Захист веб та API сервісів за допомогою FortiWeb. Інтеграція з FortiGate.

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…

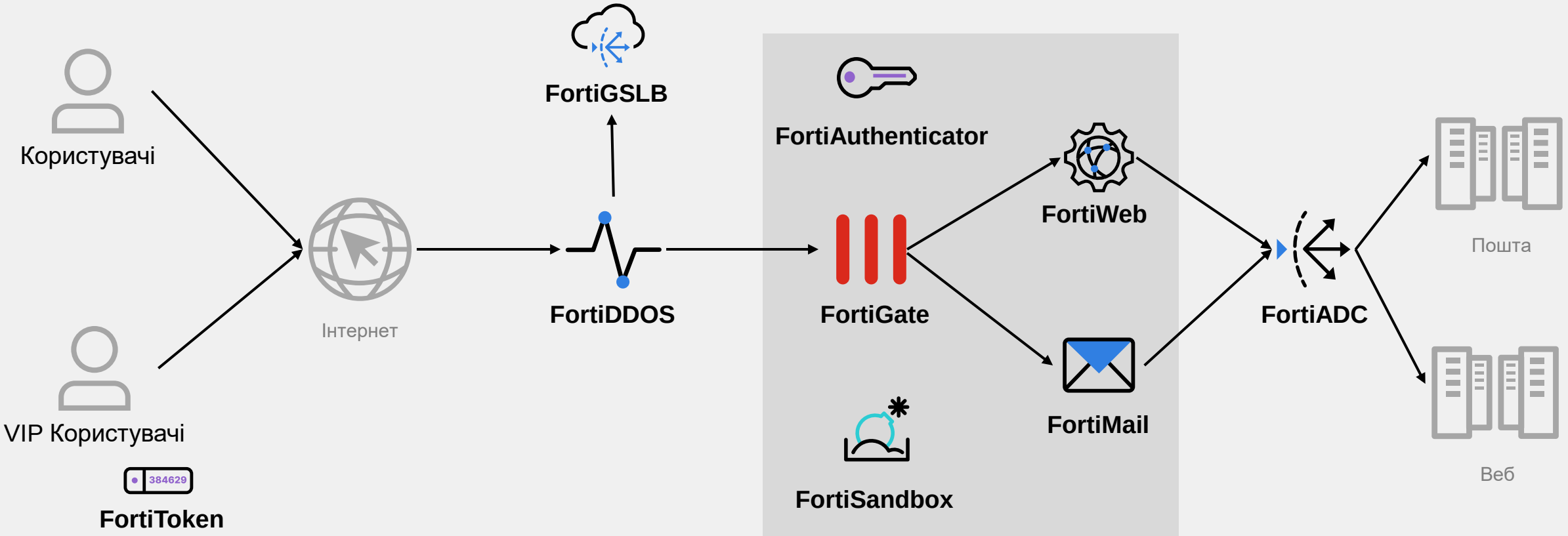
в попередніх серіях

Гібридні мережі

Сучасні реалії

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

Сценарій 1. В локальному ДЦ



Сучасність в цифрах

1,5+ роки кібервійни

FortiGuard 1H 2023

– **FortiGuard Labs Global Threat Landscape Report, 1H 2023**

> В попередніх звітах ми говорили про віруси які стирають інформацію (**wiper malware**). Пік активності цих вкрай деструктивних атак спостерігалися на початку 2022 **в основному у зв'язці з війною з росією**.

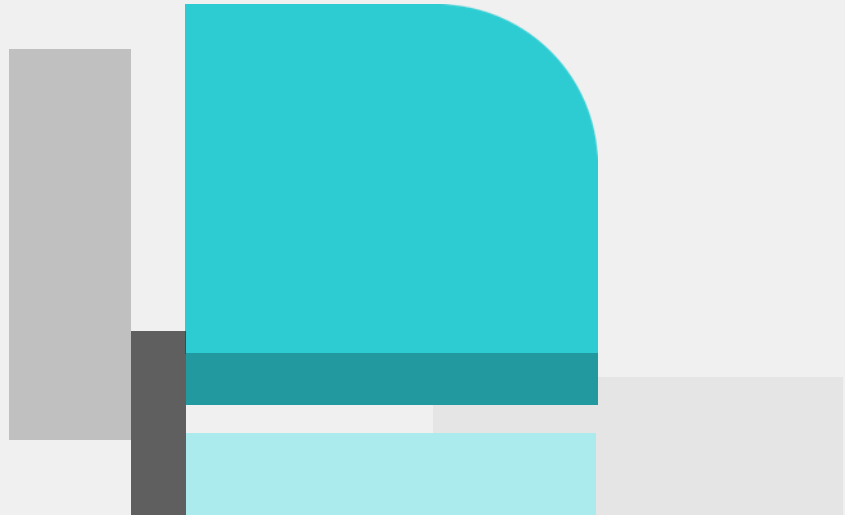
> **Група Turla (російські кібершпигуни) напевно є однією з найдосвідченіших груп в світі**. Вони працюють під багатьма псевдонімами (Snake, Venomous Bear, and Blur Python, тощо) вже пару десятків років. Їх пов'язують з більш ніж 45 спеціалізованих атак направлених на державні установи, медіа, енергетичний сектор та посольства по всьому світу. Вони досягали успіху в своїй діяльності та лишались непоміченими роками навіть в висококонтрольованих середовищах. Під час нового етапу війни **ми не були здивовані зростанням активності цієї групи.**

Світові тенденції

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media: 60%	Exploitation for Client Execution: 24%	Hijack Execution Flow: 30%	Process Injection: 34%	Obfuscated Files/Info: 19%	OS Credential Dumping: 42%	System Info Discovery: 21%	Replication Through Removable Media: 63%	Data from Local System: 29%	Application Layer Protocol: 40%	Exfiltration Over Alternative Protocol: 100%	System Shutdown/ Reboot: 56%
Phishing: 28%	WMI: 22%	Boot/Logon Autostart Execution: 20%	Hijack Execution Flow: 21%	Masquerading: 15%	Input Capture: 40%	File & Directory Discovery: 15%	Taint Shared Content: 25%	Input Capture: 23%	Non-Application Layer Protocol: 22%	Automated Exfiltration: 0.02%	Data Manipulation: 30%
Drive-by Compromise: 5%	Command & Scripting Interpreter: 19%	Create/Modify System Process: 19%	Boot/Logon Autostart Execution: 14%	Virtualiz./ Sandbox Evasion: 15%	Unsecured Credentials: 17%	Software Discovery: 13%	Remote Services: 4%	Email Collection: 21%	Ingress Tool Transfer: 19%		Data Encrypted for Impact: 5%
Exploit Public-Facing Application: 4%	Shared Modules: 13%	Scheduled Task/Job: 18%	Create/Modify System Process: 13%	Impair Defenses: 13%	Credentials from Password Stores: 0.6%	Virtualiz./ Sandbox Evasion: 11%	Use Alternate Authentication Material: 4%	Automated Collection: 15%	Encrypted Channel: 12%		Inhibit System Recovery: 3%
External Remote Services: 2%	Scheduled Task/Job: 10%	Office Application Startup: 11%	Scheduled Task/Job: 13%	Process Injection: 9%	Steal Web Session Cookie: 0.1%	Process Discovery: 9%	Lateral Tool Transfer: 2%	Archive Collected Data: 4%	Non-Standard Port: 4%		Service Stop: 3%
Valid Accounts: 1%	Native API: 6%	Event Triggered Execution: 0.3%	Access Token Manipulation: 4%	Indicator Removal on Host: 7%	Network Sniffing: 0.09%	Remote System Discovery: 8%	Exploitation of Remote Services: 1%	Clipboard Data: 3%	Proxy: 2%		Endpoint Denial of Service: 1%
	System Services: 5%	Browser Extensions: 0.3%	Event Triggered Execution: 0.3%	Hijack Execution Flow: 6%	Adversary in the Middle: 0.01%	Query Registry: 7%	Software Deployment Tools: 1%	Browser Session Hijacking: 3%	Web Service: 0.7%		Resource Hijacking: 0.7%
	Inter-Process Comm.: 0.5%	Pre-OS Boot: 0.2%	Abuse Elevation Control Mechanism: 0.07%	Hide Artifacts: 4%	Forge Web Credentials: 0.007%	System Network Configuration Discovery: 6%		Screen Capture: 0.7%	Remote Access Software: 0.07%		Data Destruction: 0.7%
	User Execution: 0.06%	Boot/Logon Initialization Scripts: 0.09%	Boot/Logon Initialization Scripts: 0.07%	Deobfuscate/ Decode Files/Info: 3%	Modify Authentication Process: 0.0006%	Application Window Discovery: 5%		Video Capture: 0.4%	Data Obfuscation: 0.02%		Defacement: 0.08%
	Software Deployment Tools: 0.005%	Create Account: 0.03%	Valid Accounts: 0.02%	Modify Registry: 3%	Brute Force: 0.0003%	System Owner/User Discovery: 1%		Data from Info Repositories: 0.3%	Data Encoding: 0.02%		Account Access Removal: 0.05%

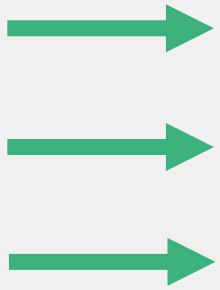
FortiWeb - захист веб додатків

Стисло про найважливіше



Еволюція назви

Web Application Firewall

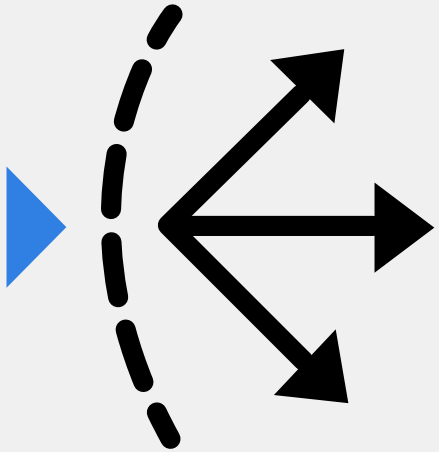


Web Application and API Firewall

WAF+ веб балансувальник

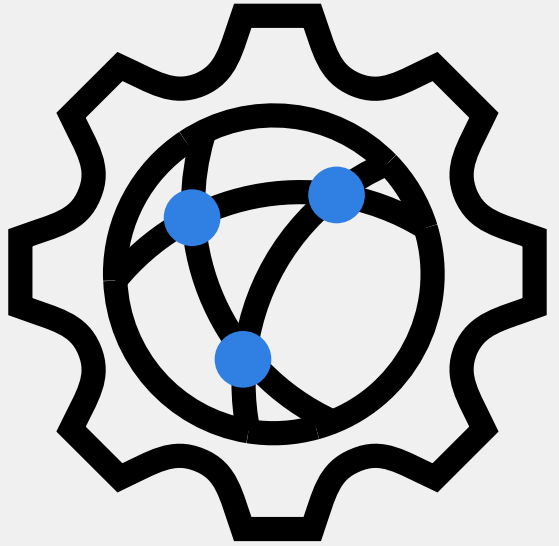
Web Application Firewall

+



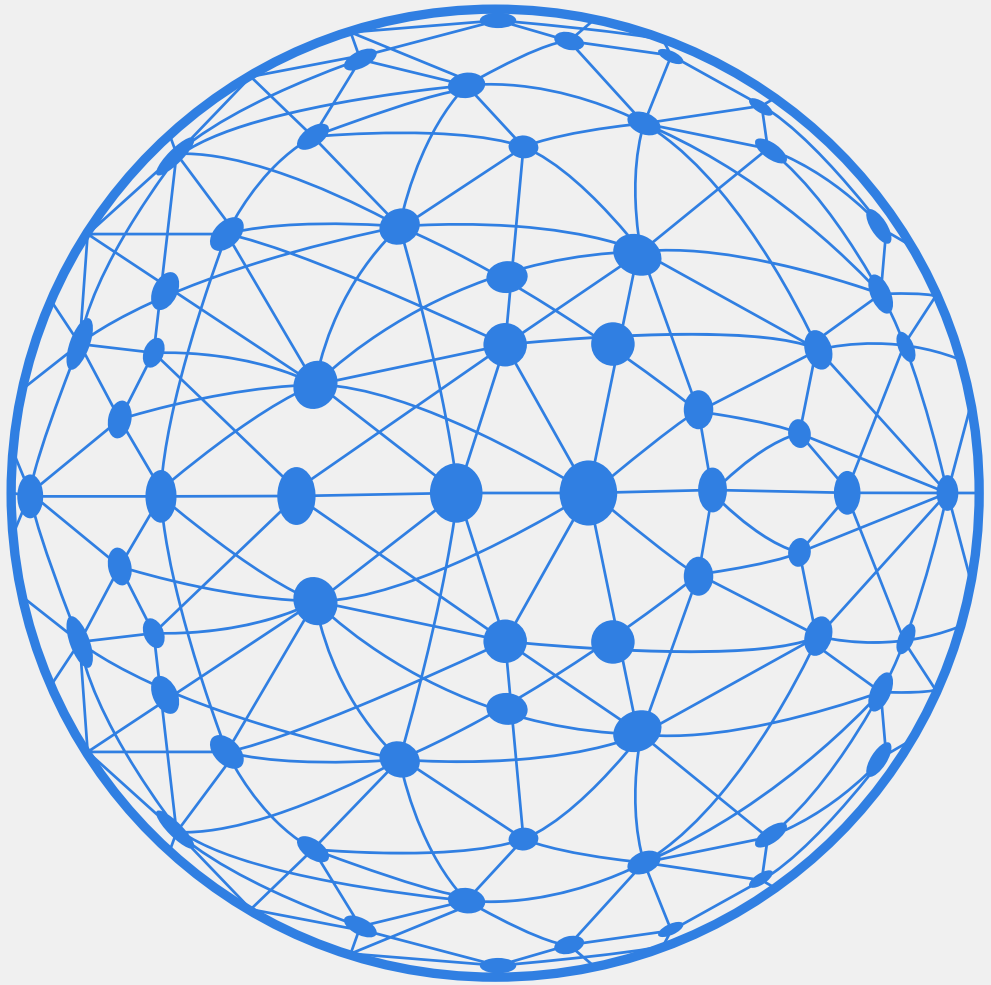
Балансувальник в рамках ДЦ

=



FortiWeb

Від чого захищаємось?



Банальні вразливості

Особливо від OWASP Top 10

Атаки експертів

в тому числі zero-day

Боти/автоматизація

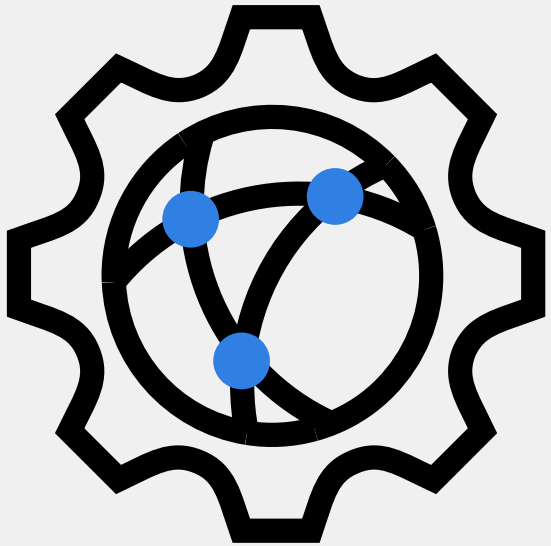
в тому числі викрадення паролю

Атаки на API

щоб вкрасти/знищити/зашифрувати інформацію

Основні сценарії використання FortiWeb

Захист веб додатків



FortiWeb

1. Захист веб додатків

Захист від OWASP top 10 і інших відомих загроз

ML для виявлення аномалій

2. Бот/DDoS захист

Блокування автоматизованої активності (DoS, сканування вразливостей, автоматизація взлому, збір даних).

ML для поведінкового аналізу

3. Вимога регулятора

Вимоги регуляторів щодо захисту, наприклад, PCI DSS та GDPR.

Обов'язкові стандарти до виконання або Best practice

4. Захист API

Захист комунікацій B2B та мобільних додатків.

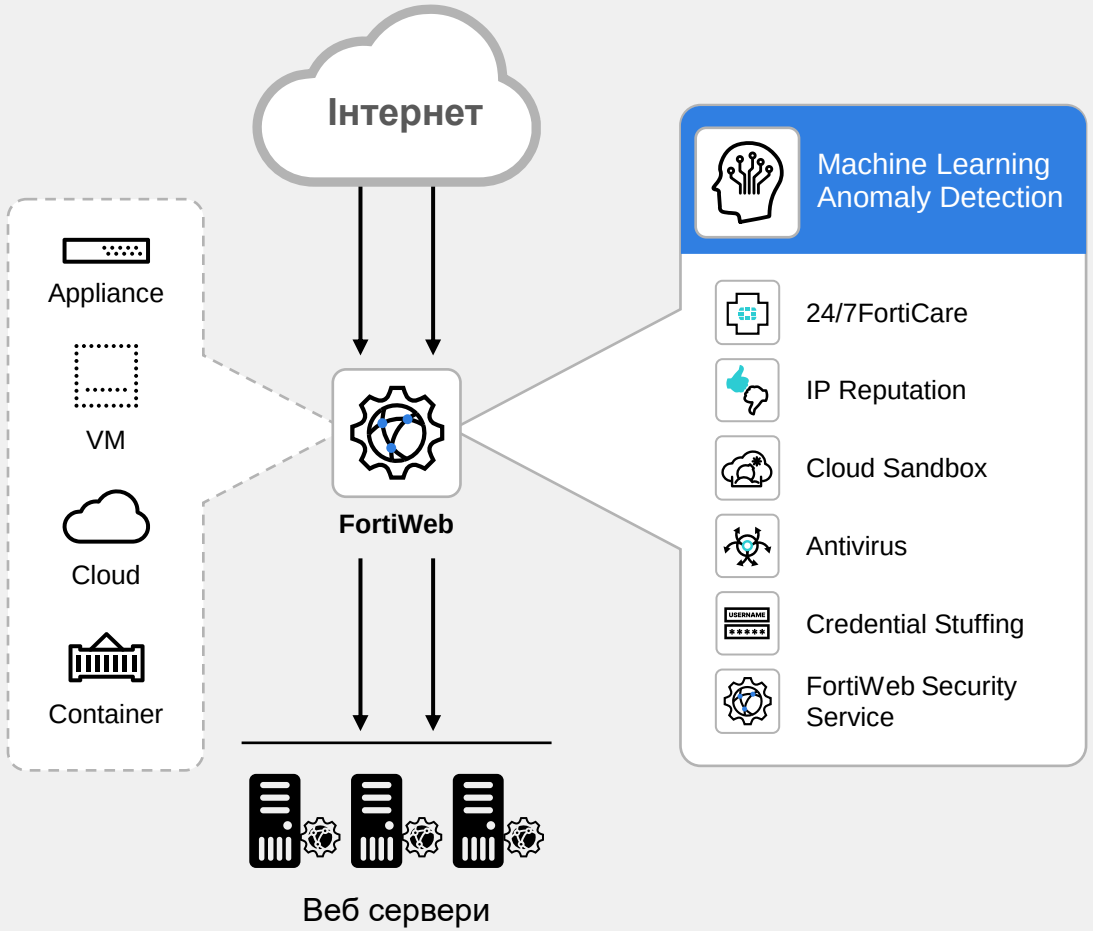
ML для аналізу та захисту API особливо в разі відсутності документації

5. Компонент SOC

WAF є одним з компонентом SOC для захисту веб протоколу який немає чим замінити для повної картини в комплексній безпеці

Використовуйте всі інструменти і звертайте увагу тільки на найважливіше

Безпека веб додатків



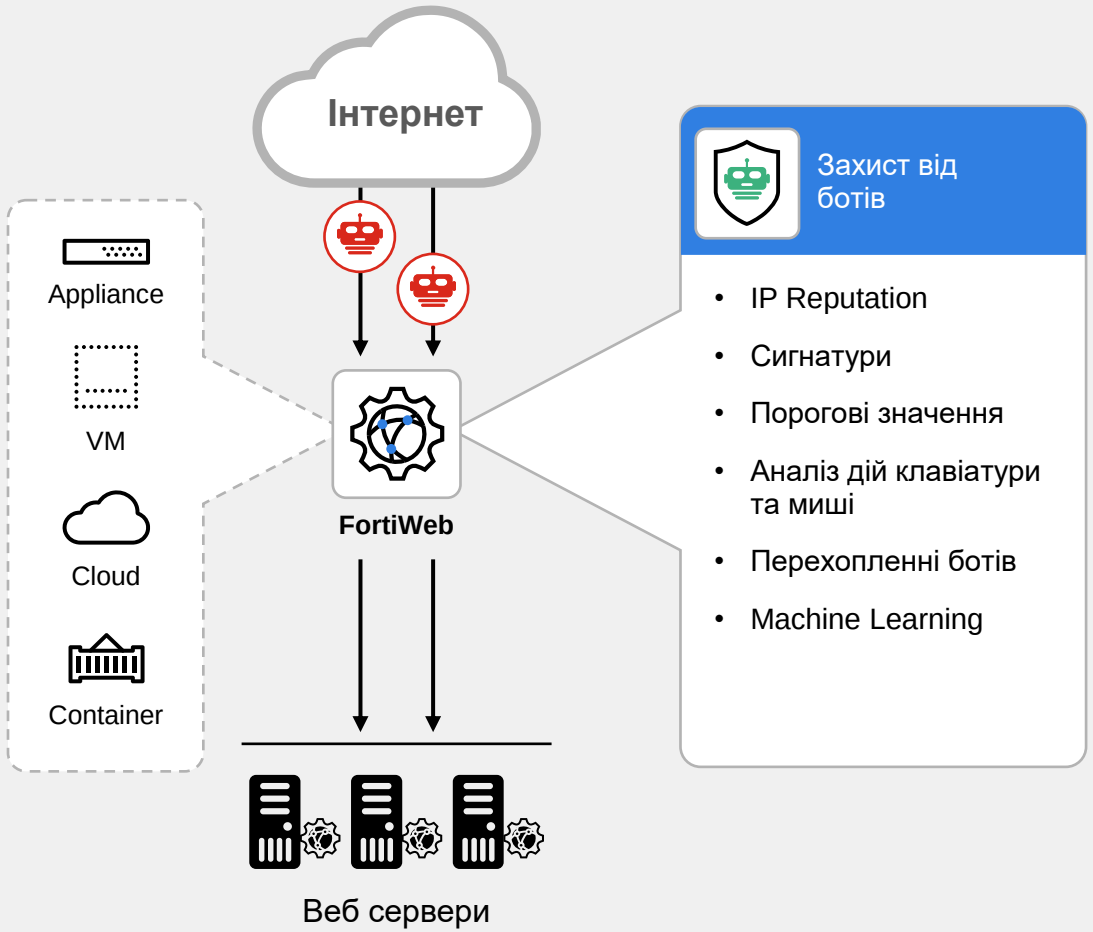
1. Безпека веб додатків

Захист від топ-10 OWASP та інших відомих та невідомих загроз

ML для виявлення аномалій

- Захист від відомих загроз починаючи з OWASP Top 10
- Поведінковий аналіз для захисту від zero-day
- ML допомагає виявити головне і не відволікатись на некритичні атаки ботів 24/7

Bot Defense



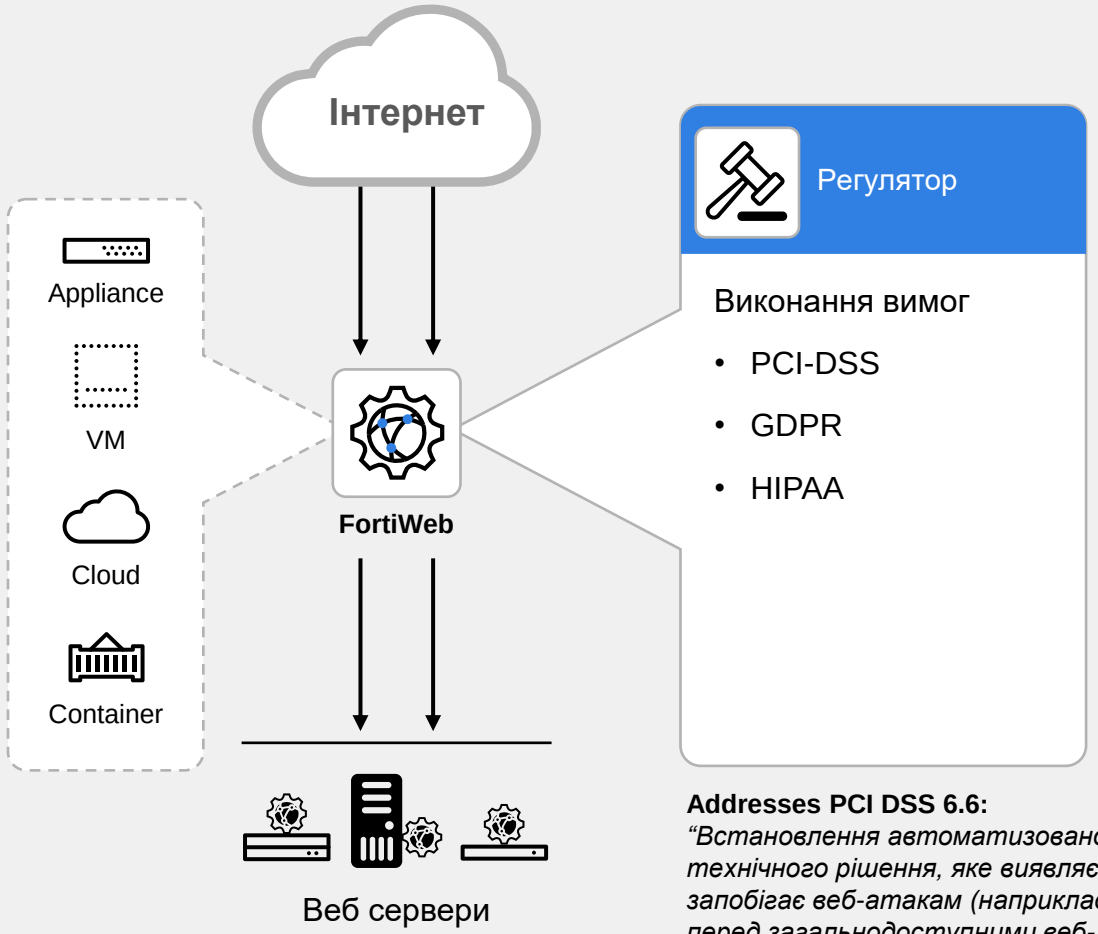
2. Бот захист

Блокуйте весь спектр шкідливої активності ботів (фішинг, DDoS, сканування тощо).

ML для виявлення ботів

- Блокує шкідливих ботів, не блокуючи користувачів і не втручаючись у діяльність «гарних» ботів (пошукові системи);
- Зменшення небажаного впливу безпеки на користувачів, наприклад, блокування чи ReCaptcha

Regulatory Compliance



Addresses PCI DSS 6.6:
“Встановлення автоматизованого технічного рішення, яке виявляє та запобігає веб-атакам (наприклад, WAF) перед загальнодоступними веб-додатками, щоб постійно перевіряти весь трафік.”

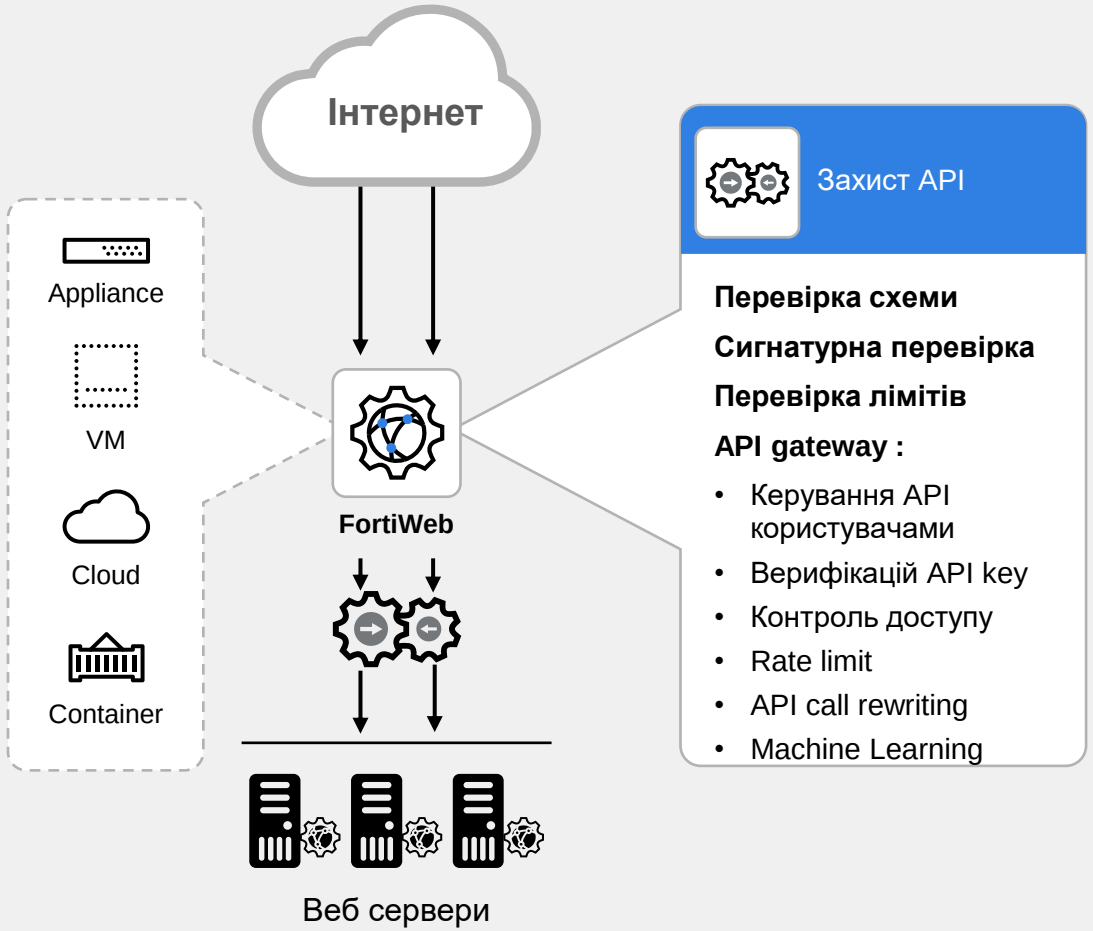
3. Вимоги регуляторів

Address regulatory compliance requirements related to public-facing applications.

Виконання вимог

- Захист від відомих атак, наприклад, OWASP Top 10.
- PCI DSS є обов'язковим у банковоvскій сфері для банків що випускають кредитні картки і поширюється на всі організації, які зберігають, обробляють або передають дані власників карток
- GDPR є обов'язковим при роботі з даними громадян ЄС

Protect Internet-Facing APIs



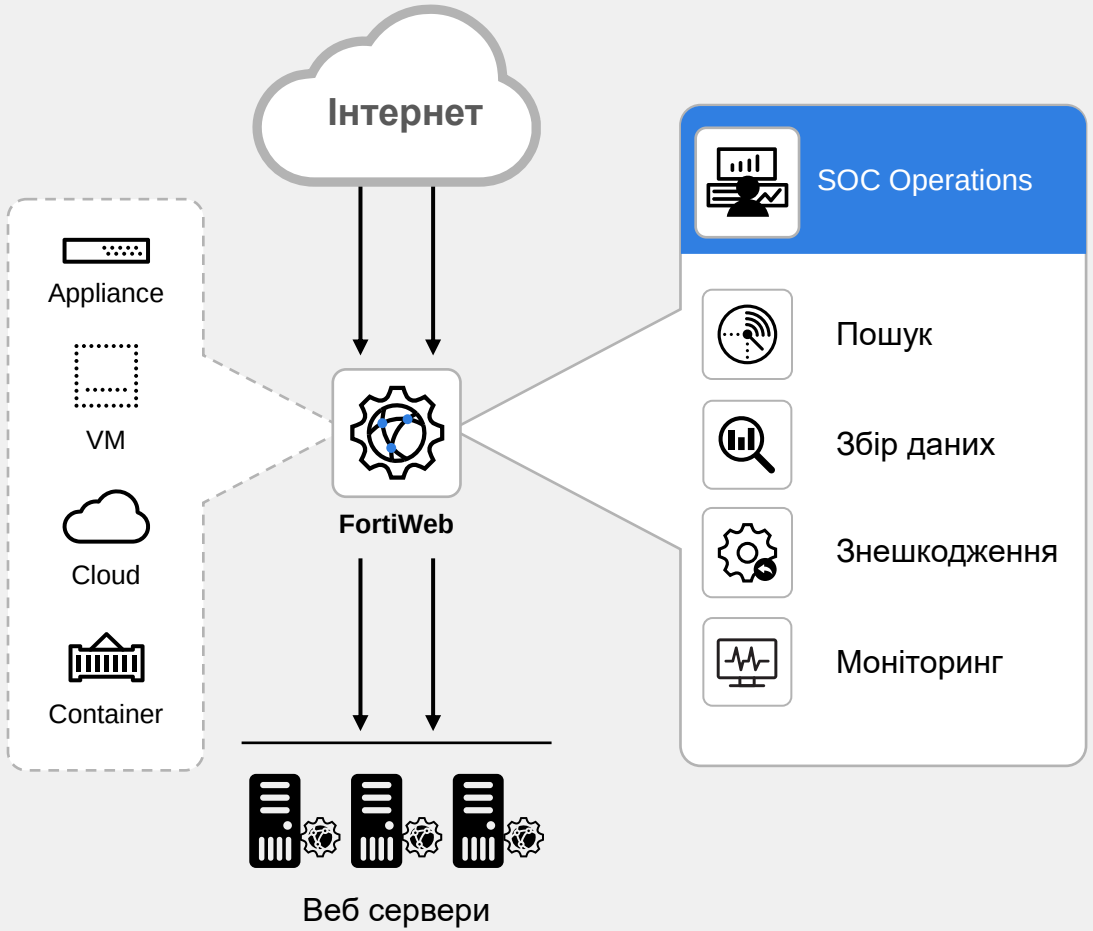
4. Захист APIs

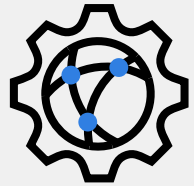
Захист комунікацій B2B та мобільних додатків.

Leverage ML to protect that APIs that support critical line-of-business capabilities

- Єдина точка входу API
- Приховування API структури
- Полегшує роботу з API та покращує швидкість
- Machine Learning на допомогу стандартним механізмам захисту

Безпека в рамках SOC





5. SOC

FortiWeb є одним з джерером даних про події для складання швидкого та чіткого уявлення про найважливіші загрози аналітикам SOC

Leverage Threat Analytics to Highlight Actionable Threat Intel

Точніша реакція шляхом консолідації окремих подій у дискретні загрози, зменшення завдань ручного аналізу

Пришвидшення розслідування та реагування

Виявлення складних атак на веб сервіси

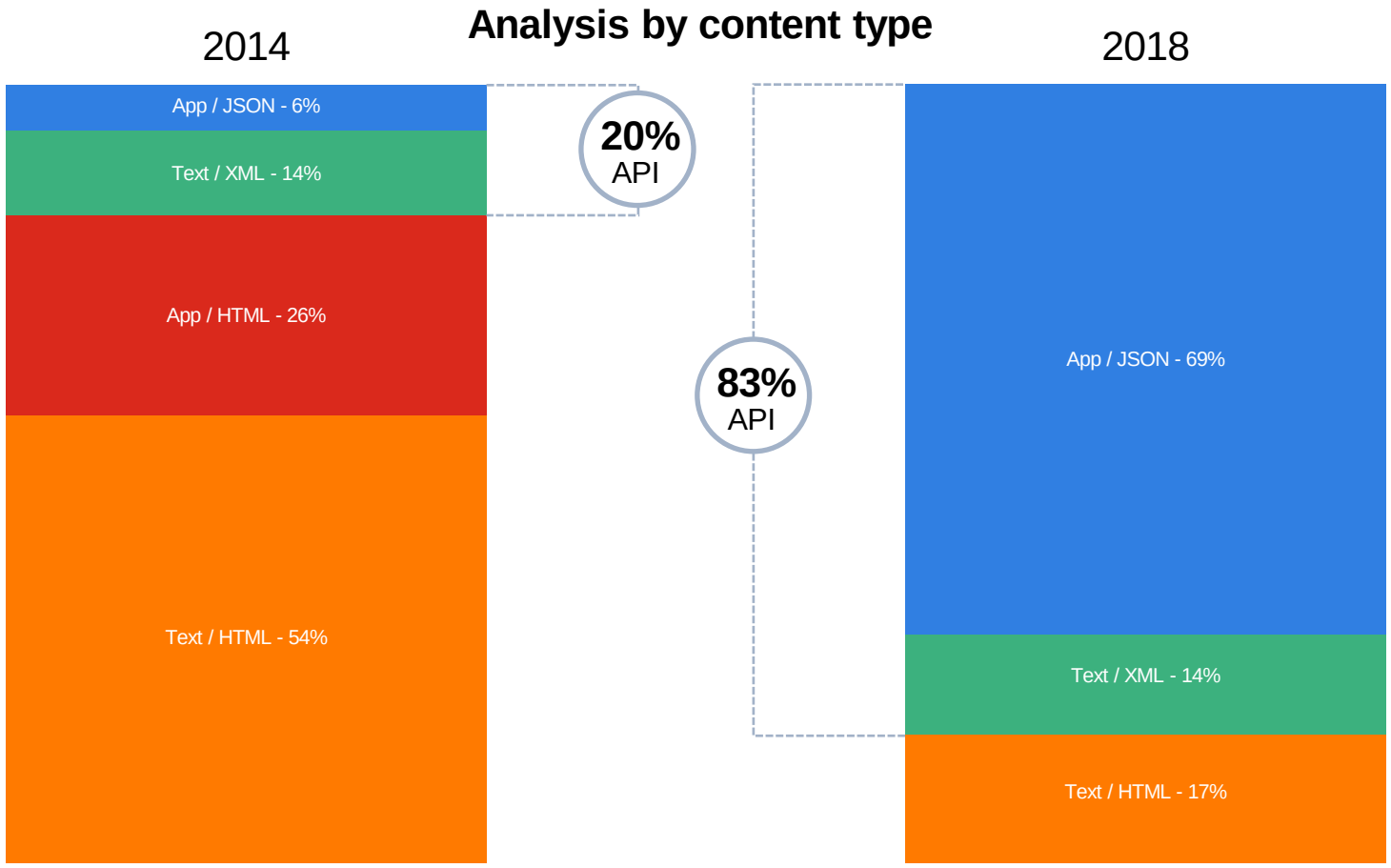
Зменшення кількості персоналу топової кваліфікації

Особливості захисту API

Чому API захищають як окремий протокол?

Розповсюдженість API

- APIs є невід'ємною складовою сучасних сервісів
- Сучасний інтерфейс для роботи з даними
- Інструмент взаємодії з клієнтами та партнерами
- Хребет мобільних додатків
- Використання стимулюється мікро сервісною архітектурою
- Основа для DevOps, CI/CD, IaC



*Source - Akamai

API атакують. Постійно.

AT&T US, T-Mobile US, Optus AU & Proximus BE

Що сталось

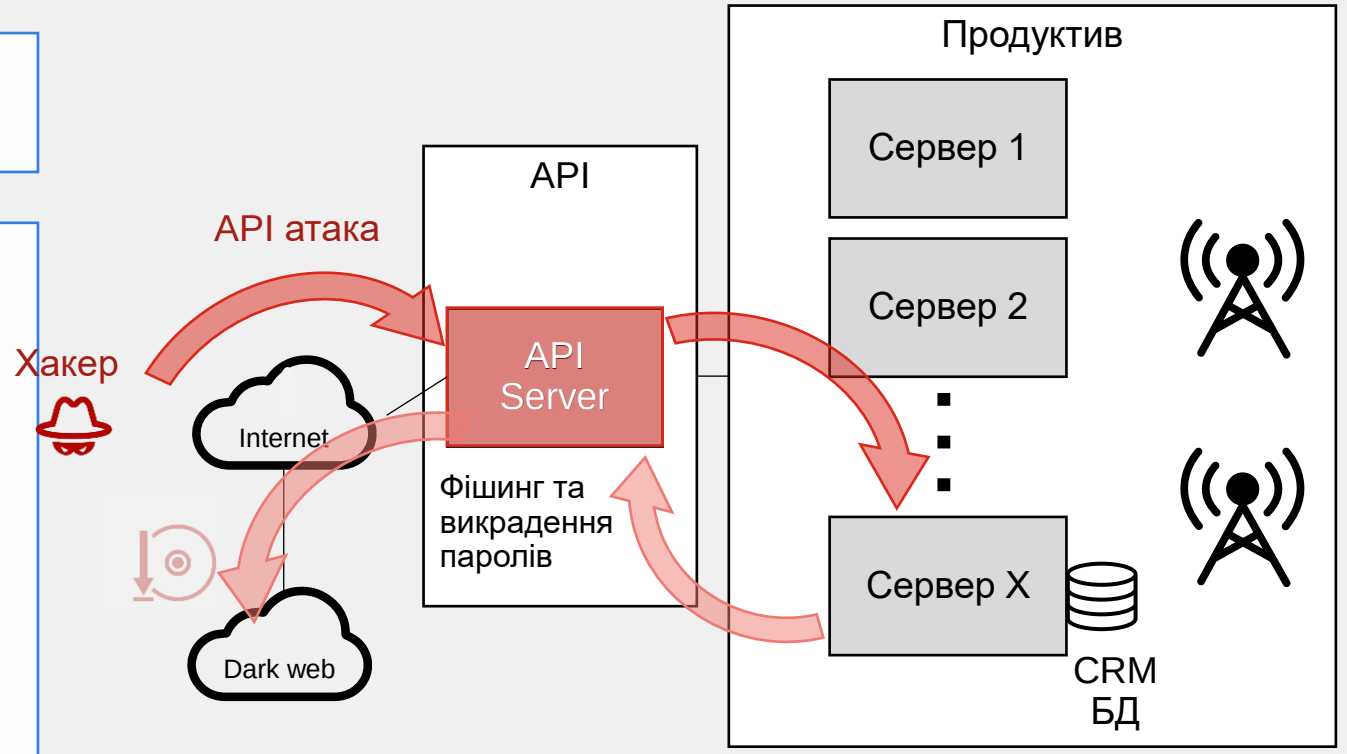
- Хакери отримали несанкціонований доступ до платформи через API (AT&T 2023-03-09) (T-Mobile 2023-01-05) (Optus, 2022-09-22) (Proximus, 2022-03-03)

Постраждалі сервіси

- Отриманий доступ через зареєстрованих користувачів. База не постраждала проте інформація з неї була вивантажена.

Наслідки

- Були викрадені такі дані клієнтів (ім'я, дата народження, номер телефону, email). В Proximus також були вкрадені номер ПДВ, стать і фізична адреса. Ніяких паролів або фінансової інформації не було викрадено.
- За допомогою AT&T хакер викрав дані 9M абонентів. Було розкрито інформацію про мережу.
- За допомогою T-Mobile хакер викрав дані 37M абонентів. Схоже, що це дозволило обмінюватися SIM-картами в Google Fi (MVNO з використанням T-Mobile), а SIM-карти використовувалися для обходу MFA.
- За допомогою Optus хакер викрав дані 11M клієнтів, а потім зажадав викуп у розмірі 1 мільйона доларів США, щоб уникнути публікації всіх записів. Optus виділив 101 мільйон доларів США на компенсацію.
- Proximus оголосив про викрадення даних 15 000 клієнтів. Злом виявили після того, як клієнти отримали фішингові електронні листи.

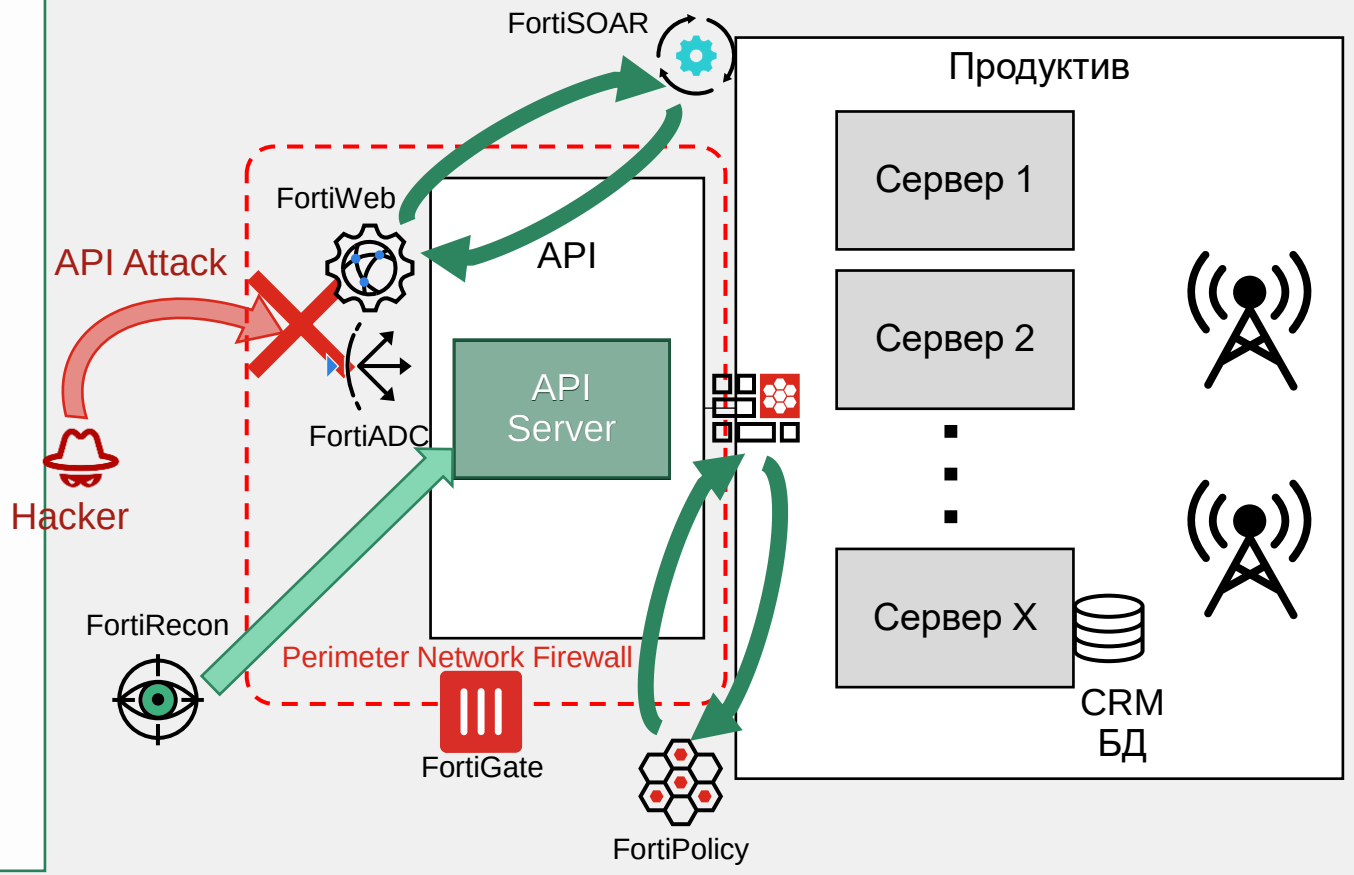


API захист

APIs це ще один вектор атак

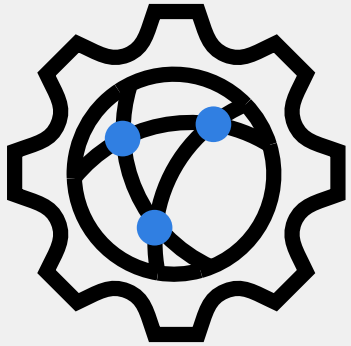
Засоби захисту

- **ОБОВЯЗКОВО:**
  - **FortiGate** в якості firewall периметру та сегментації
  - **FortiWeb/FortiADC** в якості API Gateway для очищення API запитів та аналізу API інструментами with AI/ML
- **Опційно:**
  - **FortiRecon** виявити вразливості API, перевірити репутацію бренду в darkweb
  - **FortiSOAR** автоматизувати політики безпеки та розпізнавання атак
  - **FortiPolicy** використовує ML щоб запропонувати покращення захисту



Перевірка веб запитів. Базові механізми.

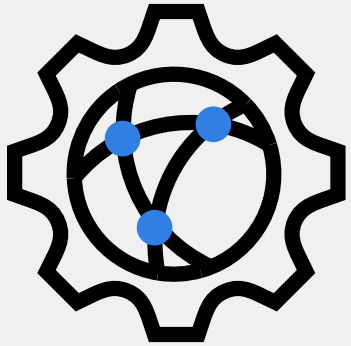
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP



FortiWeb використовує інформацію від FortiGuard Labs для перевірки запитів і блокування шкідливих.

Перевірка веб запитів. Fabric Integration

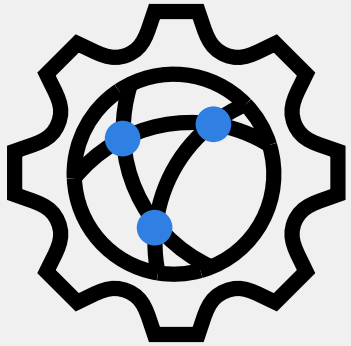
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION



Інтеграція з компонентами Fortinet Security Fabric дозволяє працювати системі безпеки як єдиному комплексу. Особлива ціна інтеграця з FortiGate та FortiSandbox.

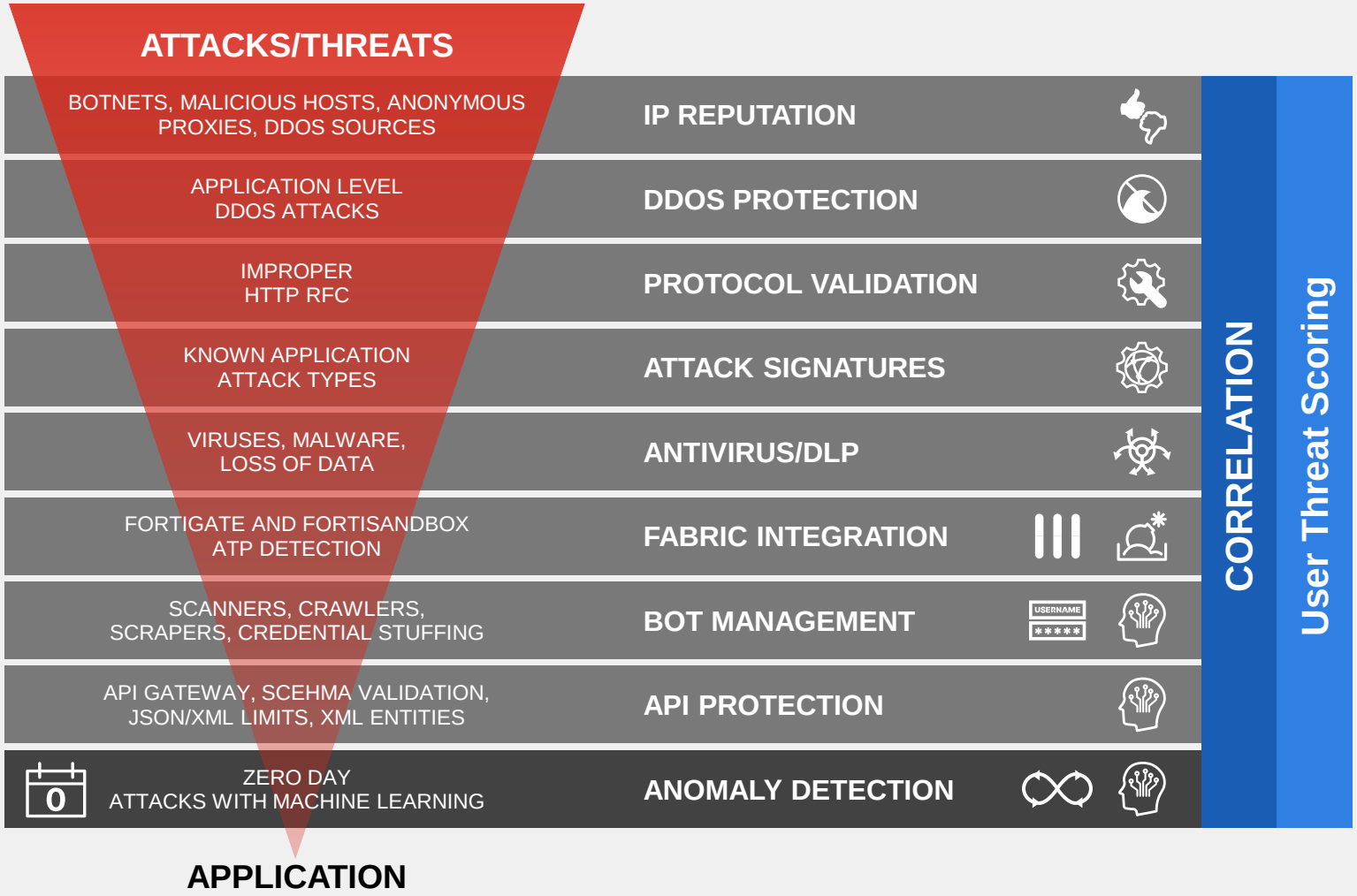
Перевірка веб запитів. Bot та API захист

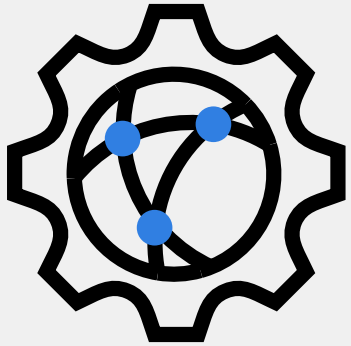
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING	BOT MANAGEMENT
API GATEWAY, SCEHMA VALIDATION, JSON/XML LIMITS, XML ENTITIES	API PROTECTION



FortWeb був би не повним additional Bot Management and API Protection capabilities to deliver a full Web Application and API Protection (WAAP) solution.

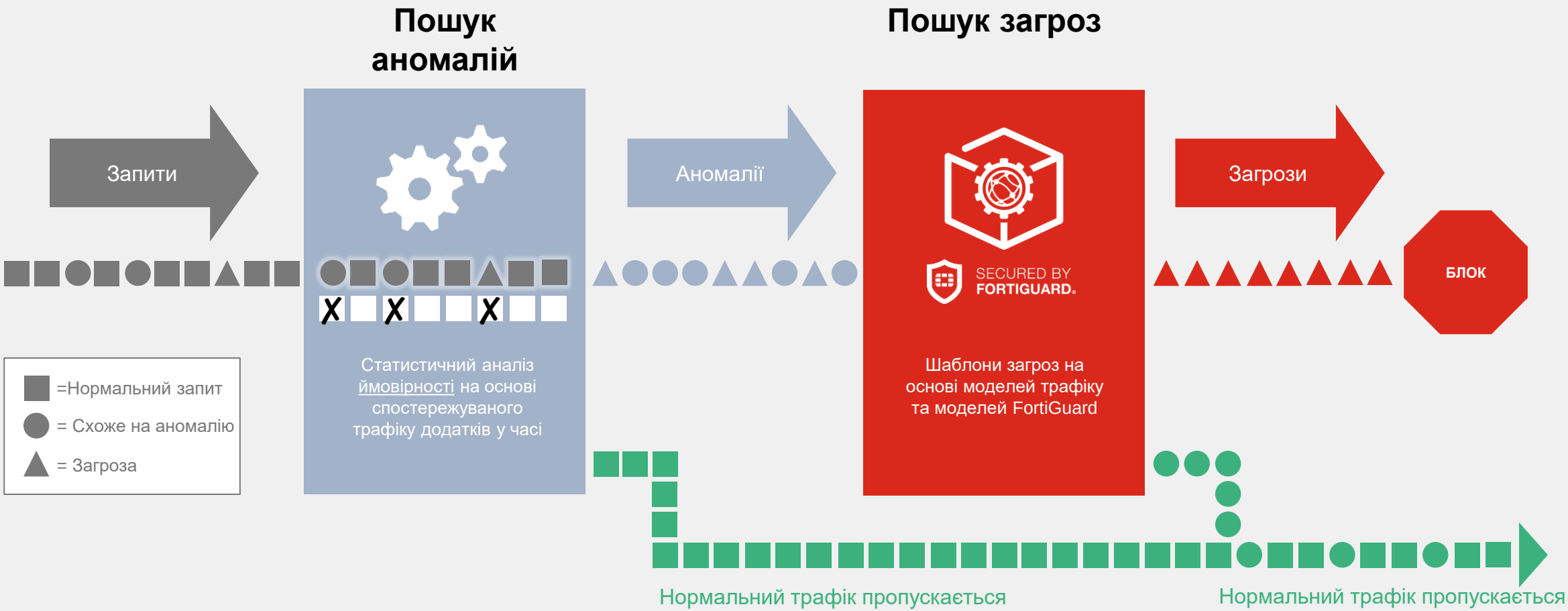
Machine Learning як інструмент перевірки





На основі ML (Machine Learning) рішення аналізує роботу користувачів для підвищення точності виявлення загроз що не тільки підвищує безпеку а і береже час відділу безпеки.

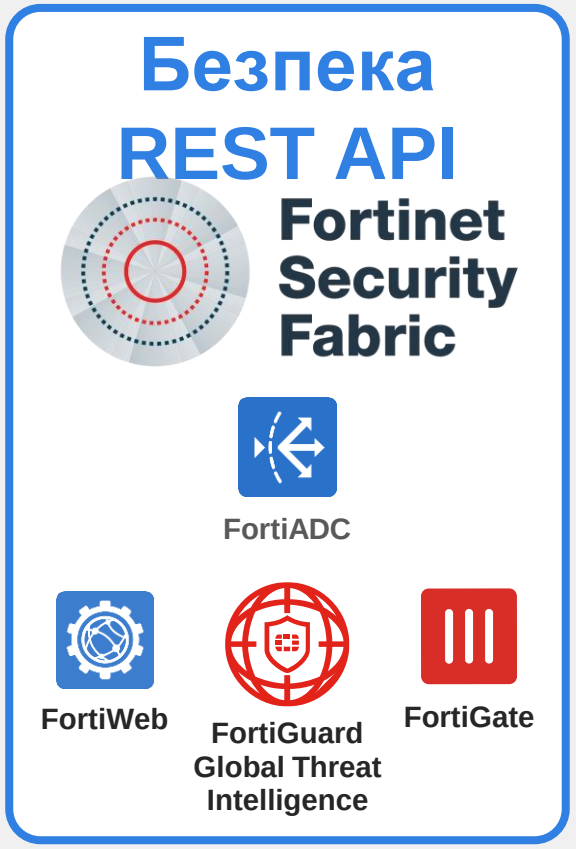
Двоетапна перевірка FortiWeb



Reduce friction when deploying web applications!

Рішення захисту API від Fortinet

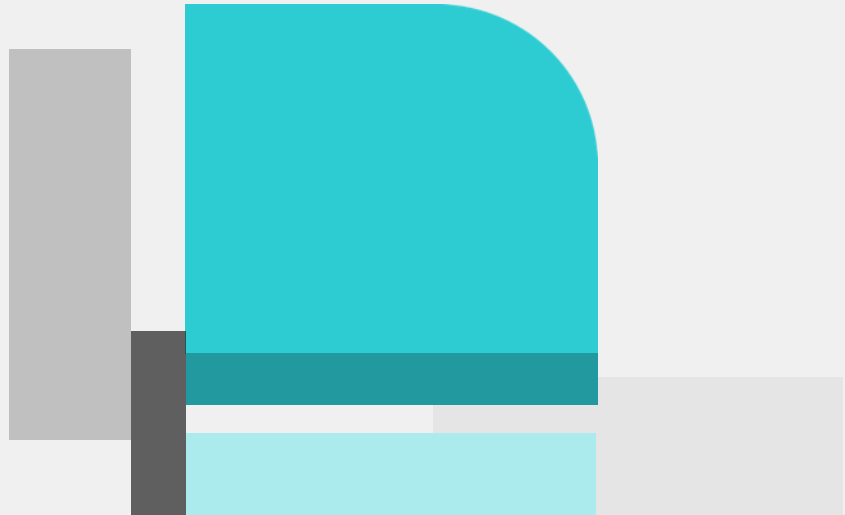
Всебічний захист



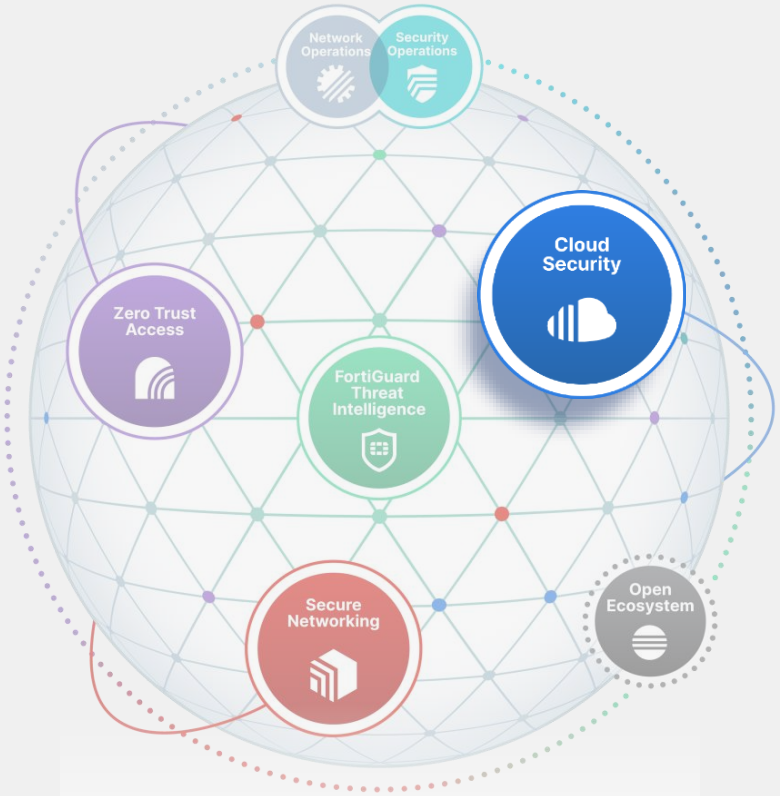
- Перевірка сертифікату
- DoS/DDoS захист, обмеження кількості запитів
- Перевірка схеми API
- IP репутація, авторські сигнатури FortiGuard
- Приховування топології, проксі, балансування
- Перевірка елементів
- Перевірка синтаксису
- Machine Learning & детектування аномалій
- Валідація протоколу в т.ч. HTTP/2
- Антивірус, відомі загрози & zero-day
- Аутентифікація & Авторизація
- SSL/TLS інспекція та crypto offload

Інтеграція

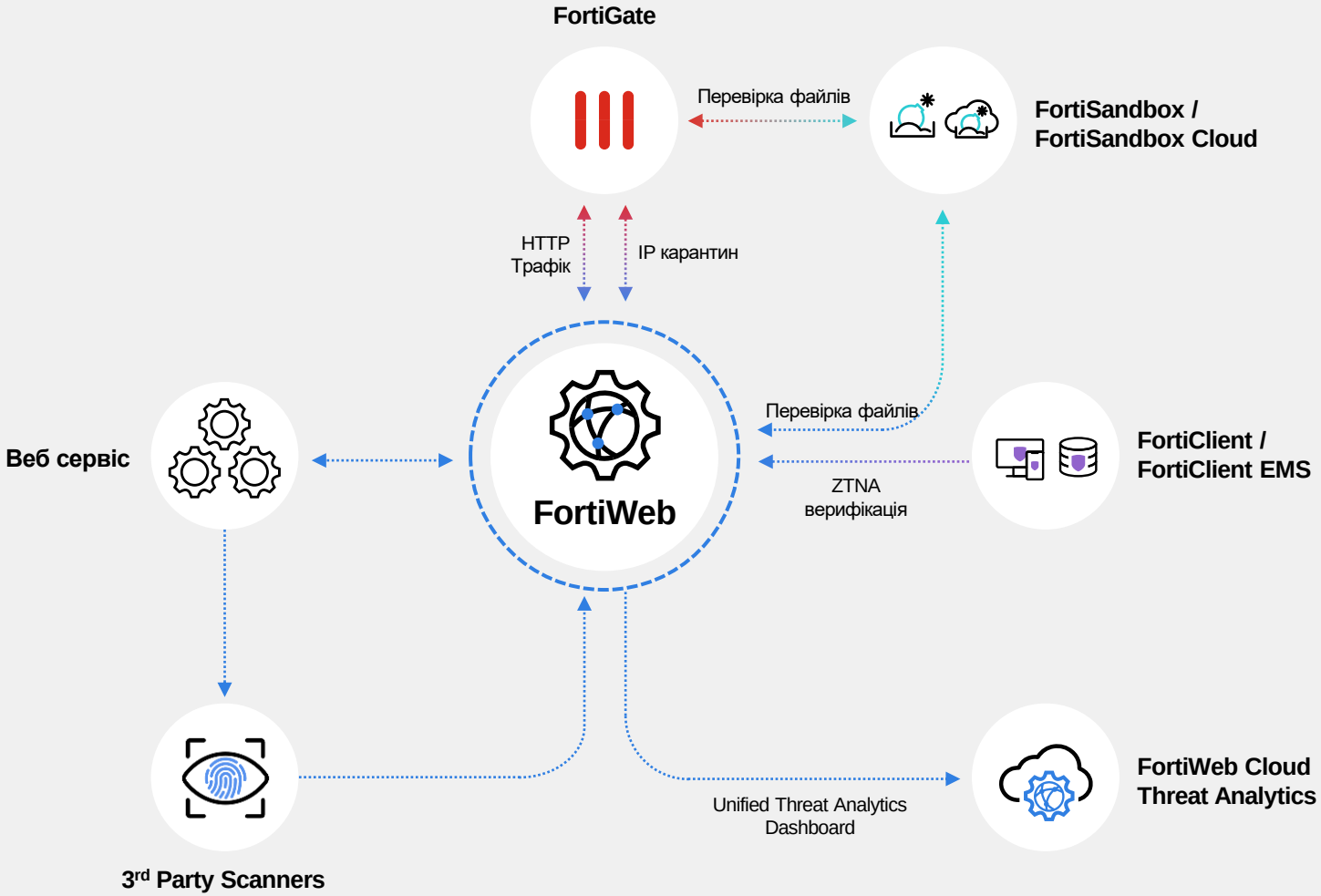
Частина Security Fabric



FortiWeb Security Fabric взаємодія

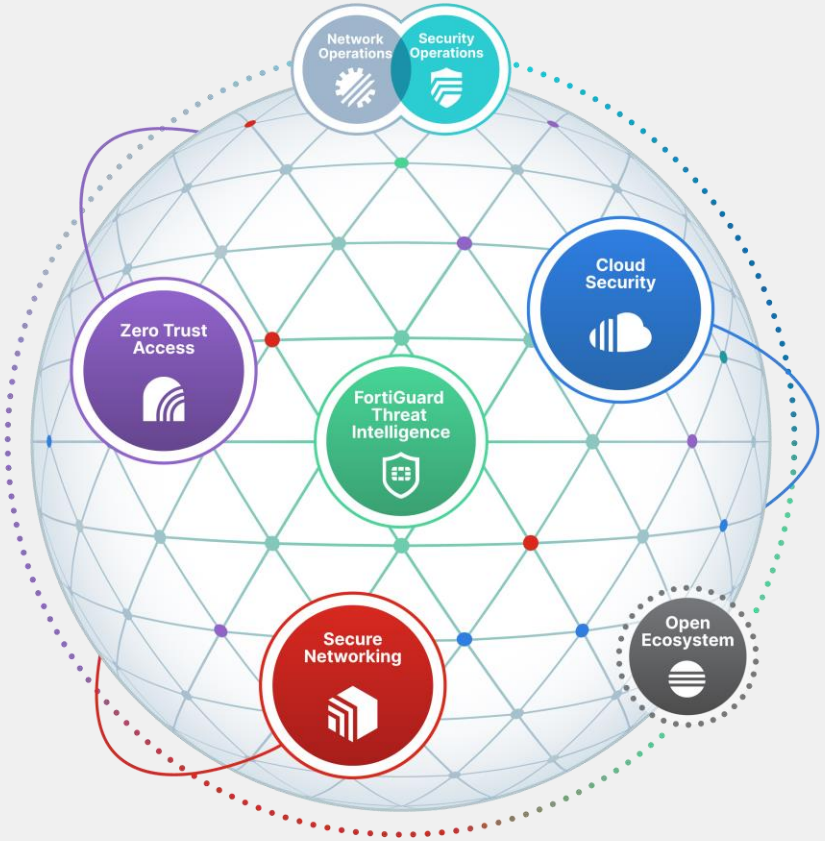


FortiWeb може бути конфігурований як частина Security Fabric на головному FortiGate

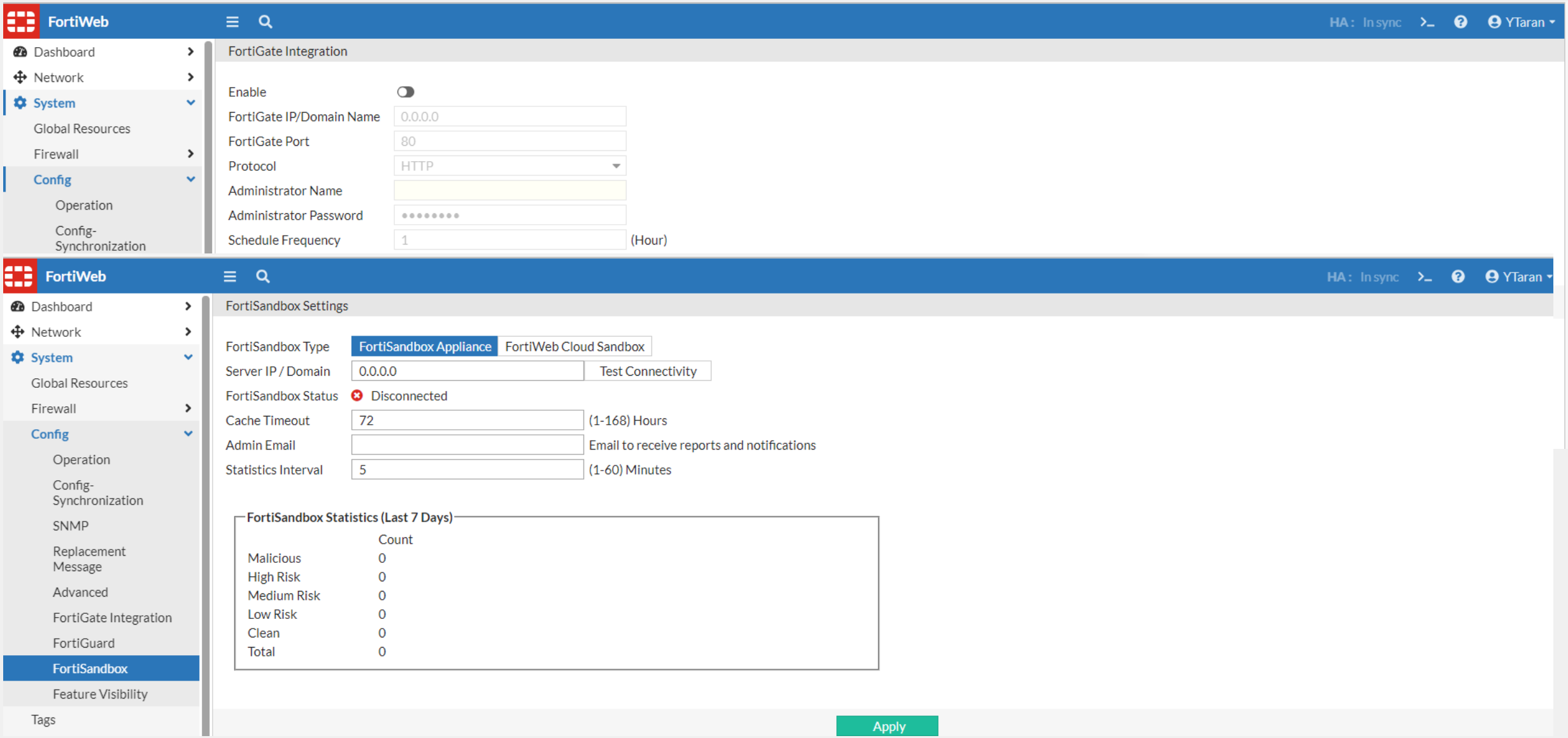


Інтеграція FortiWeb в Security Fabric

- FortiGate
  - Блокування скомпрометованих IP в парі з FortiWeb
  - Автоматизація в рамках Security Fabric
- FortiSandbox та FortiSandbox Cloud
  - Поведінковий аналіз файлів
  - APT захист
- FortiClient
  - ZTNA, перевірка сертифікатів користувача.
- FortiWeb та FortiWeb Cloud
  - Блокування веб атак та надання аналітика щодо них
- Сканери вразливостей (IBM, HPE, White Hat, and more)



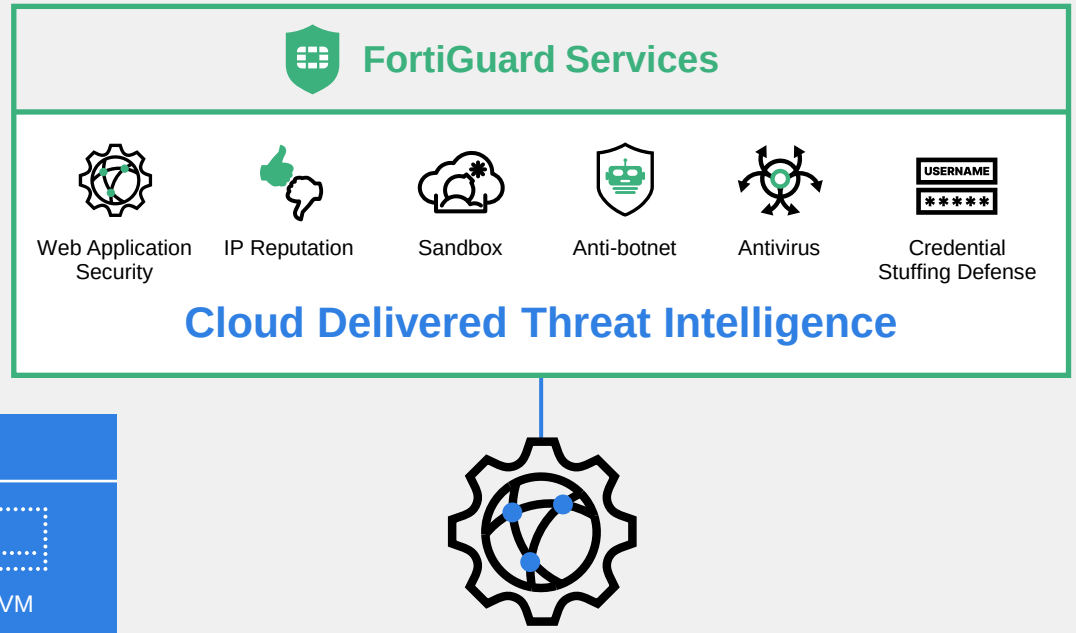
FortiWeb Security Fabric в «2 кліка»



Форм фактори та ліцензування

Сервіси безпеки FortiGuard

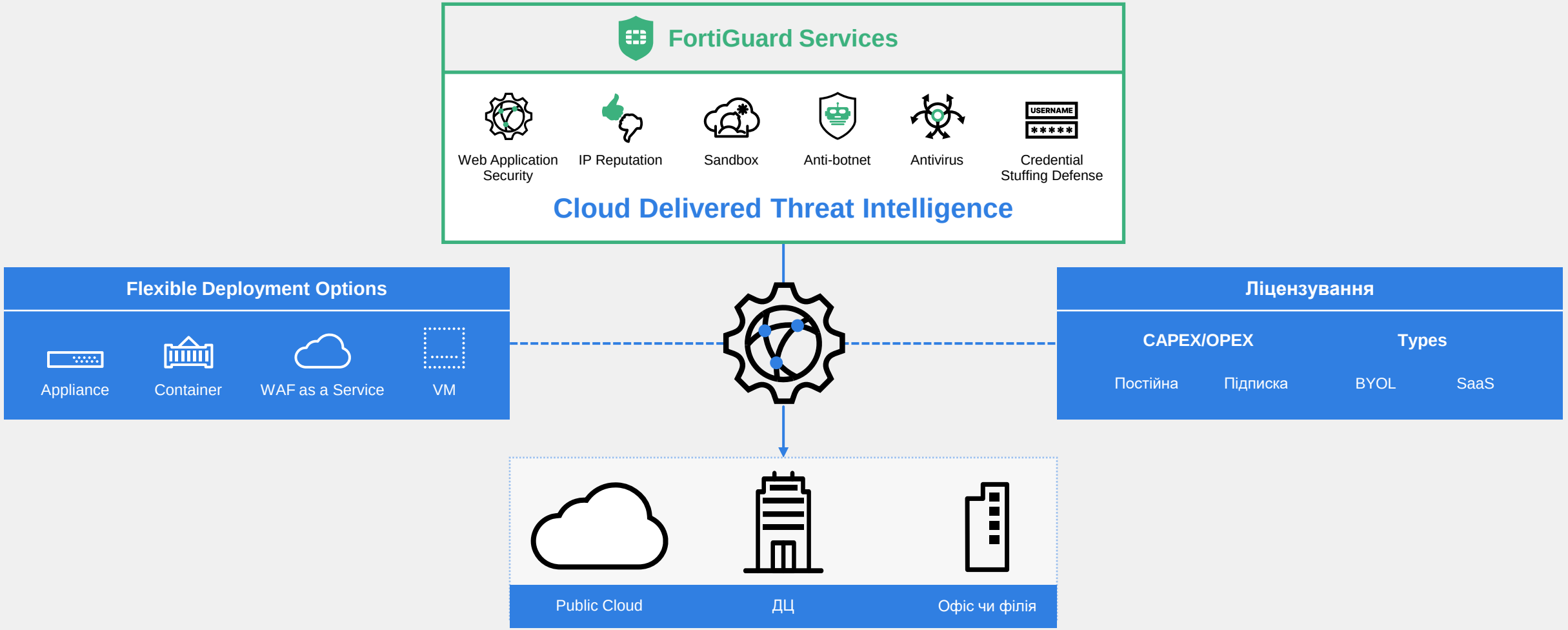
В різних формфактороах



Формфактори

Пристрій | Контейнер | WAF як сервіс | VM

3 різними моделями ліцензуванням



Підписки для FortiWeb

SECURED BY
FortiGuard

WAF Security Service

- HTTP сигнатури
- Сигнатури веб сервісів
- Machine learning моделі
- Шкідливі боти

IP Reputation

- Захист від автоматизованих атак
- База IP від різних атак (DDoS, Phishing, Botnet, Spam, anonymous proxies and infected sources)

Anti-malware

- Сканування файлів
- 2 типи вірусних БД
- Захист від zero day

STANDARD підписка

FortiSandbox Cloud

- Пісочниця на потужностях Fortinet
- Підписка
- Дозволяє обходитись без окремого пристрою

Credential Stuffing Defense

- Ідентифікація використання вкрадених даних
- Автоматичні оновлення
- Захист від небажаного доступу та викрадення даних

Threat Analytics

- Аналітика на основі AI
- Ідентифікація типових шаблонів поведінки та схожості атак
- Пріорітезація інцидентів

ADVANCED підписка

Деталі ліцензування

Детальніше про ліцензування та формфактори

Пристрої
- 7 моделей
- 50 Mbps to 70 Gbps
- Підтримка10/40GE

Віртуальні машини
- 6 моделей
- На основі CPU
- Постійні ліцензії або підписки
- VMware, Hyper-V, Xen, Citrix Xenserver, KVM, Virtualbox

Public Cloud
- 4 моделі
- BYOL або on-demand
- AWS, Azure, Google Cloud, Oracle Cloud

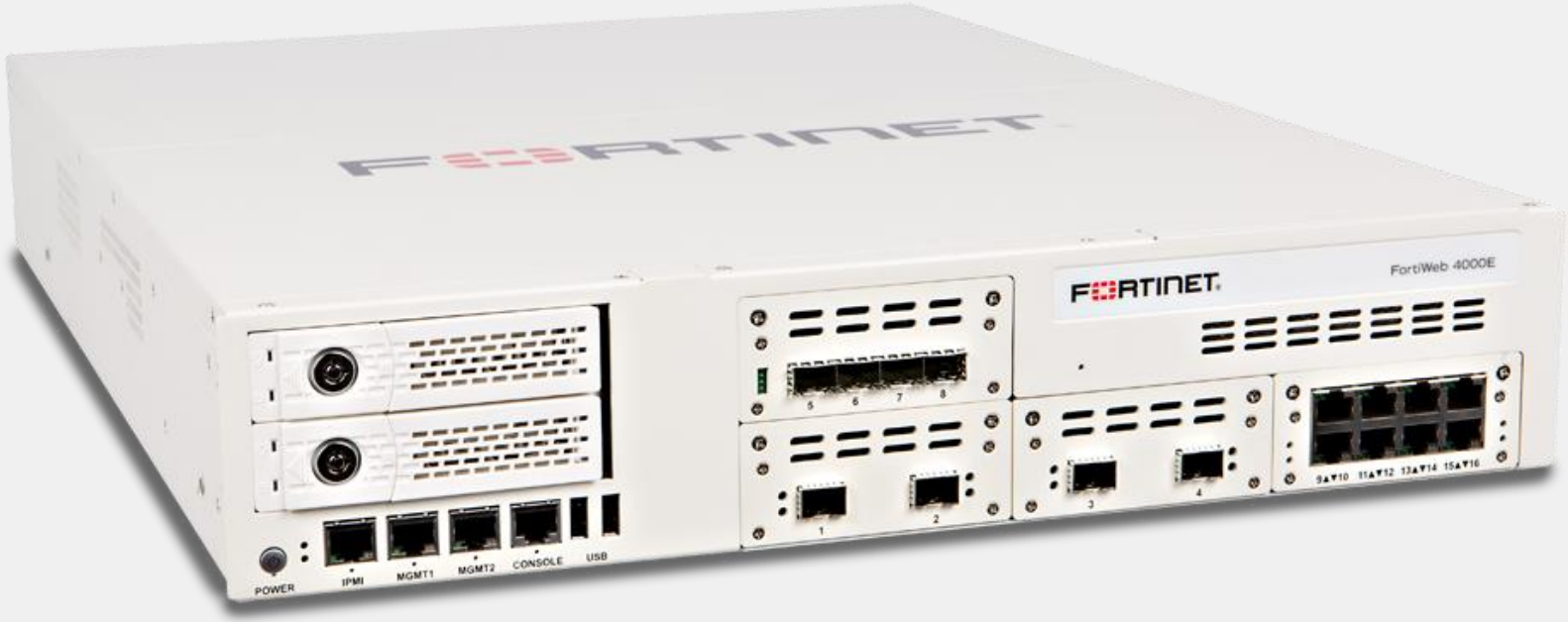
SaaS
- Підписка
- На основі трафіку або швидкості
- На потужностях Fortinet

Container
- 4 віртуальні моделі
- Від 25 Mbps до 2 Gbps
- Підтримка Docker

Partner Rules
- 5 пакетів
- додаток AWS WAF
- База для OWASP top 10

Пристрої та VM

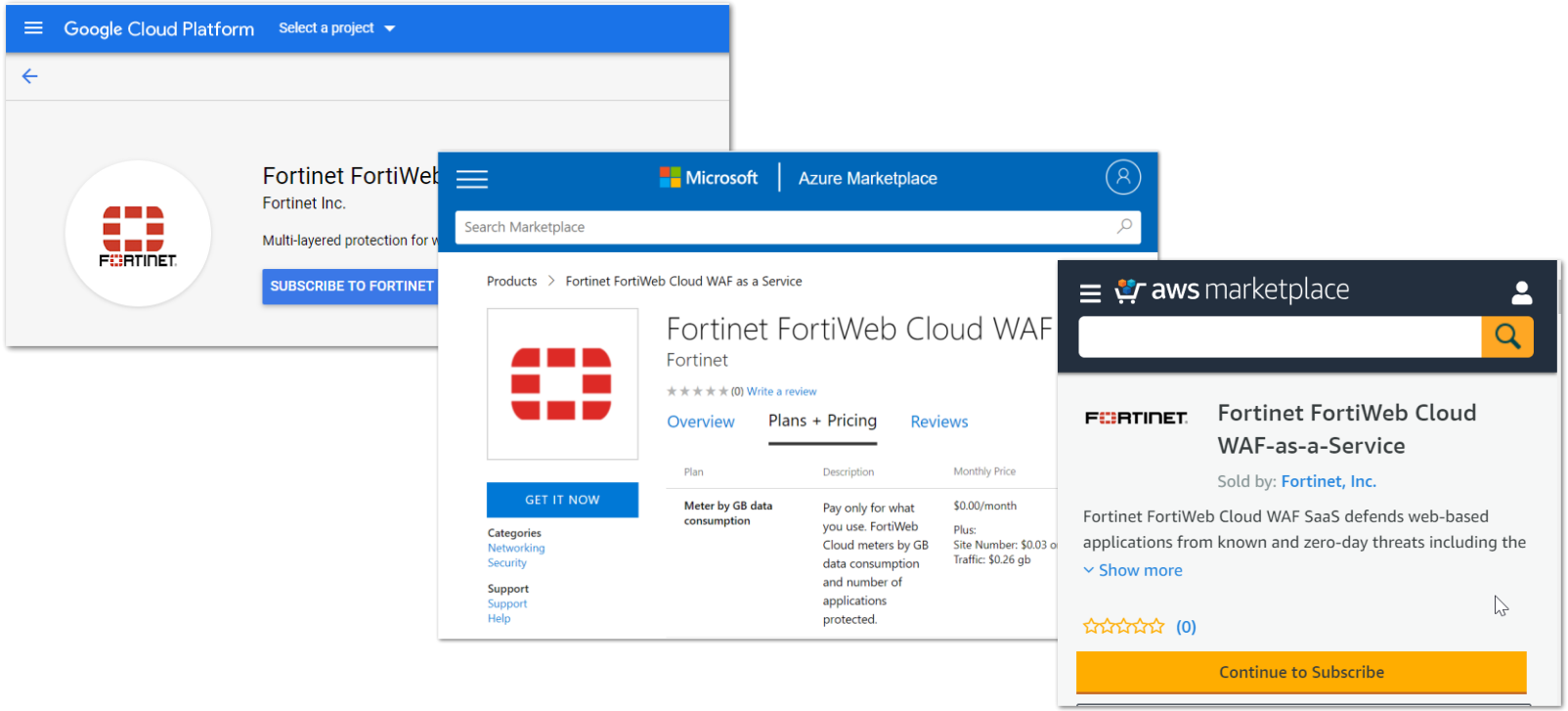
- 7 моделей апаратних пристроїв та 6 моделей віртуальних машин (від 50 Mbps до 70 Gbps)
- Віртуальні машини доступні як BYOL або PAYG в Public Cloud
- Інтеграція з FortiGate, FortiSandbox таFortiAnalyzer



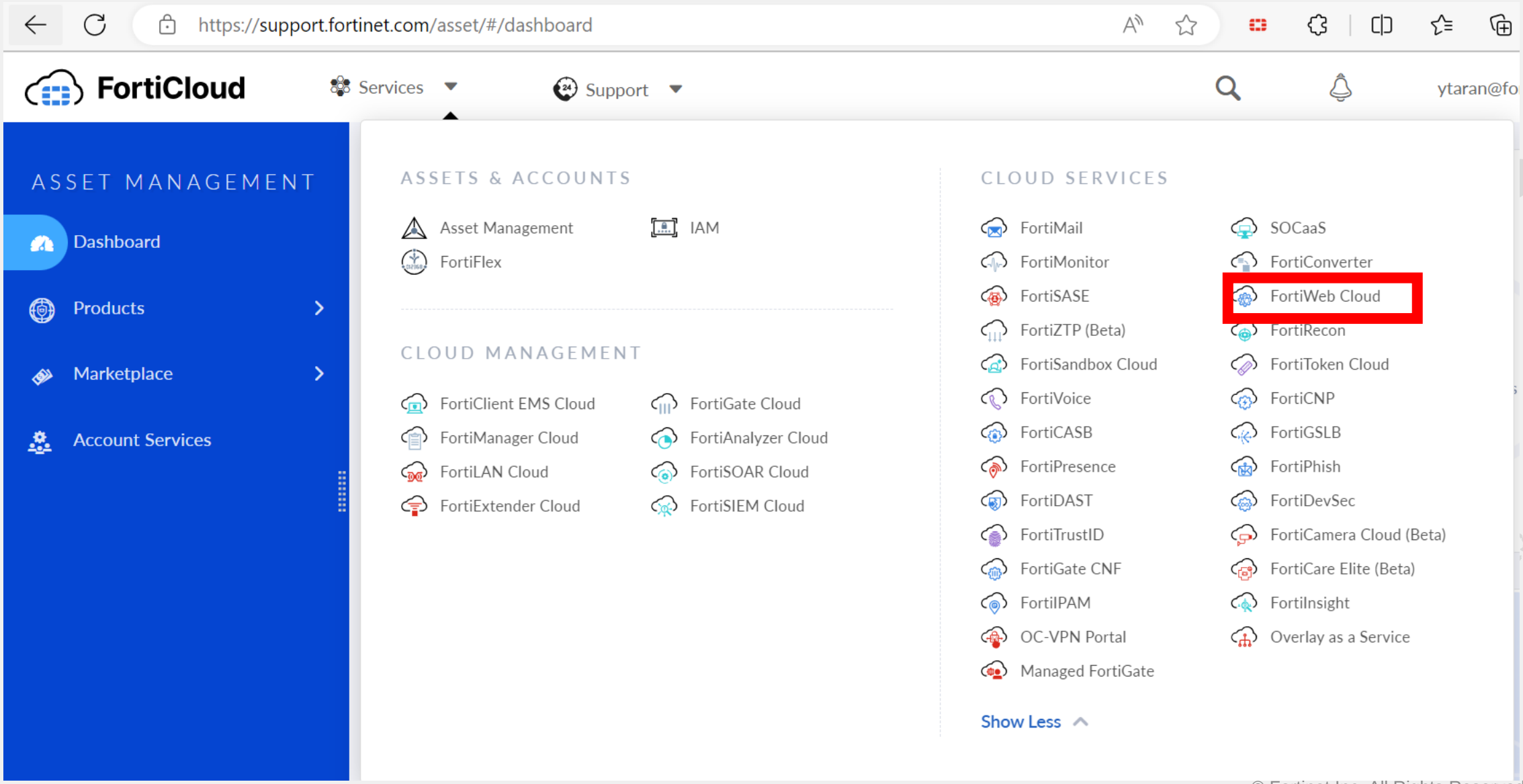
- Виявлення загроз за допомогою ML
- Захист API
- L7 DDoS-захист
- Антивірус FortiGuard
- Репутація IP
- Хмарний FortiSandbox
- Захист від вкрадених облікових даних і
- Публікування Exchange і сканування файлів
- Рідний захист HTTP/2 WAF
- REST API
- Сканер вразливостей
- Virtual patching
- Особлива увага false positive та SQLi
- Апаратні чіпи для SSL
- SSO/аутентифікація
- Балансування навантаження рівня 7

FortiWeb Cloud

- AWS, Azure, GCP, and OCI
- Найпопулярніший варіант в України - BYOL

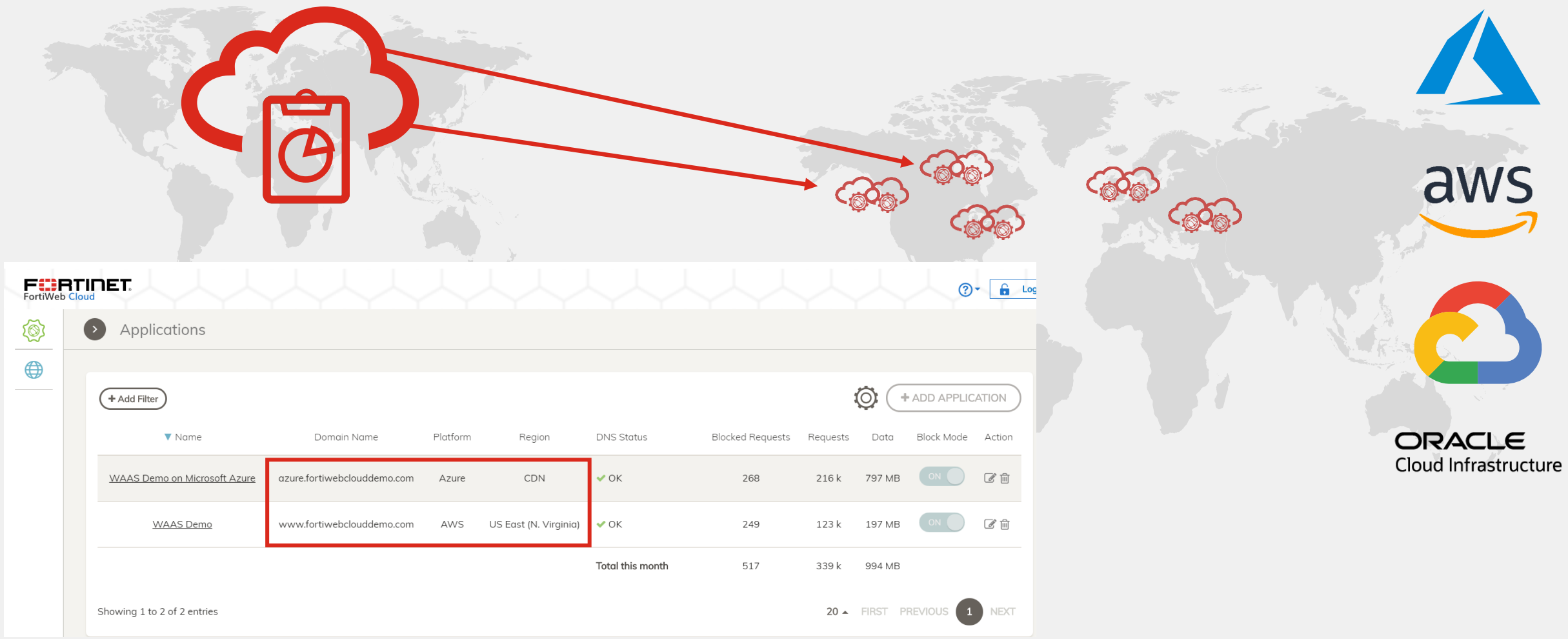


FortiWeb Cloud WAF як Сервіс



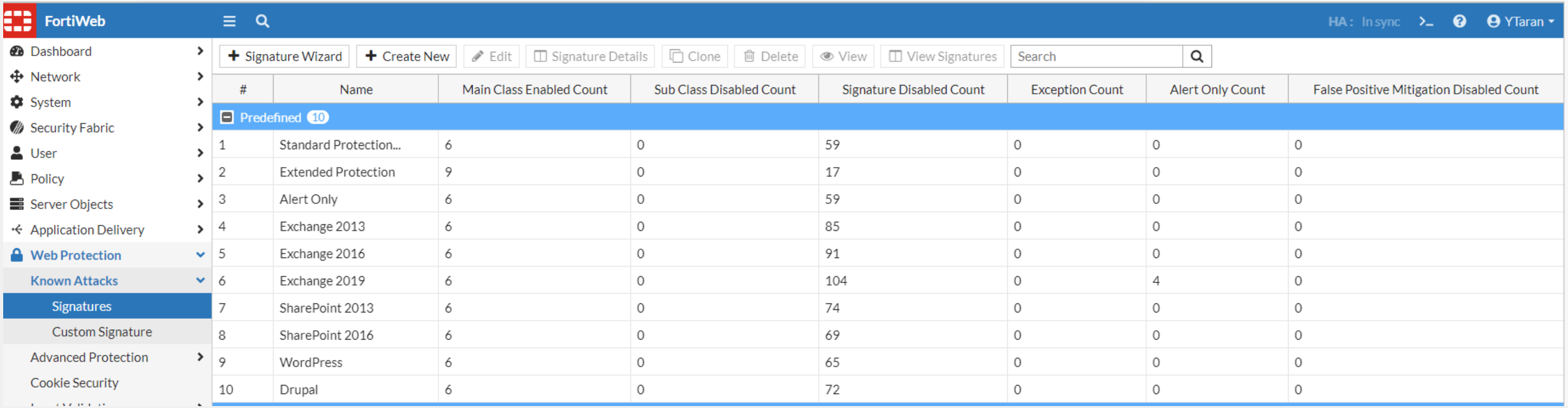
FortiWeb as a Service

SaaS



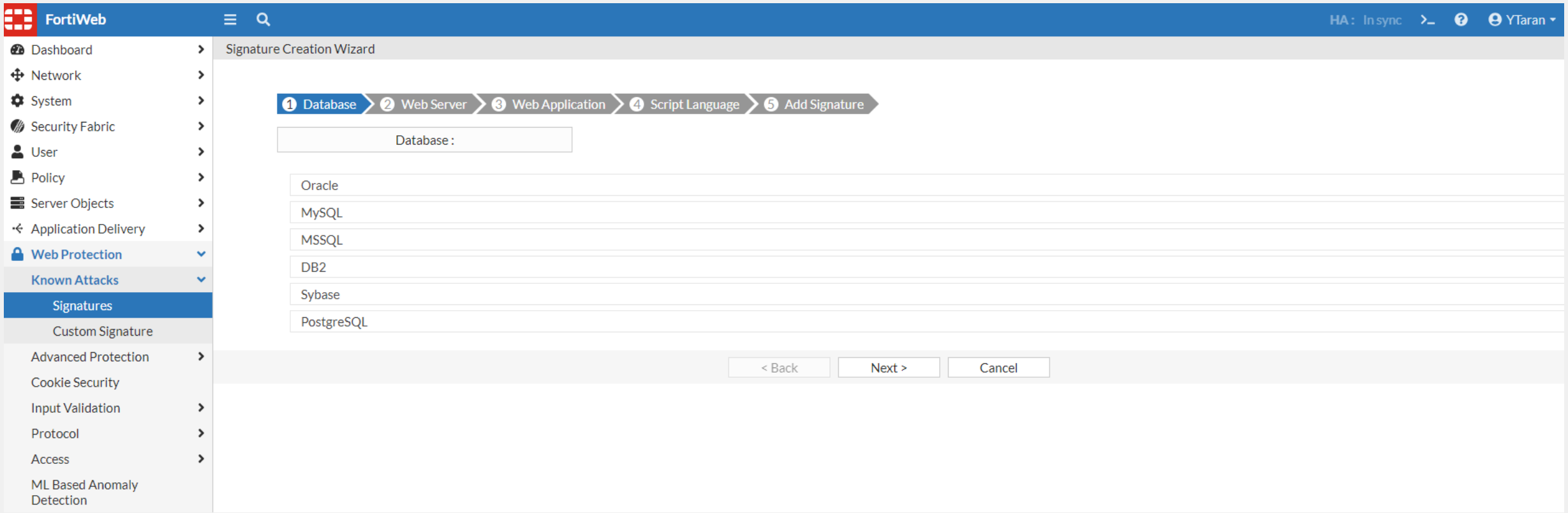
Шаблони та швидкий старт

Шаблони під розповсюджені додатки

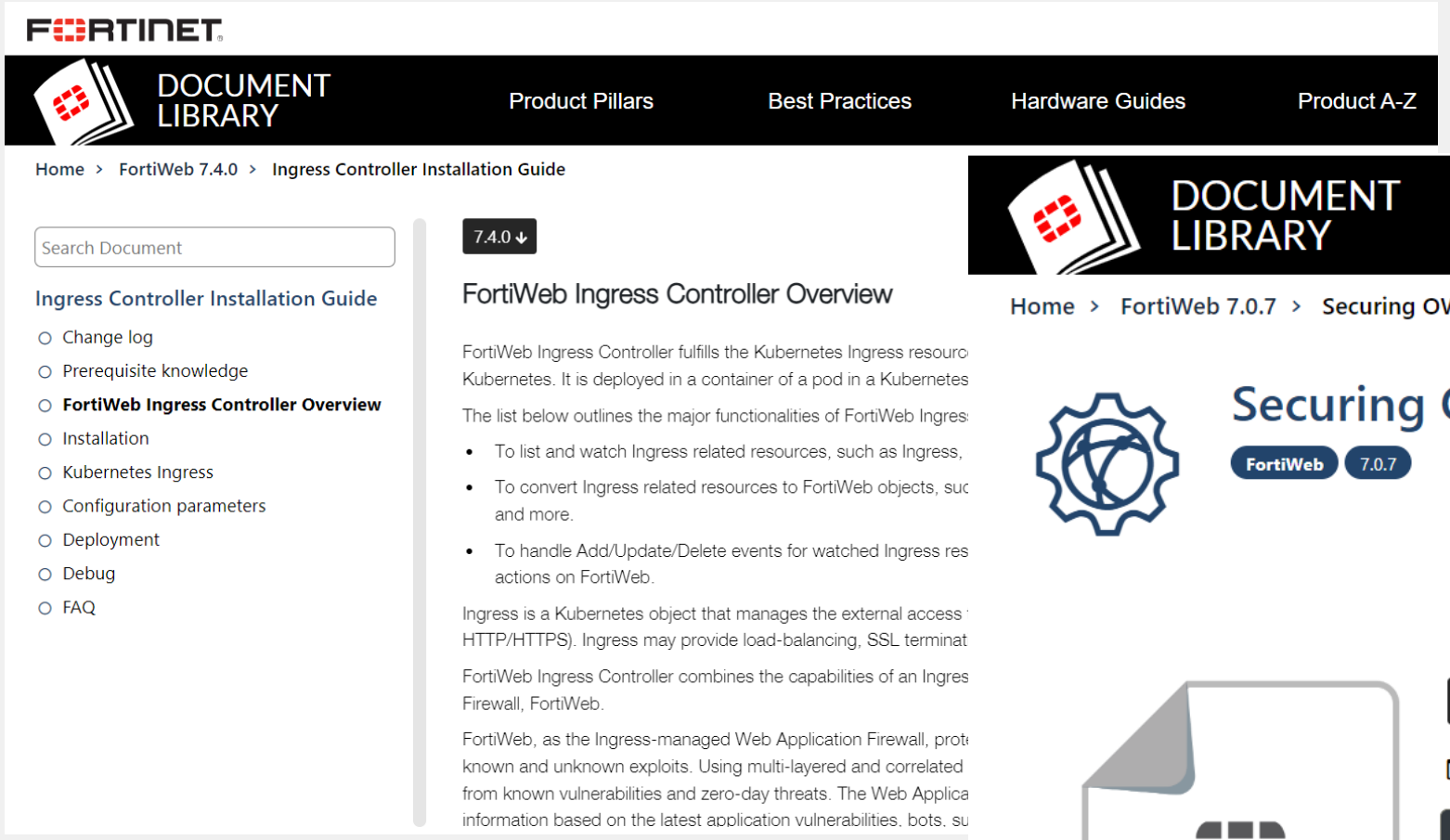


#	Name	Main Class Enabled Count	Sub Class Disabled Count	Signature Disabled Count	Exception Count	Alert Only Count	False Positive Mitigation Disabled Count
Predefined 10							
1	Standard Protection...	6	0	59	0	0	0
2	Extended Protection	9	0	17	0	0	0
3	Alert Only	6	0	59	0	0	0
4	Exchange 2013	6	0	85	0	0	0
5	Exchange 2016	6	0	91	0	0	0
6	Exchange 2019	6	0	104	0	4	0
7	SharePoint 2013	6	0	74	0	0	0
8	SharePoint 2016	6	0	69	0	0	0
9	WordPress	6	0	65	0	0	0
10	Drupal	6	0	72	0	0	0

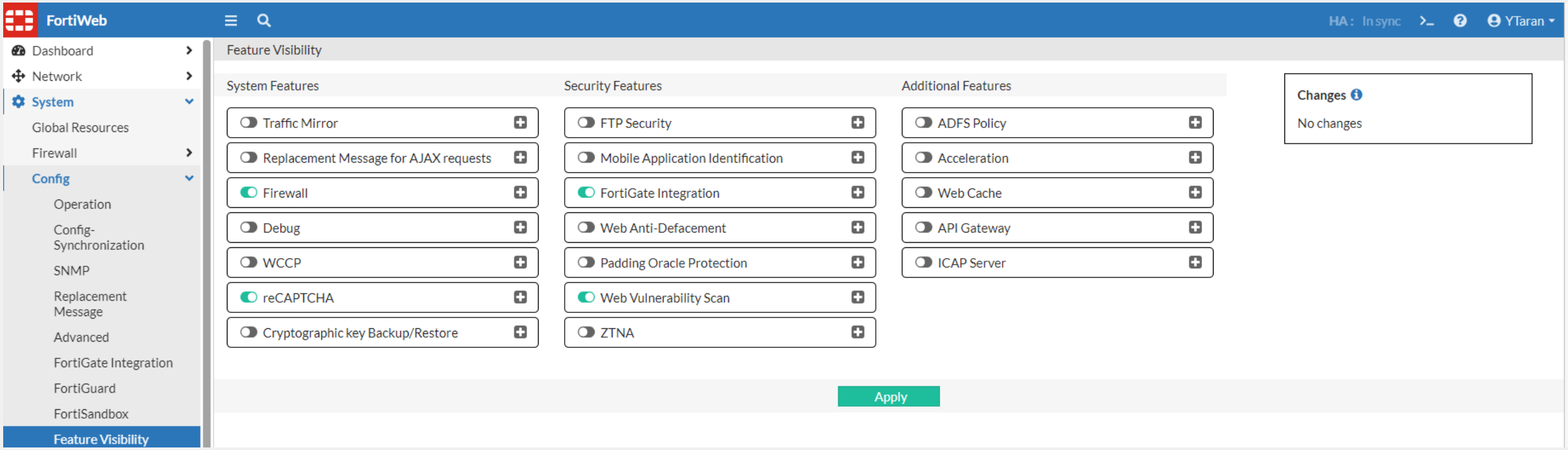
Або за хвилину можно створити свій варіант



Або за хвилину можно створити свій варіант



Не забувайте вмикати потрібні функції




FORTINET

Дякую за увагу!