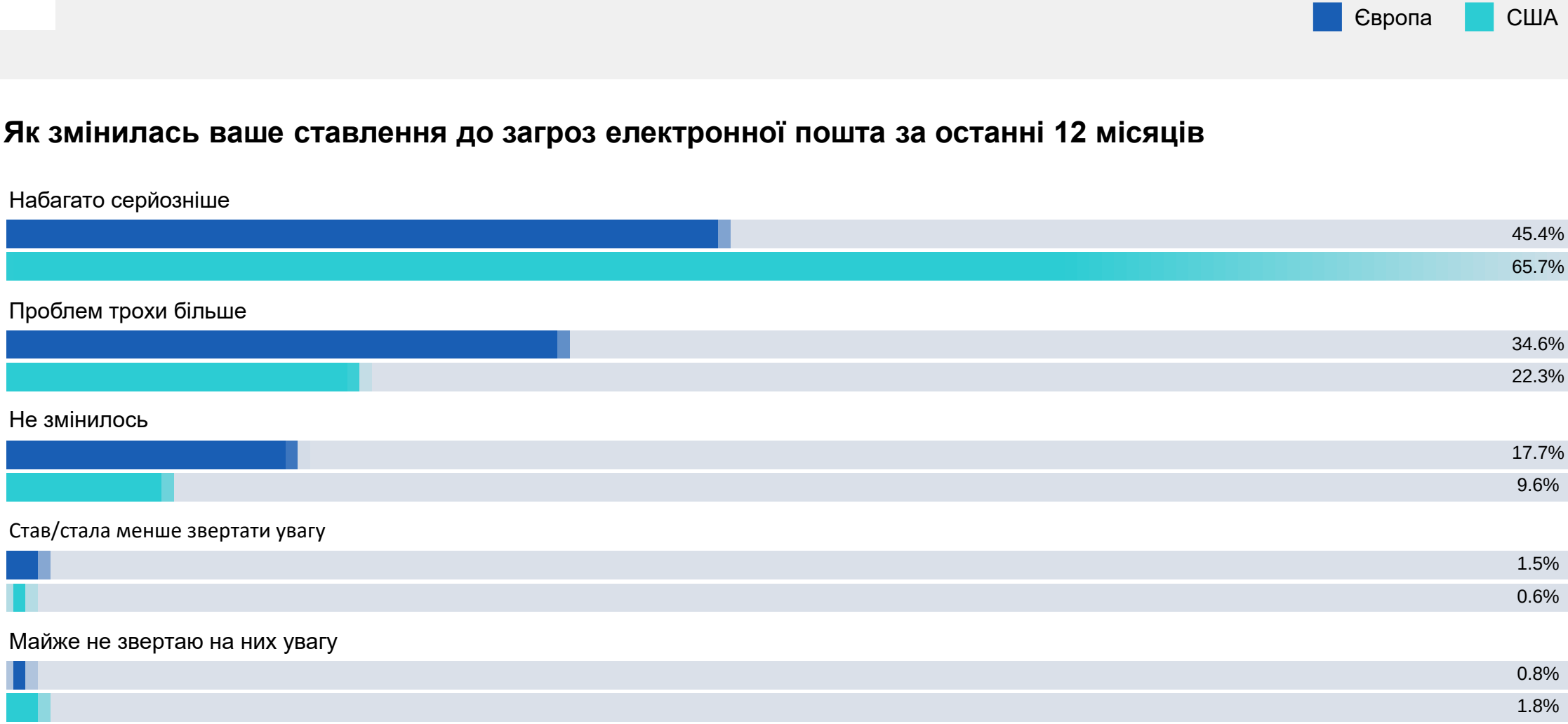
58%

Ransomware

10% ↑

Verizon Data Breach Investigations Report 2021.

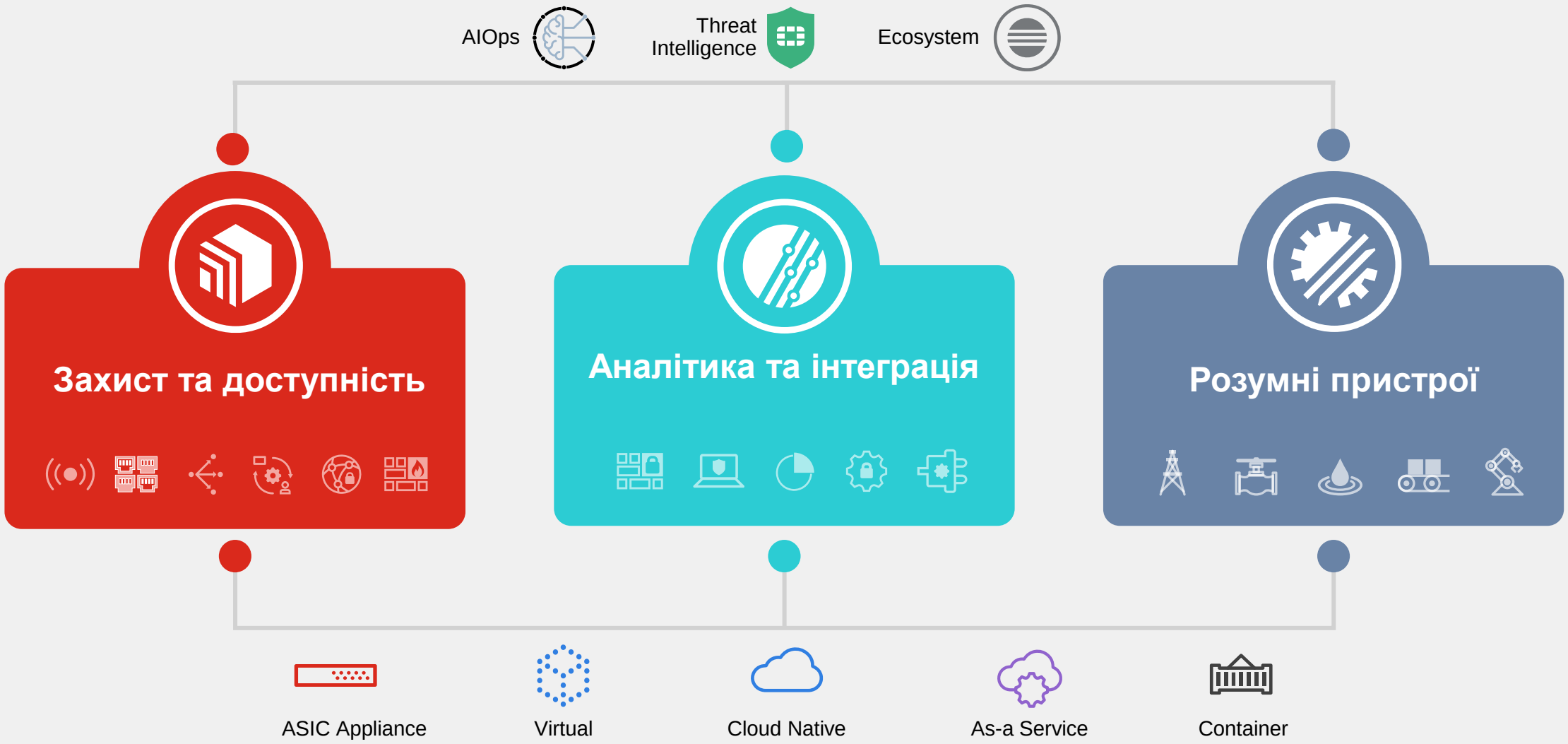
Опитування щодо поштових загроз



В попередніх серіях

~~Почнемо~~ Трохи повторимо попередній вебінар щоб бути «на одній хвилі»

Безпека – це комплекс



Гібридні мережі

Сучасні реалії

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

Fortinet Security Fabric

Всебічне охоплення

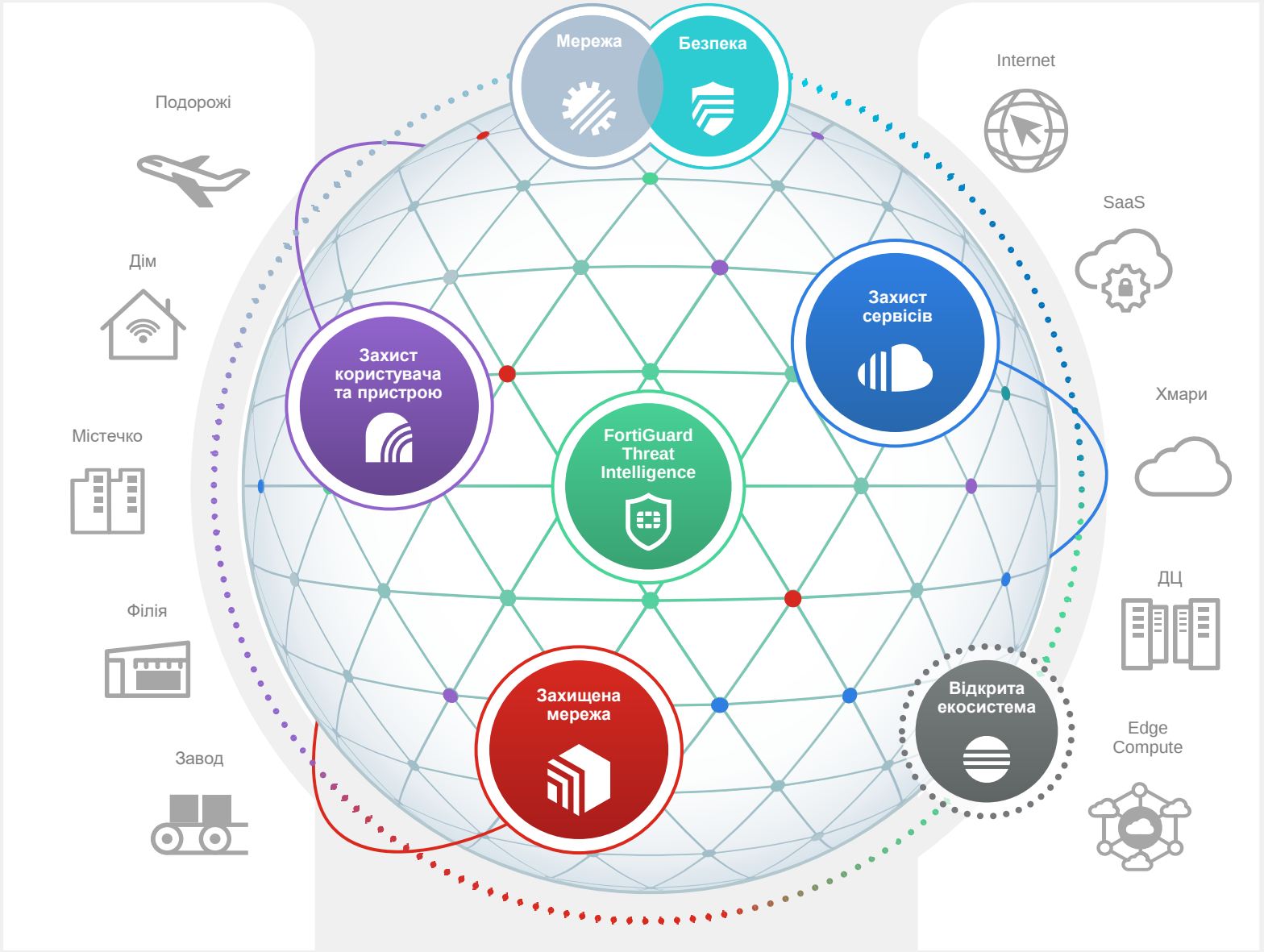
Багатовекторна видимість і захист для повного охоплення кібербезпеки

Інтеграція

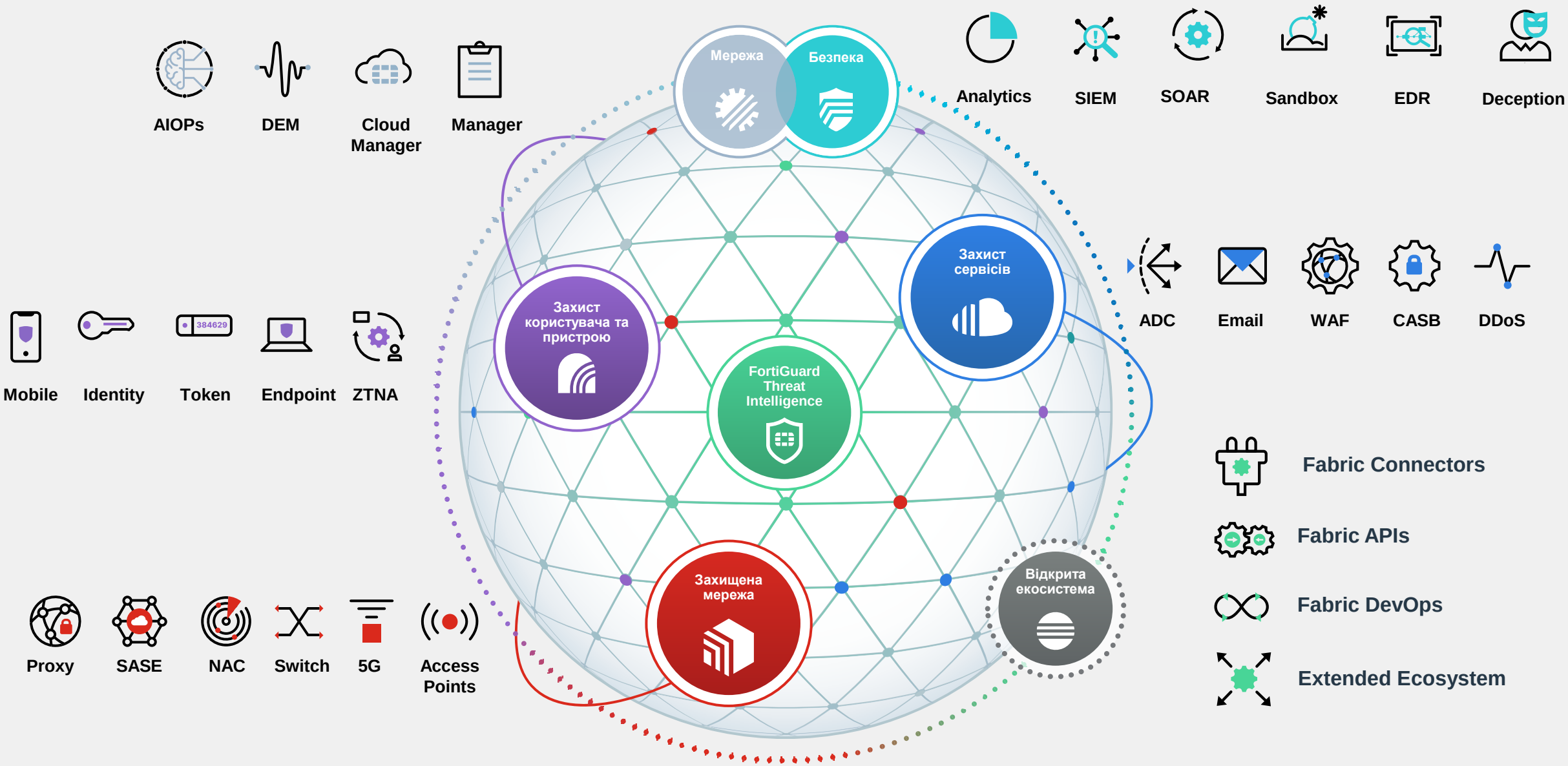
зменшує складність управління та обмінюється інформацією про загрози

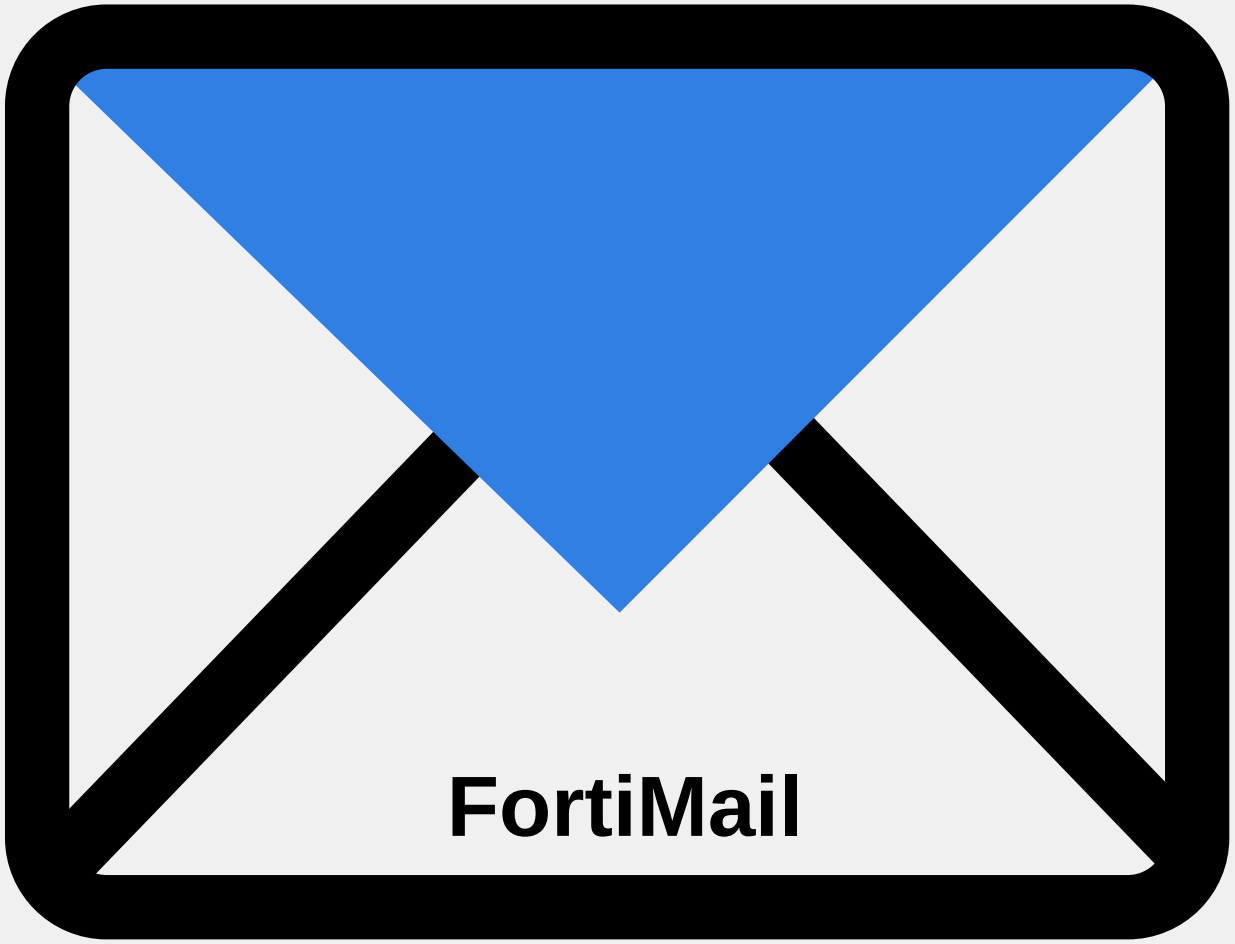
Автоматизація

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



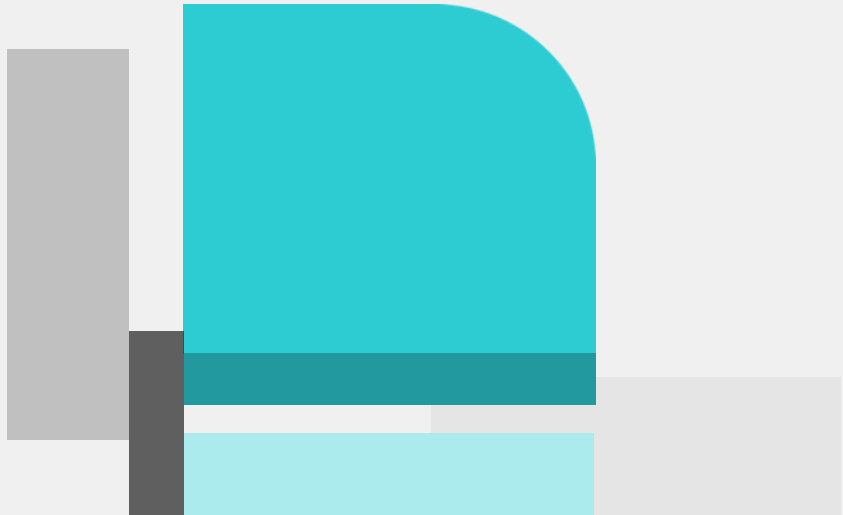
Fortinet Security Fabric



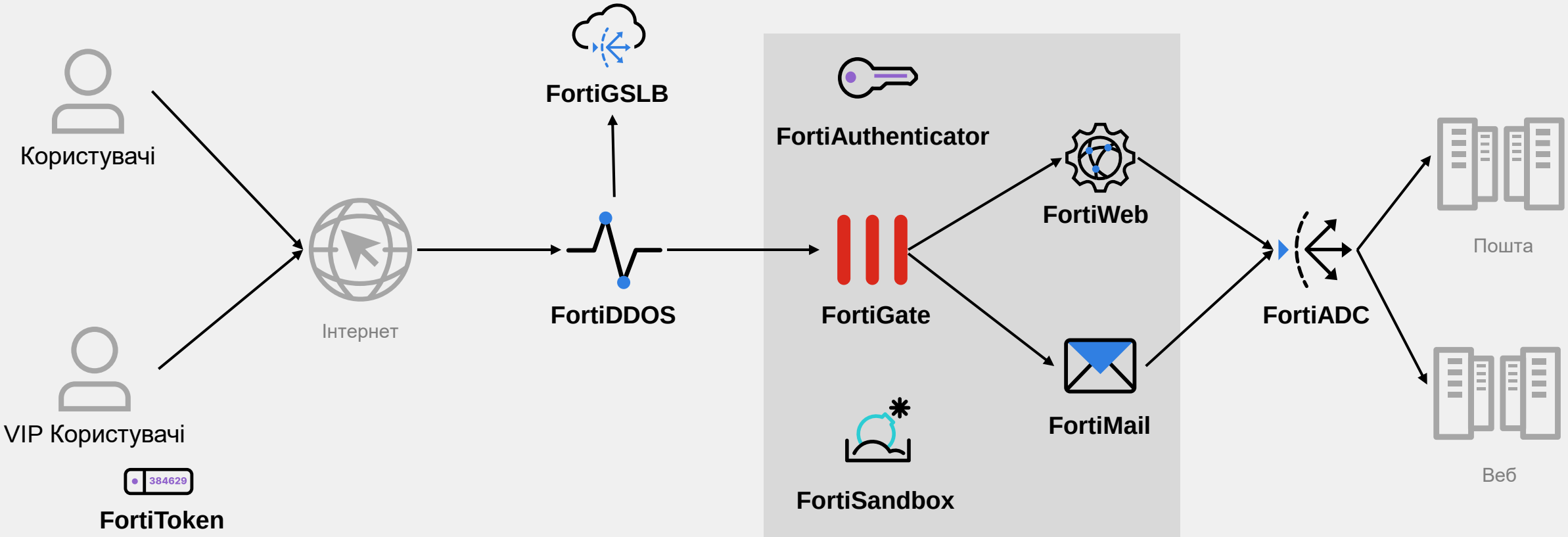


Сценарії побудови

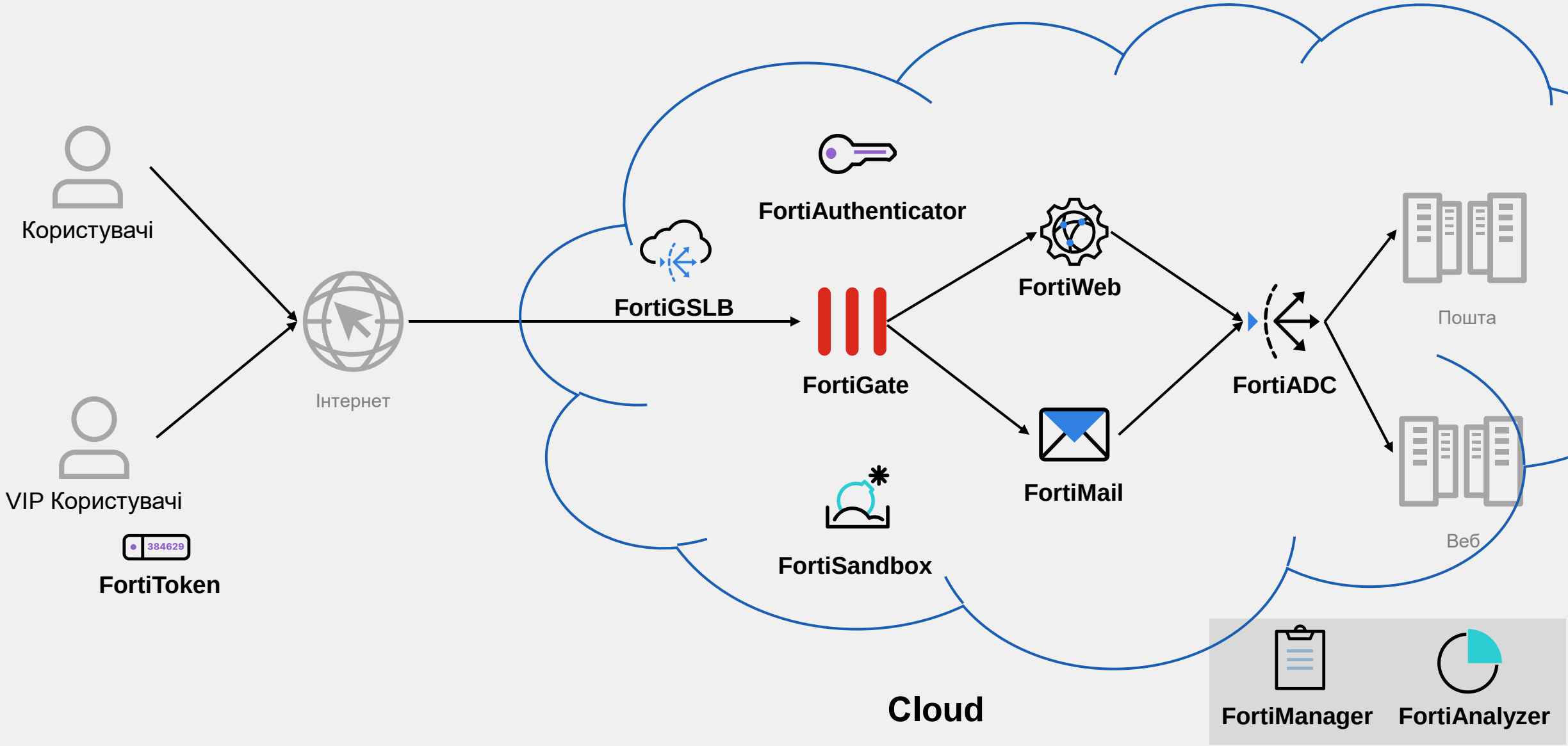
Фокусуємось на захисті пошти



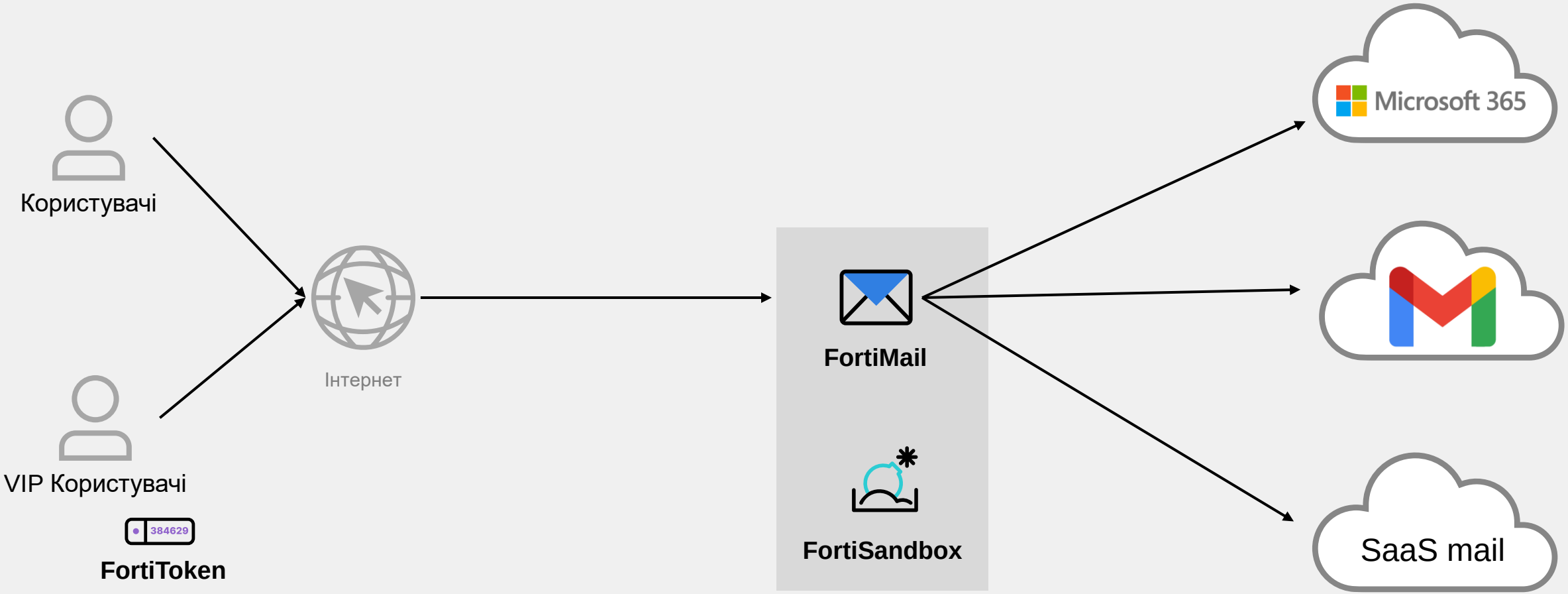
Сценарій 1. В локальному ДЦ



Сценарій 2. В хмарі

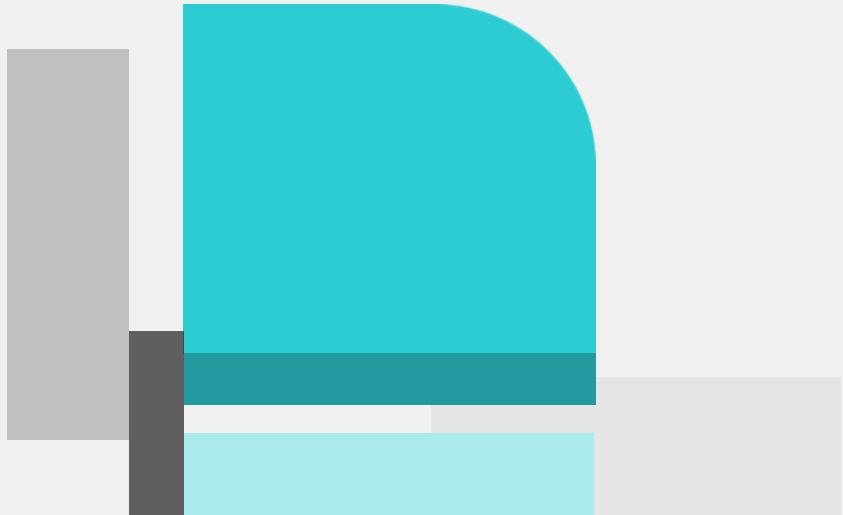


Сценарій 3. SaaS

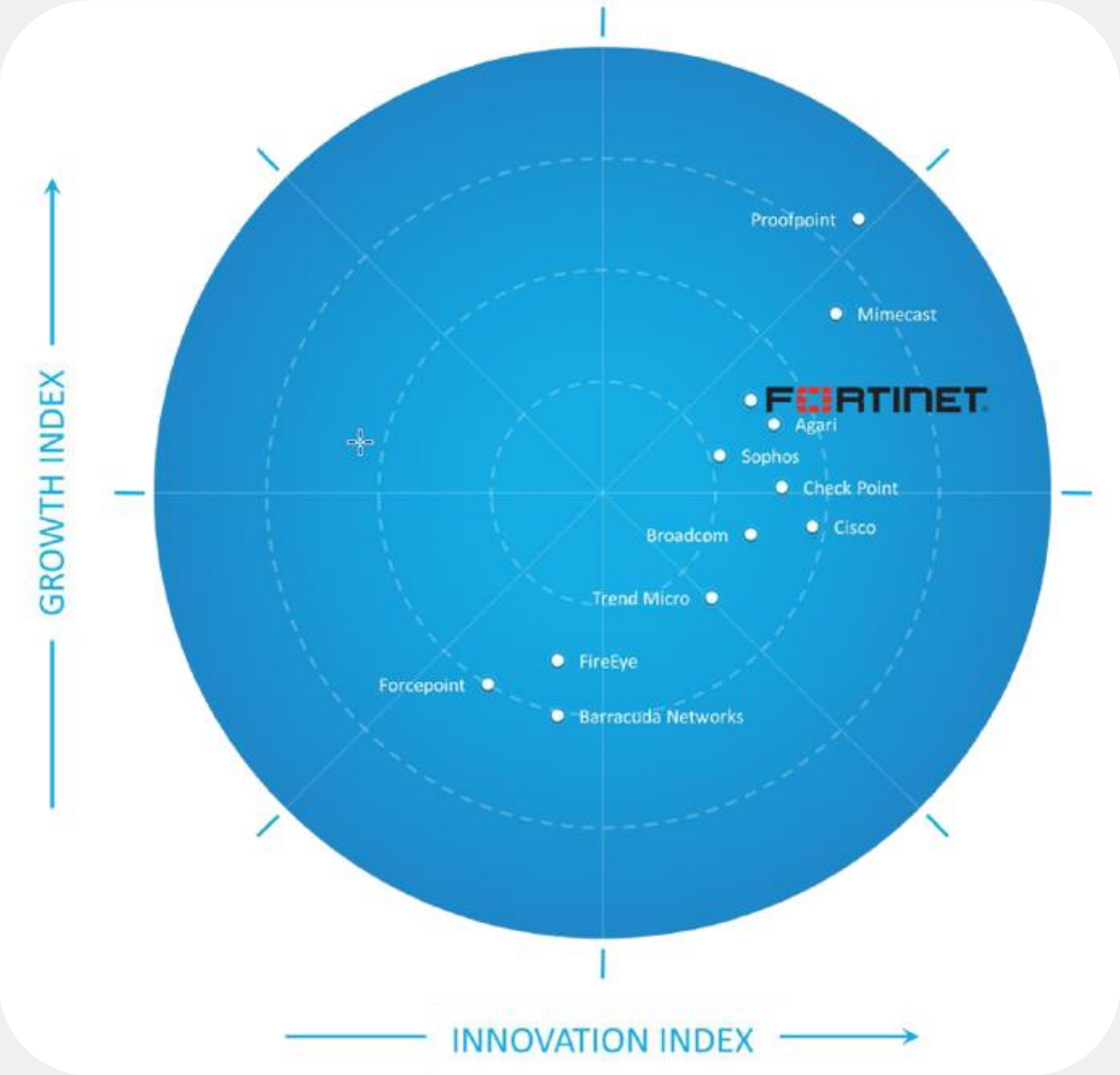


FortiMail

Чим він особливий?



Frost Radar™:
Звіт глобального ринку захисту електронної пошти



“Fortinet’s broader company vision places emphasis on the value of the Fortinet Security Fabric that integrates its extensive portfolio of security solutions.”

“Fortinet FortiMail is integrated into the Fortinet Security Fabric to enable advanced security outcomes in email (such as Sandbox, browser isolation, EDR), as well as contribute to the sharing of IOCs across security infrastructure in use by customers.”

Високі оцінки незалежних тестів

99.9%

Виявлення загроз в електронних ластах.

94%

Виявлення загроз

91%

Рівень захисту та швидкодії

90%

Точність

99.90%

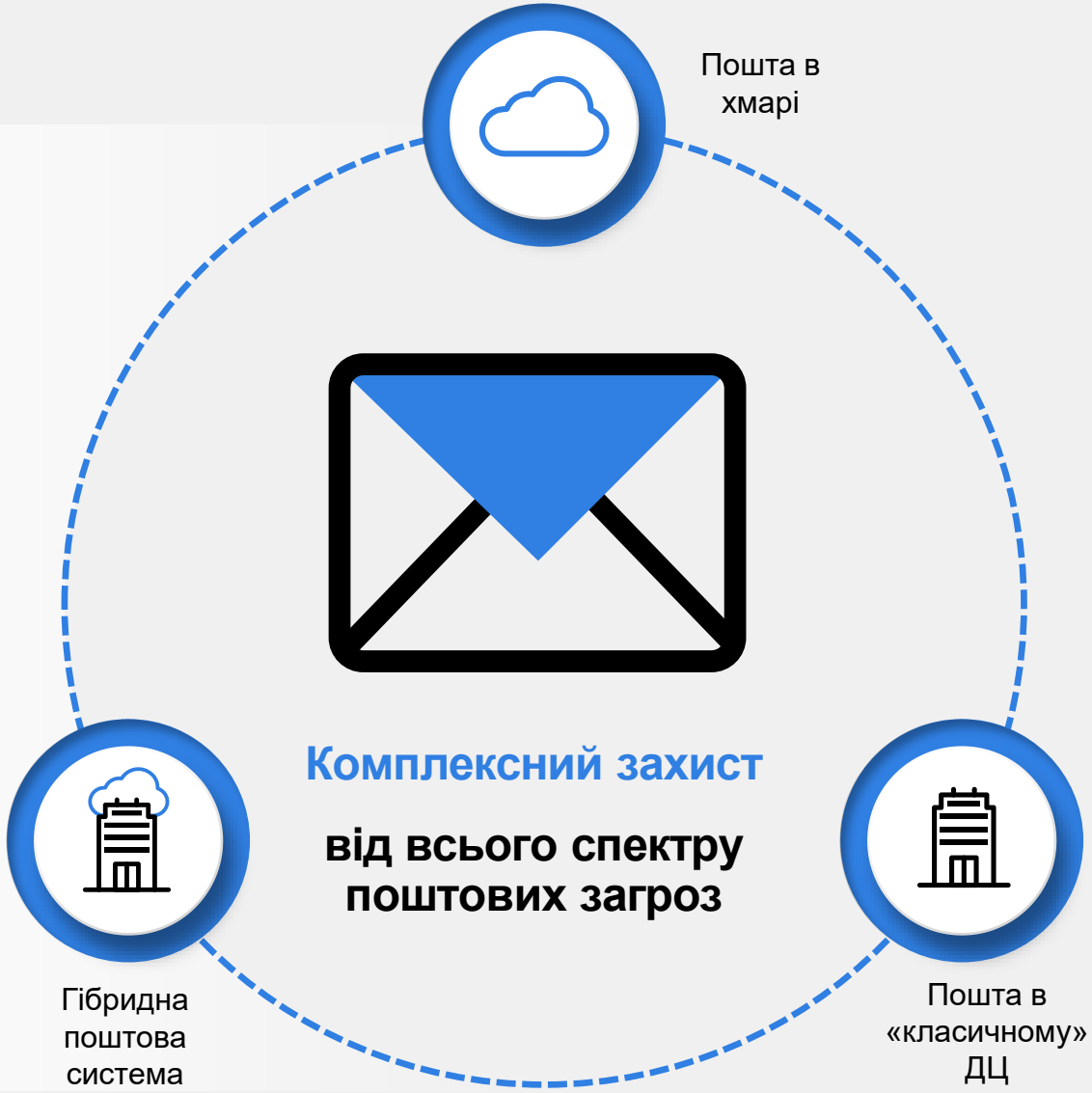
Спаму заблоковано

100%

Заражених файлів

FortiMail

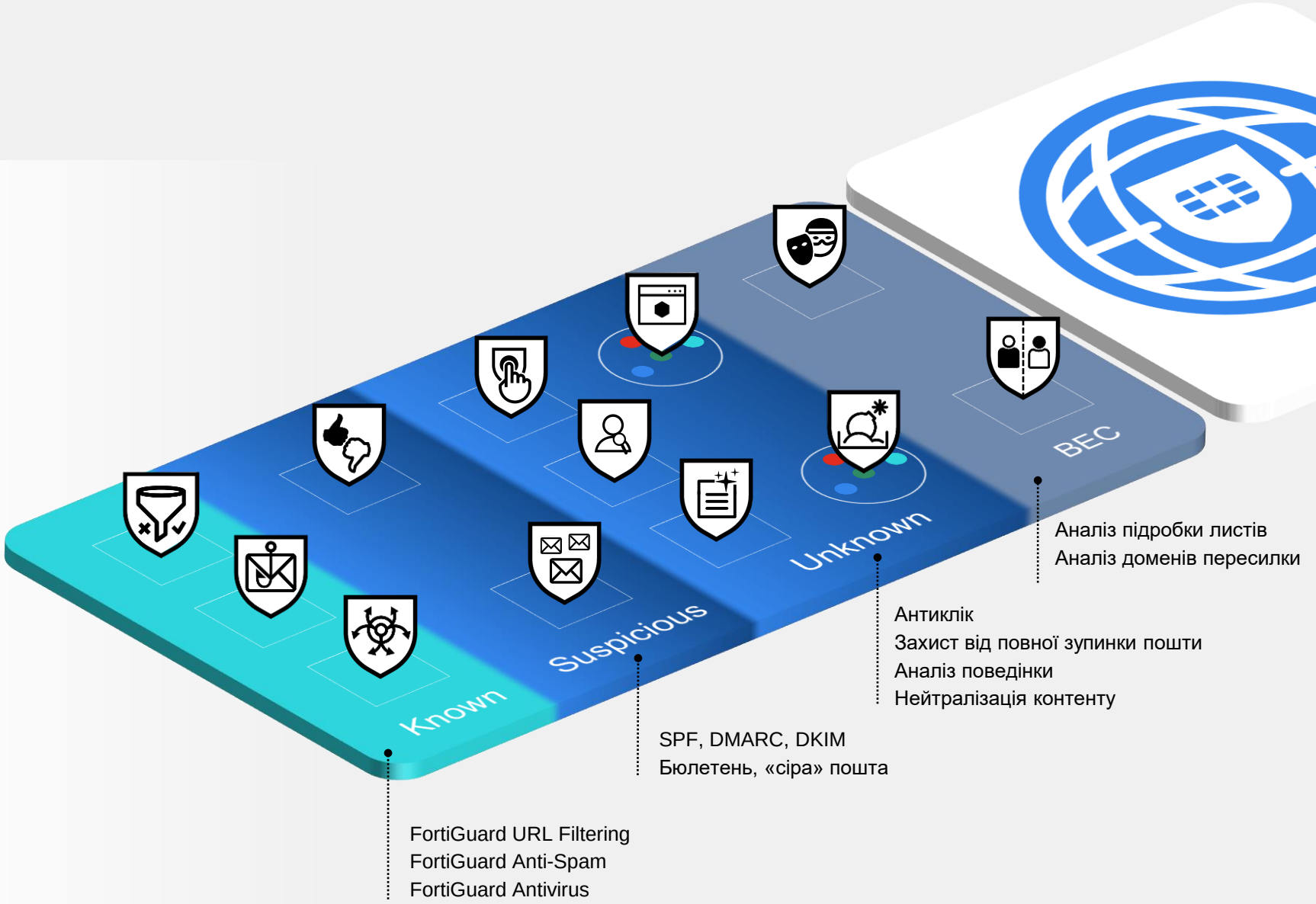
- Комплексний підхід
- Перевірена швидкодія
- Частина Security Fabric
- Власні напрацювання від FortiGuard Labs
- Лідер індустрії в категорії «ціна-швидкодія»



FortiMail

Багаторівнева безпека від:

- Відомих загроз
- Підозрілих листів
- Zero-days
- Видавання за іншу особу
- Компрометація вмісту листа



FortiMail

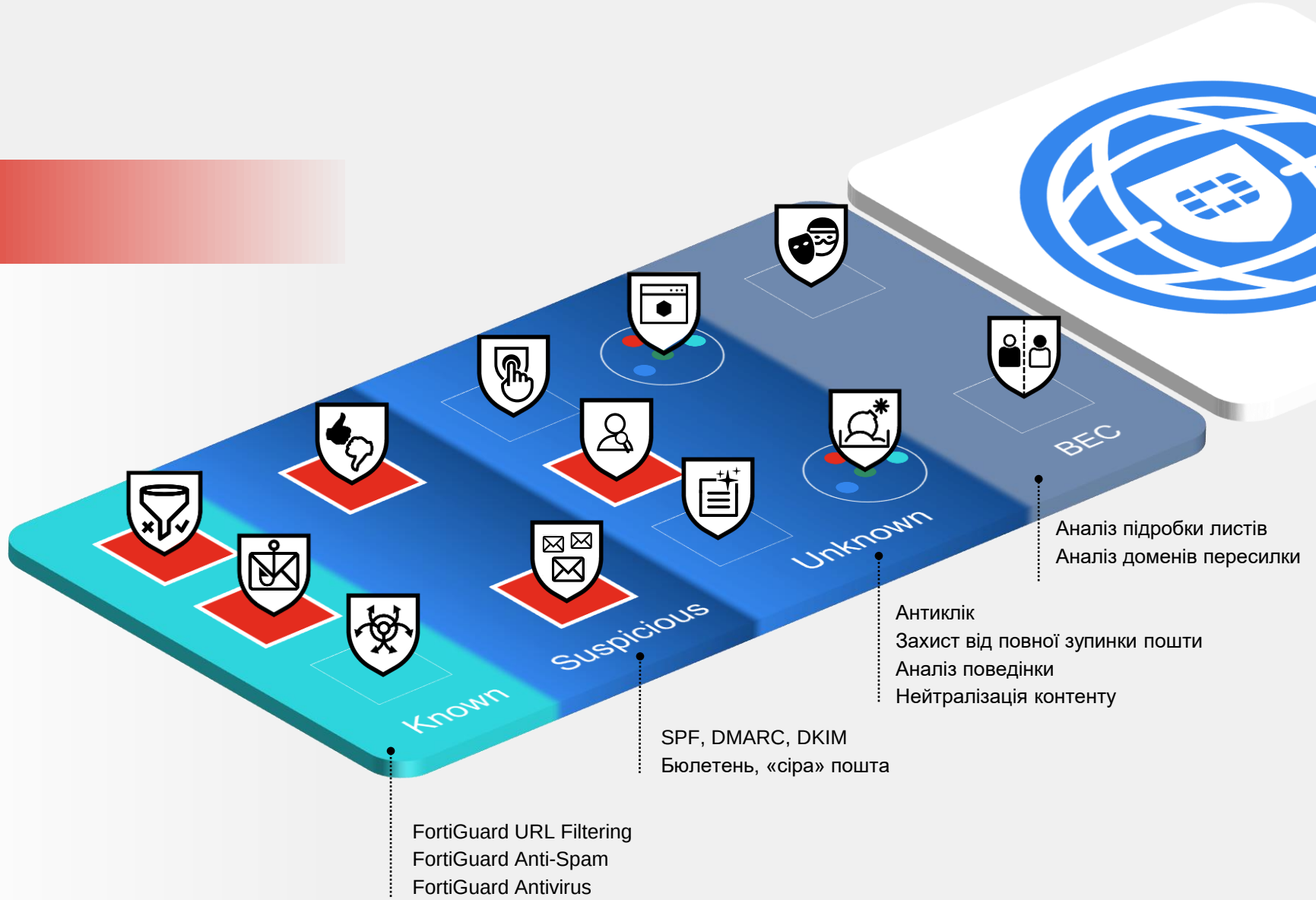
Приклад #1

Захист контенту:

- Спам, фішинг & підозріла пошта

Рішення:

- Швидко та ефективно вирішіть проблему об'ємного спаму



FortiMail

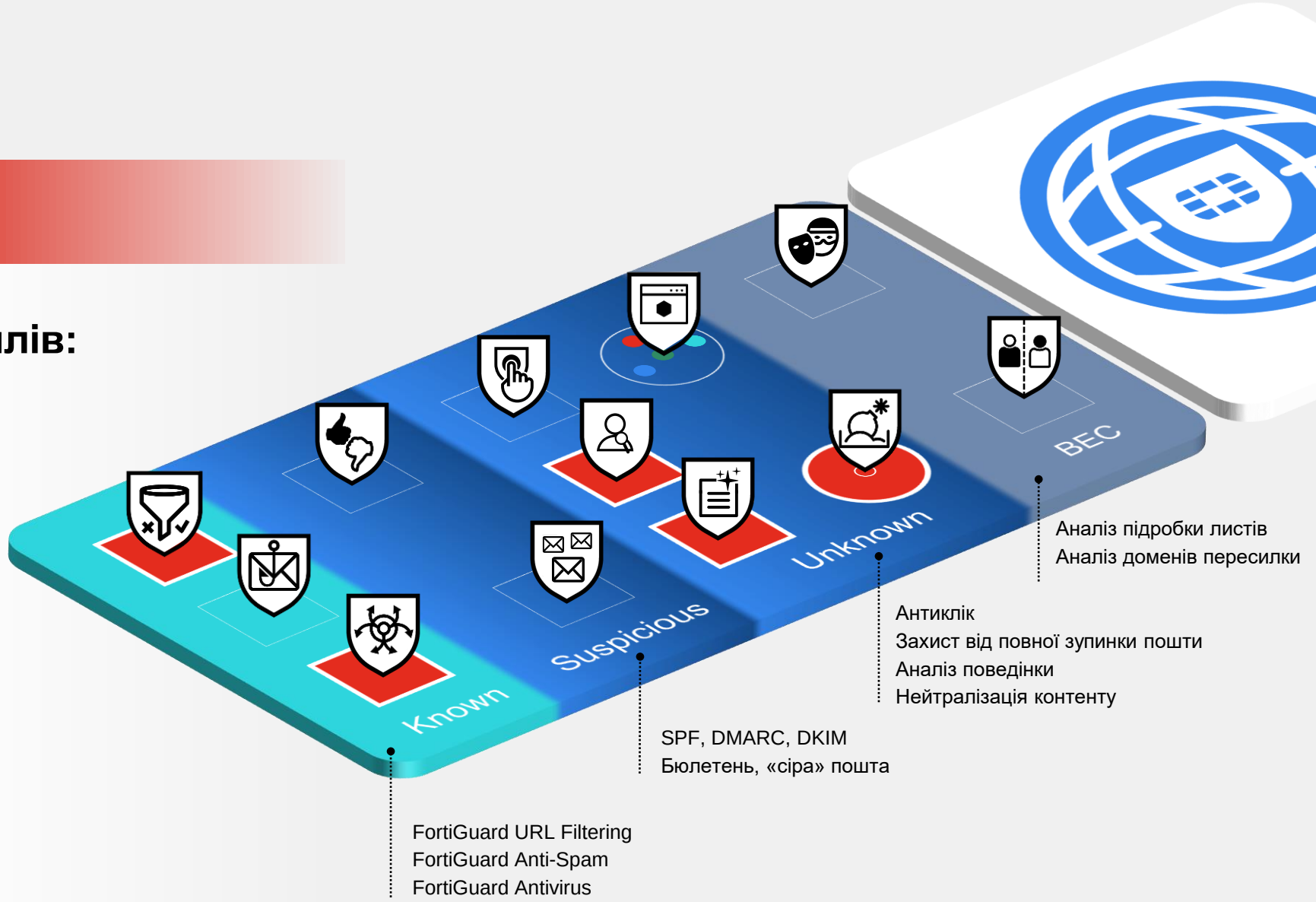
Приклад #2

Захист від шкідливих файлів:

- Файли та фішинг

Рішення:

- Розширені можливості, такі як пісочниця, аналізують підозрілі вкладення



FortiMail

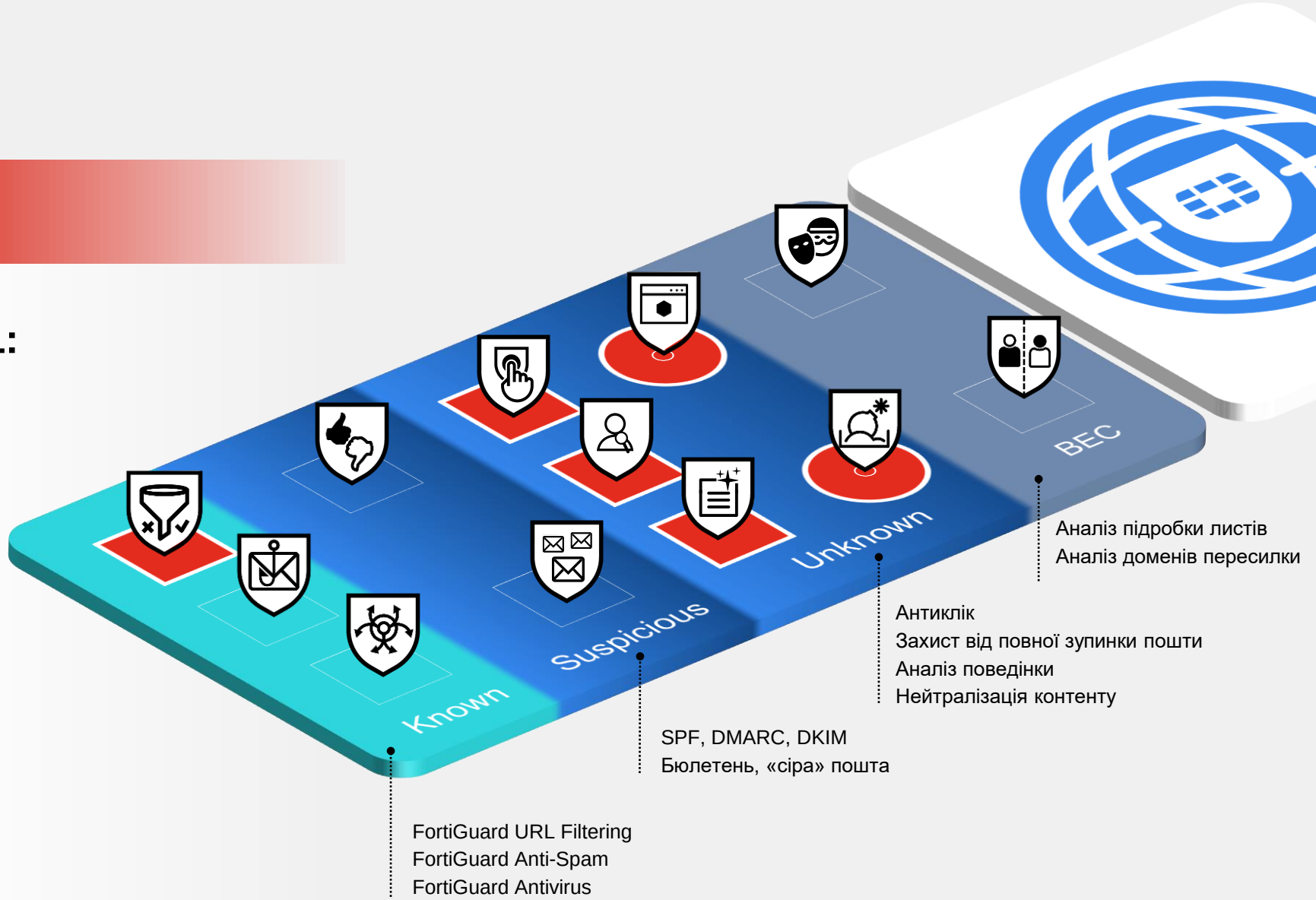
Приклад #3

Захист від шкідливих URL:

- Сайти підробки & фішинг
- Інтернет як джерело загрози

Рішення:

- Інтеграція з захистом URL-адрес, дозволяє блокувати загрози без впливу на бізнес.



FortiMail

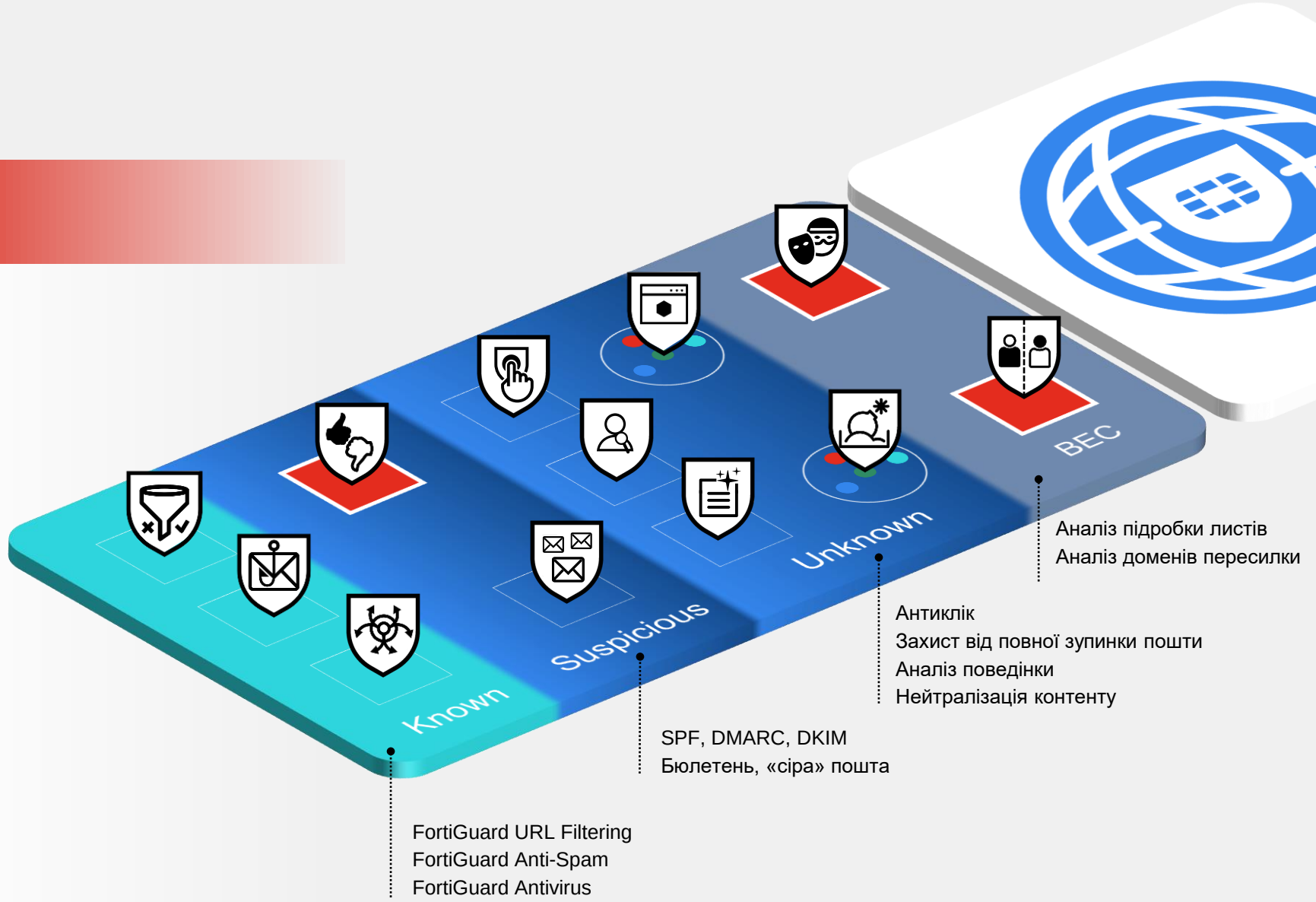
Приклад #4

Business Email Compromise Prevention:

- Спотворення листів та адресатів
- Цільові атаки

Рішення:

- Додаткові методики захисту від підробних та спотворених листів

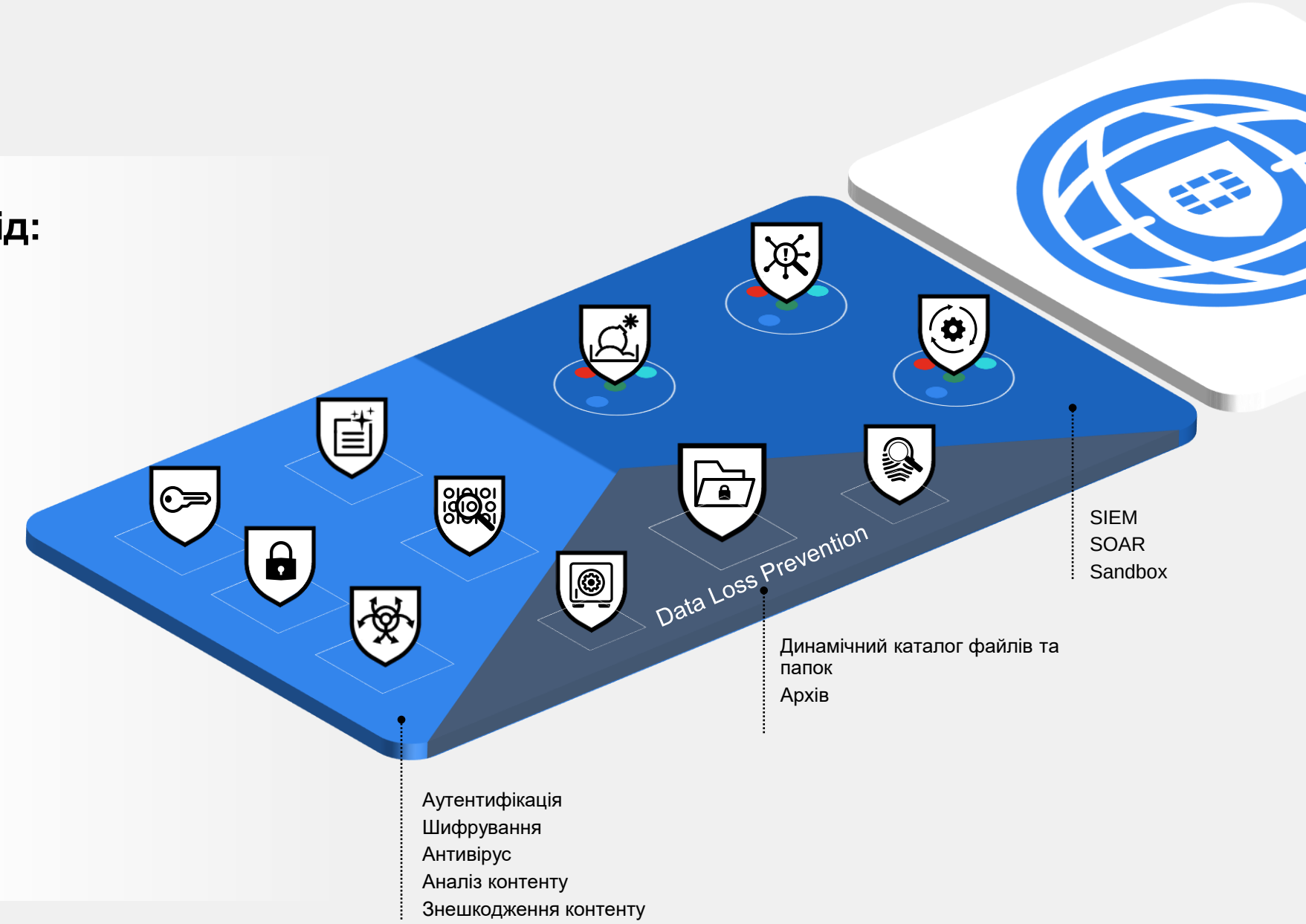


FortiMail

Багаторівневий захист від:

- Розголос конфіденційних даних
- Витік даних
- Man-in-the-Middle Attacks

З підтримкою автоматизації



Комплексний захист

Захист вхідної пошти

- Фішинг/Spear/Whale Phishing
- Підробка відправника
- Зміна вмісту
- Цільові атаки
- Ransomware за допомогою email
- Контент «для дорослих»
- СПАМ

Захист вихідної пошти

- Блокування відповідей на заражені листи
- Захист від витоку даних
- Шифрування
- Man-in-the-middle attacks

Компоненти

Шкідливий вміст

Шкідливі файли

Шкідливі URLs

Форм фактори

Appliance

VM

FortiMail Cloud

Режими роботи

Gateway

Transparent

Server

O365 API

Варіанти рішення та сайзинг

Власний пристрій

Рішення для організацій які бажають отримати повний контроль над захистом пошти

Апаратні пристрої

- 5 моделей
- До 3.2M листів на годину
- Підтримка 10GE

Віртуальні машини

- 6 моделей
- Ліцензування по CPU або подоменно
- Постійна ліцензія або підписка

Послуга захисту

Рішення які бажають отримати захист пошти в форм факторі SaaS

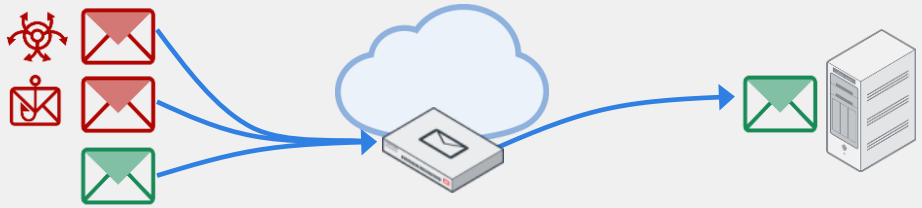
SaaS/API*

- Керується Fortinet
- Gateway або Server режими
- Standard або Premium сервіс
- Ліцензування по кількості ящиків

Режими роботи

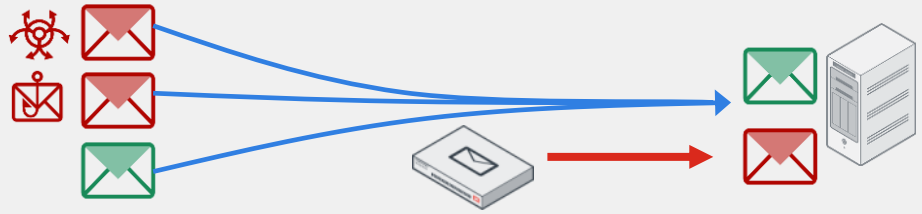
Gateway Mode (Cloud and Appliance)

Пошта доставляється в FortiMail через MX, перевіряється і пересилається на поштовий сервер призначення.



Microsoft 365 API Clawback (Cloud and Appliance)

FortiMail працює поза мережею, сканує і видаляє загрози безпосередньо в Microsoft 365 за допомогою Graph API. Також можна використовувати в режимі шлюзу.



Server Mode (Cloud and Appliance)

FortiMail розгорнуто як повноцінний поштовий сервер, що забезпечує POP3, IMAP, веб-пошту та календар на додачу до функцій безпеки.

Transparent Mode (Appliance)

Встановлюється на шляху SMTP трафіку. Не потрібні зміни конфігурації тож зазвичай використовується в середовищі де немає доступу до адміністрування поштової системи

FortiMail

	Власний пристрій		
Feature	Base Bundle	Enterprise Advanced Threat Protection Bundle	Ent. ATP with Microsoft O365 API Support Bundle
99.7% Spam detection rate	●	●	●
Advanced multi-layer malware detection	●	●	●
Inbound and outbound filtering	●	●	●
Integration with customer LDAP	●	●	●
Secure message delivery (TLS and DANE)	●	●	●
Message tracking	●	●	●
Virus Outbreak Service	●	●	●
Identity-Based Encryption (IBE)	●	●	●
Reporting	●	●	●
Email Data Loss Prevention	●	●	●
Content Disarm and Reconstruction		●	●
URL Click Protection		●	●
Impersonation Analysis		●	●
Cloud Sandboxing		●	●
Real-time scanning of Microsoft 365 mailboxes			●
Scheduled scanning of Microsoft 365 mailboxes			●
Post-delivery clawback of newly discovered email threats			●

FortiMail Cloud

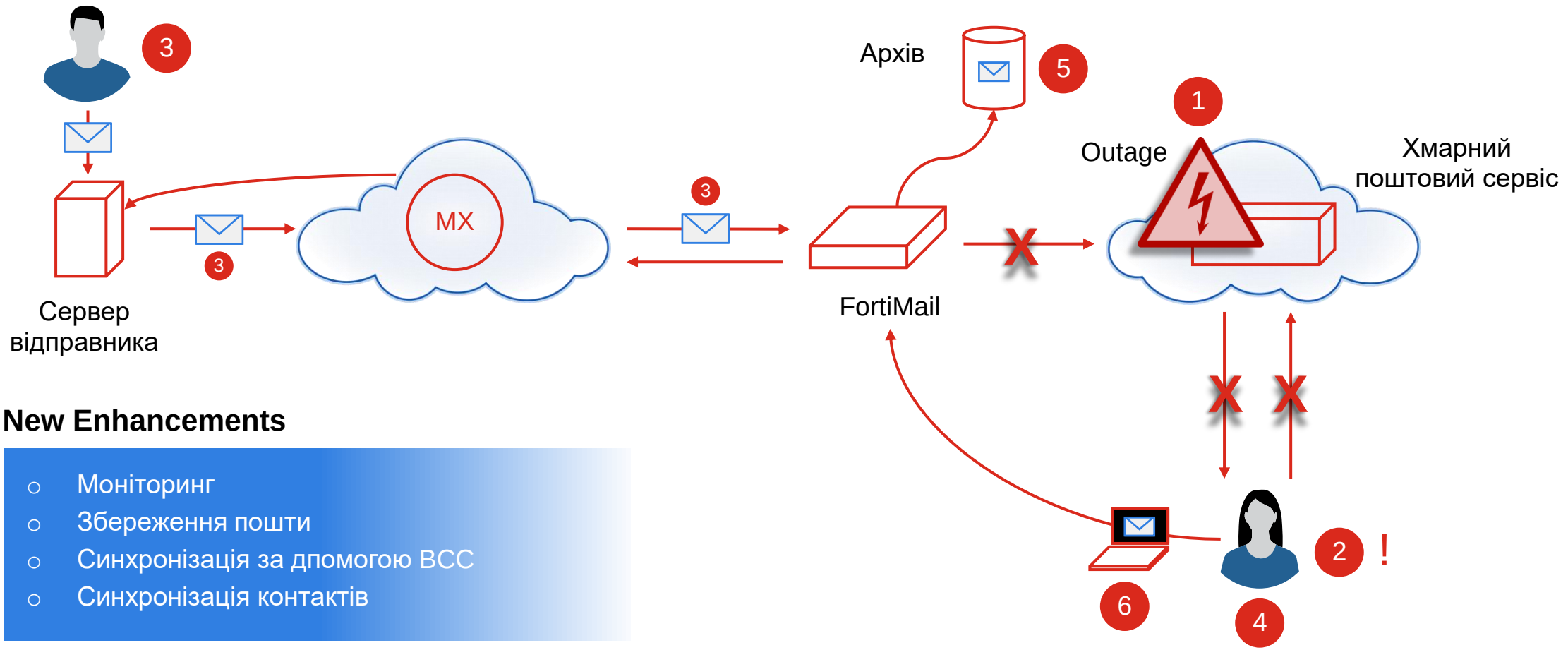
	Послуга захисту		
Feature	Cloud Gateway	Cloud Gateway Premium	Cloud Gateway Premium with Microsoft 365 API Support
Managed Service (infrastructure)	●	●	●
99.999% Service availability	●	●	●
99.7% Spam detection rate	●	●	●
Advanced multi-layer malware detection	●	●	●
Inbound and outbound filtering	●	●	●
Integration with customer LDAP	●	●	●
Secure message delivery (TLS and DANE)	●	●	●
Message tracking	●	●	●
Virus Outbreak Service	●	●	●
Reporting	●	●	●
Content Disarm and Reconstruction		●	●
URL Click Protection		●	●
Impersonation Analysis		●	●
Cloud Sandboxing		●	●
Identity-Based Encryption (IBE)		●	●
Email Data Loss Prevention		●	●
Real-time scanning of Microsoft 365 mailboxes			●
Scheduled scanning of Microsoft 365 mailboxes			●
Post-delivery clawback of newly discovered email threats			●

Безперервність пошти з FortiMail Cloud

Функція безперервності електронної пошти призначена для захисту критичної інформації надаючи послуги екстреної поштової скриньки в разі падіння основної поштової системи.

Користувачі отримують доступ до електронної пошти в безпосередньо на FortiMail.	Скорочує час відновлення майже до нуля.	Збереження пошти до 30 днів.

Безперервність пошти з FortiMail Cloud



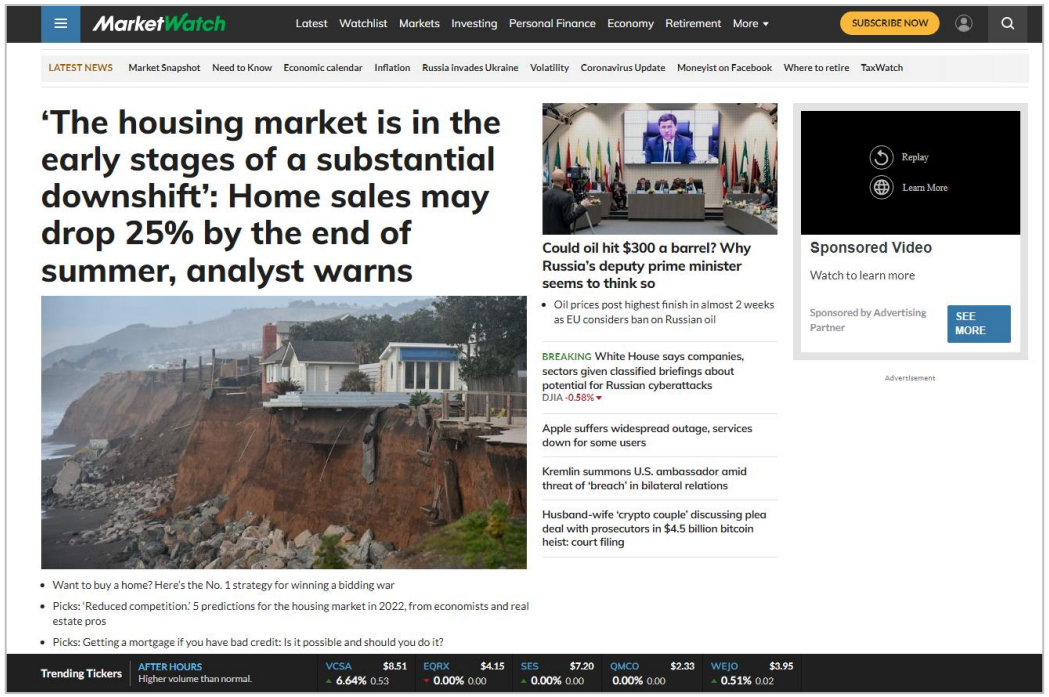
New Enhancements

- Моніторинг
- Збереження пошти
- Синхронізація за дпомогою BCC
- Синхронізація контактів

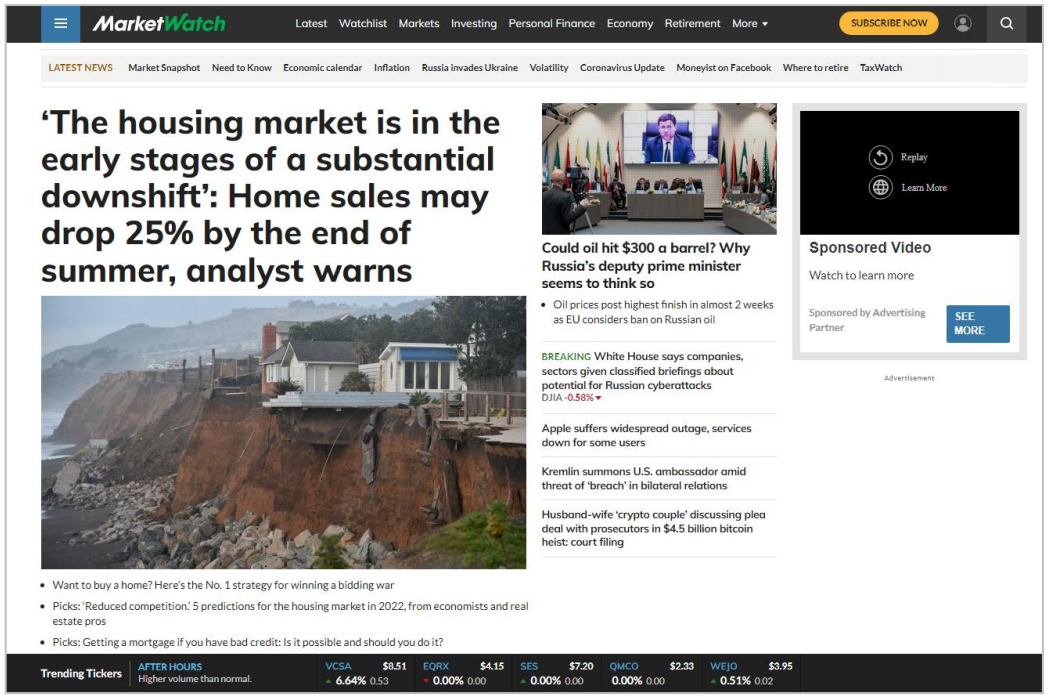
FortiIsolator – Безпечне відображення контенту

Дозволяє користувачам переглядати веб-сторінки в ізольованому середовищі, що робить безпечний вміст у віддаленому контейнері.

Прямий доступ з Chrome



Доступ через FortiIsolator з Chrome



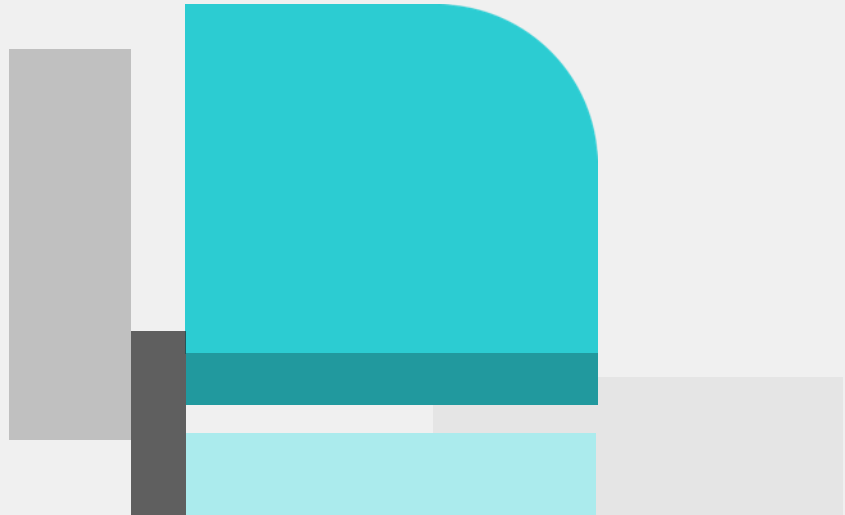
Сервіс аналізу зображень

Захищає мережу від зображень сексуального вмісту

- Визначає підозрілі вкладені зображення
- Інформує користувачів про політику компанії при виявленні сумнівного вмісту
- Відстежує та реєструє/архівує електронні листи, щоб забезпечити видимість подій
- Забезпечує дотримання політики компанії, вживаючи відповідних заходів щодо електронних листів, що містять відвертий вміст

Захист Office365

Особливості



Інтеграція з Office365

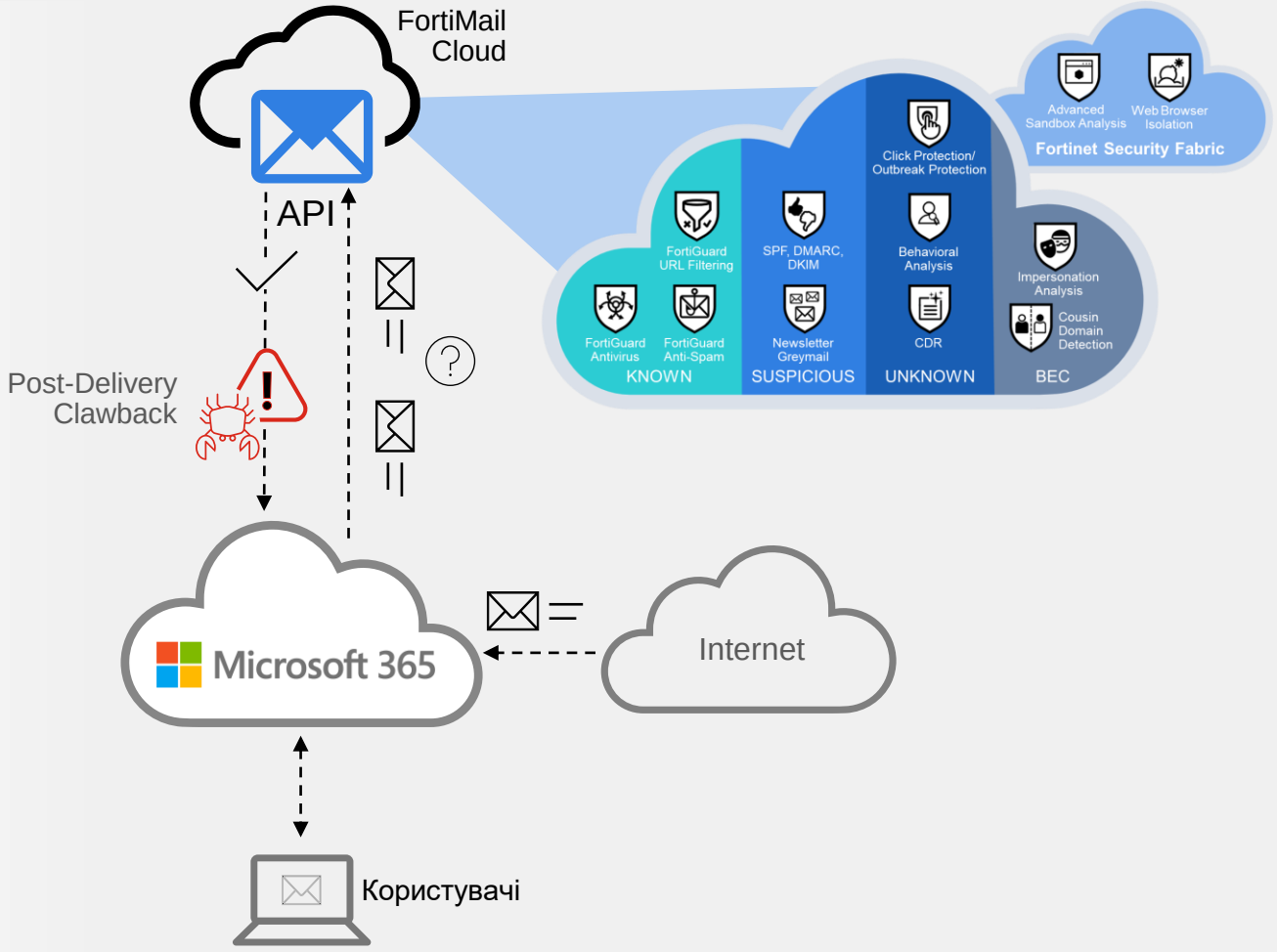
Безпека хмарної пошти

Доповнення безпеки електронної пошти Microsoft 365 за допомогою Fortinet:

- Out of band впровадження
  - Просте налаштування без зміни MX
  - Просте демо без впливу на пошту
  - Робота в реальному часі
- Сканування внутрішніх листів
- Можливість відкликання листа

Microsoft 365, FortiMail працює з Microsoft 365 в режимі API або Gateway.

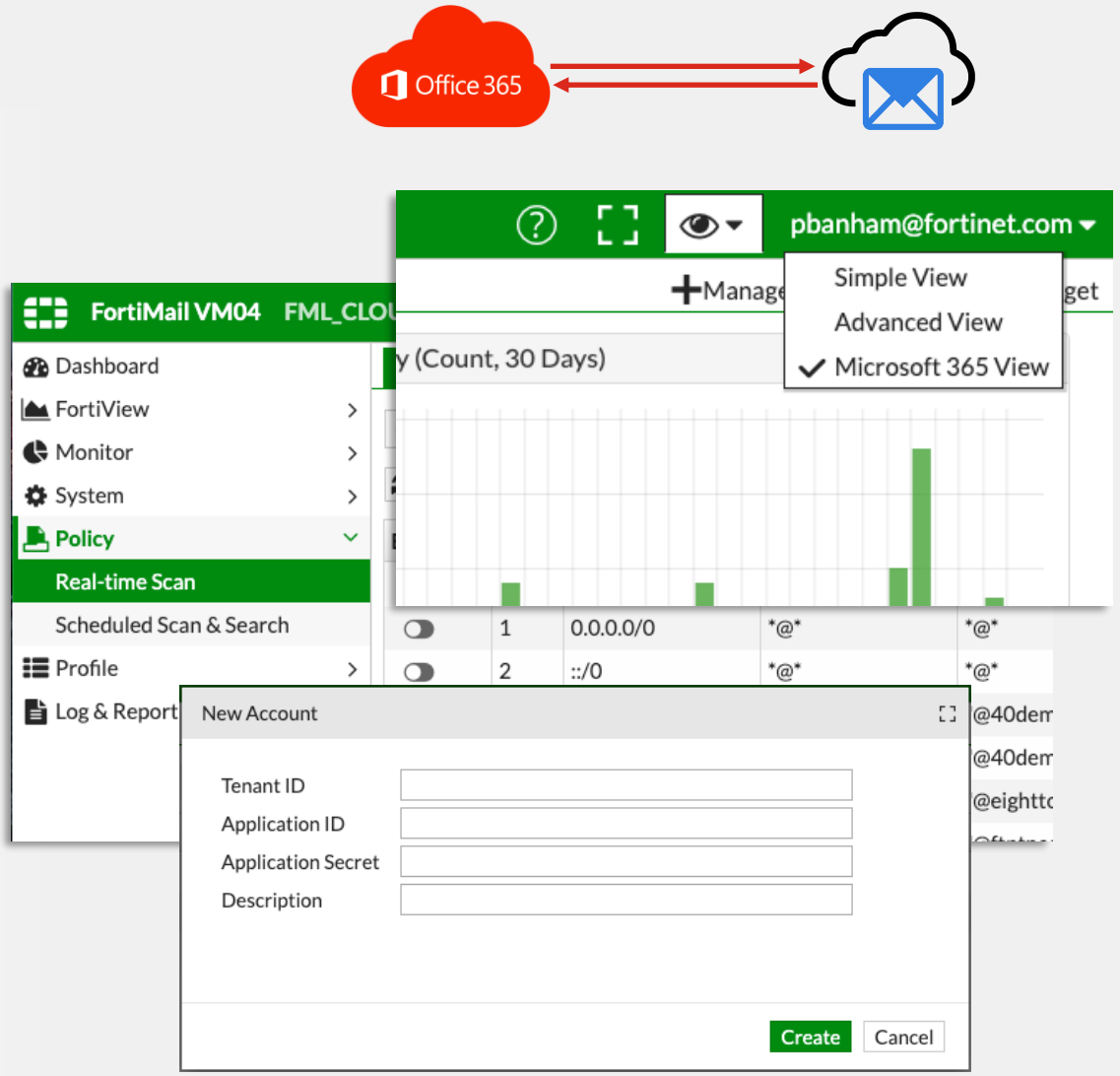
Google Workspace, Тільки в режимі Gateway



Statistics from Verizon Data Breach Investigations Report 2021

FortiMail: Microsoft 365

- Врахована специфіка Microsoft 365
- Сканування в реальному часі або «за розкладом»
- Пошук листів та карантин
- Приховує/видаляє повідомлення під час доставки або у фоновому режимі
- Доступне як на SaaS FortiMail так і на класичних пристроях/VM
- Можливість вибіркового захисту



А як щодо вбудованого захисту?

DATA SHEET | FortiMail™

SPECIFICATIONS

TECHNICAL SPECIFICATIONS FOR FORTIMAIL VIRTUAL APPLIANCES	VM01	VM02	VM04	VM08	VM16	VM32
Recommended Deployment Scenarios *						
	Small businesses, branch offices, and organizations	Small to midsized organizations	Mid to large enterprise	Large enterprise	Large enterprise	Large enterprise
Technical Specifications						
Hypervisors Supported	VMWare ESX/ESXi 6.0/6.7/7.0 and later, Citrix XenServer v5.6 SP2/6.0 and later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1 and later, AWS (Amazon Web Services), Nutanix AHV**, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure***					
Maximum Virtual CPUs Supported	1	2	4	8	16	32
Virtual NICs Required (Minimum/Maximum)	1 / 4	1 / 4	1 / 6	1 / 6	1 / 6	1 / 6
Virtual Machine Storage Required (Minimum/Maximum) ****	250 GB / 1 TB	250 GB / 2 TB	250 GB / 4 TB	250 GB / 8 TB	250 GB / 12 TB	250 GB / 24 TB
Virtual Machine Memory Required (Minimum/Maximum)	2 GB / 4 GB	2 GB / 8 GB	4 GB / 16 GB	4 GB / 64 GB	4 GB / 128 GB	4 GB / 128 GB
Performance (Messages/Hour) [Without queuing based on 100 KB message size] *****						
Email Routing	34 K	67 K	306 K	675 K	875 K	1.2 M
FortiGuard Antispam	30 K	54 K	279 K	630 K	817 K	1.1 M
FortiGuard Antispam + Antivirus	26 K	52 K	225 K	585 K	758 K	1.0 M
System Specifications						
Protected Email Domains ******	20	70	500	1000	1500	2000
Recipient-Based Policies (Domain / System) — Incoming or Outgoing	60 /300	400 / 1500	800 / 3000	800 / 3000	1500 / 7500	1500 / 7500
Server Mode Mailboxes	150	400	1500	2000	3000	3000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 400	50 / 400	50 / 600	50 / 600
Data Loss Prevention	No	Yes	Yes	Yes	Yes	Yes
Centralized Quarantine	No	Yes	Yes	Yes	Yes	Yes
Microsoft 365 API Integration	No	Optional	Optional	Optional	Optional	Optional

Sta

Microsoft Defender for Office 365 (Plan 2)

$5.00 user/month

Defender for Office 365 Plan 2 offers everything in Plan 1 plus advanced threat hunting, automation, attack simulation training, and cross-domain XDR capabilities.

Contact Sales

- Protection against advanced attacks, such as phishing, malware, spam, and business email compromise
- Protection beyond email (Microsoft Teams, SharePoint, OneDrive, and Office apps)
- Internal email protection
- Detailed reporting
- Advanced threat hunting
- Automated investigation and response

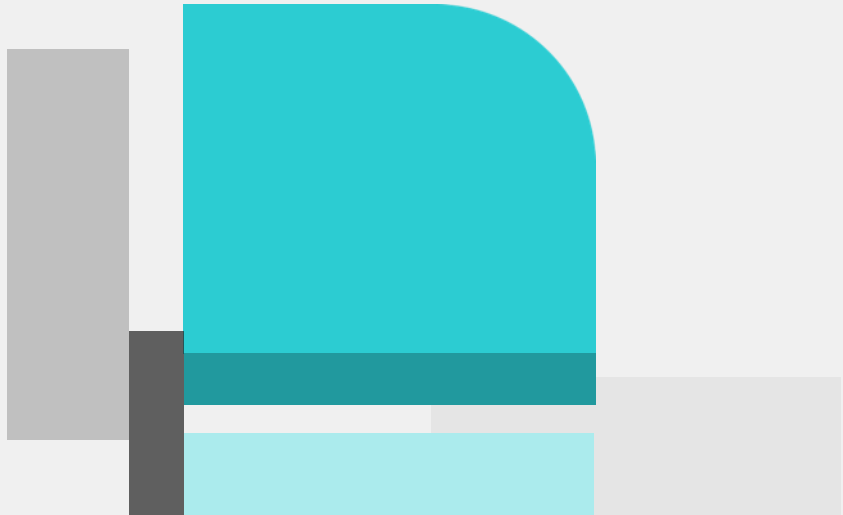
А як щодо вбудованого захисту?

Executive Summary					
Product Tested	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)	Award
Perception-Point	2,310	1,100	3,410	100%	AAA
Fortinet FortiMail Cloud Email Security	2,165	1,060	3,225	95%	AAA
Microsoft Defender for Office 365	2,230	800	3,030	89%	AAA
Google Workspace Enterprise	-180	1,100	920	27%	C

[Email Security Services Enterprise and Small Business Jane 2022 (selabs.uk)]

Як налаштовувати?

Особливості



Google setup

Add FortiMail as mail route host

https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/666636/add-fortimail-as-mail-...

FORTINET

DOCUMENT LIBRARY

Product Pillars | Best Practices | Hardware Guides | Product A-Z

Home > FortiMail 7.2.0 > Cookbook

CLI

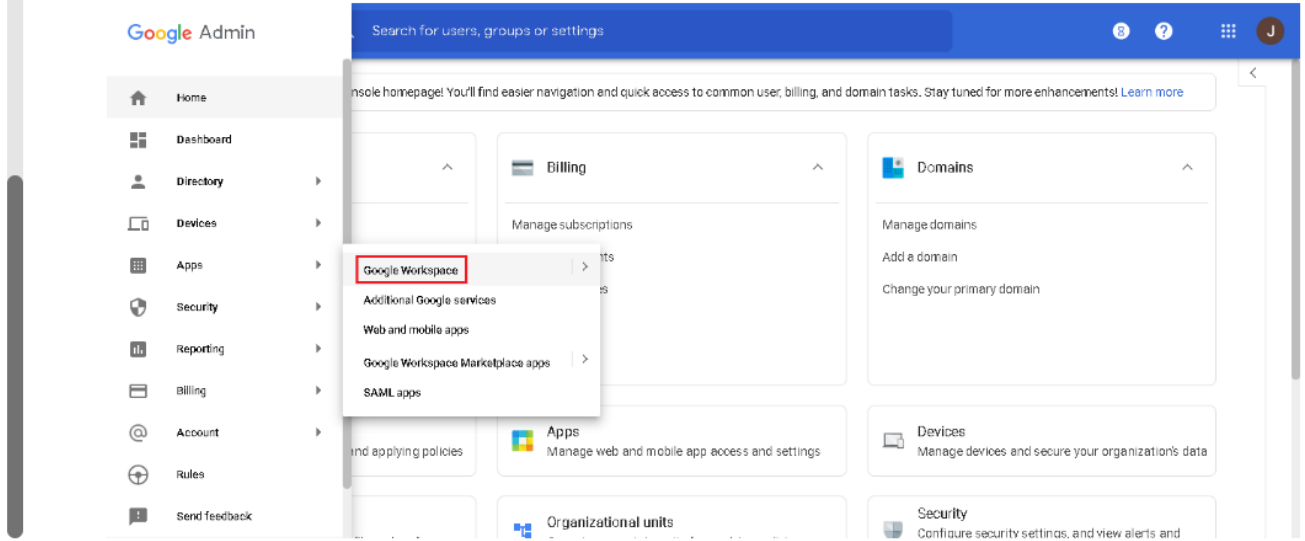
- Configuring and viewing FortiMail log messages
- Real-time scanning of Microsoft 365 email in FortiMail
- Integrating FortiSandbox with FortiMail
- Remote logging in FortiMail using FortiAnalyzer
- Securing outbound email from Google Workspace
  - **Add FortiMail as mail route host in Google Workspace**
  - Route all outbound mail from Google Workspace through FortiMail
  - Configure access control rule and recipient policy on FortiMail
- Using SMTP authentication in FortiMail
- Upgrading FortiMail firmware in HA mode
- Change Log

7.2.0 | Copy Link | Download PDF

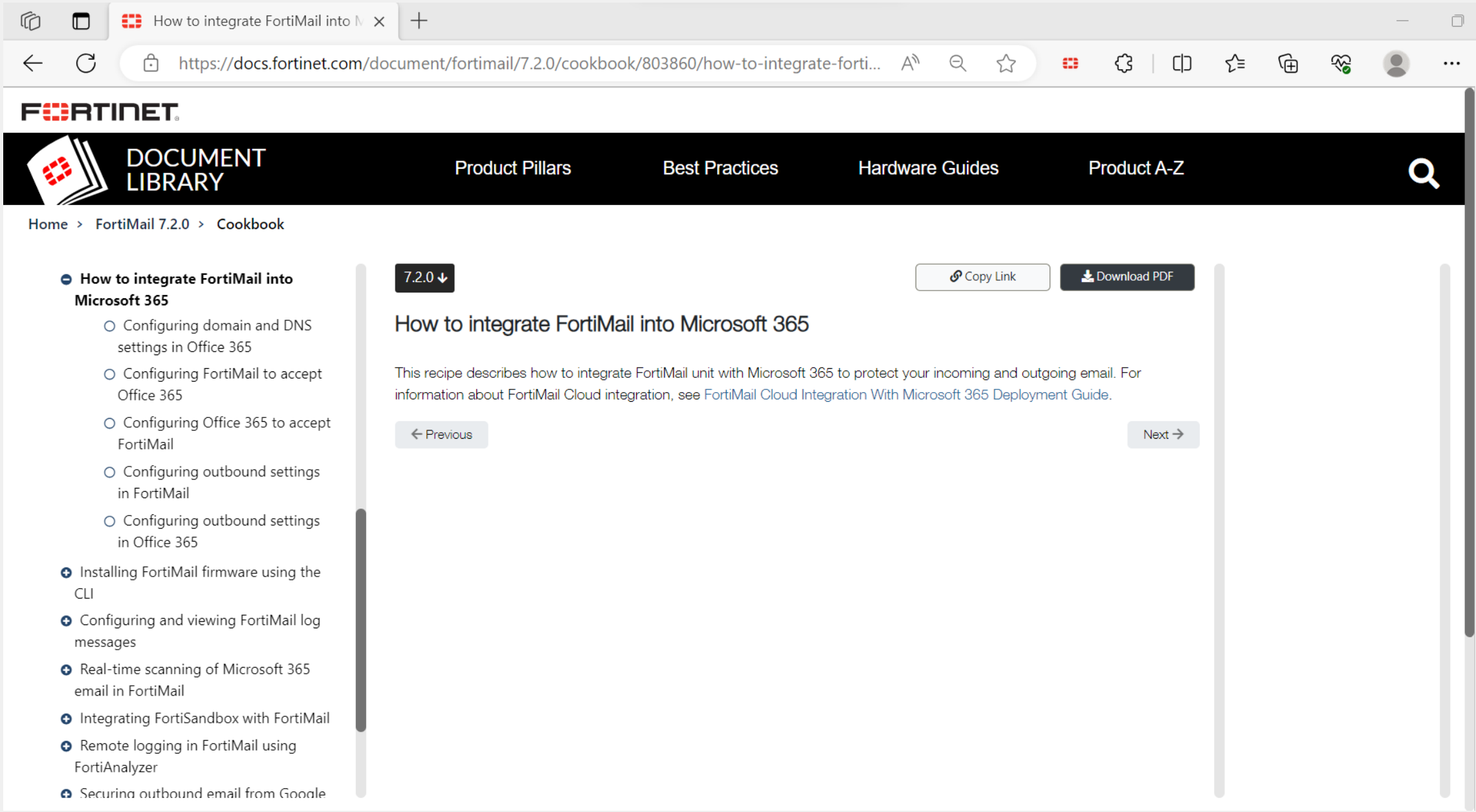
Add FortiMail as mail route host in Google Workspace

This topic describes how to add FortiMail/FortiMail Cloud as the mail route host.

1. Log in to Google Workspace using your administrative credentials.
2. From the *Admin Console* dashboard, click the expandable *Main menu* and click *Apps* > *Google Workspace*.



Office 365 setup



Безпека починається з пошти

FortiMail

- Комплексний захист
- Частина комплексу захисту Security Fabric
- Використання власного центру FortiGuard Labs.
- Перевірена продуктивність та ефективність
- Різні форм фактори та ліцензування

Дякую за увагу!


FORTINET