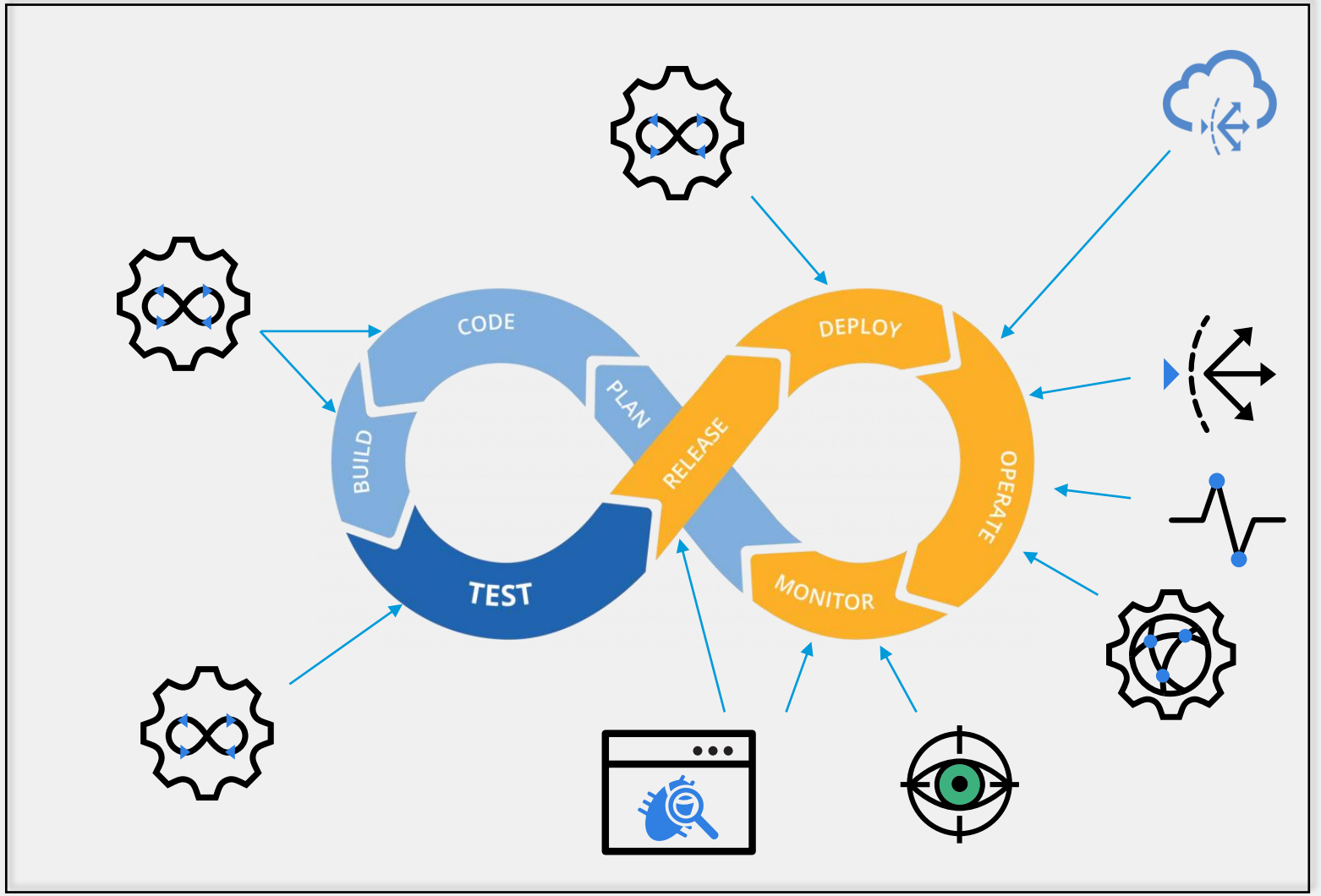
FORTINET

Рішення для захисту від атак на веб-додатки та API від Fortinet

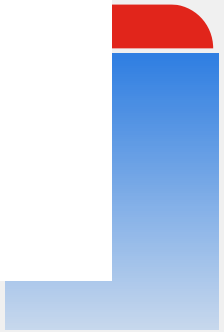
Зміст

Безпека веб-додатків з Fortinet

- FortiWeb
- FortiADC
- FortiGSLB
- FortiDevSec
- FortiDAST
- FortiDDOS
- FortiRecon

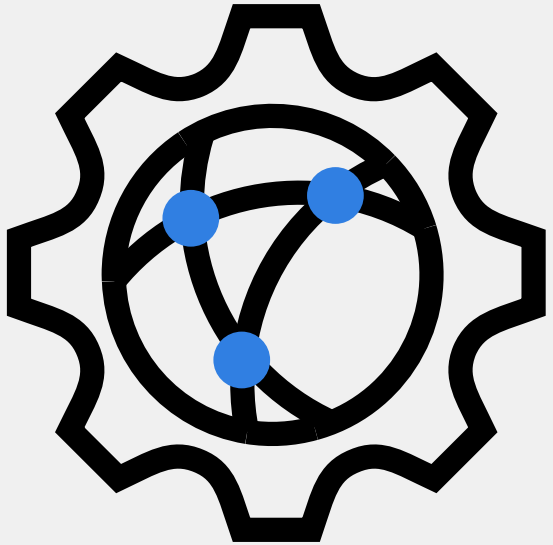


FortiWeb



Безпека веб-додатків та API з FortiWeb

Application Security

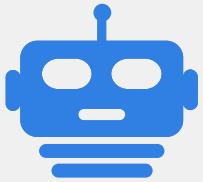


FortiWeb

Захист веб-додатків

Відповідність нормативним вимогам

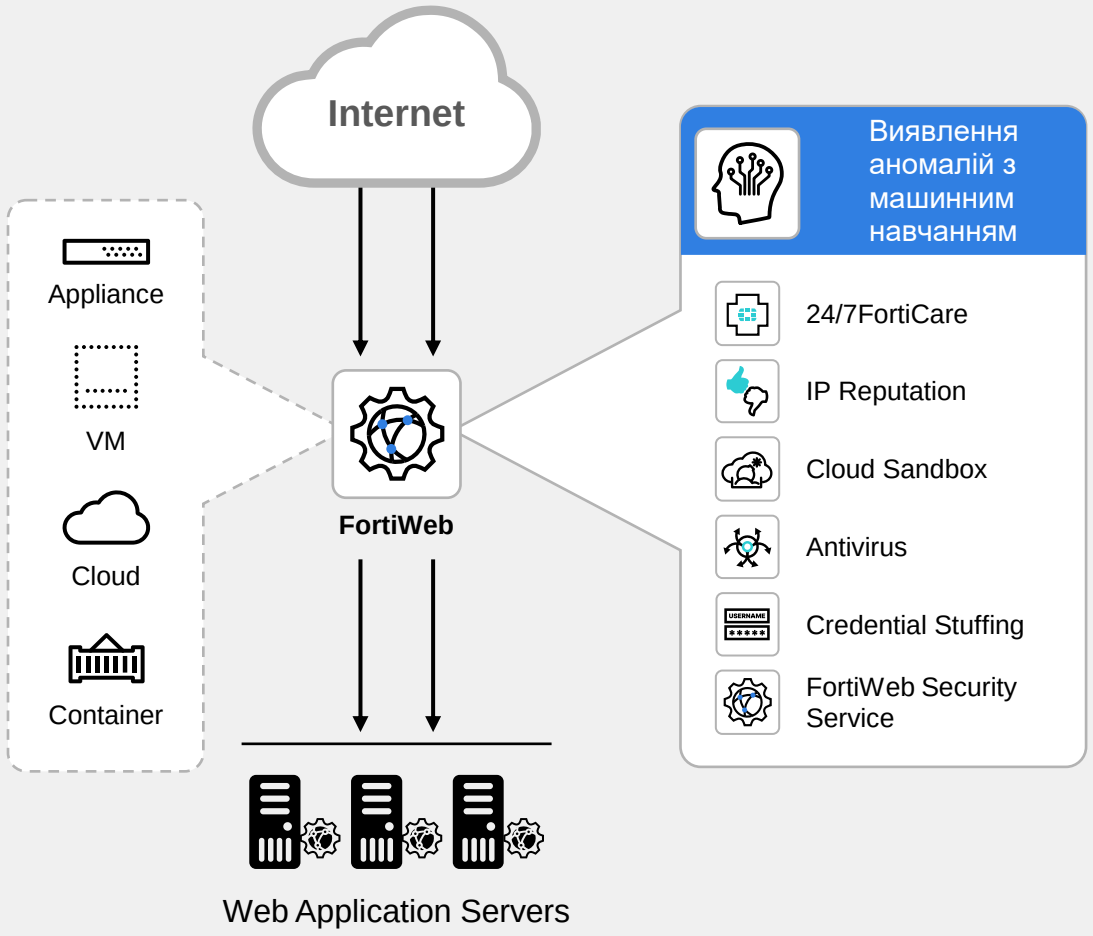
Операції SOC



Захист від ботів

Захист API

Web Application Security



1. Захист веб-додатків

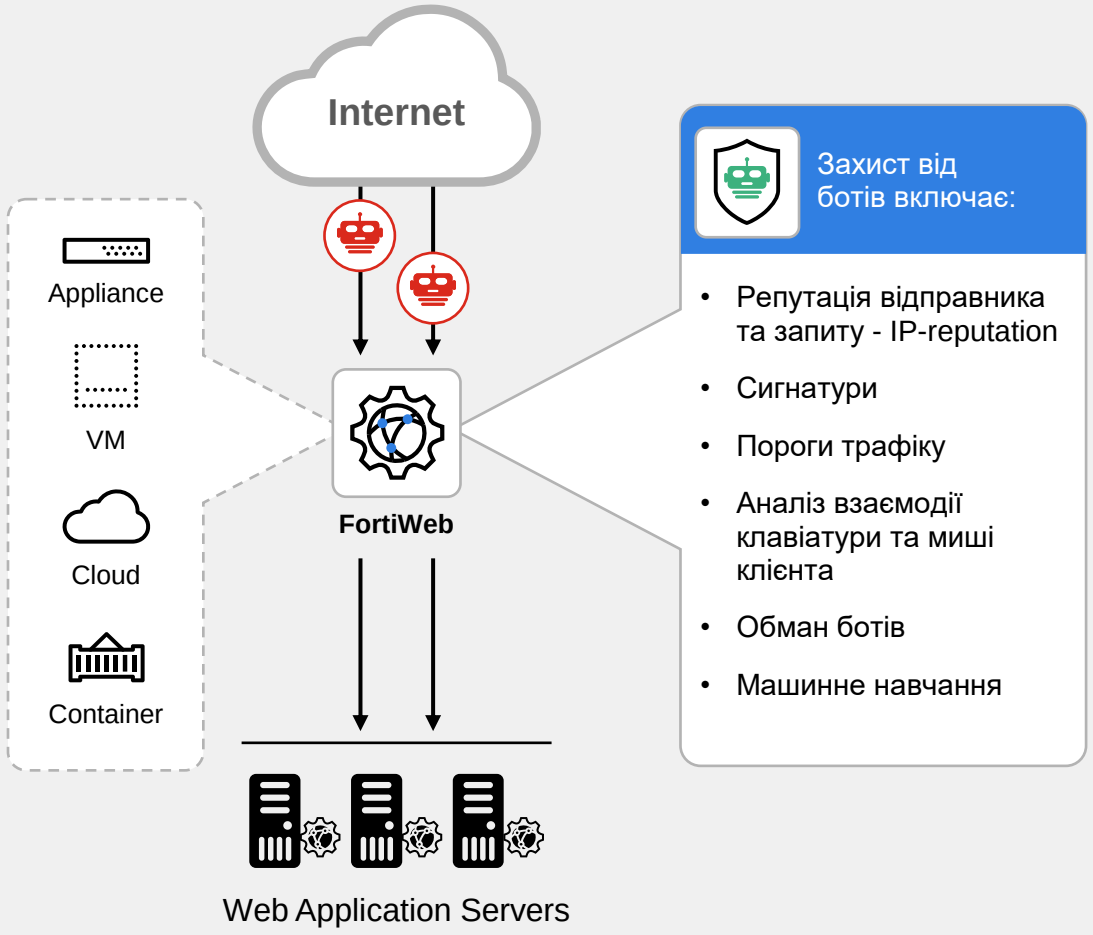
Захист від топ-10 OWASP та інших відомих загроз, а також невідомих загроз.

Оптимізована безпека бізнес-додатків з ML

Захищає від загроз веб-додатки:

- Захист від відомих ризиків, включаючи OWASP Top 10
- Захист від невідомих загроз і загроз нульового дня
- Зменшує адміністративні накладні витрати за рахунок зменшення помилкових спрацьовувань за допомогою машинного навчання

Захист від ботів



2. Захист від ботів

Блокування всі дії зловмисного бота (наприклад, сканування вмісту, DOS, збір даних, шахрайство з транзакціями).

Розширене виявлення ботів на базі ML

Захист додатків від ботів:

- Блокує шкідливих ботів, не блокуючи користувачів і не втручаючись у законну діяльність ботів, наприклад пошукових систем
- Зменшує або виключає залежність від використання методів перевірки користувача, які погіршують досвід користувачів, наприклад ReCaptcha

Відповідність нормативним вимогам

Відповідність

Забезпечує виконання нормативних вимог, зокрема специфічних вимог вимоги WAF, що викладені в стандарті безпеки даних індустрії платіжних карток (PCI-DSS), а також GDPR, HIPAA та інших

Забезпечує PCI DSS 6.6:
"Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic."

3. Відповідність до нормативів:

Забезпечує виконання нормативних вимог для публічно доступних веб-додатків

Виконання нормативних вимог

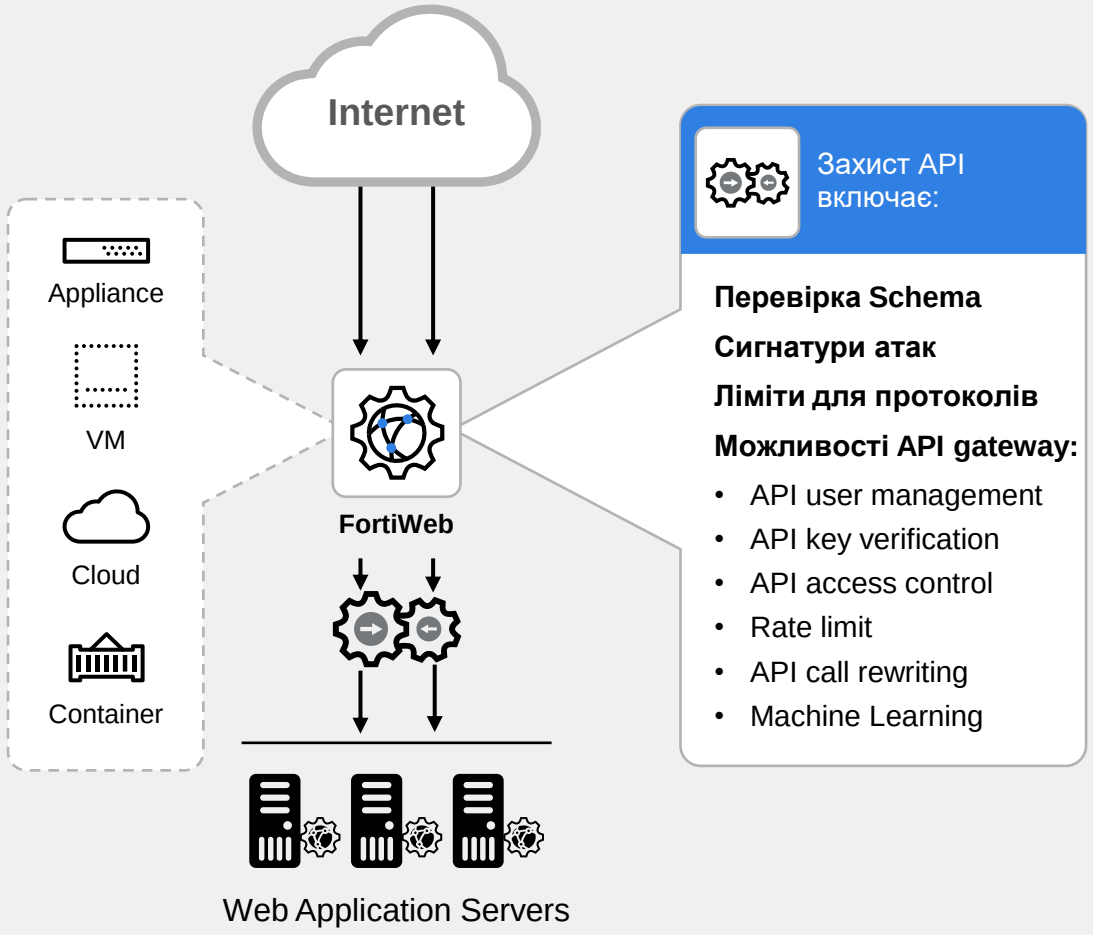
Надає спеціальні засоби контролю відповідності для захисту веб-додатків:

- Захист від відомих ризиків, у тому числі поширених веб-загроз, таких як топ-10 OWASP
- Вбудований сканер вразливостей

Виконання вимог PCI-DSS 6.6

- Виконання PCI DSS обов'язкове для компаній , що видають кредитні картки, і застосовується до всіх організацій, які зберігають, обробляють або передають дані власників карток

Захист API доступних з Internet



4. Захист API, що доступні з Інтернет

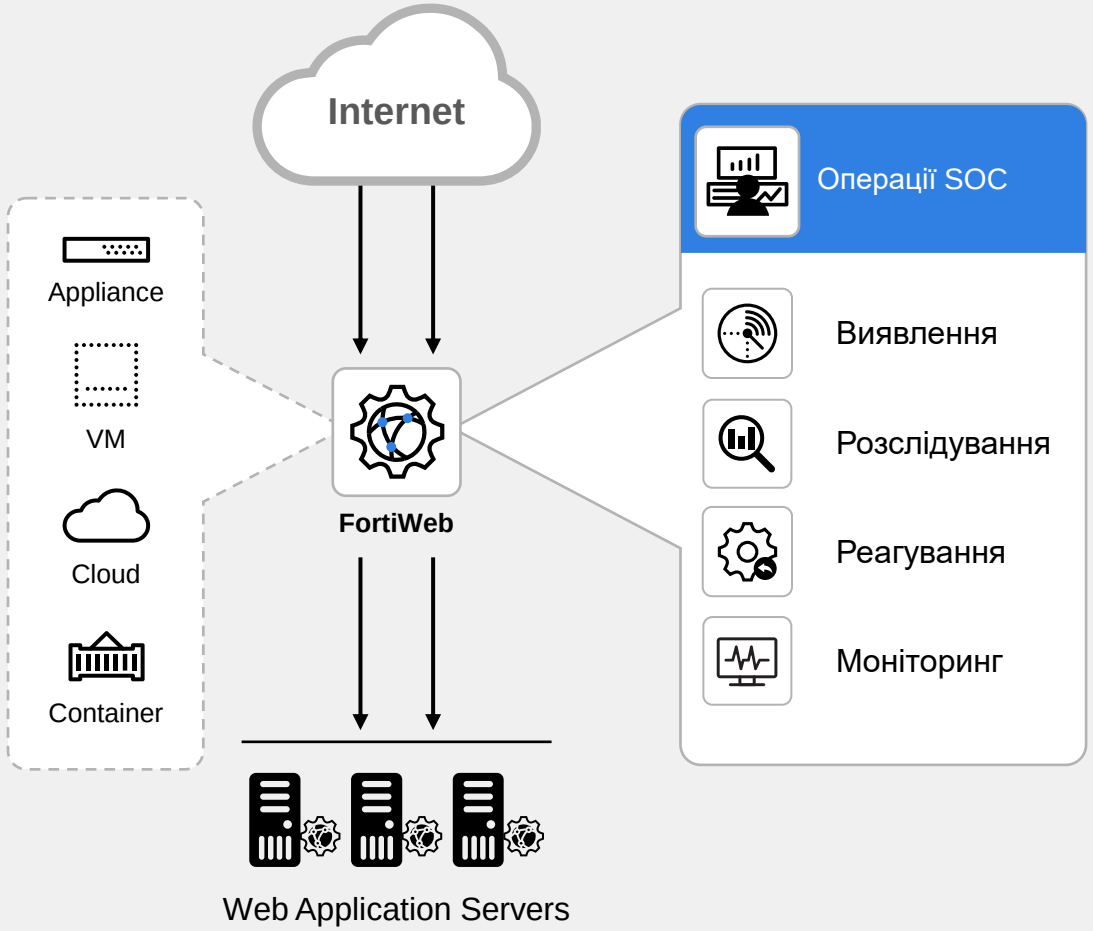
Захист API, які забезпечують спілкування B2B і підтримують мобільні програми.

Задіяння ML для захисту API, які підтримують критично важливі бізнес можливості

Розширений захист для API:

- Єдина точка доступу до API
- Приховує внутрішню структуру API від потенційних зловмисників
- Забезпечує покращену взаємодію з користувачами на різноманітних пристроях без шкоди для безпеки
- Машинне навчання для вивчення та захисту API

Операції SOC



5. Операції SOC

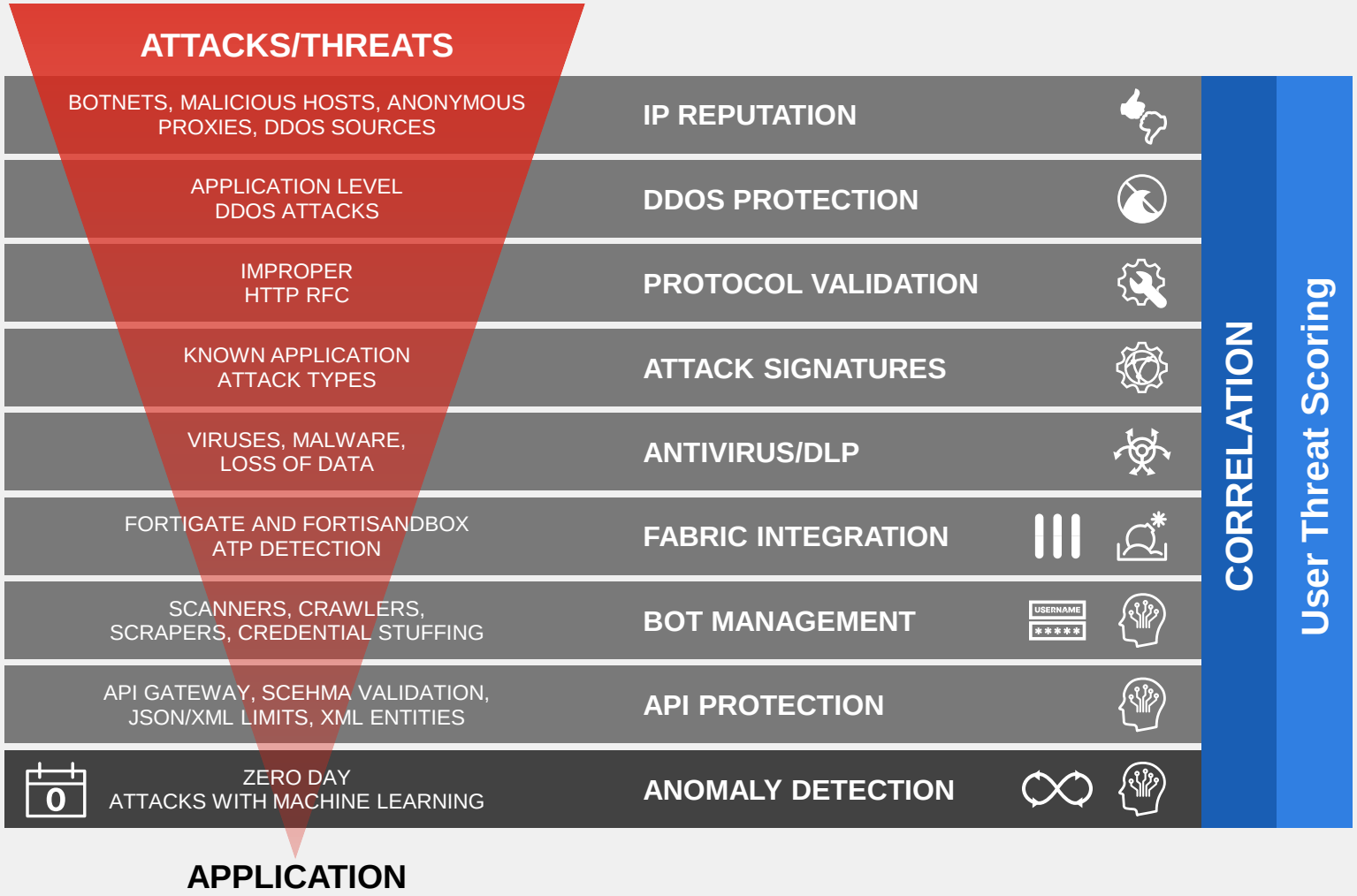
Threat Analytics консолідує необроблені дані про події в чітку картину найважливіших загроз, щоб аналітики SOC могли визначати пріоритетність блокування найбільш критичних загроз.

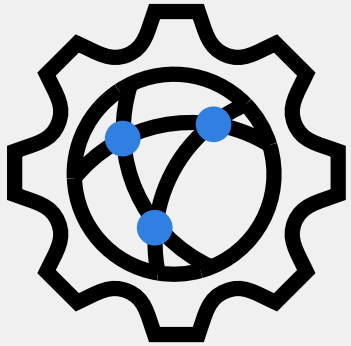
Використання Threat Analytics для виділення критичних загроз

Дозволяє команді SOC:

- Зменшення витрат на адміністрування шляхом консолідації окремих подій у дискретні загрози, скорочення завдань для ручного аналізу
- Прискорення розслідувань та забезпечення швидкого реагування
- Визначення загроз, які вимагають змін політики або додаткового моніторингу
- Зосередження обмежених ресурсів на блокування найважливіших загроз

Багаторівневий захист з FortiWeb





Багаторівневий захист з використанням ML та гнучкість налаштувань надає високий рівень блокування загроз з малою кількістю False Positives

Апаратні FortiWeb

FortiWeb	FWB-100E	FWB-400E	FWB-600E
Throughput	50 Mbps	250 Mbps	750 Mbps
GE RJ45 ports	4	4	2 + 2 Bypass
GE SFP slots	-	4	4
10GE SFP+	-	-	-
Storage capacity	32 GB	480 GB	480 GB
Form Factor	Desktop	1RU	1RU

FortiWeb	FWB-1000F	FWB-2000F	FWB-3000F	FWB-4000F
Throughput	2.5 Gbps	5 Gbps	10 Gbps	70 Gbps
GE RJ45 ports	4 Bypass	4 Bypass	8 Bypass	8 Bypass
GE SFP slots	4	4	-	-
10GE SFP+	2	4	10 (2 Bypass)	10 (2 Bypass)
Storage capacity	2x 480 GB	2x 480 GB	2x 960 GB	2x 960 GB
Form Factor	2RU	2RU	2RU	2RU

FortiWeb VM

FortiWeb-VM	FWB-VM01	FWB-VM02	FWB-VM04	FWB-VM08
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	2 Gbps
Max vCPU Supported	1	2	4	8
Memory required (Min/Max)	1 GB / Unlimited			
Storage capacity (Min/Max)	40 GB / 2 TB			

FortiWeb Container	FWB-VMC01	FWB-VMC02	FWB-VMC04	FWB-VMC08
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	2 Gbps
Memory required (Min)	4 GB			
Storage capacity (Min/Max)	30 GB / 500 GB			

Максимальні значення параметрів в конфігурації

https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/789367/appendix-b-maximum-configuration-values

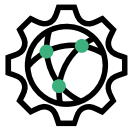
Per appliance configuration maximums - ADOMs, server policies, Virtual IPs, server objects, and domains in ML policies

The configuration maximums for the following items apply at the appliance level, and the maximums vary on each model, as shown in the following table.

FortiWeb model	ADOMs	Server policies	Virtual IPs	Server Objects			Domains in all ML policies
				Server pools	Pool members	Virtual servers	
FortiWeb 100D	0	32	1024	256	1024	1024	4
FortiWeb 100E	0	32	1024	256	1024	1024	4
FortiWeb 400C	32	64	1024	256	1024	1024	6
FortiWeb 400D	32	64	1024	256	1024	1024	6
FortiWeb 400E	32	64	1024	256	1024	1024	6
FortiWeb 600D	32	96	1024	384	1024	1024	16

Сервіси FortiGuard для FortiWeb

SECURED BY
FortiGuard



WAF Security Service

- Application layer signatures
- Web application signature to prevent any web attack
- Machine learning threat models
- Malicious Bots

IP Reputation

- Protection for automated attacks and malicious sources
- DDoS, Phishing, Botnet, Spam, anonymous proxies and infected sources

Anti-malware

- Scan file uploads
- Regular and extended AV databases
- Protect the network against exploitable vulnerabilities

FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Subscription based
- No separate sandbox required

Credential Stuffing Defense

- Identifies login attempts using stolen credentials from numerous sources
- Automatic updates
- Prevents unwanted access and defends against data breaches

Threat Analytics

- AI-based threat analytics
- Identifies common characteristics and patterns and groups them into meaningful security incidents
- Incident risk prioritization

STANDARD SUBSCRIPTION

ADVANCED SUBSCRIPTION

FortiWeb Threat Analytics

Simplifies Threat Detection and Response

Пришвидшує розслідування інцидентів безпеки

Допомагає аналітикам **фокусуватись** на найважливіших загрозах

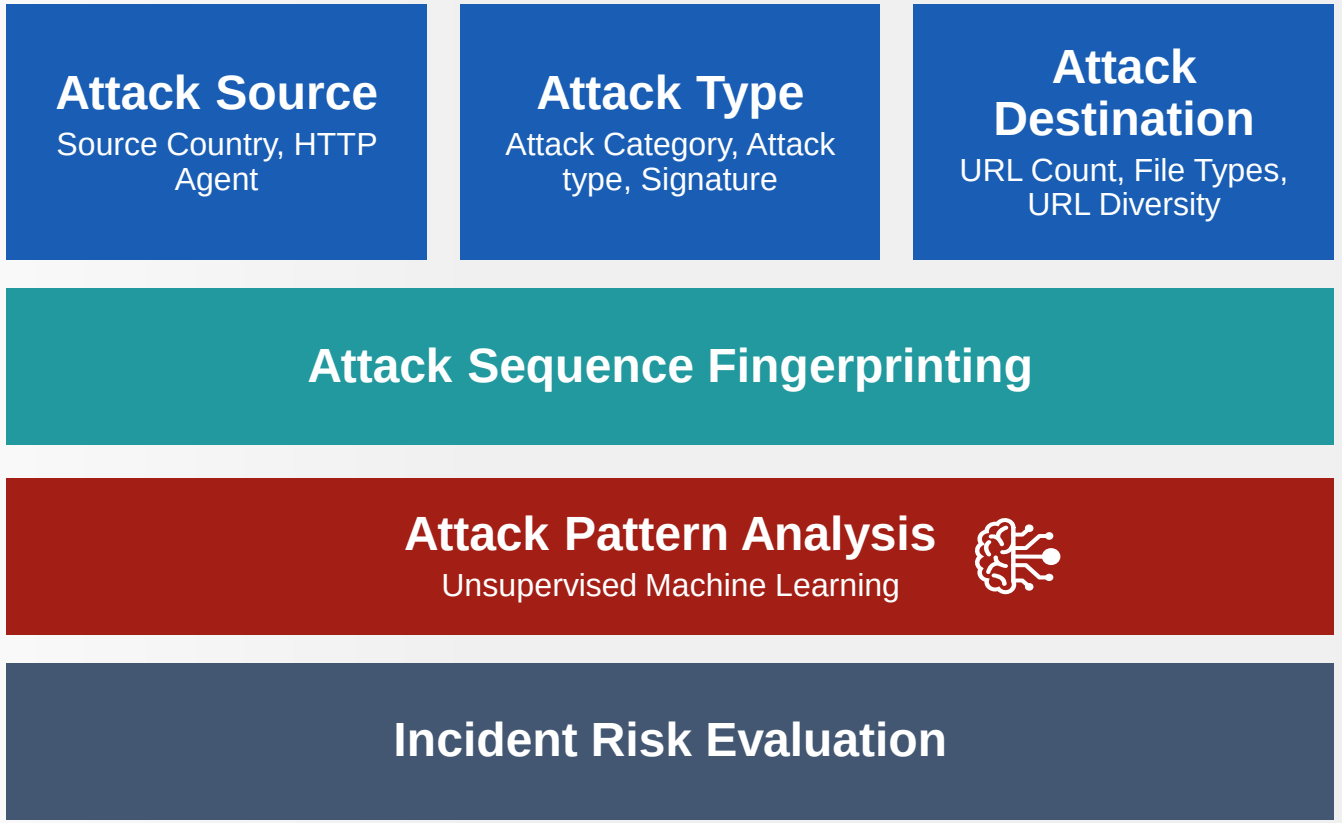
Надає рекомендації щодо посилення безпеки на основі отриманих даних

Концентрує події з усіх ваших гібридних хмарних середовищ

Як це працює

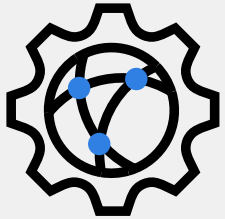
FortiWeb Threat Analytics використовує алгоритми машинного навчання для виявлення шаблонів атак і агрегування їх в інциденти безпеки в для всіх веб-додатків підприємства.

- Агрегація атаки в послідовності
- Створення fingerprints для послідовностей атак
- Використання ML для ідентифікації шаблонів у fingerprints
- Агрегування послідовностей в інциденти
- Оцінка ризику інциденту. На Severity впливає –
  - Severity кожної атаки в інциденті
  - Кількість атак в інциденті
  - Різноманітність типів атак



FortiWeb VM

Користувач **купляє**: VM
(perpetual)



FortiWeb VM

FortiGuard
Bundle

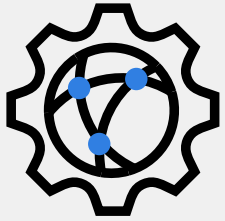
Користувач **підписується**: Bundle
(щорічні підписки)

CAPEX модель

All Supported Hypervisor

FortiWeb VM-S(підписка)

FWB VM for „FREE”



FortiWeb VM

FortiGuard Bundle

Користувач **підписується** : Bundle

OPEX модель

All Supported Hypervisor

FortiWeb VM-S(підписка)

порівняння

FortiWeb VM

- Аванс: дорого на початку
- Довгий строк : економія витрат

VM-01 Advanced Bundle

1st Year: ~$14 200

2nd Year: ~$5 800 (Advanced Bundle only)

3rd Year: ~$ 5 800 (Advanced Bundle only)

Total Cost: ~$25,800

4th Year: ~$ 5 800 (Advanced Bundle only)

Total Cost: ~$31,600

FortiWeb VM-S

- Аванс : дешево на початку
- Довгий строк : дорожче

VMS-01 Advanced Bundle

1st Year: ~$8 200

2nd Year: ~$8 200

3rd Year: ~$8 200

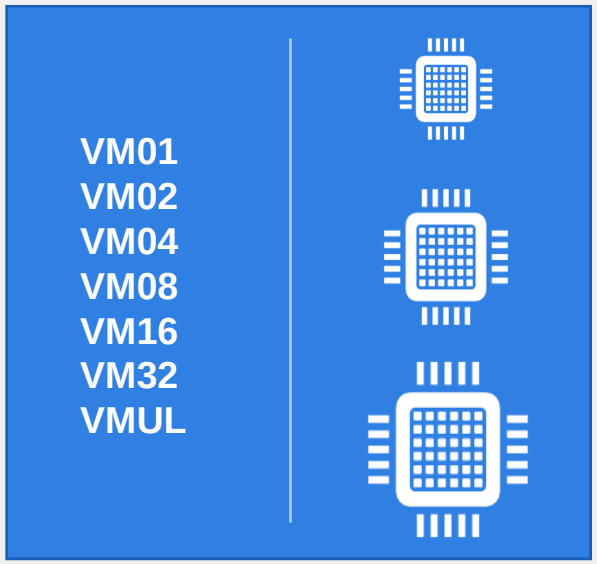
Total Cost: ~$24,400

4th Year: ~$8 200

Total Cost: ~$32,800

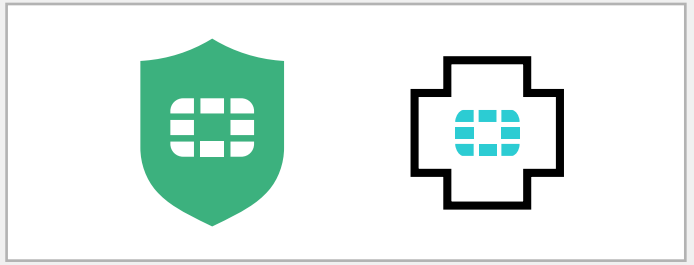
Програма FortiFlex

Гнучке споживання для всіх впроваджень



Scale and Performance

Any Size
Any Service
Any Environment
Portal Managed
Pay for Usage



Security & Support Services

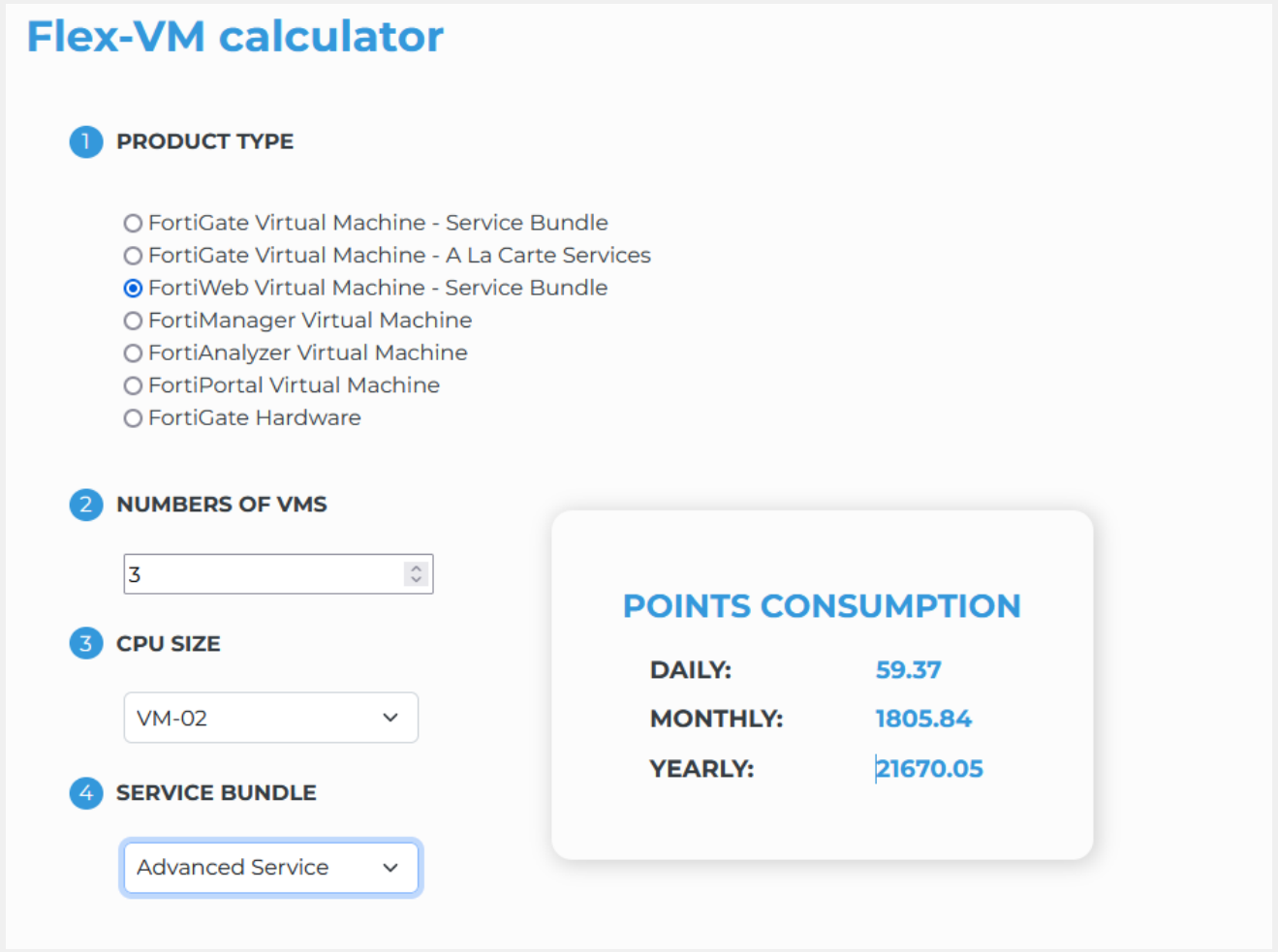
Public or Hybrid Cloud

Щоденний розрахунок оплати

FortiWeb VM and Services

- Використання VM та сарвісів розраховується **щодня**
  - » Користувач може будь-коли змінити кількість CPU, і новий розрахунок вступить в силу
  - » Щоденна плата за найбільшу конфігурацію VM та services за цей день
- Приклад 4-vCPU FortiWeb VM з Standard Bundle
  - » VM04 з Standard bundle буде споживати 40.74 балів на день
  - » VM04 який використовує лише 2 vCPUs, все одно споживатиме 40.74 балів на день
- Планування ємності
  - » Розгортання **3 VM04s і 1 VM02s** з **Standard web security bundle** протягом **365 днів** коштує **50,731 балів**

FortiFlex калькулятор



https://fndn.fortinet.net/index.php?/tools/flexvm/

Функціональність в різних режимах

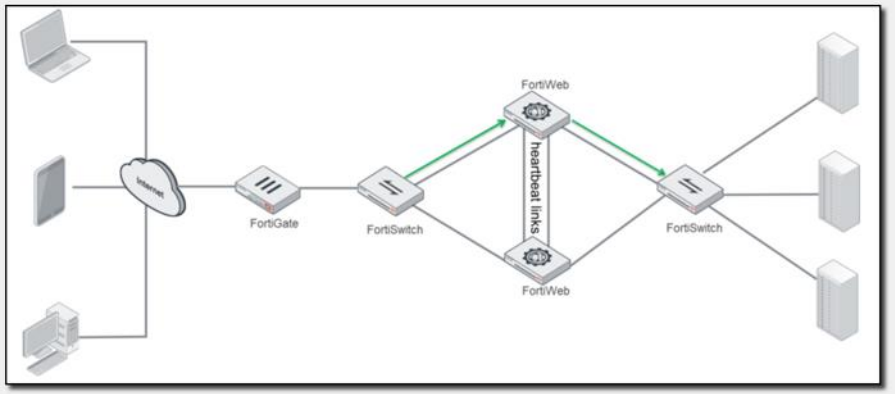
	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection
Matches by	•Server port •Virtual Server	•Data Capture Port •Server Farm	•V-zone (bridge) •Server Farm	•V-zone (bridge) •Server Farm
Violations	•Block •Modify	•Attempt to block by sending TCP reset	•Block •Modify	•Attempt to block by sending TCP reset
SSL	•Offloading capabilities • Optional re-encryption	•Decrypt and Scan only	•Decrypt and Scan only	•Decrypt and scan only
Forwarding	•Forwarding to a single server •Load balancing to server farm	•Pass-through to server farm member	•Pass-through to server farm member	•Pass-through to server farm member

https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/211763/planning-the-network-topology

Режими високої доступності

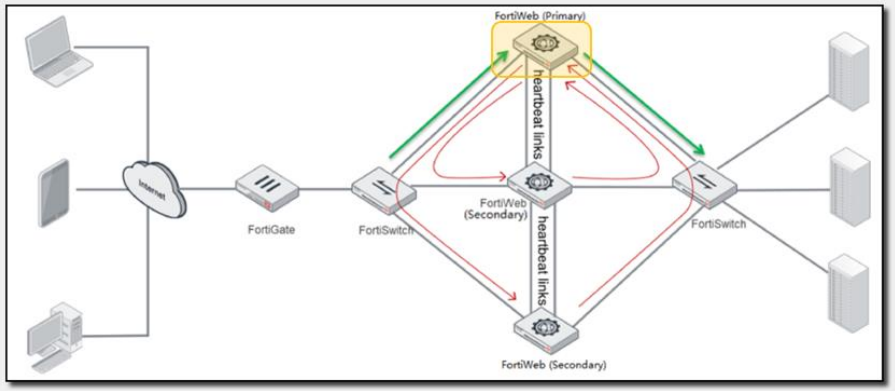
Active-Passive (2 пристрої)

Private Cloud (VMware/KVM/Hyper-V/OpenStack)
Public Cloud (GCP/OCI/Azure/AWS)



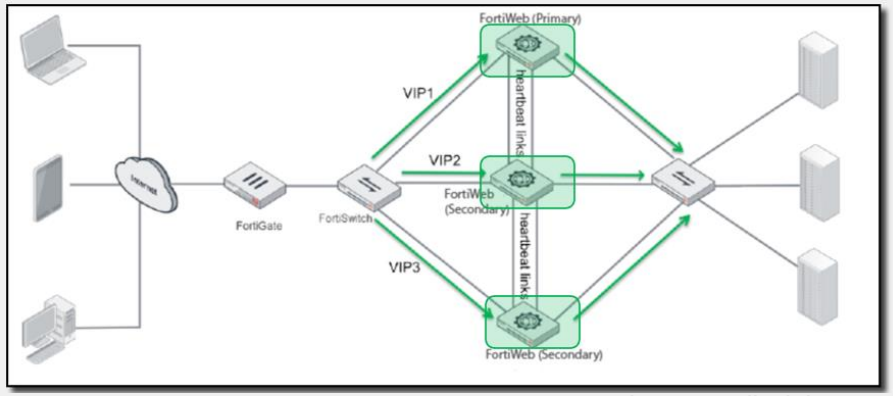
Active-Active (до 8 пристроїв)

Private Cloud (VMware/KVM/Hyper-V/OpenStack)



Active-Active-High Volume (до 8 пристроїв)

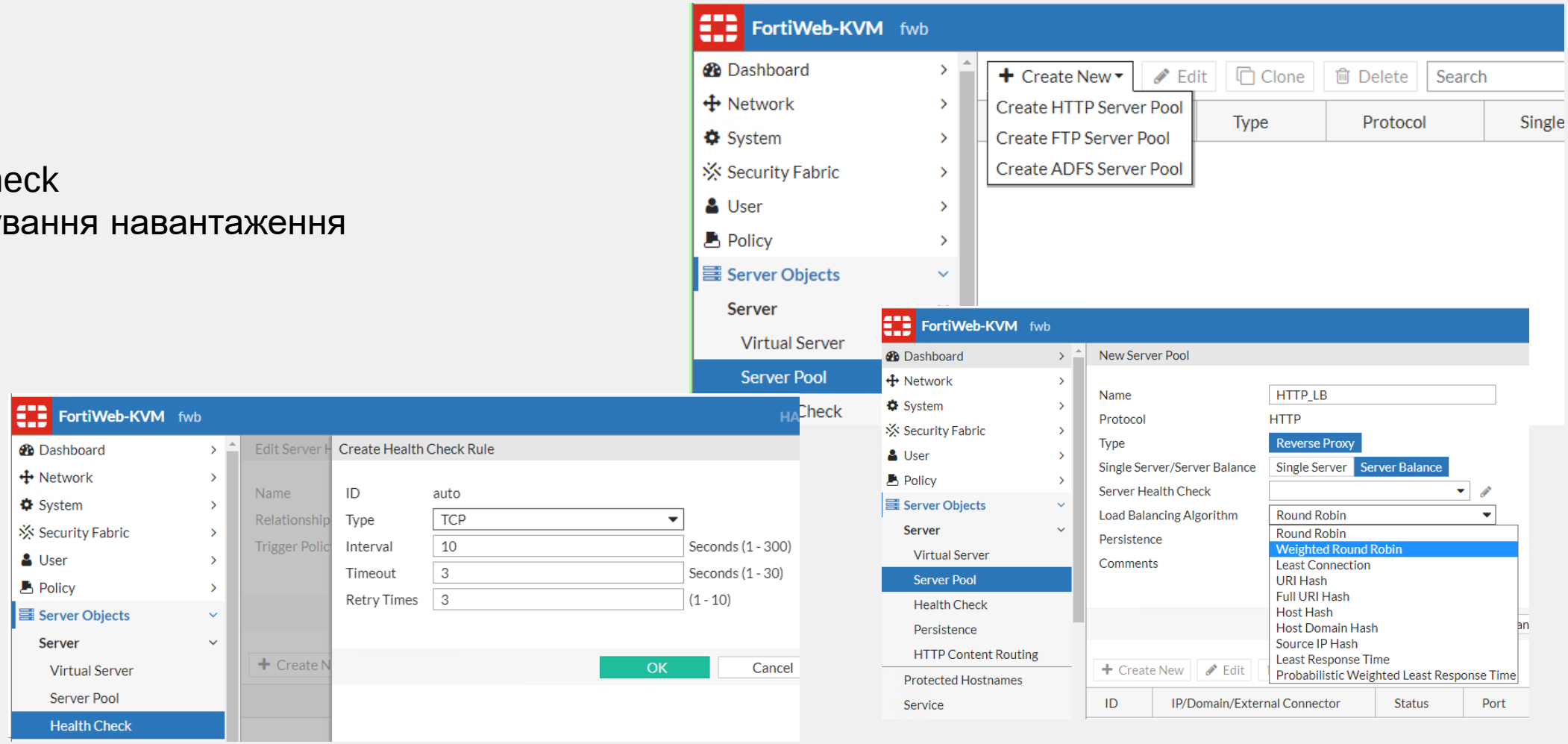
Private Cloud (VMware/KVM/Hyper-V/OpenStack)
Public Cloud (GCP/OCI/Azure/AWS)



https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/319533/fortiweb-high-availability-ha

Балансування HTTP / FTP

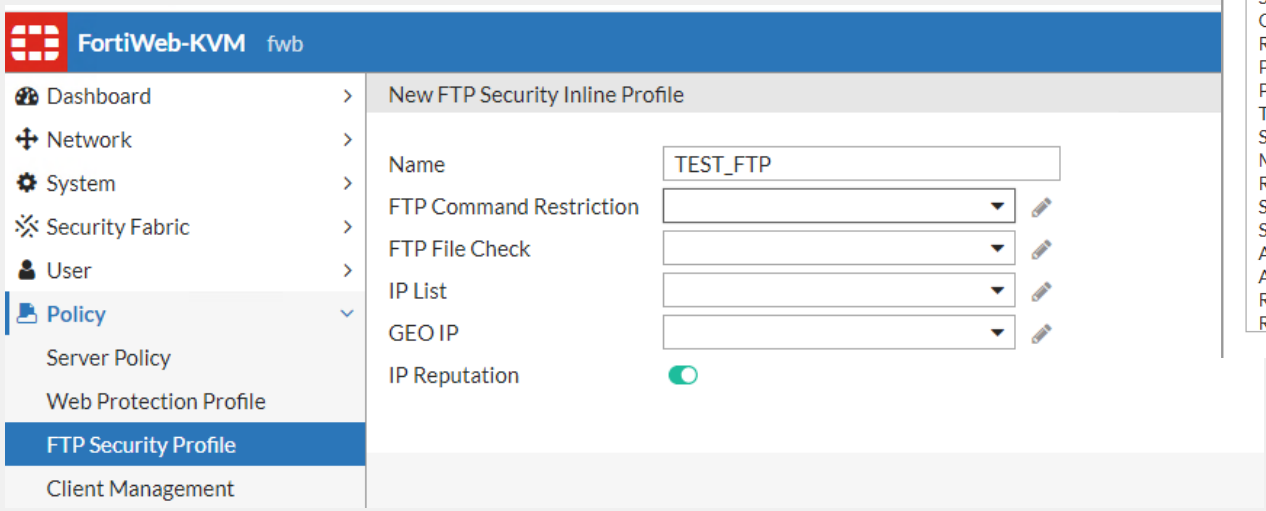
- Healthcheck
- Балансування навантаження

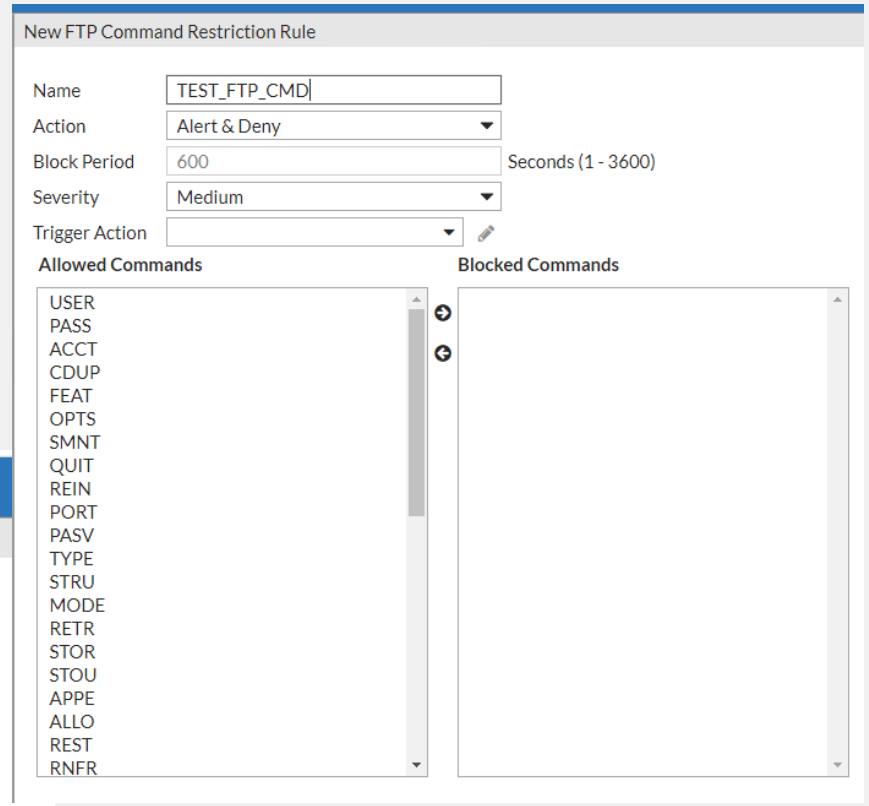


https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/399384/defining-your-web-servers

Захист FTP

- Фільтр по src IP list / GEO IP / IP reputation
- Обмеження команд FTP
- AV / Sandbox перевірка файлів

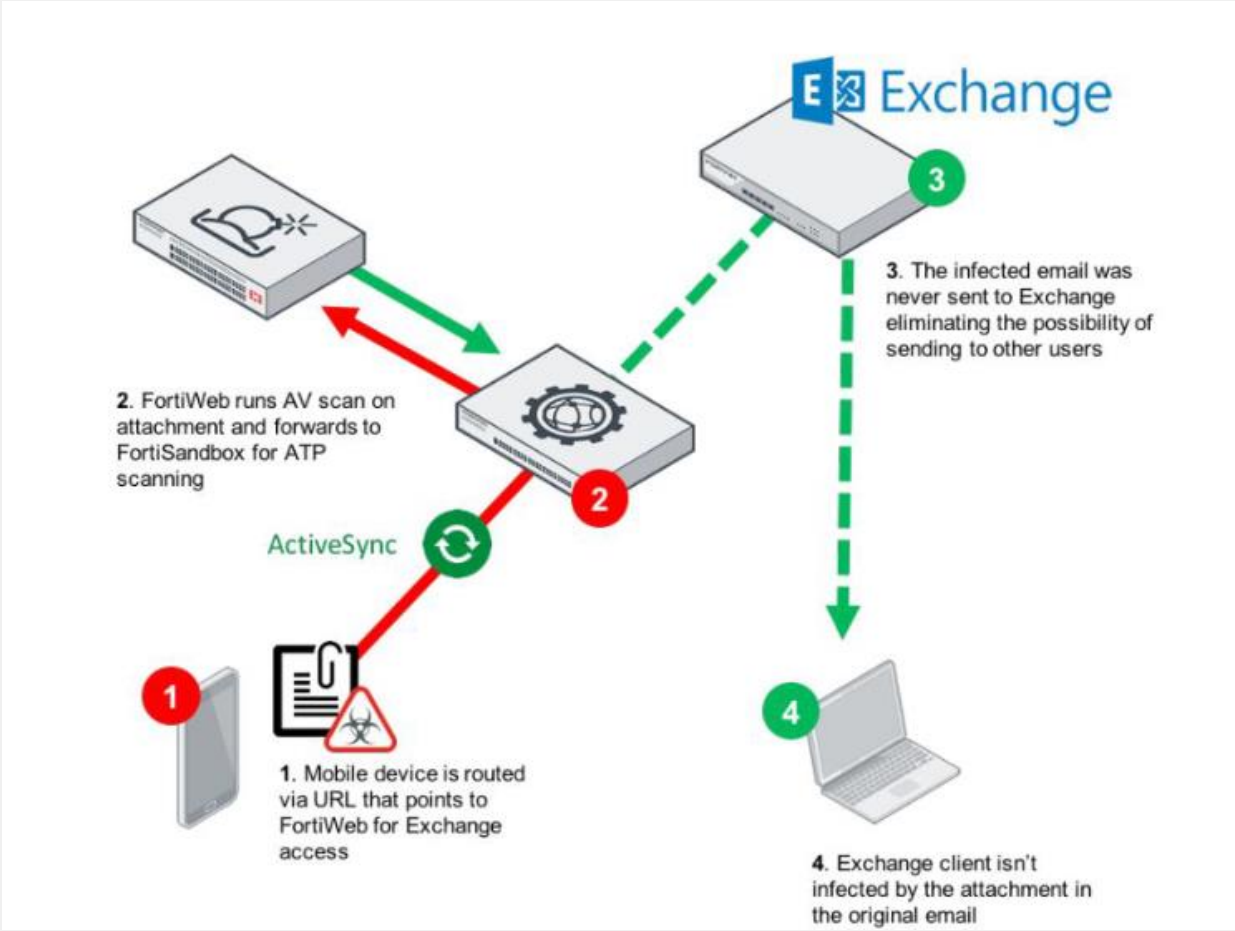




https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/621246/configuring-ftp-security

Публікація OWA

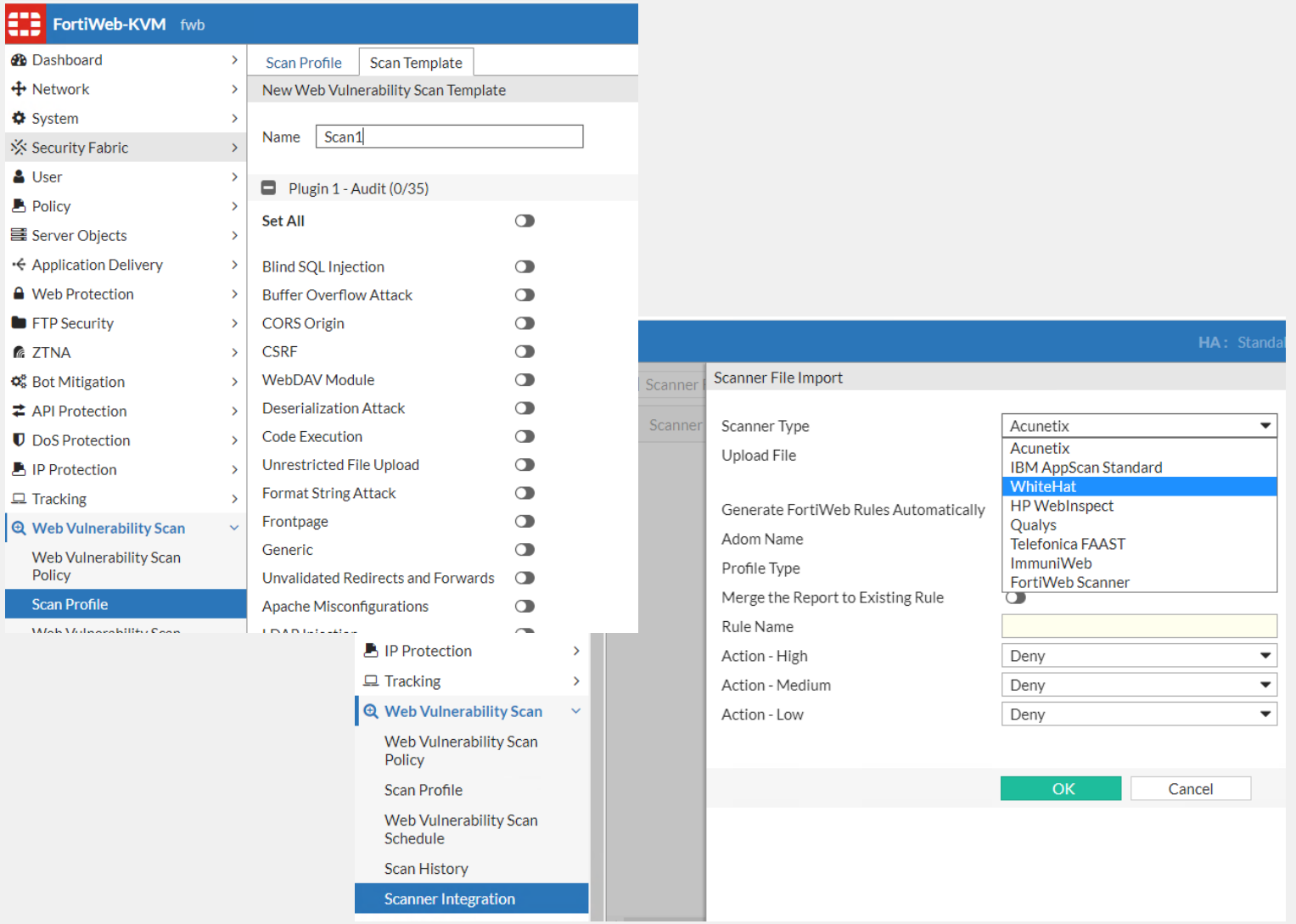
- Захист веб трафіку з WAF
- Блокування malware в ActiveSync



https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/cda1d277-10bb-11ea-9384-00505692583a/Protecting_OWA_and_ActiveSync_with_FortiWeb.pdf

Сканування вразливостей

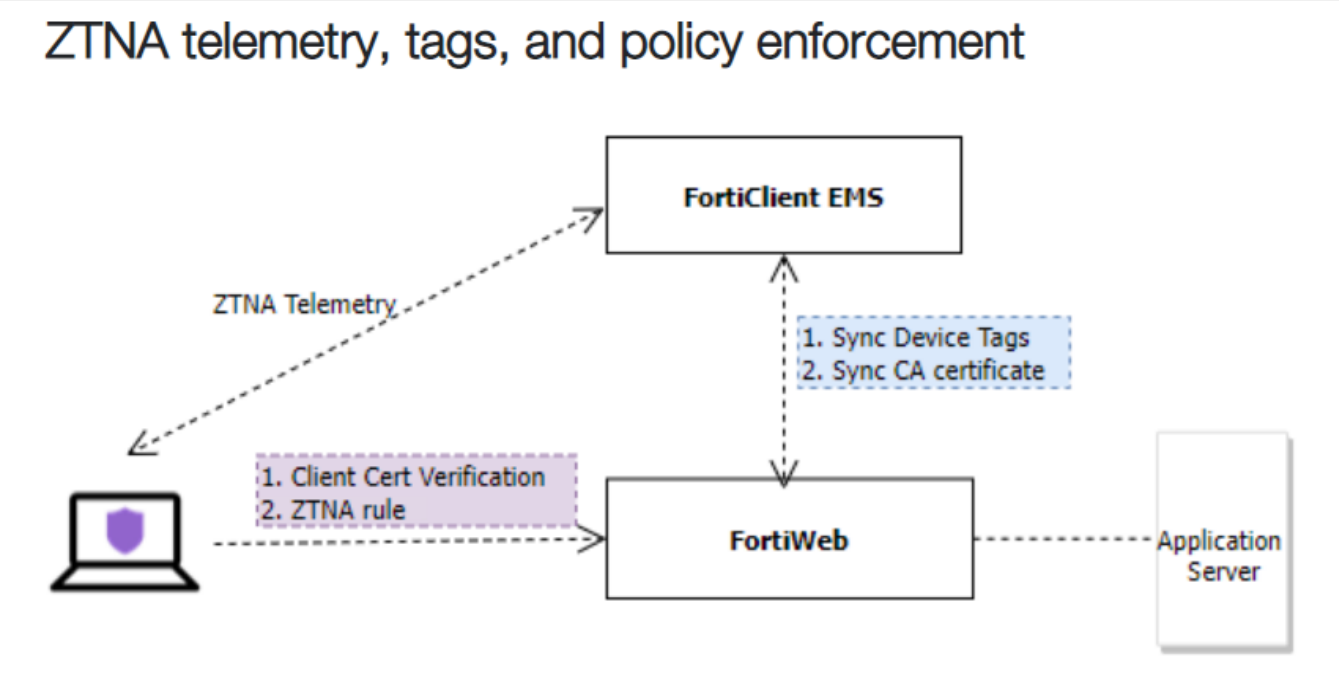
- Вбудований сканер вразливостей
- Підтримка сторонніх сканерів:
  - Acunetix
  - IBM AppScan Standard
  - WhiteHat
  - HP WebInspect
  - Qualys
  - Telefonica FAAST
  - ImmuniWeb
- Генерування профілю захисту за результатами сканування



https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/645669/vulnerability-scans
https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/59030/generating-a-protection-profile-using-scanner-reports

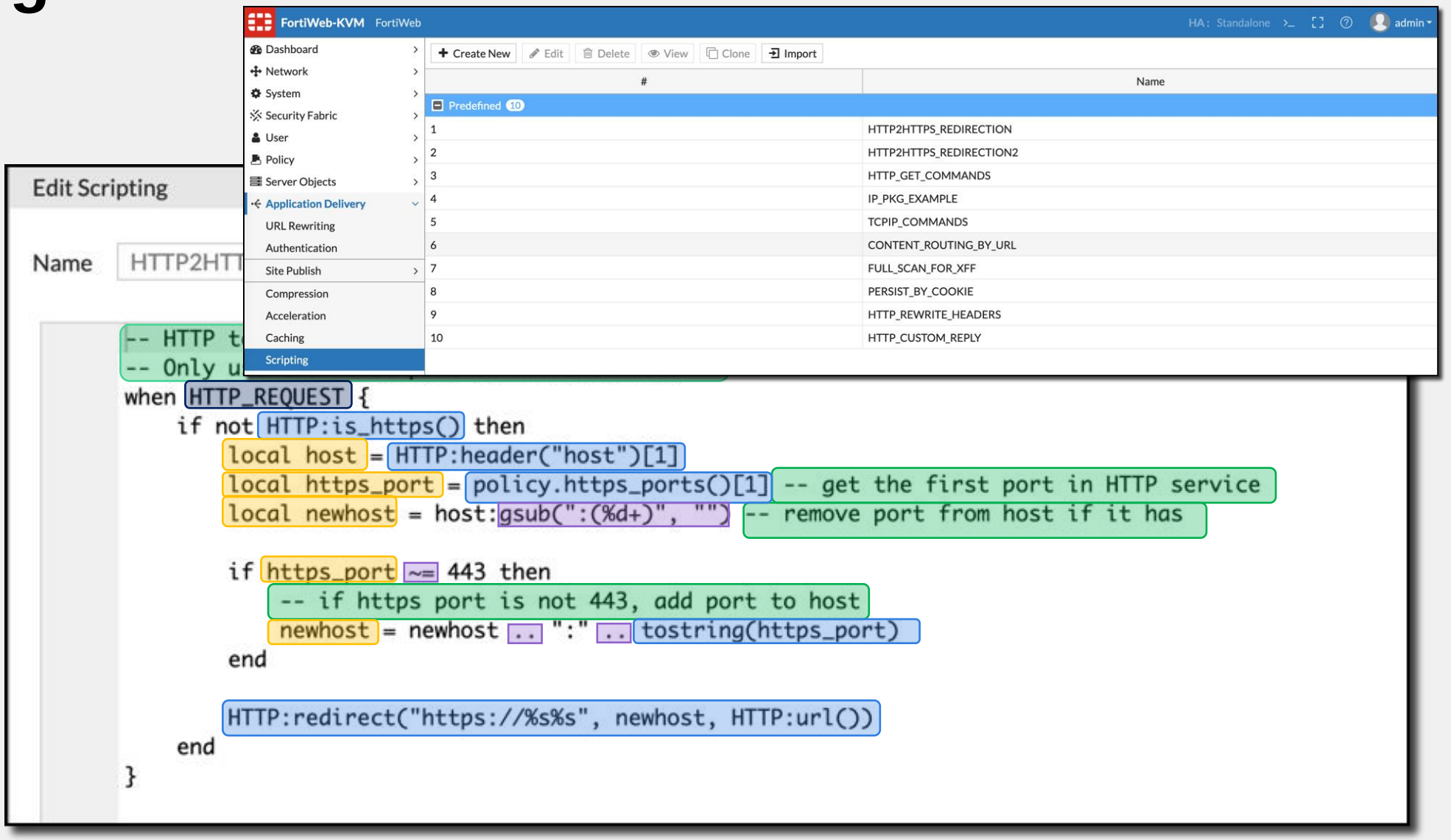
ZTNA

- Перевірка стану клієнта через FortiCleint ZTNA
- Обмеження доступу за результатами перевірки



https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/155485/zero-trust-network-access-ztna

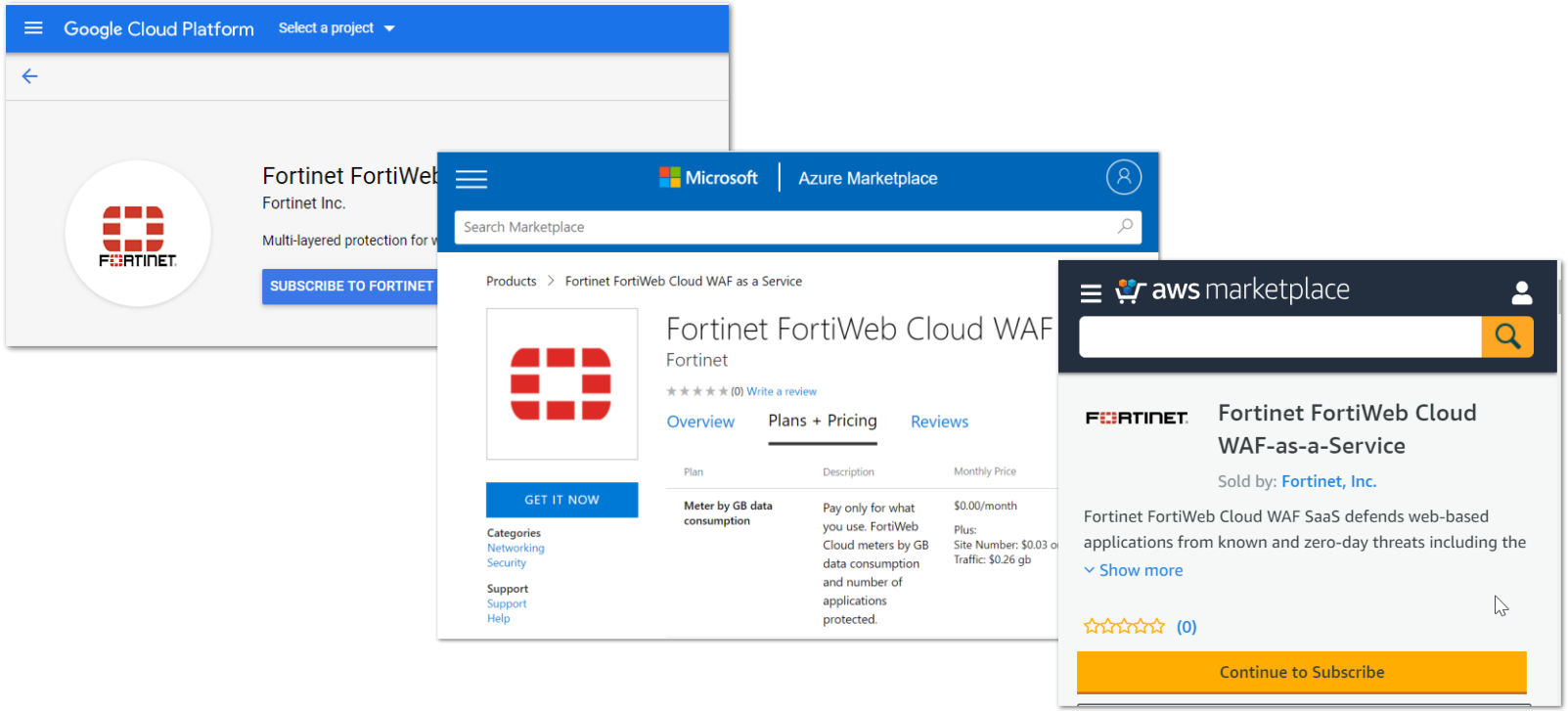
Scripting



https://docs.fortinet.com/document/fortiweb/7.0.2/script-reference-guide/104452/introduction

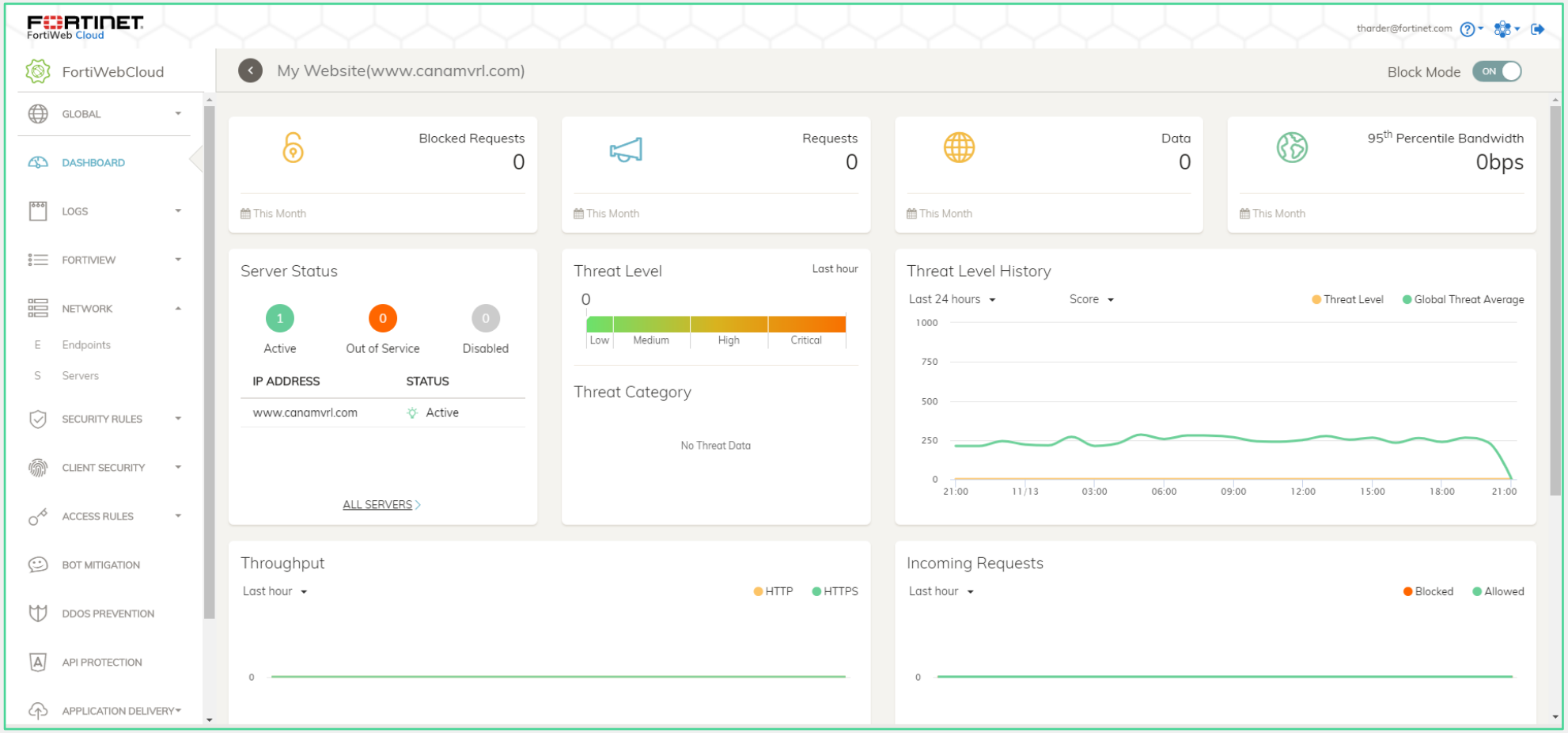
FortiWeb Cloud

- Доступний в AWS, Azure, GCP та OCI
- Придбання річного контракту або через public cloud marketplaces



- Підписка на основі споживання і кількості сайтів
- Підтримка CDN
- Блокування загроз з Machine Learning
- Layer 7 DDoS захист
- FortiGuard antivirus, IP reputation, FortiSandbox Cloud, Credential Stuffing Defense, та WAF сигнатури
- Захист HTTP/2 WAF
- REST API
- Розширене зменешення false positive
- Вдосконалене виявлення SQLi
- API Discovery
- API Protection

Інтерфейс FortiWeb Cloud WAF-as-a-Service



Налаштування DNS для FortiWeb-Cloud

Manual DNS verification – FQDN-level

$ dig www.domain.com. any

```
; <<>> DiG 9.10.6 <<>> www.domain.com. any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23067
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.domain.com.                IN      ANY

;; ANSWER SECTION:
www.domain.com.         38400   IN      CNAME   www.domain.76016.fortiwebcloud.net.

;; Query time: 1 msec
;; SERVER: 192.168.254.7#53(192.168.254.7)
;; WHEN: Mon Mar 21 15:52:01 CET 2022
;; MSG SIZE  rcvd: 97
```

Підписки

Marketplace (Self-Service)

Fortinet FortiWeb Cloud WAF-as-a-Service	
Units	**Cost**
Hourly charge per web application protected by FortiWeb Cloud	$0.03 / unit
Total data transferred via FortiWeb Cloud (GB)	$0.4 / unit

Price + payment options	Billing term
$0.00/one-time payment Plus: Traffic: $0.40 gb Site Number: $0.03 one web site	1-month

Data Transferred	USD 0.40 /gibibyte
Web Application Protection	USD 0.03 /hour

Annual Subscription SKUs

SKU	Description
FC1-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service—20Mbps average throughput—Annual Subscription. Select number of sites separately
FC2-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service—50Mbps average throughput—Annual Subscription. Select number of sites separately
FC1-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service—Additional 1 web site—Annual Subscription
FC2-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service—Additional 5 web sites—Annual Subscription

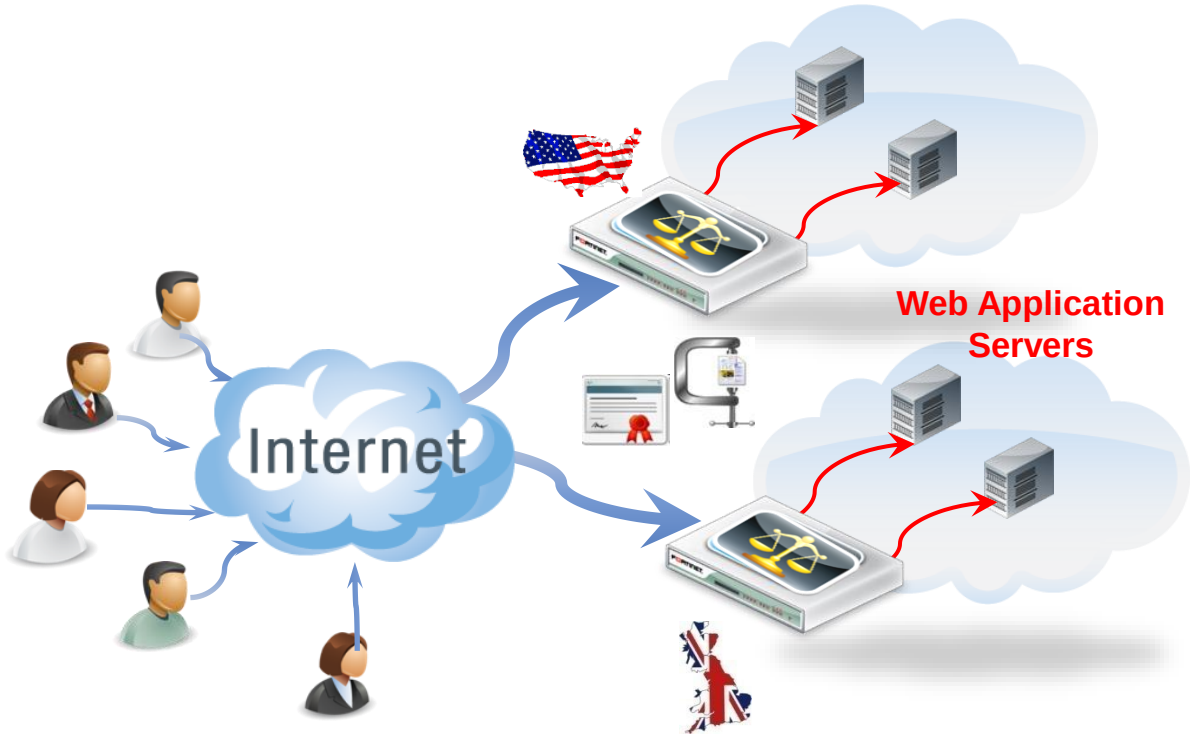
FortiADC

FortiADC

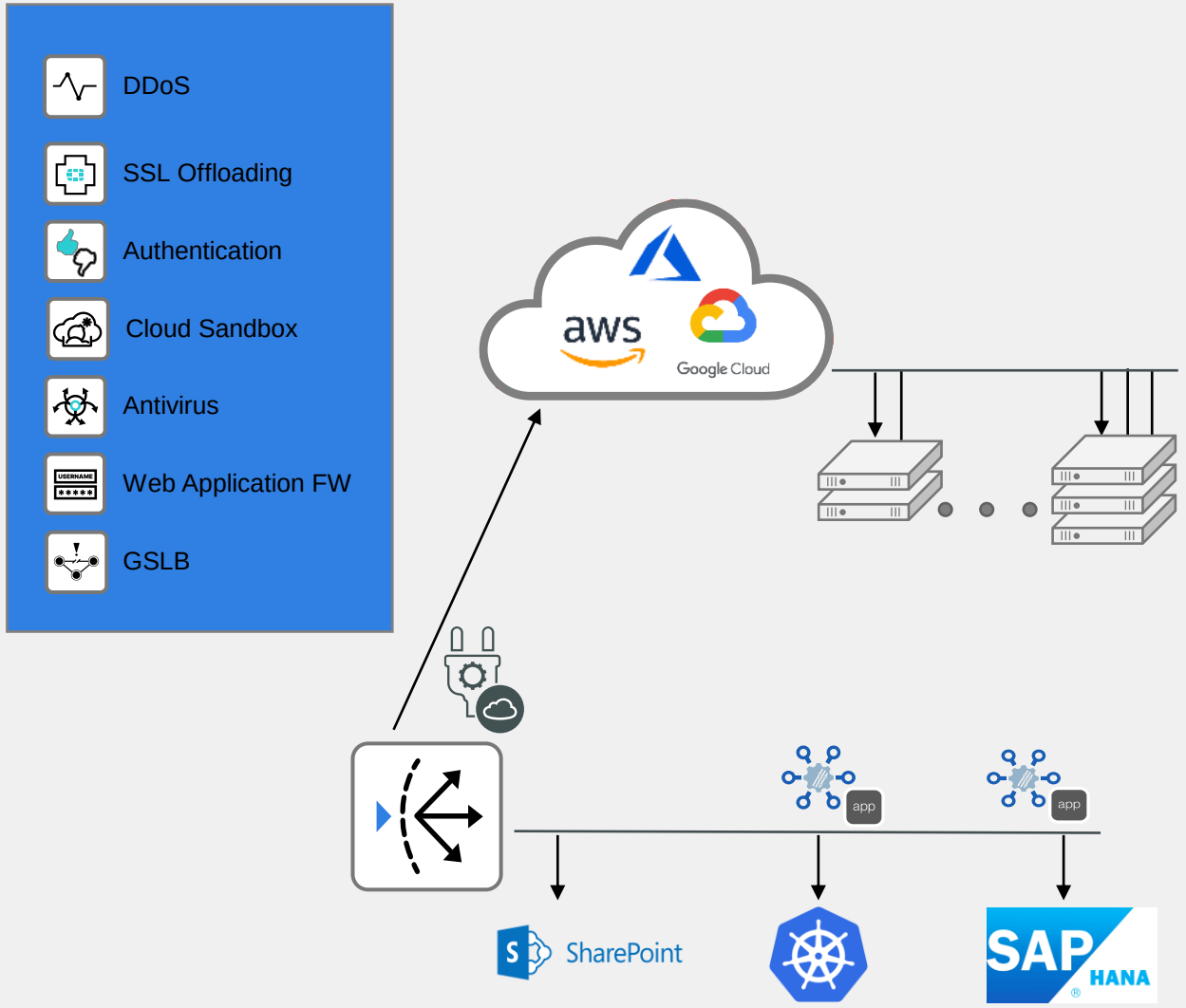
Appliance | Virtual Machine | Cloud

Розширений ADC, який забезпечує доступність додатків, їх безпеку та оптимізацію додатків.

- Розширене балансування навантаження додатків та глобальний LB
- Web Application Protection для OWASP Top 10 attacks (WAF)
- SSL inspection, offloading і видимість з апаратними рішеннями
- Автоматизація та Fabric connectors для інтеграції з іншими рішеннями
- Автентифікація користувачів та авторизація доступу
- Видимість додатків та трафіку



Масштабування та покращення додатків



1. Масштабування та покращення додатків

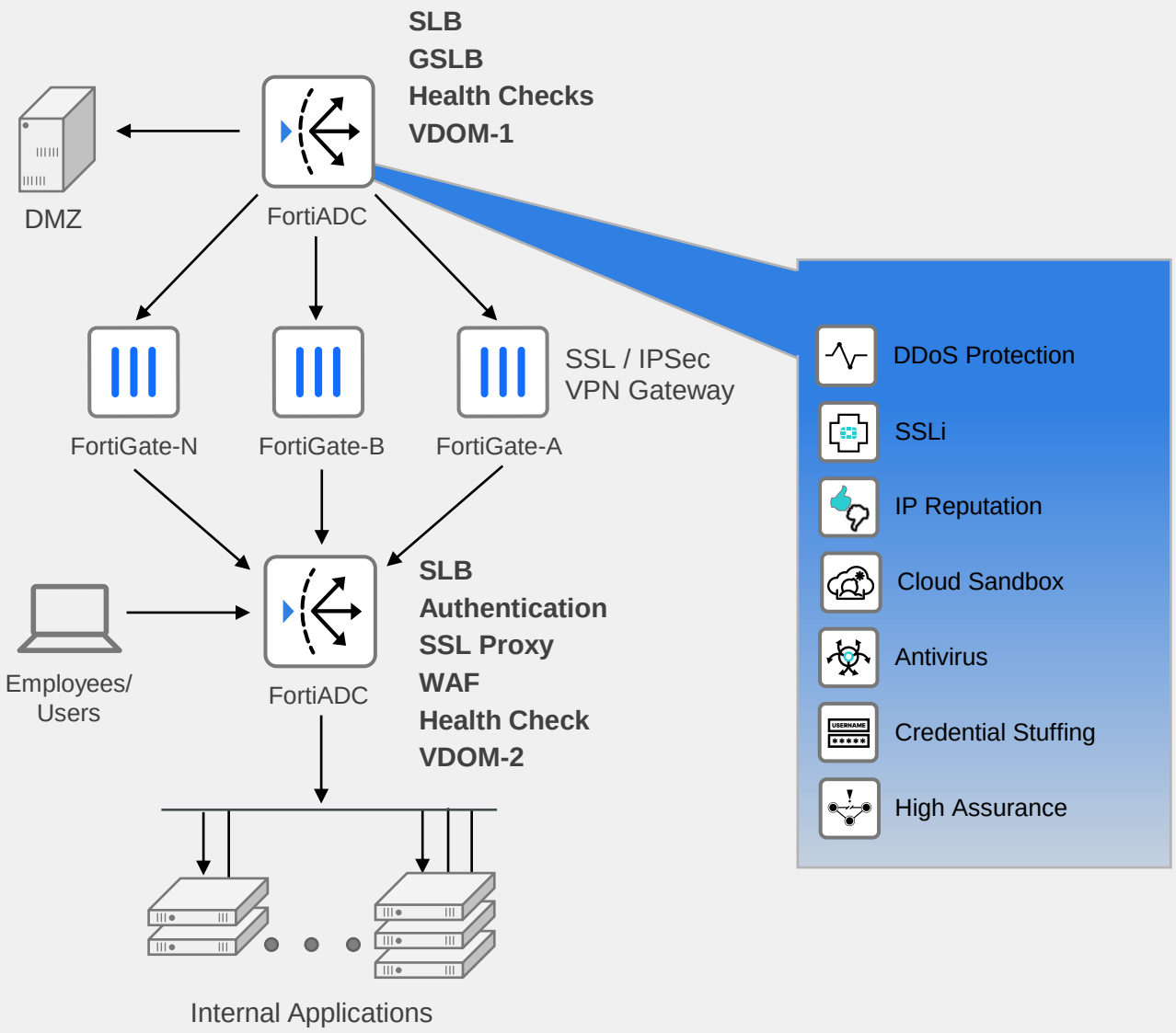
Балансування трафіку додатків локально або глобально, для підвищення продуктивності і доступності.

Покращення досвіду користувачів через забезпечення доступності додатків

Пріоритезація та оптимізація трафіку :

- Балансування та прискорення трафіку
- L7 правила для – HTTP, FTP, RDP, RADIUS, DIAMETER, SIP, SMTP, RTMP, ISO8583, RTSP, MySQL, MSSQL,
- Автоматичне перемикання для серверів або локацій при відмовах
- Розвантаження SSL
- DDoS, WAF, Sandboxing та інші служби безпеки

Прискорення безпеки



2. Прискорення безпеки

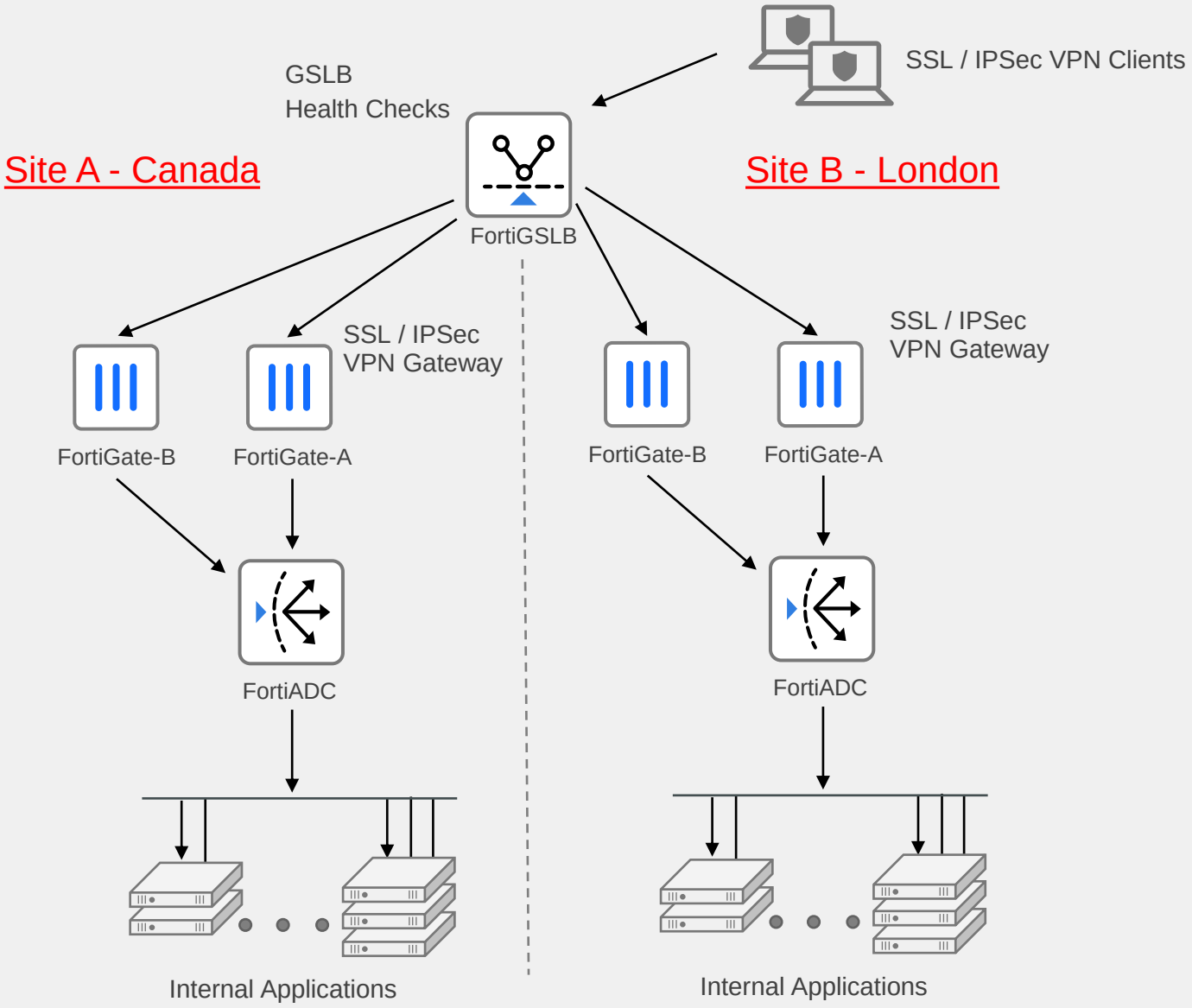
Підвищення продуктивності і доступності FortiGates за допомогою розвантаження SSL, попередньої фільтрації безпеки та балансування навантаження.

Балансування трафіку між пристроями, розвантаження SSL і балансування навантаження

Прискорення ключового функціоналу:

- Масштабування FortiGates
- SSL Offload
- A/A HA для FortiGates
- Додаткова безпека
  - WAF
  - DDoS Protection

VPN Accelerator



3. Масштабування VPN Gateways

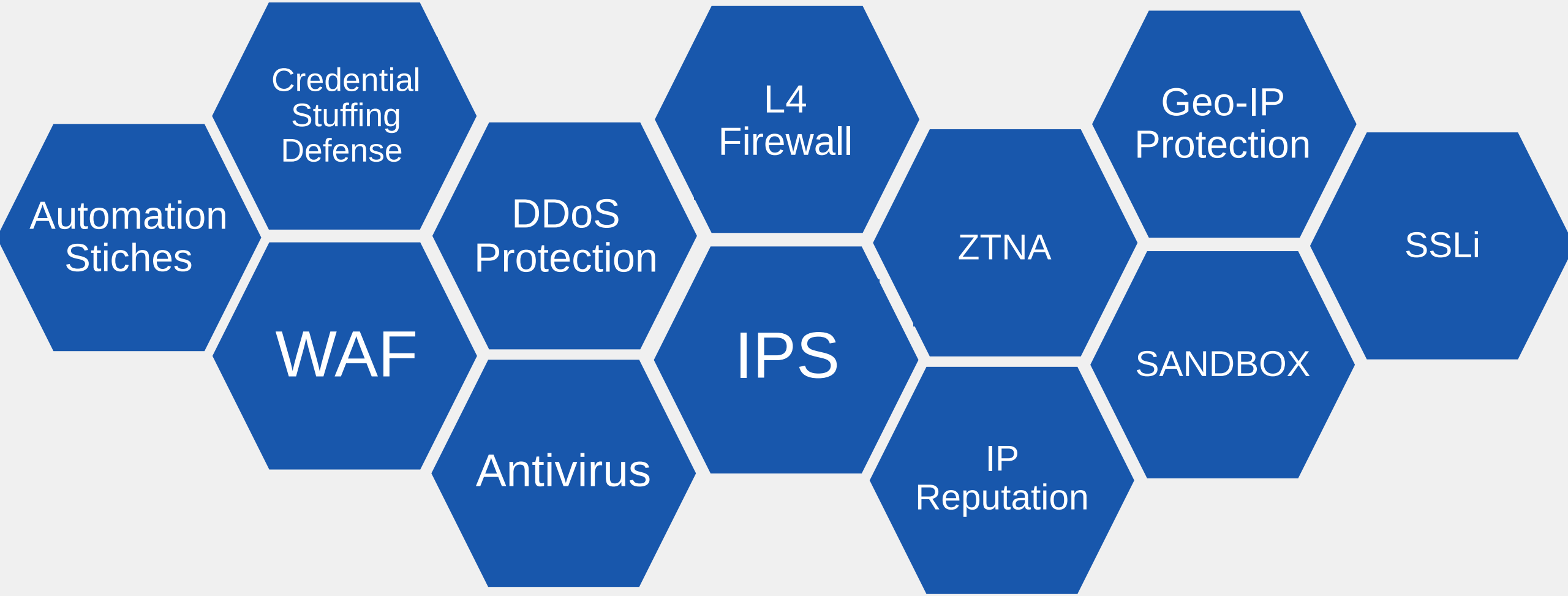
Направляйте клієнтів VPN на оптимальний шлюз VPN, відстежуючи працездатність FortiGate.

Покращуйте роботу клієнтів, гарантуючи, що трафік VPN слідує за найкращим доступним шляхом

Оптимізація продуктивності VPN:

- Збільшення продуктивності VPN
- Покращення досвіду користувачів
- Збільшення доступності VPN
- Масштабування FortiGates
- "Always On" VPN

Функціонал безпеки в FortiADC



Web Application Firewall

OWASP Top 10 Protection

SQLi/XSS Protection, Web Scraping, Brute Force, Web Defacement, CSRF Protection

Web Vulnerability Scanner

Security Fabric Integration

FortiSandbox & FortiGate

Web Attack Signatures

Protocol Validation

HTTP/S, URL Protection

Input Validation

File Restriction, Hidden Files

API Protection

API Gateway, XML, JSON and SOAP validation. OpenAPI validation

Sensitive Data Protection

Cookie Security, DLP

Bot Detection

FortiADC HW

FortiADC	FAD 120F	FAD 220F	FAD 300F	FAD 400F	FAD 1200F	FAD 2200F	FAD 4200F	FAD 5000F
L4 Throughput	3 Gbps	5 Gbps	8 Gbps	15 Gbps	40 Gbps	60 Gbps	100 Gbps	250 Gbps
L7 Throughput	2.2 Gbps	4 Gbps	6 Gbps	12 Gbps	30 Gbps	35 Gbps	80 Gbps	220 Gbps
L4 CPS	80,000	160,000	300,000	400,000	1 Million	1.2 Million	1.8 Million	4 Million
L4 HTTP RPS	230,000	500,000	1 Million	1.5 Million	3 Million	4 Million	5 Million	18 Million
L4 Concurrent Connection	4.5 Million	6 Million	12 Million	12 Million	36 Million	72 Million	144 Million	160 Million
SSL Bulk Encryption Throughput	500 Mbps	1.2 Gbps	3 Gbps	6 Gbps	20 Gbps	25 Gbps	50 Gbps	120 Gbps
Total Interfaces	6x GE RJ45	4x GE RJ45 4x GE SFP	4x GE RJ45 4x GE SFP	2x 10 GE SFP+, 4x GE SFP, 4x GE RJ45	8x 10 GE SFP+, 8x GE SFP, 8x GE RJ45	12x 10 GE SFP+, 8x GE SFP	4x 40 GE QSFP+, 8x 10GE SFP+	4x 100 GE QSFP28, 8x 40 GE QSFP
Power Supply	Single	Single	Single	Single (optional Dual)	Dual	Dual	Dual	Dual

FortiADC VM

FortiADC	FAD-VM01	FAD-VM02	FAD-VM04	FAD-VM08	FAD-VM16	FAD-VM32
L4 Throughput	1 Gbps	2 Gbps	4 Gbps	10 Gbps	16 Gbps	24 Gbps
VDOM	10	10	10	10	15	20
vCPU support (Max)	1	2	4	8	16	32
Memory support (Min/Max)	4 GB / Unlimited	4 GB / Unlimited	8 GB / Unlimited	16 GB / Unlimited	32 GB / Unlimited	64 GB / Unlimited

Максимальні значення параметрів в конфігурації

https://docs.fortinet.com/document/fortiadc/7.2.1/handbook/894761/appendix-d-maximum-configuration-values

Parameters	400D/400F/1000F/ 1200F/2000F/2200F	4000F/4200F/5000F
Virtual Servers with alone mode enabled	2048	4096
HW SSL Process Number with QAT SSL in polling mode	400F: 64 1200F/2200F: 192	4200F/5000F: 192
HW SSL Process Number with QAT SSL in epoll mode	400F: 16 1200F/2200F: 48	4200F/5000F: 48
HW SSL Process Number with Cavium SSL	400D/1000F/2000F: 30720	4000F: 61440

Maximum configuration values - hardware models when HW SSL acceleration is enabled

Parameters		VM01	VM02	VM04	VM08	VM16	VM32
System							
Administration	Administrative users	300	300	300	300	300	300
	Access profiles	8	16	64	64	64	64
	Virtual domains (VDOMs)	10	10	10	10	15	20
Certificate	Any configuration object	256	256	256	256	256	256
Shared Resources	Address	512	1024	2048	4096	4096	4096
	Address group	256	256	256	256	256	256
	Health checks	64	128	256	512	512	512
	ISP address book	32	32	32	32	32	32

Сервіси FortiGuard для FortiADC

SECURED BY FORTIGUARD®

WAF Security Service

- Application layer signatures
- Web Application signature to prevent any web attack

IP Reputation

- Protection for automated attacks and malicious sources
- DDoS, Phishing, Botnet, Spam, Anonymous proxies and infected sources

STANDARD BUNDLE

Antivirus and IPS

- Scan file uploads
- Regular and extended AV databases
- Protect the network against exploitable vulnerabilities

FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Subscription-based
- No separate sandbox required

Credential stuffing Defense

- Identifies login attempts using stolen credentials from numerous sources
- Automatic updates
- Prevents unwanted access and defends against data breaches

Web Filtering

- Manage SSL FP scanning exceptions
- Enable/disable SSL inspection by category
- Automatic updates

ADVANCED BUNDLE

FortiADC VM-S(підписка)

порівняння

FortiADC VM

- Аванс: дорого на початку
- Довгий строк : економія витрат

FortiADC VM-S

- Аванс : дешево на початку
- Довгий строк : дорожче

VM-01 Advanced Bundle

1st Year: ~$11 000

2nd Year: ~$3 900 (Advanced Bundle only)

3rd Year: ~$3 900 (Advanced Bundle only)

Total Cost: ~$18,800

4th Year: ~$3 900 (Advanced Bundle only)

Total Cost: ~$22,700

VMS-01 Advanced Bundle

1st Year: ~$5 900

2nd Year: ~$5 900

3rd Year: ~$5 900

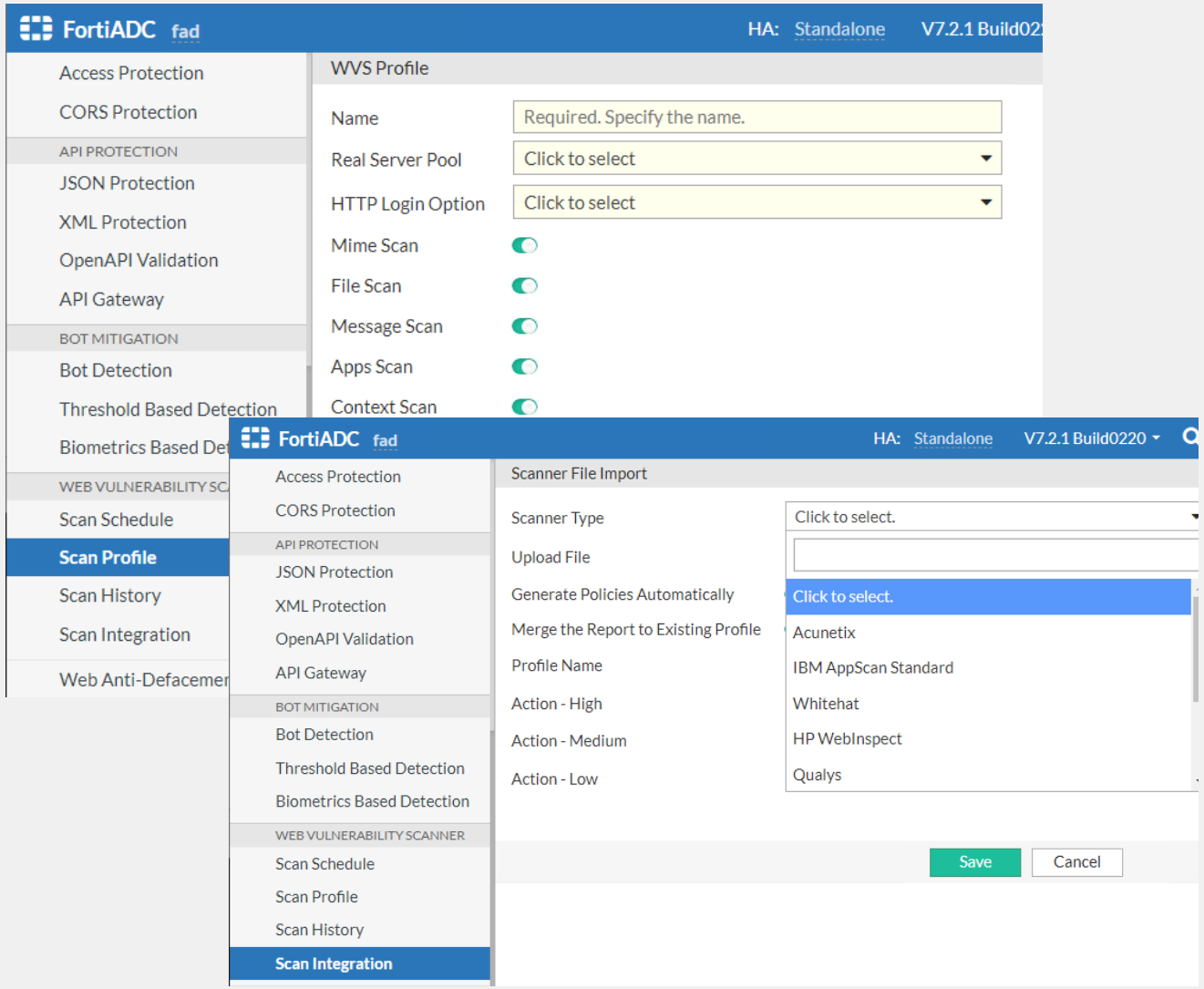
Total Cost: ~$17,700

4th Year: ~$5 900

Total Cost: ~$23,600

Сканування вразливостей

- Вбудований сканер вразливостей
- Підтримка сторонніх сканерів:
  - Acunetix
  - IBM AppScan Standard
  - WhiteHat
  - HP WebInspect
  - Qualys
  - Telefonica FAAST
  - ImmuniWeb
- Генерування профілю захисту за результатами сканування

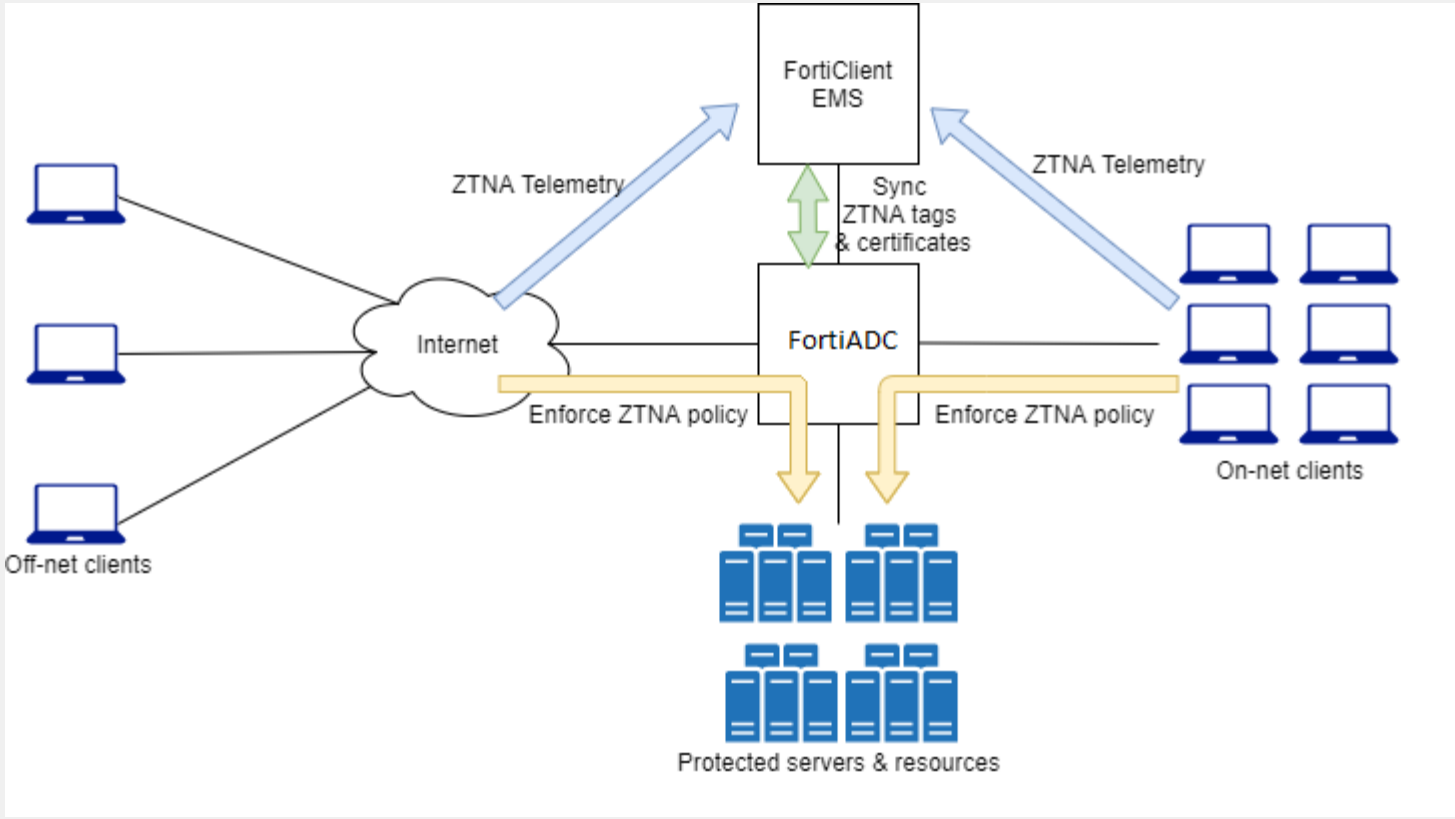


https://docs.fortinet.com/document/fortiadc/7.2.1/handbook/99930/web-vulnerability-scanner

https://docs.fortinet.com/document/fortiadc/7.2.1/handbook/397993/scan-integration

ZTNA

- Перевірка стану клієнта через FortiCleint ZTNA
- Обмеження доступу за результатами перевірки



https://docs.fortinet.com/document/fortiadc/7.2.1/handbook/155485/zero-trust-network-access-ztna

FortiGSLB

FortiGSLB Cloud

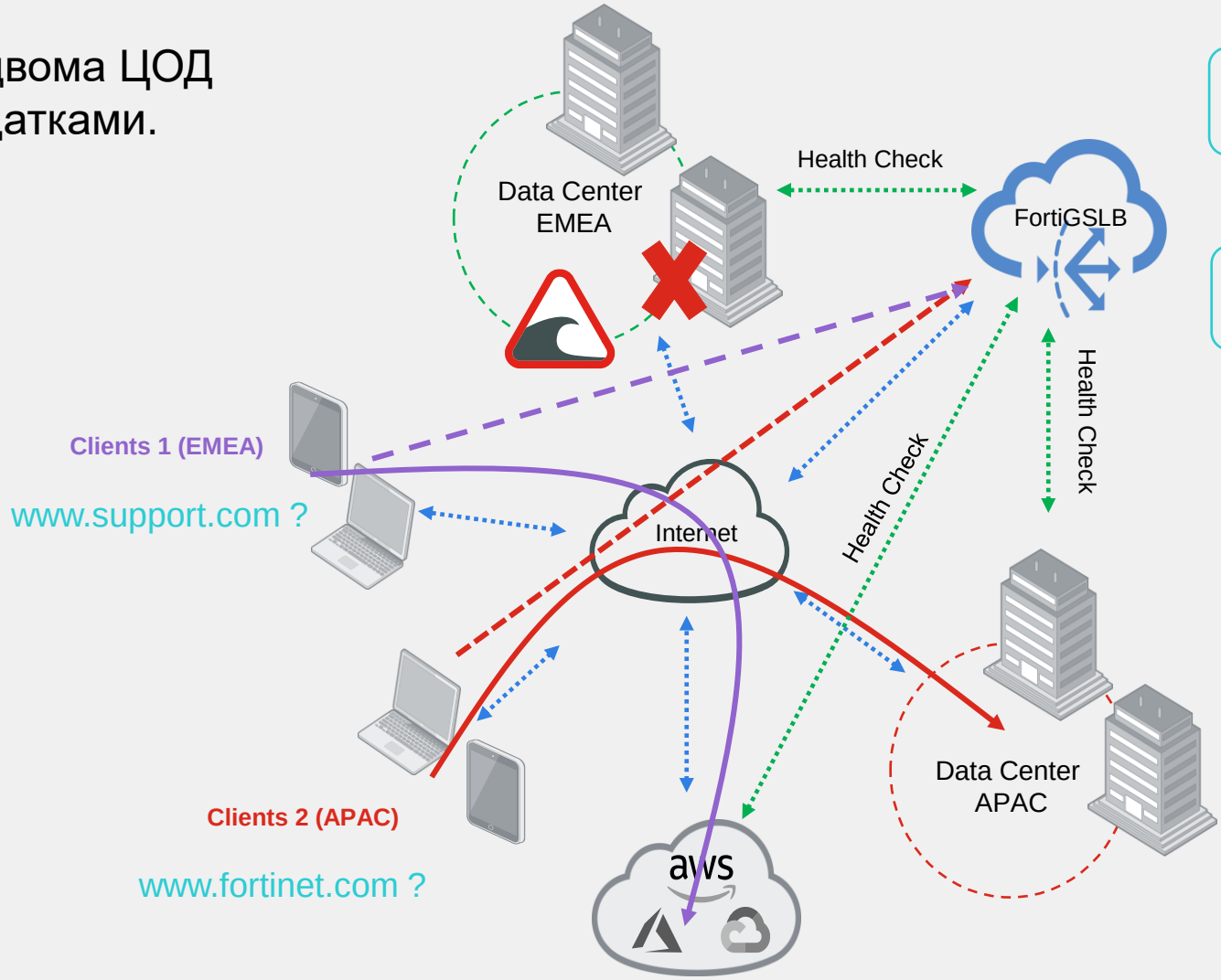
Cloud

Допомагає підтримувати бізнес клієнтів онлайн, коли локальна мережа зазнає неочікуваних перевантажень або простоїв.

- **Відмовостійкість кількох сайтів і безперервність сервісів**
  - **Доступність** послуги під час та після відмови
  - **Масштабування** послуги, коли додатки працюють повільно
- **Переваги**
  - Швидке відновлення (міграція/налаштування не потрібні)
  - Просте розгортання та перевірені варіанти використання
  - Видимість сайту
  - Покращення продуктивності сайту та часу відповіді
  - Повноцінна служба DNS
  - Масштабована ліцензія
  - Інтеграція з Fortinet Security Fabric

Як працює

Приклад: замовник з двома ЦОД (A/A) та хмарними додатками.



FQDN: www.fortinet.com

Client2 = APAC DC & AWS
Client1 = EMEA DC & Azure

FQDN: www.support.com

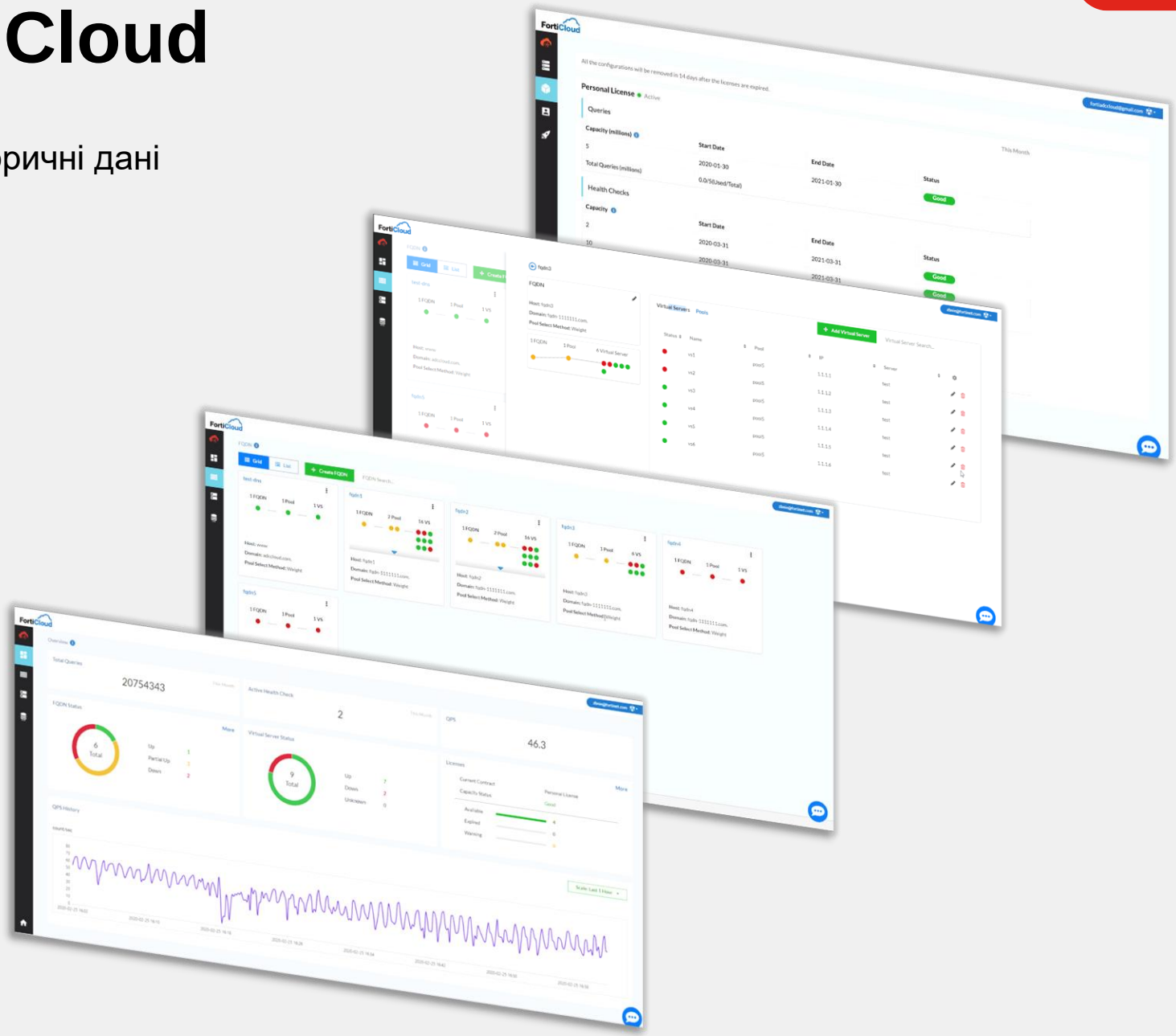
Client1 = EMEA DC & Azure
Client2 = APAC DC & AWS

Інтерфейс FortiGSLB Cloud

Забезпечує моніторинг у реальному часі та історичні дані трафіку DNS

Керування:

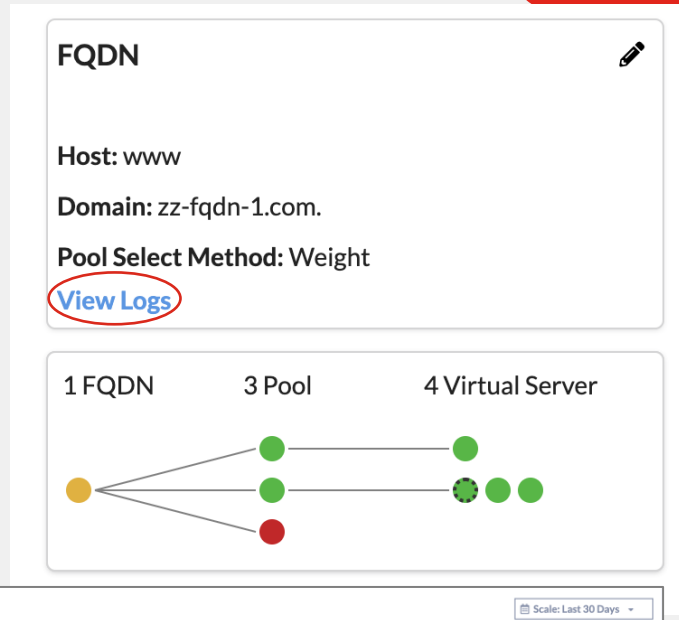
- Швидке додавання сайтів
- Multiple Organization - MSP
- Просте налаштування через WebUI
- Моніторинг і прогнозування ліцензій
- Журнал подій
- Central view
- Моніторинг та звіти для сайтів
- Історія і статистика DNS
- Інтегрована Geo-IP DB



Журнали

Audit/Event :

- Event/audit logs до 1 року
- Оповіщення
- Фільтри по user/message/type/status
- Журнали по:
  - Зміна налаштувань
  - Health Check
  - License capacity
  - License expiration
  - Журнали по FQDN



Приклад-1: FortiGSLB з FortiGate (SSL/IPsec VPN LB)

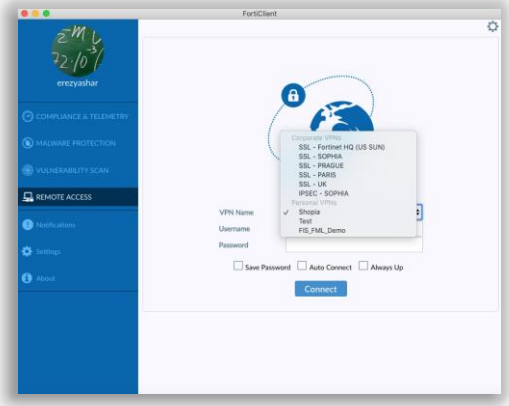
Приклад: Висока продуктивність SSL/IPsec VPN для дистанційних працівників і доступність послуг

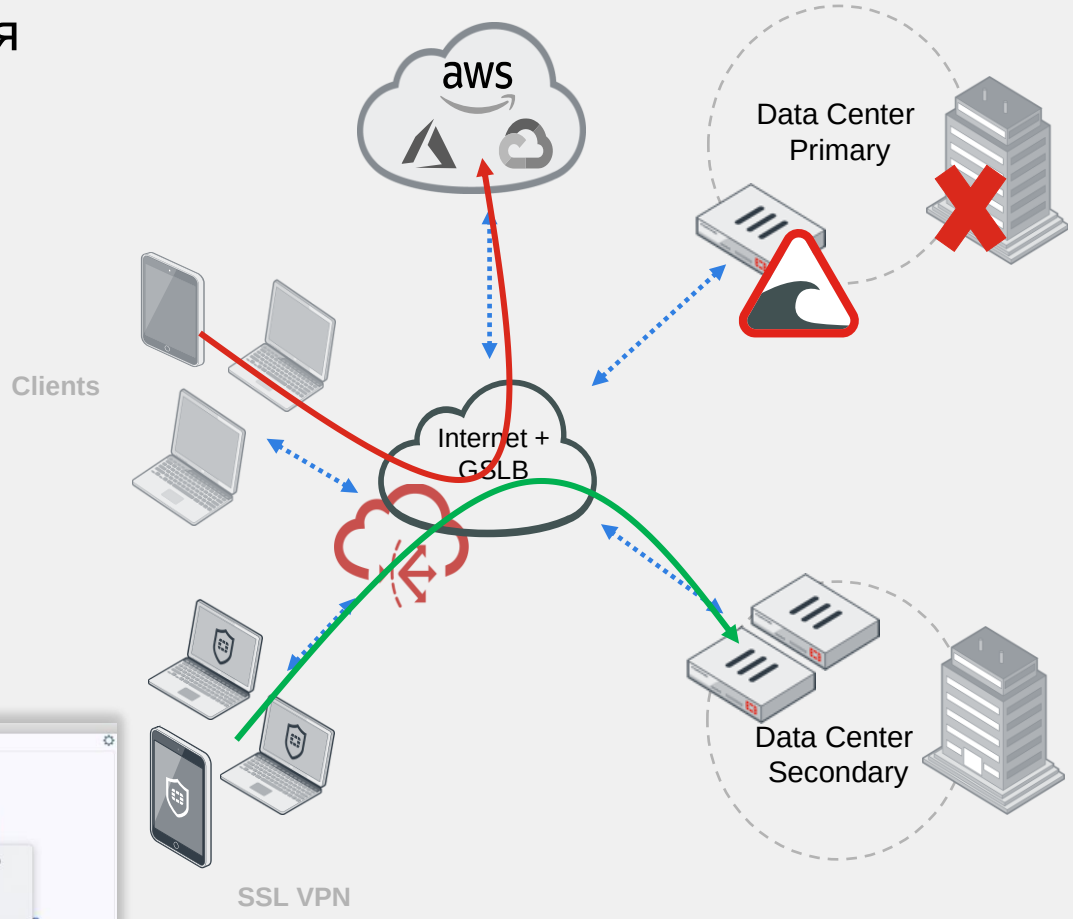
Бізнес драйвери :

- Гнучкість і зниження TCO
- Безперервність бізнесу
- “Always ON” безпека

Ключові переваги для клієнтів :

- Покращена безпека
- Покращення досвіду користувача
- Безперервність сервісу





Приклад-2: FortiGSLB з SD-WAN (Inbound Link LB)

Приклад: True Multihoming

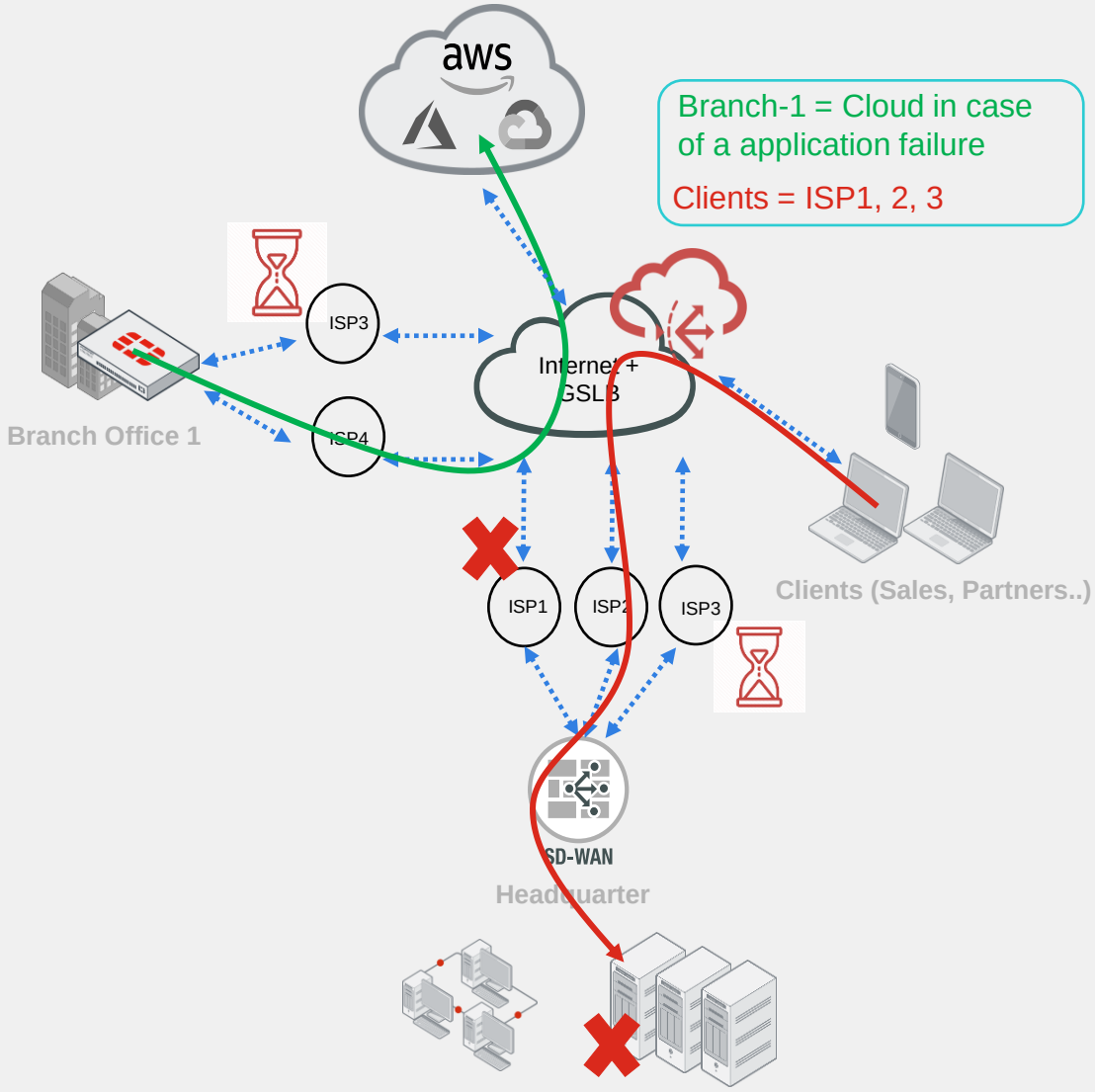
- Inbound Link LB для клієнтів
- Доступність сервісу для Branch office

Бізнес драйвери :

- Покращення продуктивності
- Безперервність бізнесу
- Гнучкість і зниження TCO

Ключові переваги для клієнтів:

- Підвищення ефективності
- WAN Optimization
- Покращення досвіду користувача
- Безперервність сервісу



Приклад-3: FortiGSLB with FortiADC/FortiWeb

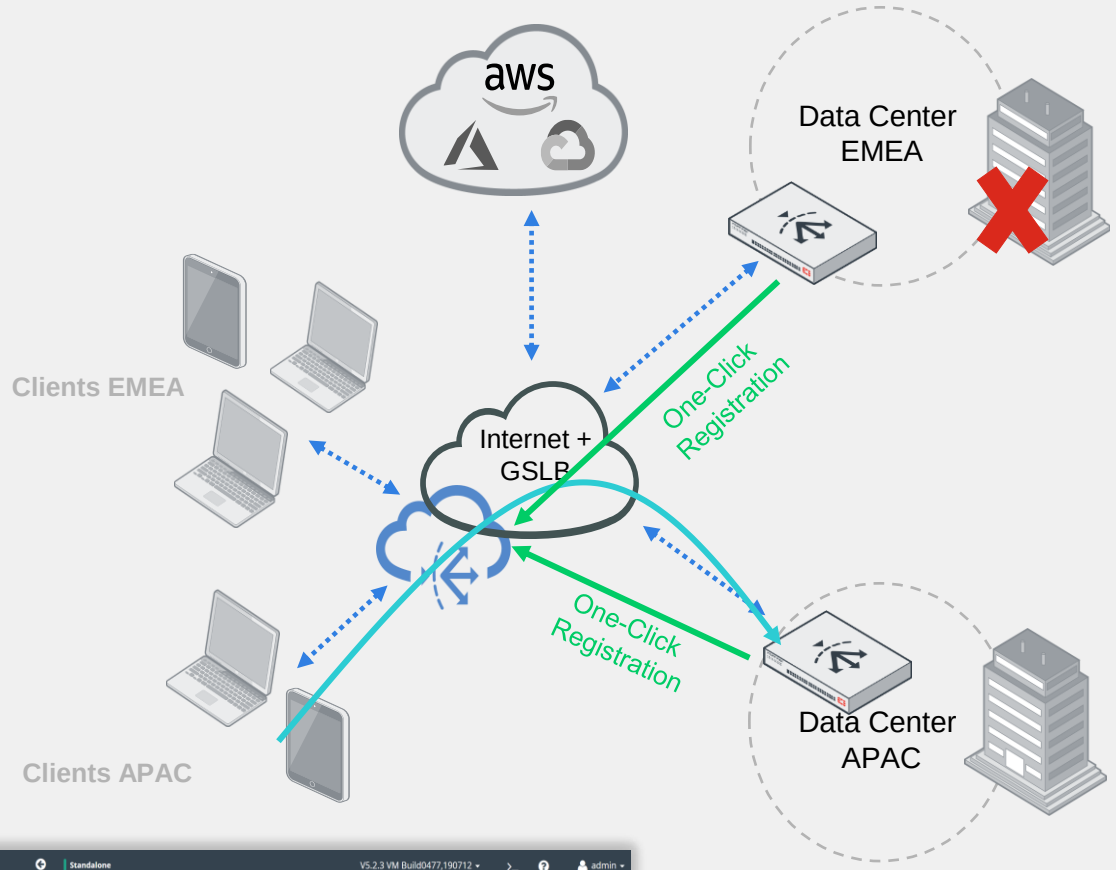
Приклад: Балансування навантаження між кількома ЦОД відповідно до завантаження/стану сервера, Geo-IP і затримки

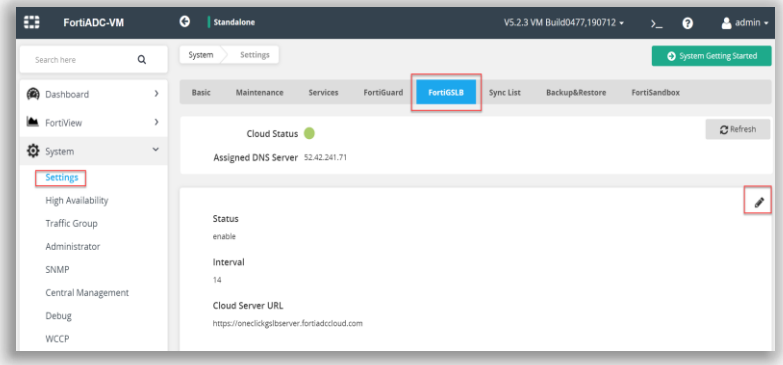
Business Drivers:

- Гнучкість і зниження TCO
- Безперервність бізнесу (active/active)

Ключові переваги для клієнтів :

- FortiADC “One-Click-GSLB” конектор
- Покращення досвіду користувача
- Безперервність сервісу
- Multi-site видимість
- LB в залежності від Geo-IP, load, latency та доступності додатків





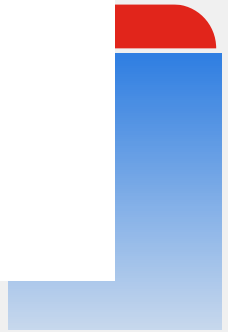
Ліцензування FortiGSLB

- Щорічні платежі по DNS QPS (Query Per Second) та Health Checks.
- Stackable License

SKU	Description
FC2-10-CGSLB-330-02-DD	FortiGSLB Cloud Service - **100 DNS QPS** (queries per second) - Annual Subscription. Includes 24x7 FortiCare. Add Health Checks separately
FC3-10-CGSLB-330-02-DD	FortiGSLB Cloud Service - **500 DNS QPS** (queries per second) - Annual Subscription. Includes 24x7 FortiCare. Select Health Checks separately
FC4-10-CGSLB-330-02-DD	FortiGSLB Cloud Service – **1,000 DNS QPS** (queries per second) - Annual Subscription. Includes 24x7 FortiCare. Select Health Checks separately

SKU	Description
FC1-10-CGSLB-332-02-DD	FortiGSLB Cloud Service - **2 Advanced Health Checks**
FC2-10-CGSLB-332-02-DD	FortiGSLB Cloud Service - **10 Advanced Health Checks**
FC4-10-CGSLB-332-02-DD	FortiGSLB Cloud Service - **100 Advanced Health Checks**

FortiDDOS

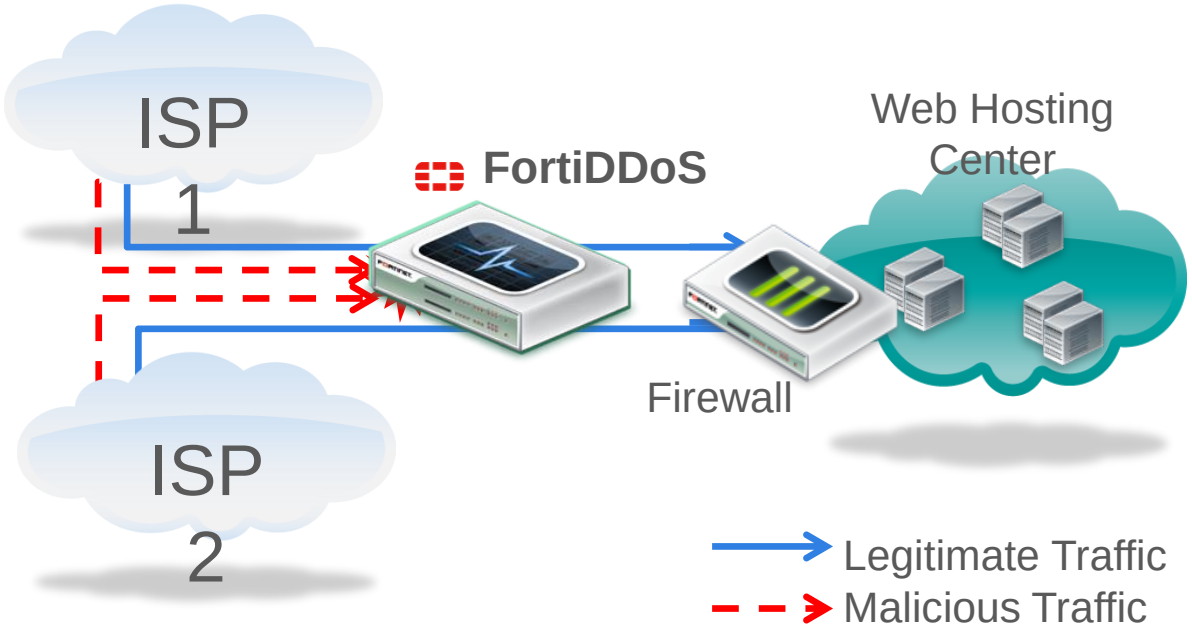


FortiDDoS

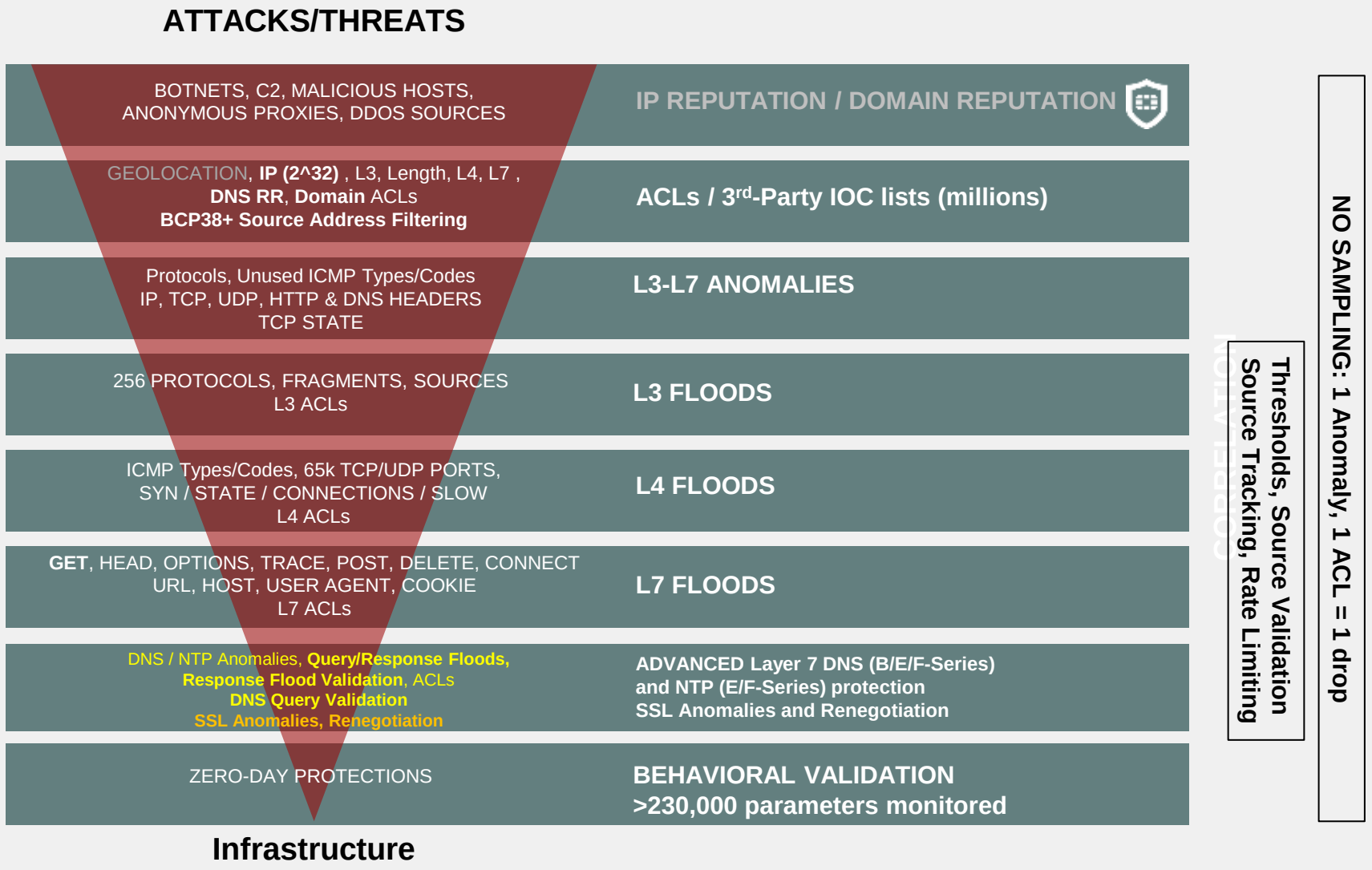
Appliance

Захист від DDoS з апаратним прискоренням

- (SPU)-based layer 3, 4, та 7 захист від DDoS
- Захист від DDoS на основі поведінки без потреби в сигнатурах
- Мінімальна кількість false positives завдяки безперервній оцінці загроз
- Можливість одночасного моніторингу величезної кількості параметрів
- Досконалий захист від bulk volumetric, layer 7 атак
- Захист від атак на DNS-сервіси за допомогою спеціалізованих засобів



Багаторівневий захист з FortiDDoS



FortiDDoS – просте налаштування в три кроки

Legitimate Users

Internet

WAN

FortiDDoS

LAN

FireWall

WEB
Service Protection Profile

Subnets
x.x.x.x/m

Multi Vectors
DDoS Attack

1000 PPS

x3= 3000 PPS= Adaptive Threshold

Drop ALL Zone

Source Tracking Zone

x2= 2000 PPS= Minimum Threshold

Allow ALL zone

Legitimate Traffic
Burst
➔ Allowed

DDoS Traffic
mitigated
➔ Attacks Drops

t

1. Learning Phase

if ☺?

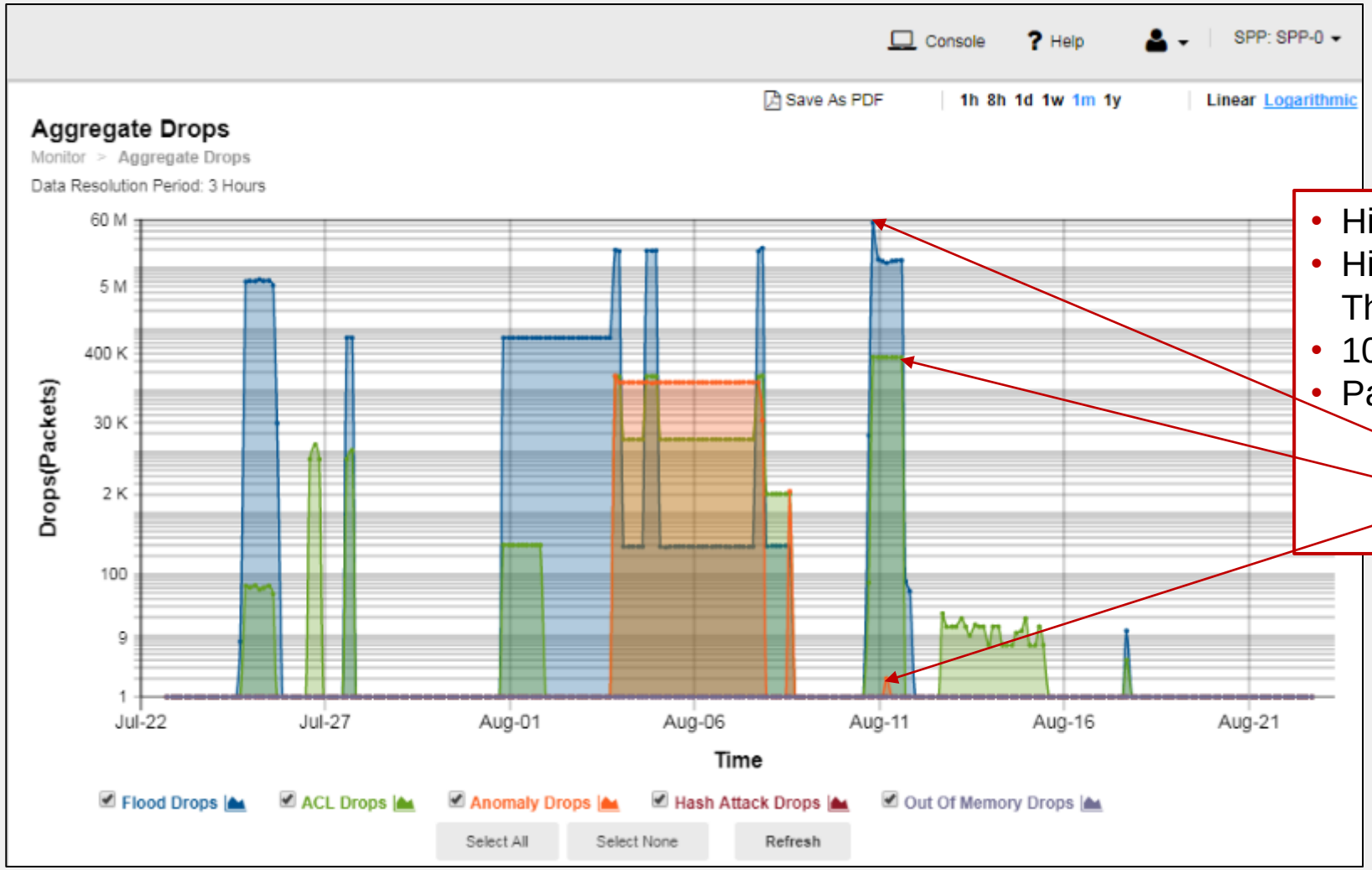
2. Detection Phase
(alerting only)

and ☺?

3. Prevention Phase
(alerting+blocking)

so ☺ NO TUNING

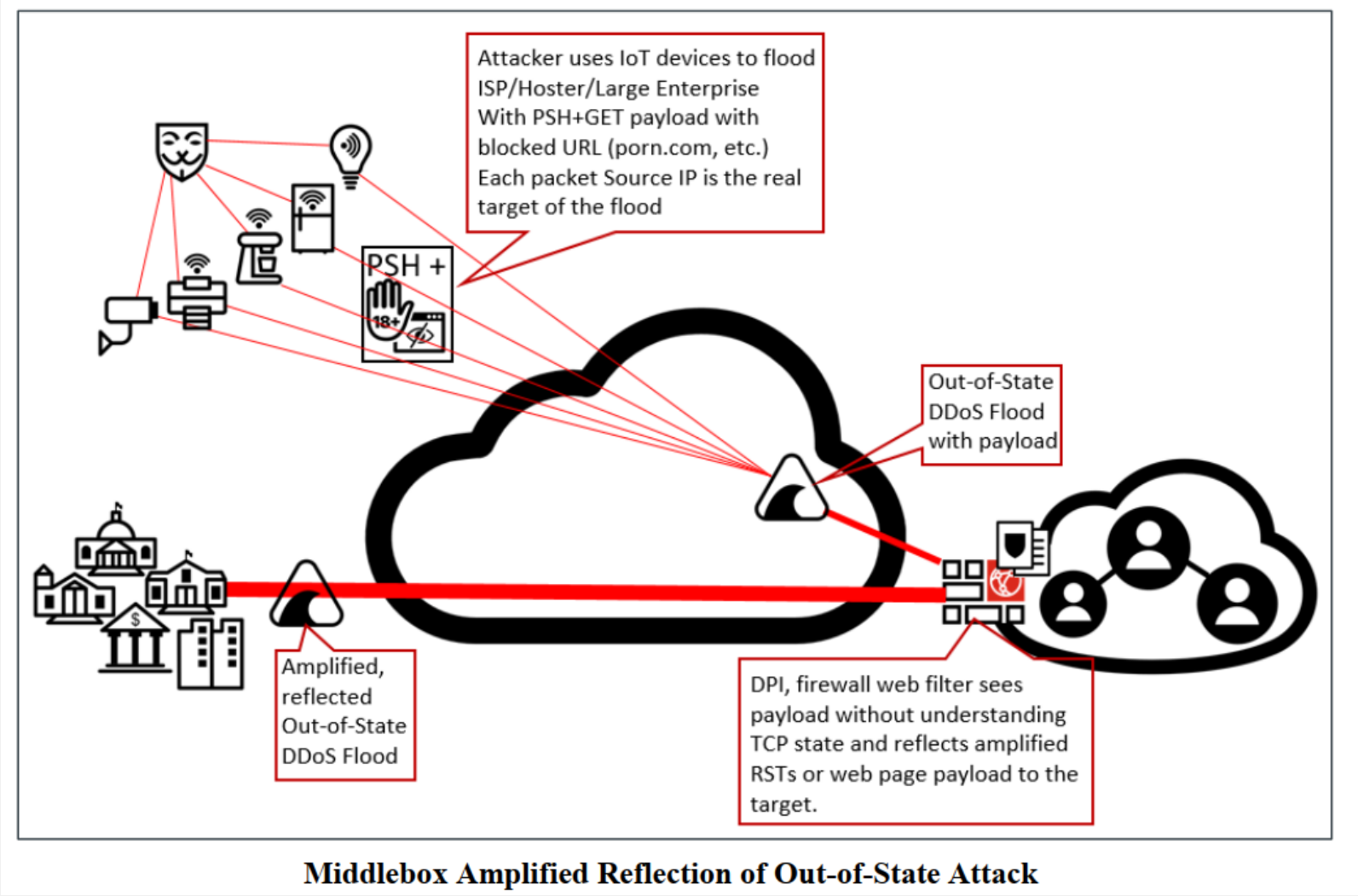
Детальна звітність



- High bps Throughput
- High Small-Packet (60Byte) pps Throughput
- 100% packet inspection
- Parallel Inspection/Mitigation:
  - 60M-packet Flood Drops
  - 400k-packet ACL Drops
  - 2-packet Anomaly Drops

FortiDDoS рахує кожне блокування і можемо бачити і 2, і 60M.
В цьому прикладі 60M drops = ~200k pps flood.

Middlebox TCP Reflection Amplification

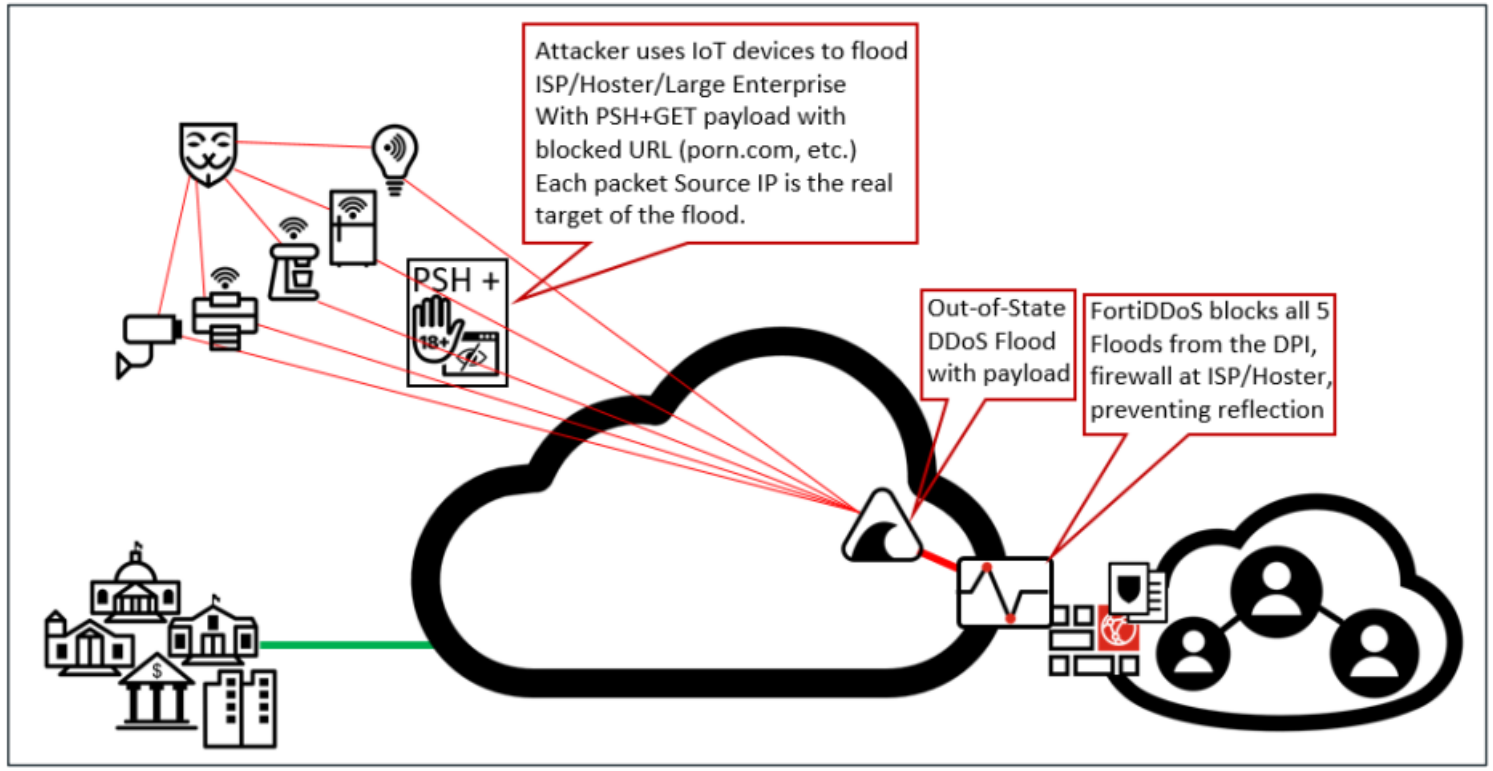


Middlebox Amplified Reflection of Out-of-State Attack

Захист від Middlebox TCP Reflection Amplification

На стороні рефлектора

- Пакет PSH як TCP Invalid Flag flood і блокується з першого пакета.
- Пакет PSH-ACK має дозволені flags але блокується з першого пакета з **Foreign Packet Validation** оскільки він не є частиною жодного з'єнання.
- Нема впливу на **легітимний трафік**.
- Захист інших виробників – більшість бачить PSH invalid flag і блокує цей пакет без впливу на інший трафік. Більшість не звертає уваги на **PSH-ACK**. В КРАЩОМУ випадку **можуть мати ACK Threshold** який детектуватиме PSH-ACK flood. Такий threshold **блокує BCI ACKs,** що має значний **негативний вплив** на інший TCP трафік.

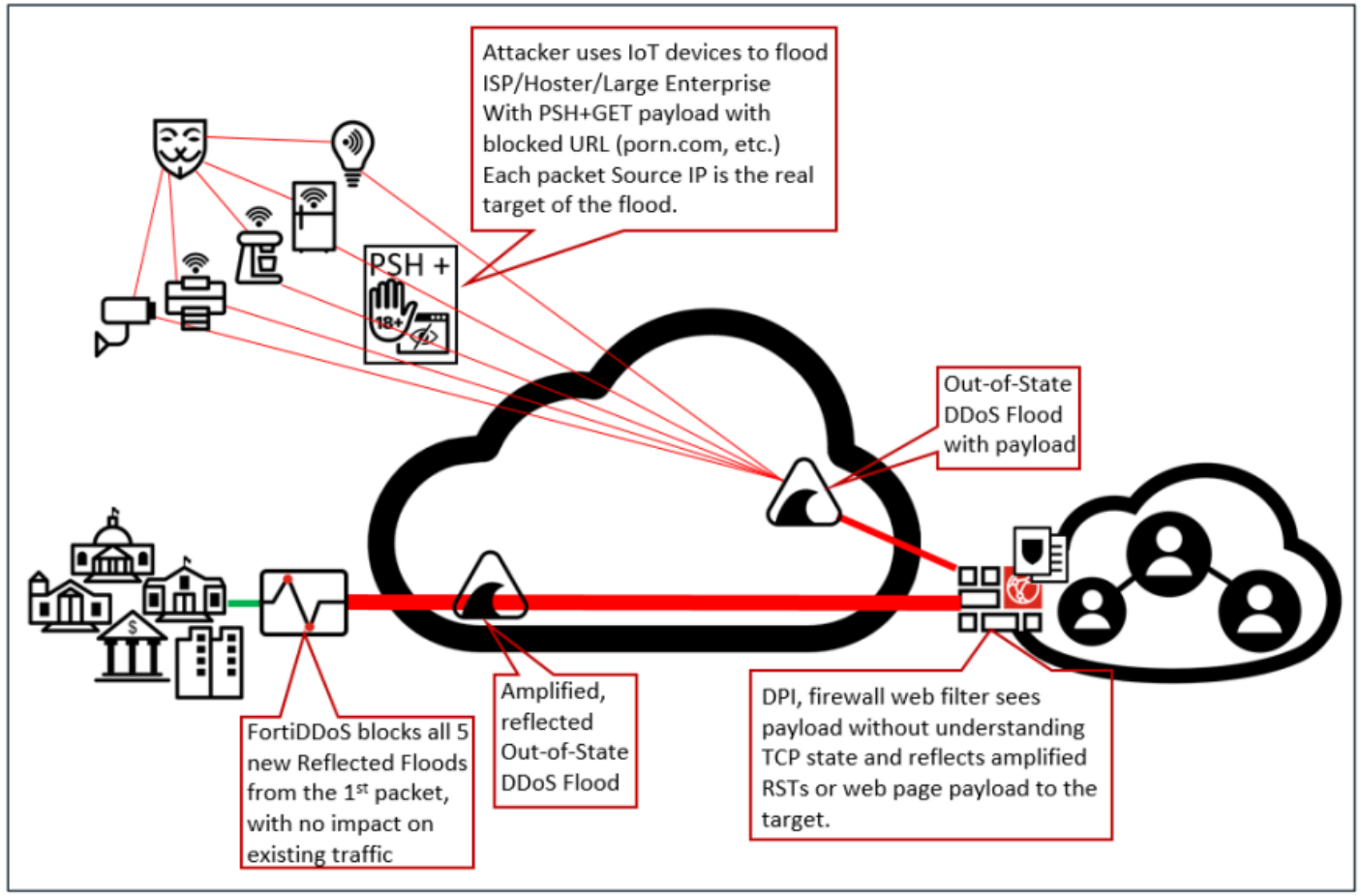


FortiDDoS Protection at the Reflector (ISP, Hoster, Large Enterprise Firewall)

Захист від Middlebox TCP Reflection Amplification

На стороні жертви

- Відбитий трафік може містити різні пакети RST, RST-ACK, PSH-FIN-ACK з payload.
- Дослідники* знайшли 12 основних типів відповідей але більш ніж 63,000 різних варіацій відповідей!
- FortiDDoS детектує всі out-of-state пакети через **Foreign Packet Validation** і **блокує з першого пакету**.
- Нема впливу на «користний» трафік.
- Захист від конкурентів буває різним. У більшості нема концепції Foreign Packet Validation. Вони **можуть мати RST, FIN чи ACK Thresholds** (аналіз заголовків від рефлекторів). Як і в попередньому прикладі - ACK threshold **значно впливає** на інший TCP трафік. Більшість провайдерів та рішень інших виробників **взагалі не побачать** такий тип атаки



FortiDDoS Protection at the target (School, Gov't, Finance, Health-Care, Enterprise, etc.)

* https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf

FortiDDoS HW

	FDD-200F	FDD-1500E/-DC	FDD-1500F	FDD-2000E/-DC	FDD-2000F
Throughput (Full Duplex)	8 Gbps	35 Gbps	30 Gbps	70 Gbps	76 Gbps
Simultaneous Connections	4.2 Mil	12 Mil	16.7 Mil	25 Mil	33 Mil
Session Setup/ Teardown	375,000 /s	>1.5M /s	700,000 /s	>3 Mil /s	920,000 /s
Latency	< 50 µs	< 50 µs	< 50 µs	< 50 µs	< 50 µs
Interfaces	8 LAN/WAN Interfaces (Copper/SFP)	16x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 100GE QSFP28	4x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 10GE SFP/+	16x LAN & WAN 10GE SFP/+, 4 LAN & WAN bypass 100GE QSFP28	4x LAN & WAN 10GE SFP+, 4x LAN & WAN 40GE QSFP+
HW acceleration		3x TP3		6x TP3	

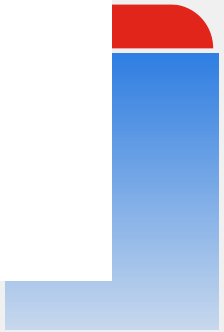
FortiDDoS VM

	FDD-VM04	FDD-VM08	FDD-VM16
Hypervisor Support	VMware ESX/ESXi 6.x / 7.x with hardware-assisted virtualization (VT) enabled in the BIOS		
Throughput (Full Duplex)	3 Gbps	5 Gbps	10 Gbps
Session Setup/ Teardown	375,000 /s	>1.5M /s	700,000 /s
Service Protection Profiles	4	8	16
vCPU	4	8	16
Network Interface Support	8 (4 bridged port-pairs). Interface speeds dependent on hardware.		

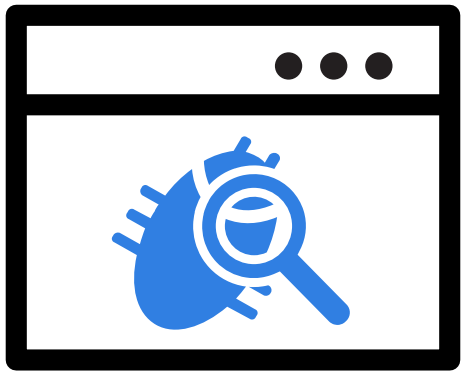
Ліцензування

Dedicated DDoS Appliances	FDD-200F	Supports up 1G
	FDD-1500F	Supports up to 10G
	FDD-1500E	Supports up to 40G
	FDD-2000E	Supports up to 100G
DDoS Virtual Machines (VMs)	FDD-VM04	4 xCPU variant of FortiDDoS VM
	FDD-VM08	8 xCPU variant of FortiDDoS VM
	FDD-VM16	16 xCPU variant of FortiDDoS VM
Add-ons: Add on licenses to enhance the FortiDDoS Protection Solution.	FC-10-FIM04-140-02-DD	IP Reputation Service: Database of malicious source IP addresses from the FortiGuard distributed network of threat sensors, which FortiDDoS uploads daily. (Normally recommended for Hosters/MSSPs/ISPs only)
	FC-10-FIM04-191-02-DD	Domain Reputation Service: Database of known malicious fully qualified domain names from the FortiGuard network of threat sensors, which FortiDDoS uploads daily. (Normally recommended for Hosters/MSSPs/ISPs only)
	FDD-CM-BASE/FDD-CM-UL	The FortiDDoS Central Manager VM manages multiple FortiDDoS **E-Series** appliances with shared management attributes. BASE: Manages 1- 10 appliances UL: Manages 1- Unlimited appliances

FortiDAST



FortiDAST



Black-box сканування вразливостей

Cloud-based

On-premise

Proxy

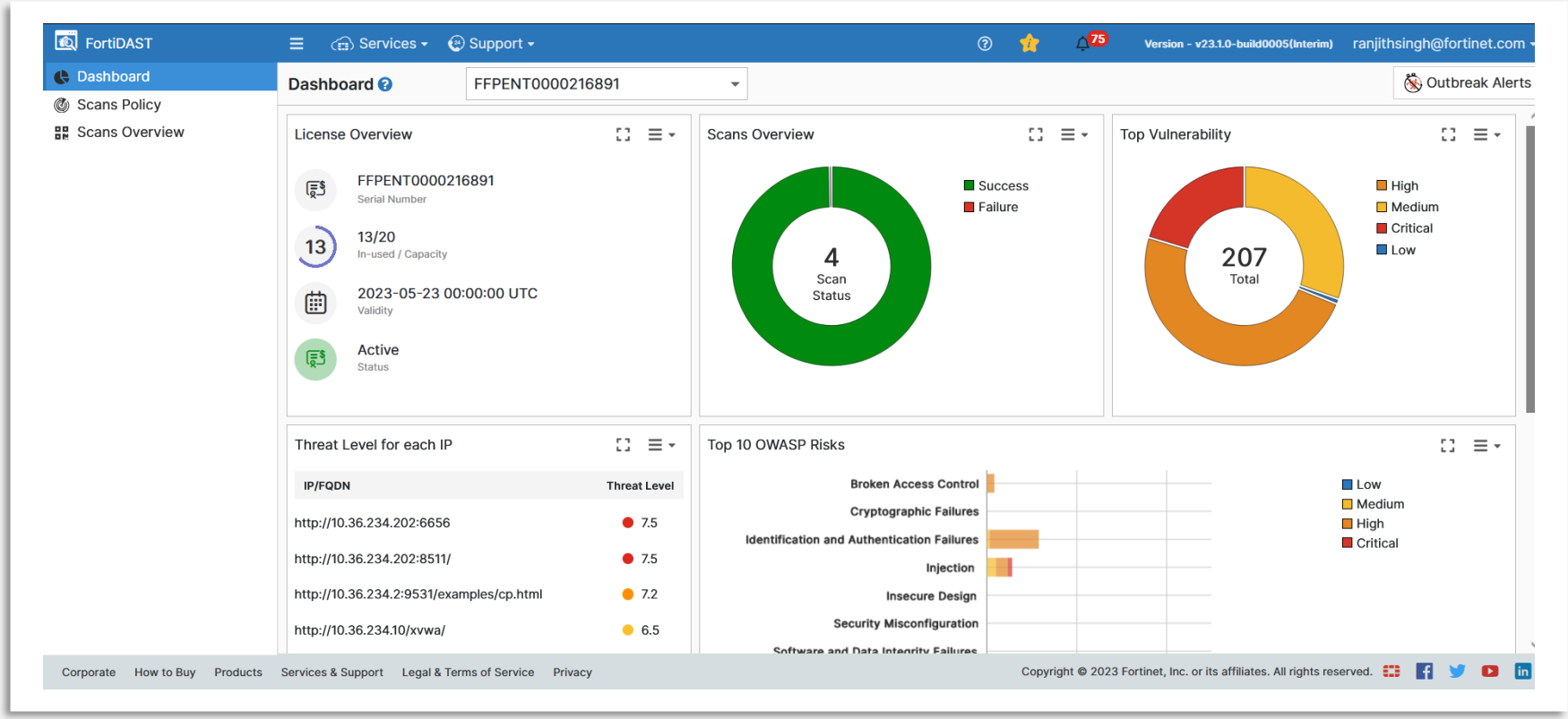
- Автоматизоване Vulnerability Scanning
- Сигнатури з FortiGuard Labs
- Advanced Crawler
- Fuzzer
- Детальна звітність

Автоматизоване сканування на вразливості

Автоматизація

Автоматичне сканування налаштованих IP чи FQDN

- Розклад сканувань для уникнення впливу на бізнес процеси
- Налаштування тригерів для запуску сканувань

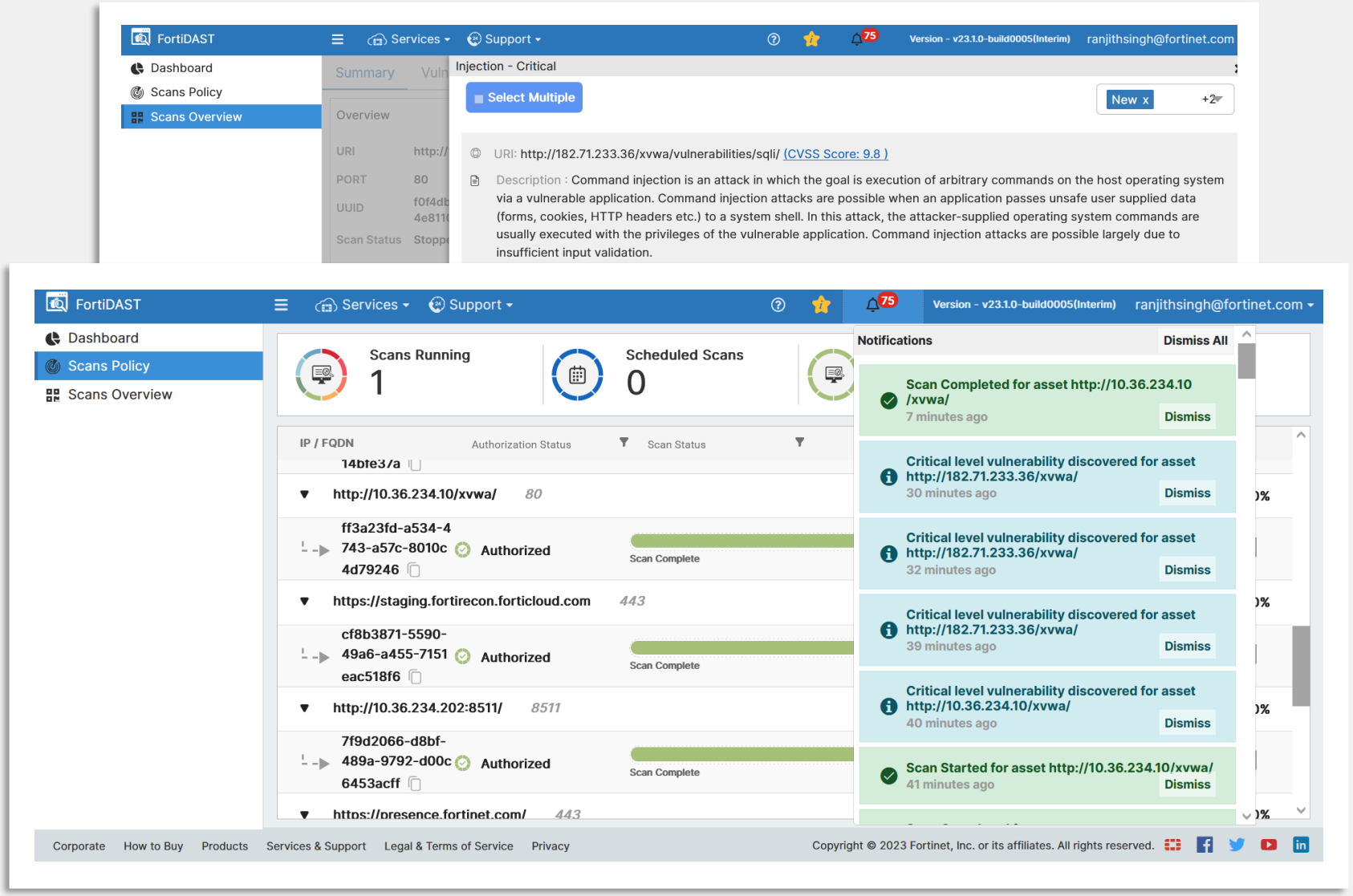


Автоматизоване сканування на вразливості

Сканування вразливостей

Використовує реальні підходи до атак для тестування веб-додатків на OWASP Top 10 та інші вразливості

- Імітація справжнього браузера для імітації поведінки людини
- Використовує дослідження та базу знань FortiGuard Labs



FortiDAST виявляє OWASP Top 10 та інші ризики

“The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.”

- Trusted development resource for current landscape of known attack vectors.
- List is built from of common vulnerabilities that result in application insecurities.

https://owasp.org/

2021 Top 10 Risks	
A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfigurations
A06:2021	Vulnerable and Outdated Compoinents
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A10:2021	Service-Side Request Forgery (SSRF)

FortiDAST виявляє OWASP Top 10 та інші типи вразливостей

FortiGuard Labs

500+ FortiGuard Labs Global Threat Hunters and Researchers

480+ TI, detection, enforcement and remediation partners

215B+ Threats Blocked Per Day

Advanced Services

FortiGuard AI-powered Security Services

20 best-of-breed security services integrated into solutions across the Fortinet Security Fabric to deliver coordinated prevention, detection and response in real-time.

FortiGuard Expert Services

- Incident Response
- Readiness and Response Services
- SOC-as-a-Service
- Managed Detection and Response

Industry-leading Threat Intelligence Capabilities

10+ Years experience in AI/ML

6M+ Solution telemetry

1.6 PB Of threat samples

▼

1,000+ Zero-days discovered

1B+ Updates per day

Coordinated Real-Time Protection Against Known and Unknown Threats

What we process per day

43.2 B Botnet and C2 attempts thwarted

31.4 B Network intrusion attempts blocked

88.8 B Malware programs neutralized

380 M Malicious website access blocked

538 M Phishing blocked

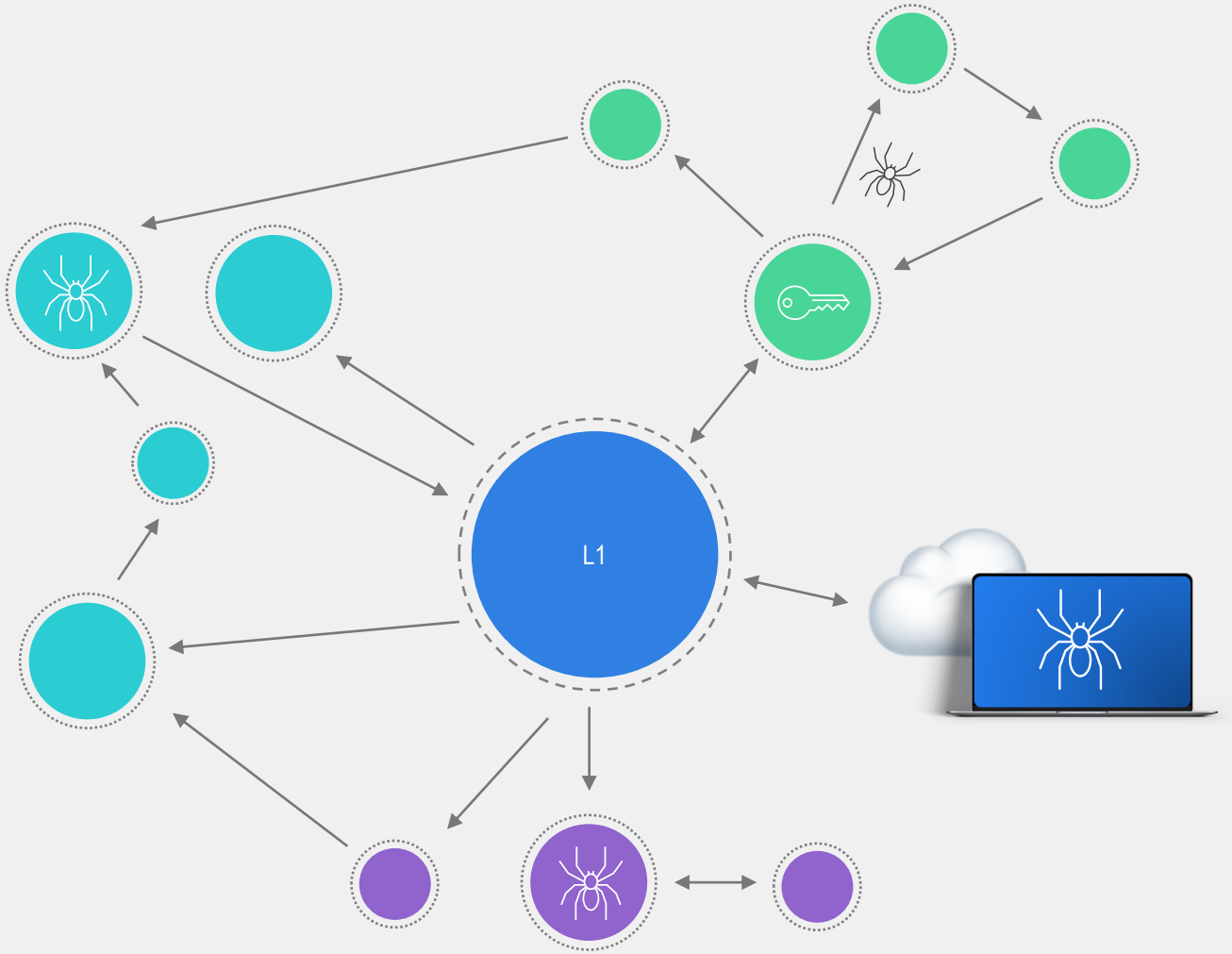
…

Вдосконалений Crawler

Вдосконалений Crawler

Знаходить всі шляхи і розгалуження веб-додатку

- Проводить комплексний аналіз веб-додатку на наявність вразливостей
- Може сканувати зони захищені аутентифікацією



More…

Вискоефективний Fuzzer

Fuzzer

Високоефективне сканування з експертизою Fortinet

- У Fortinet працює команда експертів, які мають великий досвід написання правил і тестів для Fuzzer
- Підвищує загальну ефективність

Injection
- Remote Code Execution
- Server-Side Template Injection
- File inclusion
- LDAP Injection
- NoSQL Injection
- SQL Injection
- XPATH Injection
- Code Injection
- XSS (Cross site scripting)
- Insecure file upload and manipulation via WebDAV
- Open Redirect
- Path Traversal
- ORM Injection
- Expression Language (EL) / Object Graph Navigation Library (OGNL) Injection

Broken Access Control
- Forced Browsing
- Server Side Request Forgery
- Indirect object referencing (IDOR)

Cryptographic Failures
- SSL Tests
- Weak Ciphers

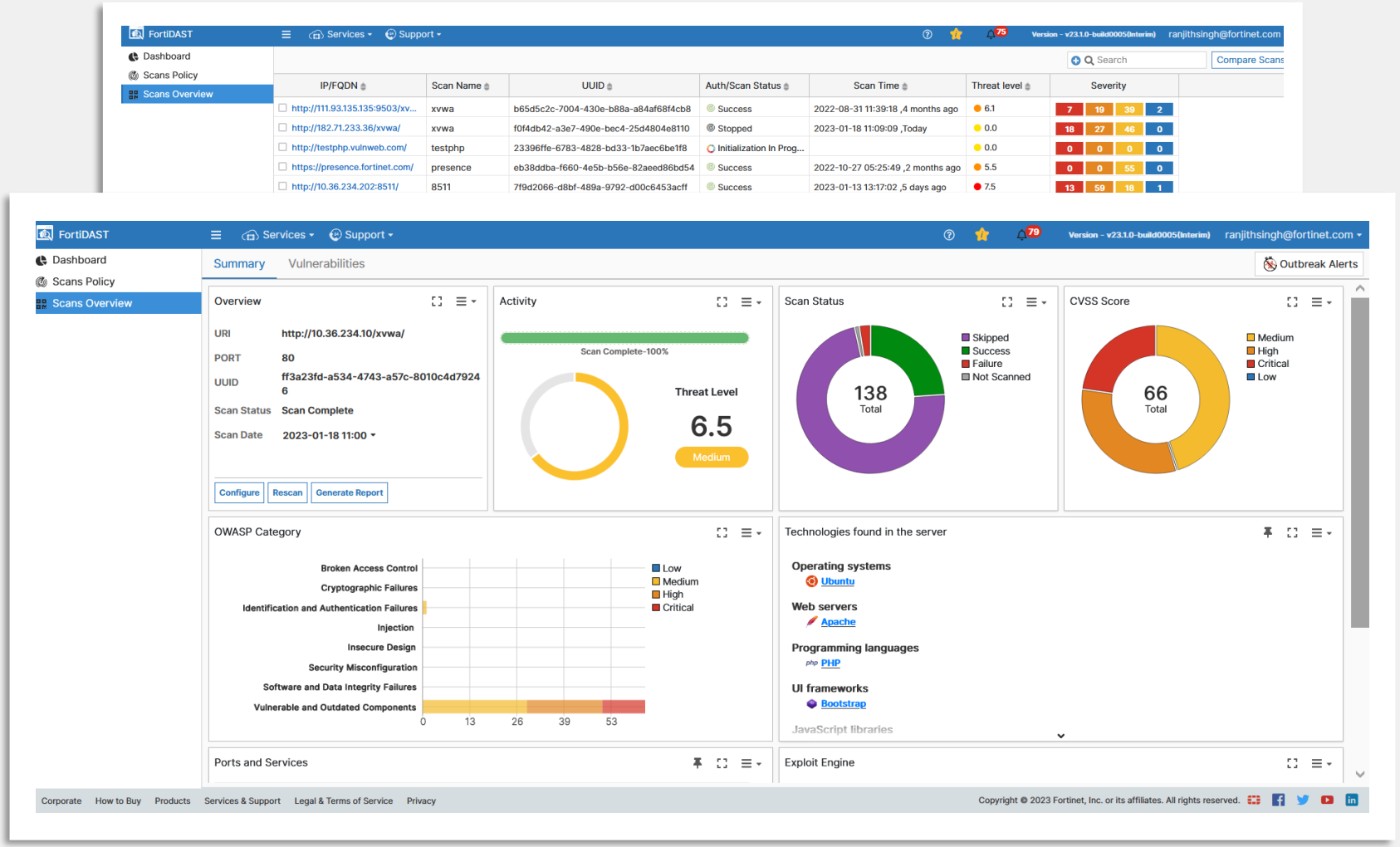
Security Misconfiguration
- XML external entity (XXE) injection
- Information Disclosure

Детальна звітність

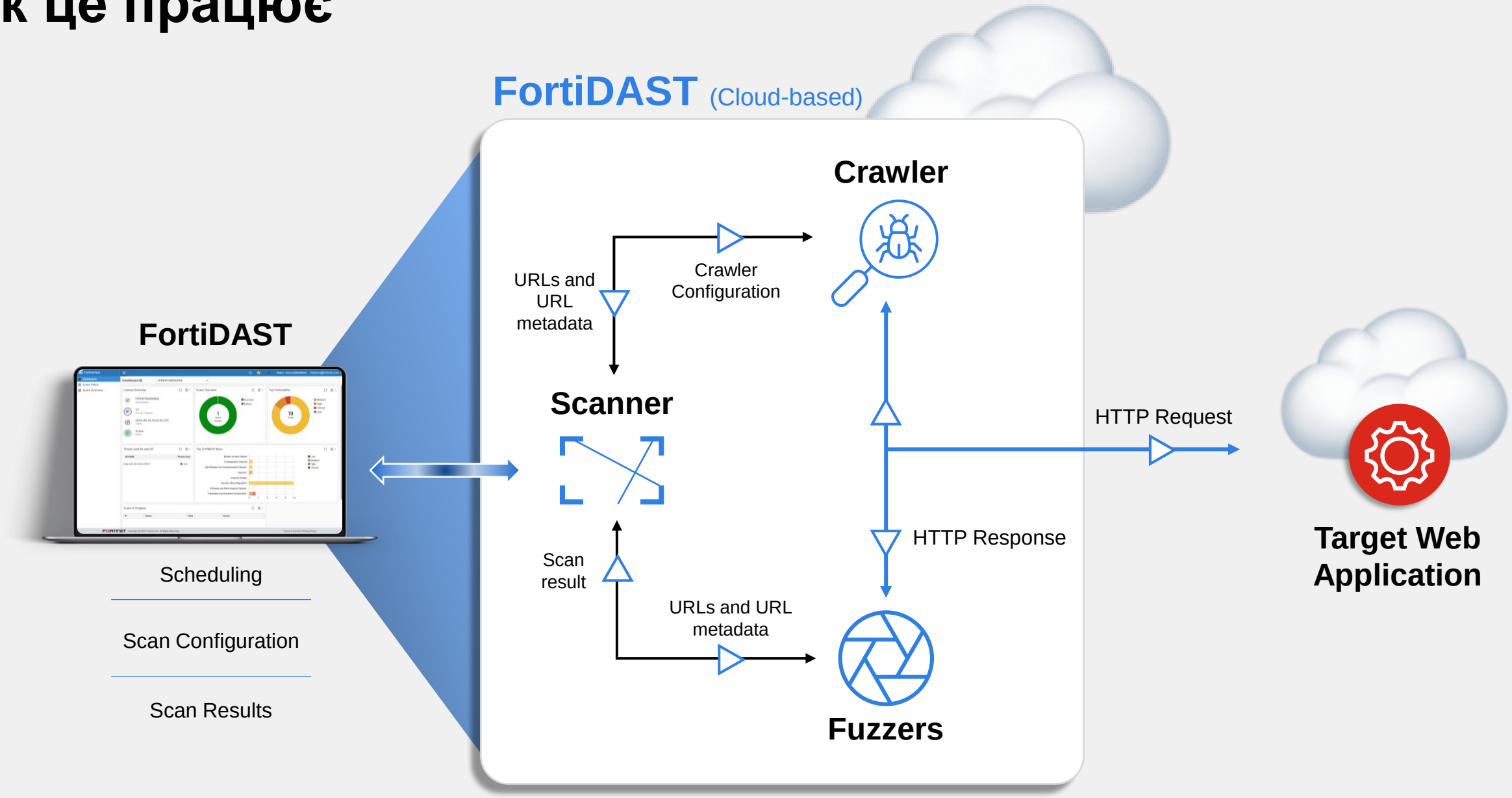
Результати та звітність

Агрегованя або детальні звіти про поточні сканування та вразливості

- Візуалізація ризиків безпеки для top-10 OWASP та інших вразливостей
- Відображення покращення з часом
- Звіти для демонстрації відповідності до регуляторних вимог



Як це працює



Ліцензування FortiDAST

	Description
FC-10-FPENT-236-02-DD	Dynamic Application Security Testing (DAST) subscription service for detection of critical vulnerabilities in websites / web applications, including those in OWASP top 10. Each subscription covers 10 IP/FQDN.

FortiDevSec

FortiDecSec

Виявлення проблем різними типами сканування.

SAST

Static Application Security Testing

Виявляє вразливості у вихідному коді

SCA/OSS

Software composition analysis

Виявляє вразливості у сторонніх бібліотеках і бібліотеках з відкритим кодом, напр. log4j

Secrets

Secret scanning

Аналізує всі версії вихідного коду програми, журналів і пов'язаних файлів на наявність секретів (наприклад, паролів, облікових даних, ключів SSH тощо)

FortiDAST

DAST

Dynamic Application Security Testing

Симулює експлойти на front-end URL додатку за допомогою FortiDAST

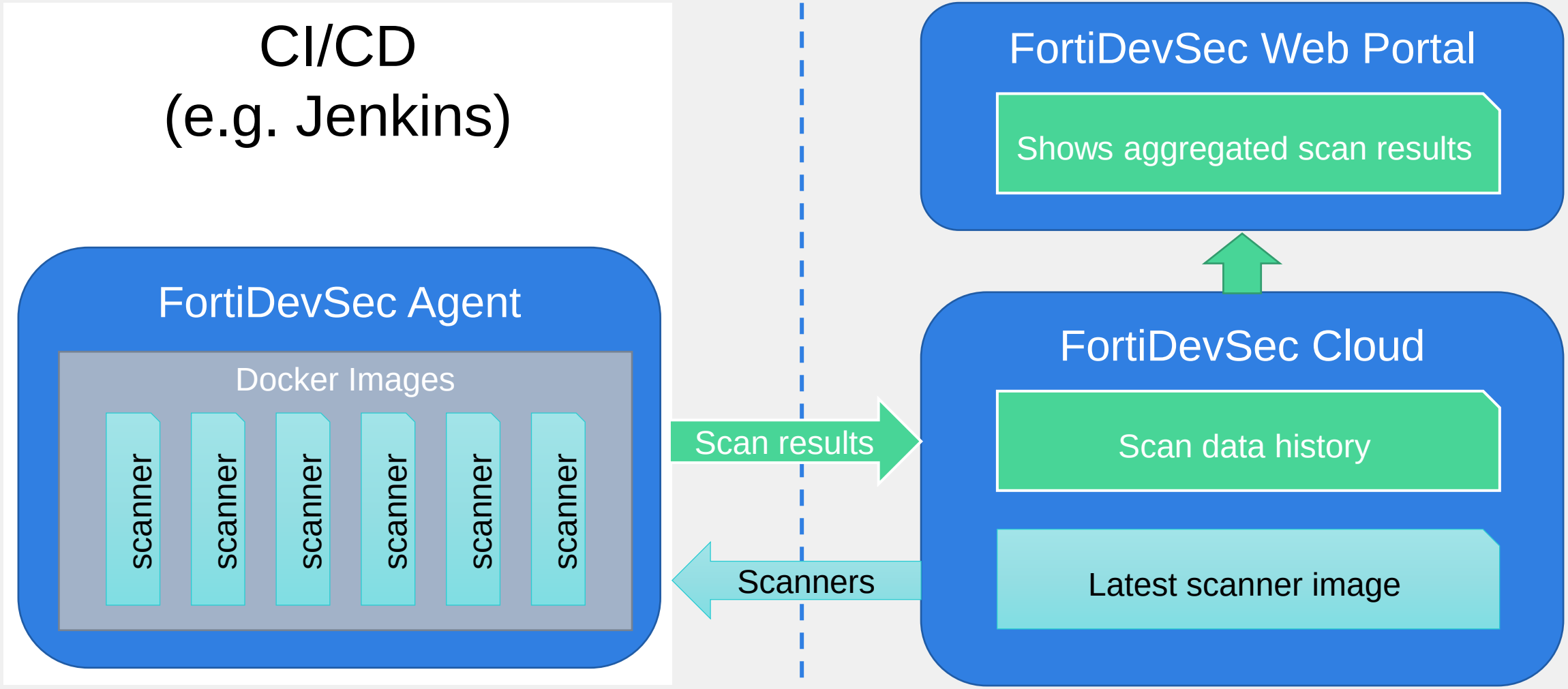
IaC (Infrastructure-as-Script scanning)

Сканування скриптів IaC, таких як terraform тощо.

Containers

Сканування **контейнерів**, які вбудовані в pipeline.

Архітектура FortiDevSec



FortiDevSec: спрощує безпеку

Спрощує безпеку при розробці сучасних додатків

Організовує та автоматизує безперервне тестування безпеки додатків на платформах CI/CD без потреби в експертних знаннях у сфері безпеки

Впроваджує методику DevSecOps “ShiftLeft”

Легке інтегрування в DevOps

- **Повна інтеграція в багато основних платформ CI/CD**
- **Підтримка всіх основних мов та фреймворків DevOps**
- **Дозволяє AppSec працювати з швидкістю DevOps**
- **Експертиза в AppSec не потрібна**

Легка інтеграція в CI/CD платформи

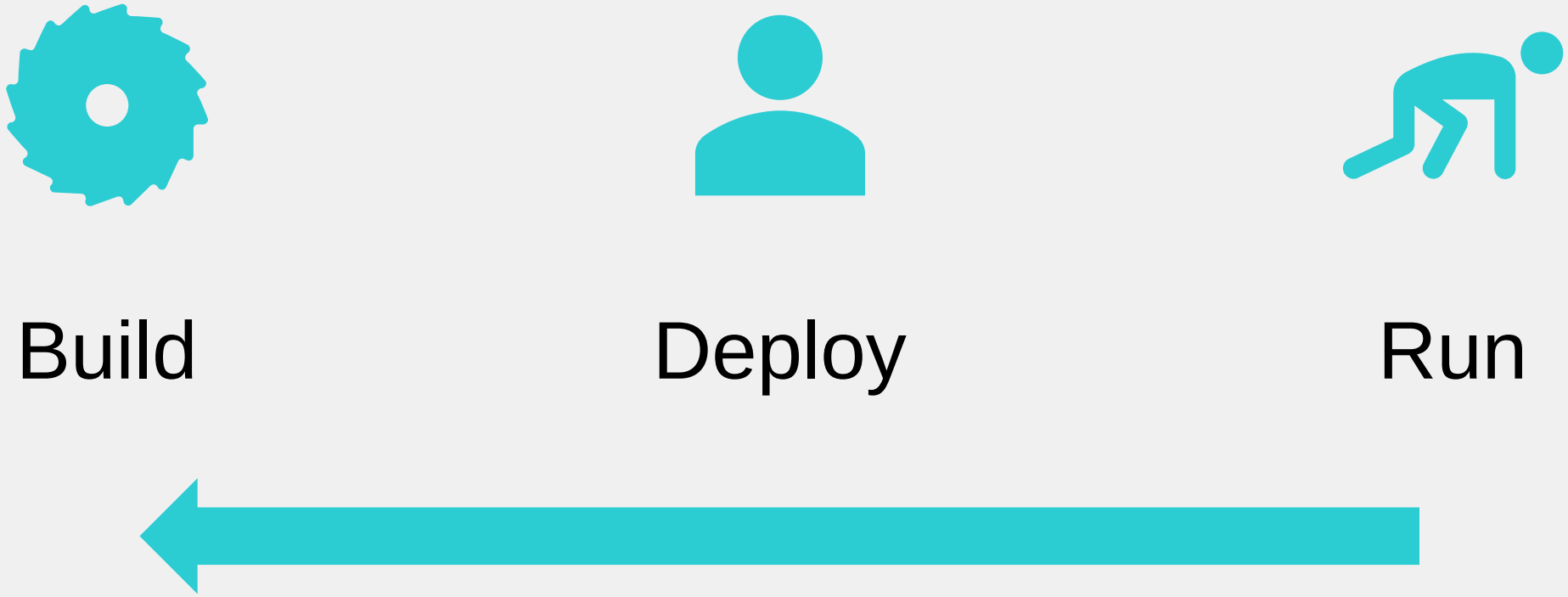
```
SAST scan:
        docker login –username $DOCKERHUB_USERNAME –password
$DOCKERHUB_PASSWORD
        docker run –rm –mount type=b
registry.fortinet-us.com/fortidevsecops/

DAST scan:
        docker login –username $DOC
$DOCKERHUB_PASSWORD
        docker run –rm –mount type=b
registry.fortinet-us.com/fortidevsecops/
```

```
orgid: your-org-id-here

appid: your-app-id-here
# Optional param section starts

buildtool: jenkins.      # Optional param, values=jenkinsltravis
scaanner: sast,dast,sca      # Optional param, default is All
language: python, javascript      # Optional param, default is Auto Detect

variables:
   DAST_URL: https://your.url.com      # Optional param

   # Optional param section end
   # end of file
```

Jenkins (with plug in) · Harness CI · GitHub Action · Circle CI · Bamboo · Travis CI · Azure DevOps

Shift-Left Security

Перехід до забезпечення безпеки на етапі розробки



https://docs.fortinet.com/document/fortidevsec/23.2.0/user-guide/480750/support-matrix

Scanner	Description
SAST	Scans the source code of an application during development to minimize zero-day vulnerabilities. The application languages supported for SAST are *Shell, Java, Ruby on Rails, Python, Golang, PHP, JavaScript/NodeJS, C* and *C++*.
SCA	Scans for vulnerabilities in the open-source libraries/components used by the application. The programming languages supported by the SCA scanner are *Java, Javascript, Ruby, Python, Golang, and PHP.*
Secret	Scans to detect certificates and other secrets committed into Git.
IaC	Scans your IaC configuration files for *Terraform, Cloud Formation, Docker* and *Kubernetes*, to detect configuration issues.
Container	Scans container components to identify potential vulnerabilities.
DAST	Scans a deployed application at runtime to detect vulnerabilities. The DAST scanner supports scanning of assets/targets hosted on both the internal network of an organization and the external/public network using FortiDAST proxy server. See FortiDAST Proxy Server. The DAST scanner allows you to configure a full or a quick scan using the FortiDAST, for more information see FortiDAST Scanner.

Supported CI/CD Pipeline Tools

Support for the following CI/CD tools is a

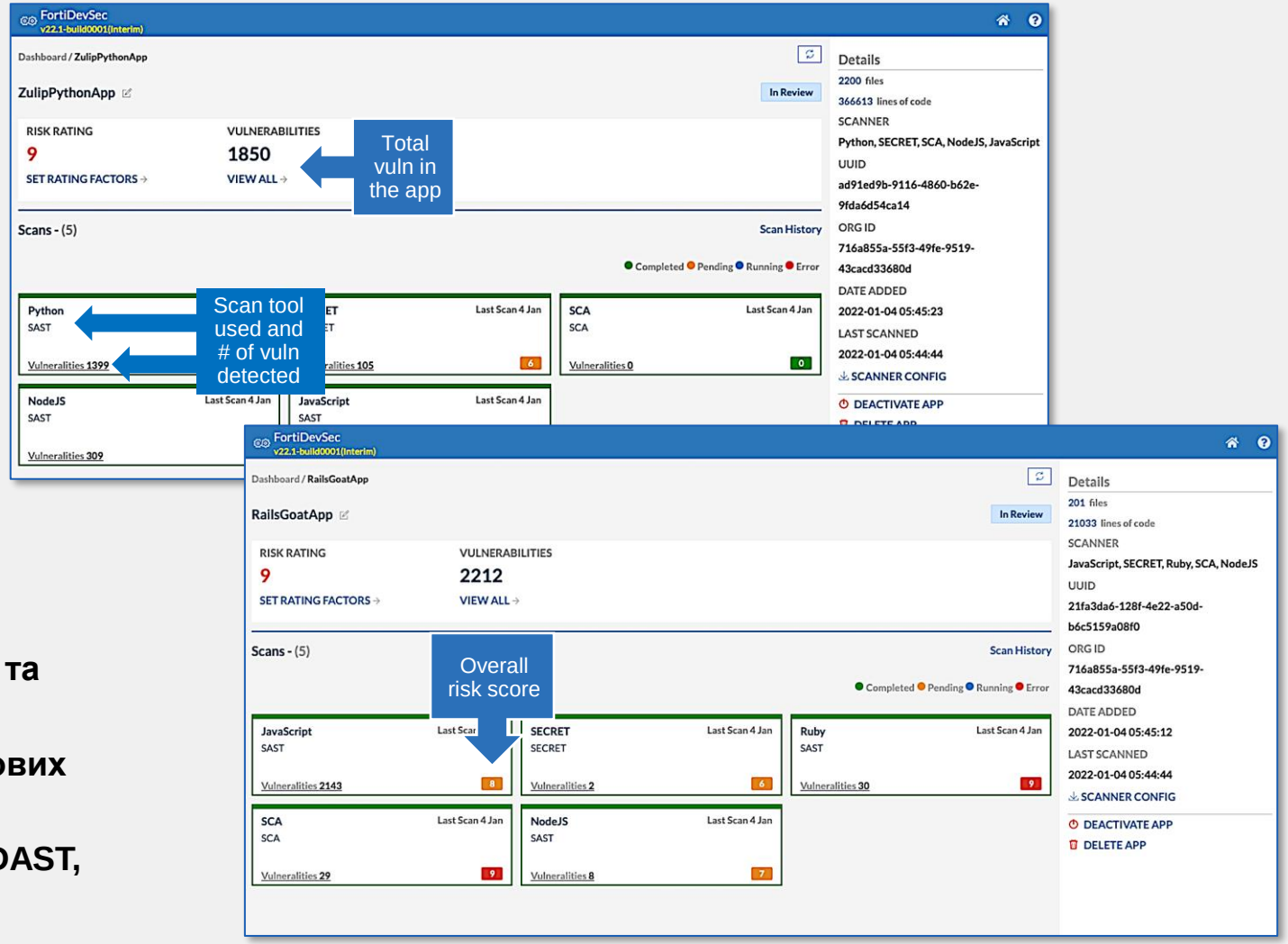
- AWS CodePipeline
- Azure DevOps
- Bamboo
- CircleCI
- Drone CI
- GCP Cloud Build
- GitHub Actions
- GitLab
- Jenkins
- Travis CI

FortiDevSec: комплексне управління вразливостями

Комплексне управління вразливістями

Захищає ландшафт вразливостей шляхом автоматичного аналізу, вибору та налаштування кількох типів сканерів безпеки додатків

Захищає ландшафт загроз



Комплексне сканування та тестування

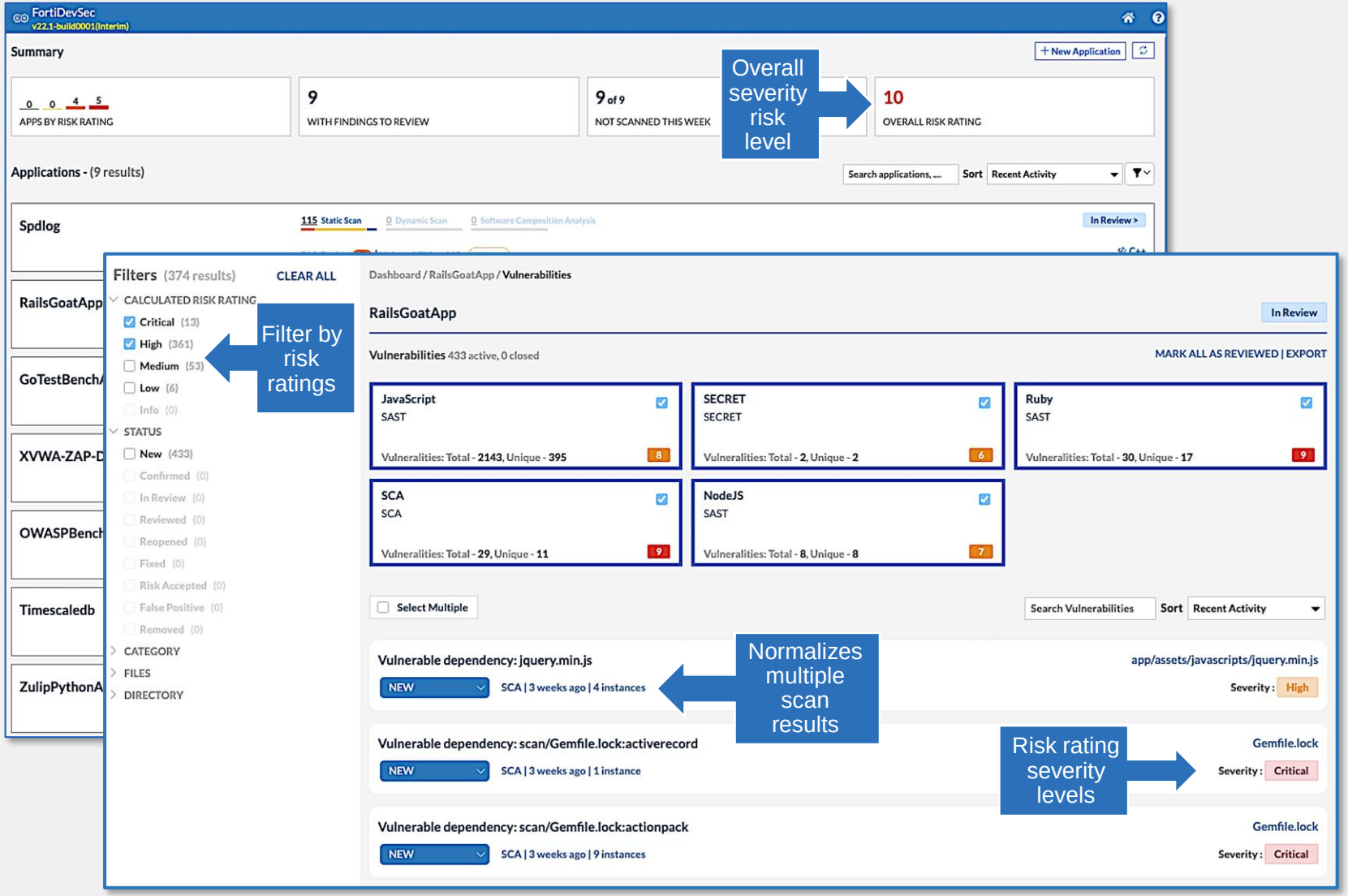
- **Автоматично розгортає відповідний сканер на основі атрибутів додатку (платформи розробки та мов) і налаштувань**
- **Постійне тестування додатків для виявлення нових вразливостей, що можуть з’явитись**
- **Унікальне рішення, яке поєднує сканери SAST, DAST, SCA/OSS і Secrets для захисту ландшафту вразливостей**

FortiDevSec: уніфікована інформаційна панель

Консолідована інформаційна панель

Корельоване управління ризиками та визначення пріоритетів

Пріоритезує критичні ризики для усунення



Пріоритезує та агрегує результати сканування

- **Співвідносить результати між типами сканування та зменшує шум**
- **Результати нормалізуються для точного встановлення пріоритетів і класифікації загроз**
- **Оцінка ризику визначає, які вразливості потрібно усунути в першу чергу**
- **Інтелектуальна пріоритезація та нормалізація ризиків, що дозволяє DevOps зосереджуватися на найбільш критичних ризиках, які необхідно усунути**

Інтегрований FortiDAST

```yaml
version: v1

id:
  org: d642d710-29c9-47f1-xxxx-10600d9632c0
  app: a2dccb8b-f76d-413d-xxxx-913f4fcbbc23

# Optional parameters.
scanners:
- sast
- dast
- secret
- sca

languages:
- python
- javascript

dast:
url: https://your.url.com
fortipentest_scanner: true #true|false
full_scan: true #true|false

resource:
serial_scan: false #true|false
```

- Клієнти, які мають існуючу ліцензію FortiPenTest/FortiDAST, можуть використовувати її для DAST-сканування програми.
- Результати сканування буде інтегровано в FortiDevSec.

Ліцензування

License	Validity in years	Maximum users	Maximum assets/apps supported for DAST scanner
FortiDevSec Standard	1	5	5
FortiDevSec FortiDAST Add-on(Optional)	1	n/a	5*

FortiRecon

FortiRecon

FortiRecon забезпечує видимість та аналітику, що дозволяють клієнту вживати контрольованих заходів безпеки на основі ризиків :

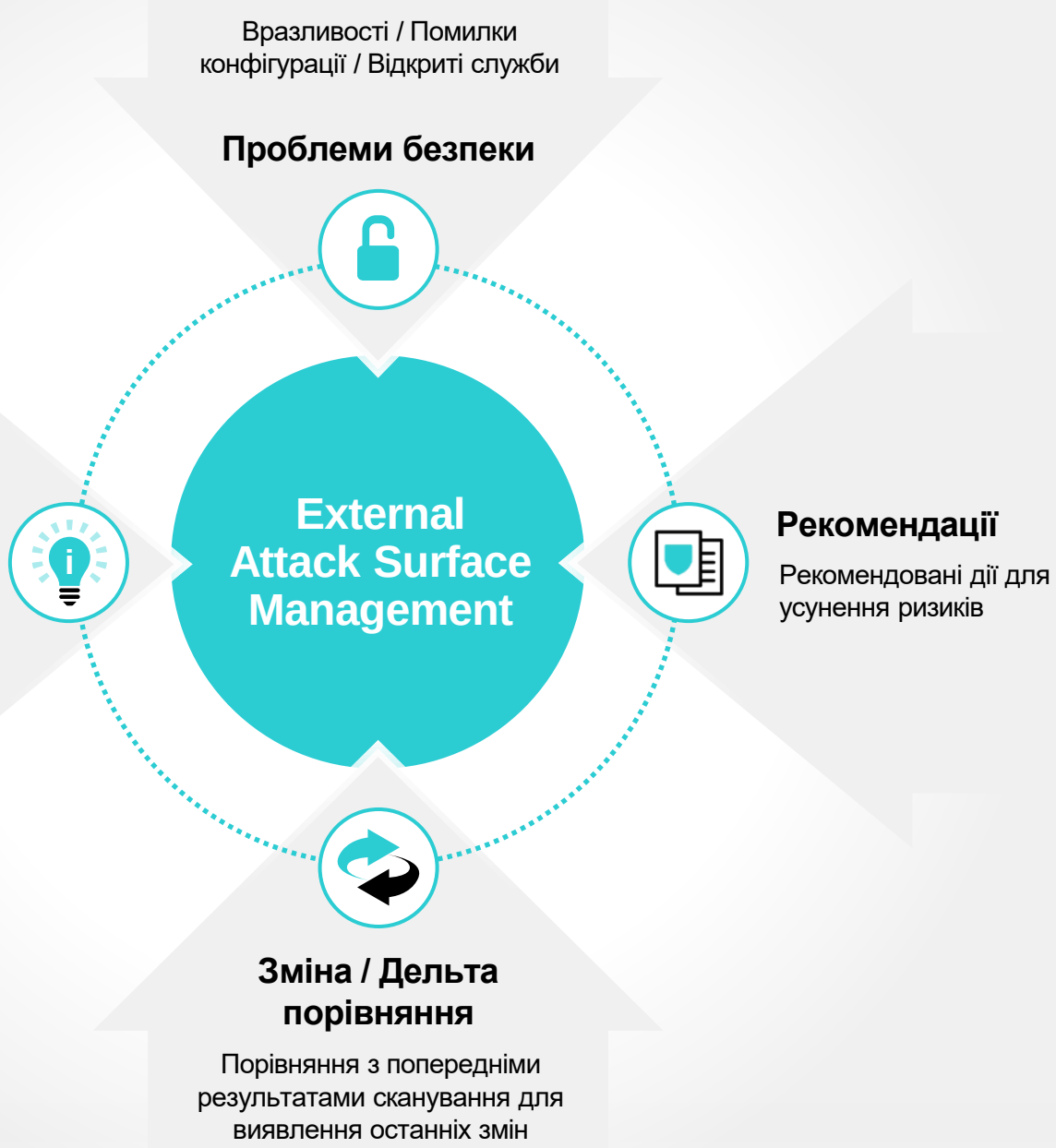
- Доповнює існуючі рішення для повної видимості поверхні атаки.
- Надає клієнтам уявлення про те, **що бачать зловмисники** (EASM)
- Надає клієнту бачення того, **що роблять зловмисники** (Brand Protection)
- Надає клієнту уявлення про те, **що планують зловмисники** (ACI)

Вживання упереджувальних заходів щодо блокування/виправлення, щоб попередити/зменшити наслідки від кібератак

- Захист репутації бренду організації

External Attack Surface Management (EASM)

FortiRecon External Attack Surface Management (EASM) забезпечує зовнішній погляд на організацію та її дочірні компанії, щоб ідентифікувати відкриті відомі та невідомі активи підприємства та пов’язані з ними вразливості, щоб допомогти визначити пріоритетність усунення.



Brand Protection (BP)

FortiRecon Brand Protection (BP) виявляє фішингові атаки в Інтернеті, підробні сайти (Typosquatting), підробні шахрайські додатки, витік облікових даних і імперсонації бренду в соціальних мережах - поширені методи, які використовують кібер зловмисники.

Раннє виявлення активності та вжиття заходів, наприклад видалення (**takedown**) веб-сайту чи програми, Brand Protection допомагає організаціям захистити цінність свого бренду, довіру, цілісність і репутацію.

Brand Monitoring & Protection

Credentials Monitoring

Моніторинг витоків облікових даних

Typosquatting

Відстеження схожих доменних імен

Rogue Apps Monitoring

Відстеження підробних мобільних додатків

Social Media

Відстеження підробних акаунтів у соціальних мережах

Phishing Monitoring

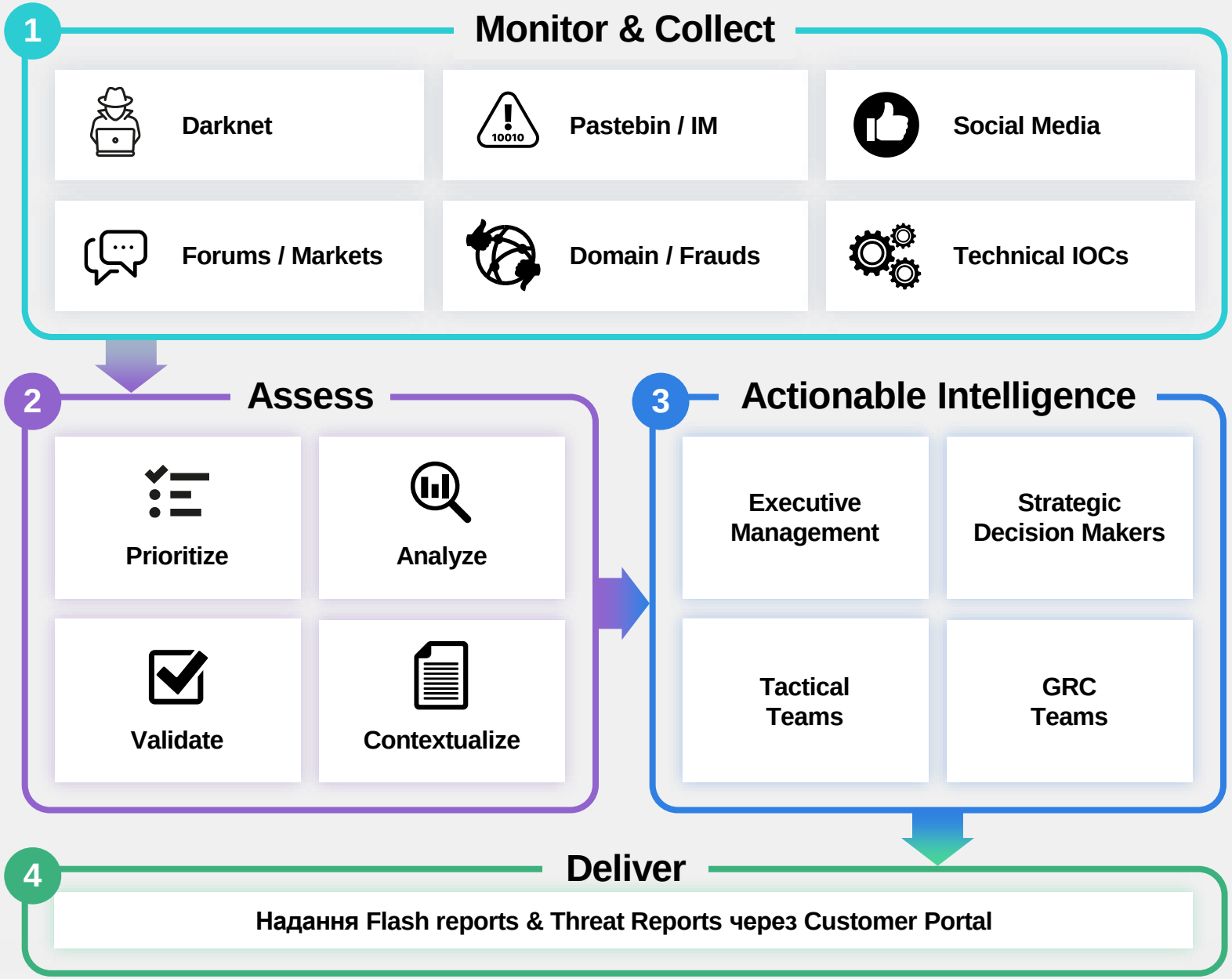
Відстеження фішингових кампаній проти брендів

Cloud Exposure

Виявлення неправильної конфігурації хмари, яка розкриває дані

Adversary Centric Intelligence (ACI)

FortiRecon Adversary Centric Intelligence (ACI) надає контекстне розуміння неминучих загроз для організацій і дозволяє їм швидше реагувати на інциденти, краще розуміти зловмисників і захищати свої активи.



Adversary Centric Intelligence

Приклад DARKNET Flash Report звіту

- Скомпрометовані email адреси
- Атрибути:
  - Darknet
  - Flash Report
  - High relevancy
  - High TLP
  - Reliable source
  - Confirmed info
- Деталі по вкрадену базу даних

Flash Report – 2022030317339 Ver 1.0

Darknet | FortiGuard Threat Research

A total of 7290 unique email addresses affiliated with Acme Demo [acmedemo.com] domain found to be part of various data breaches

Feb 28, 2022 | High TLP

Associations

Source : A-Reliable
Information: 1-Confirmed

Multiple

Cyber Crime

Global

All Sectors

Data Breach

Personal Information Identification (PII)

Account(s) Compromised

Threat Summary:

This report provides data relating to 'Acme Demo' email addresses affiliated to the domain [acmedemo.com], which are found to be part of various data breaches shared by threat actors on darknet/Clearnet forums. Cyber threat actors regularly share stolen data on various Darknet/Clearnet cyber-crime forums. The breached data could be from website compromise, combo-list, or data belonging to an organizational entity.

Threat Detail

FortiGuard Threat Research identified a total of 7,365 email addresses of the acmedemo.com domain present across 44 leaked databases dating back to 2019. Out of 7,365 email addresses, 5,630 are unique. The complete list of email addresses can be found in the seperate Excel sheet.

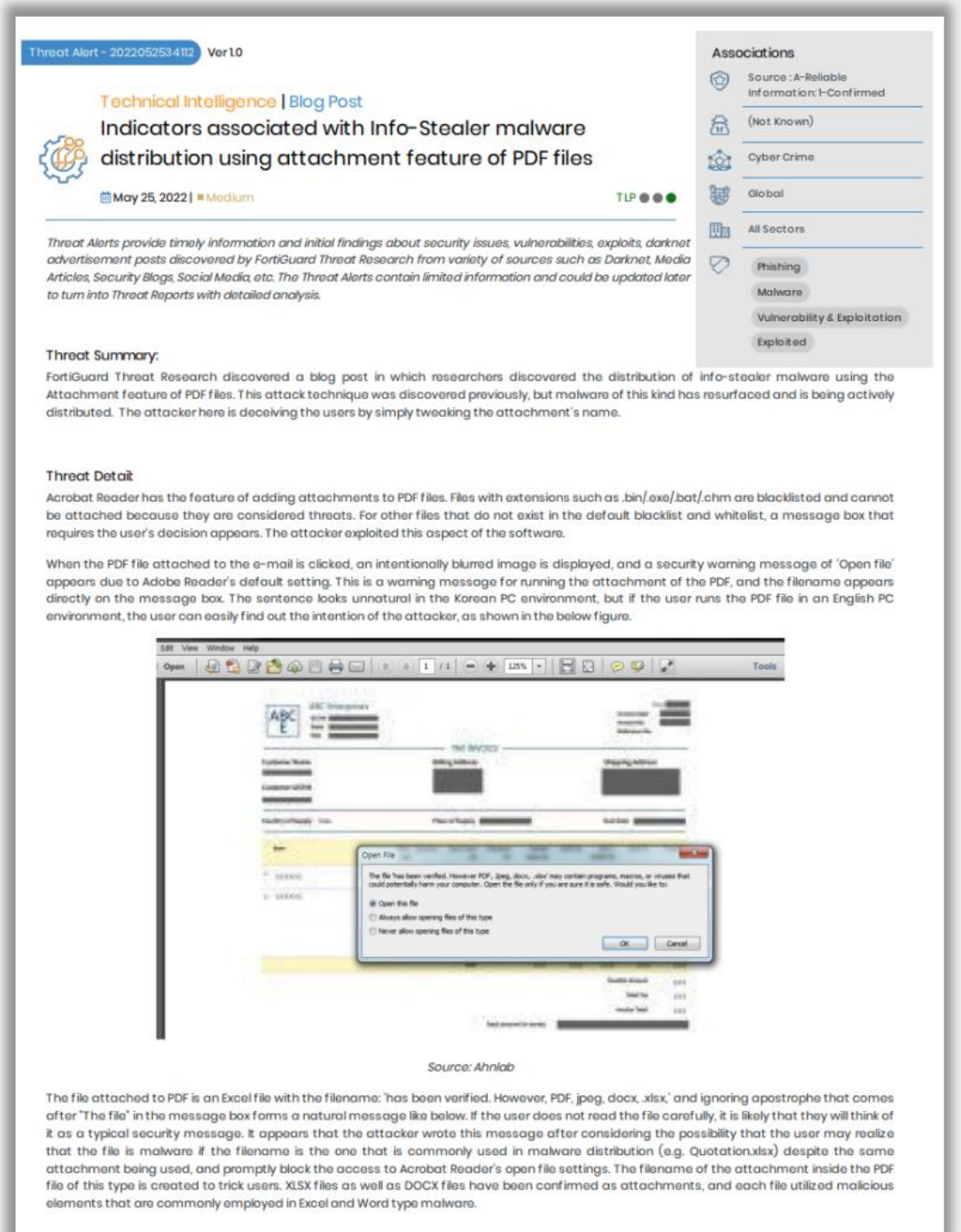
Below are the name of the databases and the timeline of breaches, where the 'Acme Demo' affiliated domain email addresses were identified:

Sr. No.	Database name	Breach date	Compromised accounts	Compromised data	Breach details	Number o acmeden emails fo
1	LimeTray [www.limetray.com]	May 1, 2021	4000000	Brand user ID, Brand ID, Created at, Email address (1605568 unique emails), First non void order time, First order time, First void order time, Full name, Last interaction time, Loss, Mobile, Revenue, Source ID, Source name, Total discount, Total failed orders, Total loyalty amount, Total non void orders, Total orders, Total pre-orders, Total void orders	On May 01, 2021, actor 'datahub' shared the database claiming to be of an Indian web-presence and web-marketing platform provider, LimeTray [www.limetray.com]. The database was shared on the English language cyber-crime forum 'Raid'.	38

Adversary Centric Intelligence

Приклад TECHINT Threat Alert звіту

- Індикатори фішингової кампанії
- Атрибути:
  - TECHINT
  - Treat Alert
  - Medium relevancy
  - Low TLP
  - Reliable source
  - Confirmed info
- IOC для кампанії



Threat Alert - 2022052534112 Ver 1.0

Technical Intelligence | Blog Post

Indicators associated with Info-Stealer malware distribution using attachment feature of PDF files

May 25, 2022 | Medium

TLP

Threat Alerts provide timely information and initial findings about security issues, vulnerabilities, exploits, darknet advertisement posts discovered by FortiGuard Threat Research from variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc. The Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Associations

Source : A-Reliable
Information: 1-Confirmed

(Not Known)

Cyber Crime

Global

All Sectors

Phishing

Malware

Vulnerability & Exploitation

Exploited

Threat Summary:

FortiGuard Threat Research discovered a blog post in which researchers discovered the distribution of info-stealer malware using the Attachment feature of PDF files. This attack technique was discovered previously, but malware of this kind has resurfaced and is being actively distributed. The attacker here is deceiving the users by simply tweaking the attachment's name.

Threat Detail

Acrobat Reader has the feature of adding attachments to PDF files. Files with extensions such as .bin/.exe/.bat/.chm are blacklisted and cannot be attached because they are considered threats. For other files that do not exist in the default blacklist and whitelist, a message box that requires the user's decision appears. The attacker exploited this aspect of the software.

When the PDF file attached to the e-mail is clicked, an intentionally blurred image is displayed, and a security warning message of 'Open file' appears due to Adobe Reader's default setting. This is a warning message for running the attachment of the PDF, and the filename appears directly on the message box. The sentence looks unnatural in the Korean PC environment, but if the user runs the PDF file in an English PC environment, the user can easily find out the intention of the attacker, as shown in the below figure.

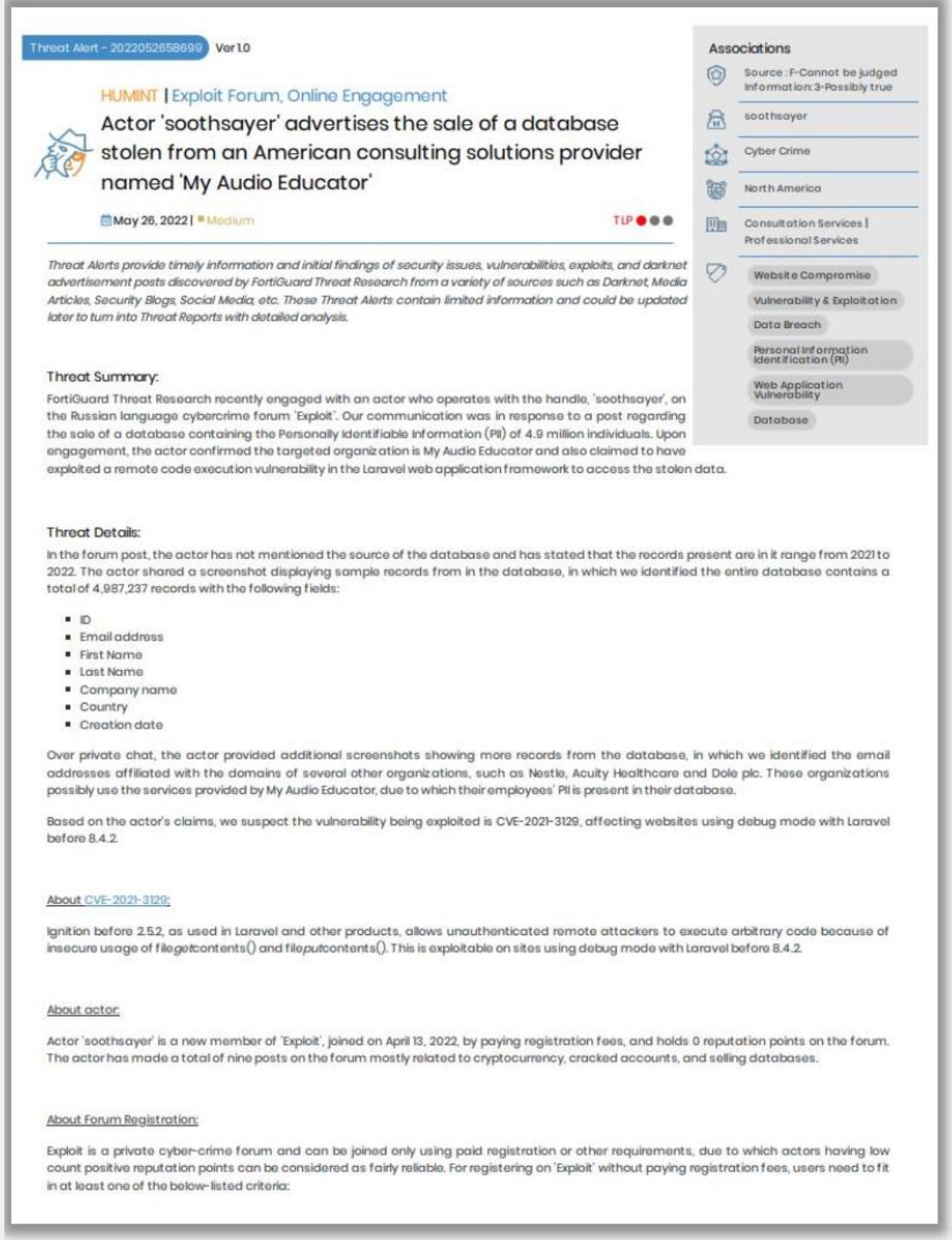
Source: Ahnlab

The file attached to PDF is an Excel file with the filename: 'has been verified. However, PDF, jpeg, docx, .xlsx,' and ignoring apostrophe that comes after "The file" in the message box forms a natural message like below. If the user does not read the file carefully, it is likely that they will think of it as a typical security message. It appears that the attacker wrote this message after considering the possibility that the user may realize that the file is malware if the filename is the one that is commonly used in malware distribution (e.g. Quotation.xlsx) despite the same attachment being used, and promptly block the access to Acrobat Reader's open file settings. The filename of the attachment inside the PDF file of this type is created to trick users. XLSX files as well as DOCX files have been confirmed as attachments, and each file utilized malicious elements that are commonly employed in Excel and Word type malware.

Adversary Centric Intelligence

Приклад HUMINT Threat Report звіту

- Витік персональних даних
- Атрибути:
  - HUMINT
  - Treat Report
  - Medium relevancy
  - High TLP
  - Fairly reliable source
  - Possibly true
  - Details about the leak
- Screenshots спілкування зі зловмисником



Threat Alert - 2022052658699 Ver 1.0

HUMINT | Exploit Forum, Online Engagement

Actor 'soothsayer' advertises the sale of a database stolen from an American consulting solutions provider named 'My Audio Educator'

May 26, 2022 | Medium

TLP

Threat Alerts provide timely information and initial findings of security issues, vulnerabilities, exploits, and darknet advertisement posts discovered by FortiGuard Threat Research from a variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc. These Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Associations

Source : F-Cannot be judged Information: 3-Possibly true

soothsayer

Cyber Crime

North America

Consultation Services | Professional Services

Website Compromise

Vulnerability & Exploitation

Data Breach

Personal Information Identification (PII)

Web Application Vulnerability

Database

Threat Summary:

FortiGuard Threat Research recently engaged with an actor who operates with the handle, 'soothsayer', on the Russian language cybercrime forum 'Exploit'. Our communication was in response to a post regarding the sale of a database containing the Personally Identifiable Information (PII) of 4.9 million individuals. Upon engagement, the actor confirmed the targeted organization is My Audio Educator and also claimed to have exploited a remote code execution vulnerability in the Laravel web application framework to access the stolen data.

Threat Details:

In the forum post, the actor has not mentioned the source of the database and has stated that the records present are in it range from 2021 to 2022. The actor shared a screenshot displaying sample records from in the database, in which we identified the entire database contains a total of 4,987,237 records with the following fields:

- ID
- Email address
- First Name
- Last Name
- Company name
- Country
- Creation date

Over private chat, the actor provided additional screenshots showing more records from the database, in which we identified the email addresses affiliated with the domains of several other organizations, such as Nestle, Acuity Healthcare and Dole plc. These organizations possibly use the services provided by My Audio Educator, due to which their employees' PII is present in their database.

Based on the actor's claims, we suspect the vulnerability being exploited is CVE-2021-3129, affecting websites using debug mode with Laravel before 8.4.2.

About CVE-2021-3129:

Ignition before 2.5.2, as used in Laravel and other products, allows unauthenticated remote attackers to execute arbitrary code because of insecure usage of file*get*contents() and file*put*contents(). This is exploitable on sites using debug mode with Laravel before 8.4.2.

About actor:

Actor 'soothsayer' is a new member of 'Exploit', joined on April 13, 2022, by paying registration fees, and holds 0 reputation points on the forum. The actor has made a total of nine posts on the forum mostly related to cryptocurrency, cracked accounts, and selling databases.

About Forum Registration:

Exploit is a private cyber-crime forum and can be joined only using paid registration or other requirements, due to which actors having low count positive reputation points can be considered as fairly reliable. For registering on 'Exploit' without paying registration fees, users need to fit in at least one of the below-listed criteria:

Ліцензування

[FortiRecon Ordering Guide (fortinet.com)]

- Ліцензія формується з 2 частин:
  - **Кількість активів**
    - В діапазоні
    - Не сумується
  - **feature bundle**
    - EASM
    - EASM + BP
    - EASM + BP + ACI
- Takedown ліцензується окремо
  - 2 credits включено до ліцензії BP
  - Додаткові credits можна докупити
  - Один takedown – один credit

ORDERING GUIDE

FortiRecon

Product Offerings

FortiRecon is a Digital Risk Protection (DRP) service that allows customers to gain visibility of their digital attack surface, receive targeted threat intelligence, and reduce organizational risk. The solution consists of three main components:

- **External Attack Surface Management (EASM)** — Provides an adversary's view of the organization digital attack surface and prioritizes risks and exposures, enabling customers to mitigate threats in a controlled manner before they become a problem.
- **Brand Protection (BP)** — Continually monitors the organization's public-facing brand, to detect web-based phishing attacks, typosquatting, rogue applications, credential leaks, and brand impersonation in social media, which may impact brand value, integrity, and trust.
- **Adversary Centric Intelligence (ACI)** — Leverages FortiGuard Threat Analysis to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights, to enable organizations to respond proactively, assess risks, respond faster to incidents, better understand their attackers, and guard assets.

The following shows a summary of FortiRecon product offerings. For details, see the FortiRecon datasheet.

SOLUTION BUNDLES	FEATURE	FORTIRECON EASM	FORTIRECON EASM AND BP	FORTIRECON EASM, BP, AND ACI
EASM	Asset Discovery	✓	✓	✓
	Security Issues	✓	✓	✓
	Asset Reports	✓	✓	✓
	Monthly Scanning	✓	✓	✓
	Weekly Scanning			✓
	On-demand Scans (Two per Year)			✓
BP	Third-party Credential Leaks	✓	✓	✓
	Source Code Sensitive Leaks		✓	✓
	Open Cloud Storage Buckets		✓	✓
	Domain Typosquatting		✓	✓
	Rogue Mobile Apps		✓	✓
	Phishing Monitoring - Digital Watermarking		✓	✓
	Takedowns		✓	✓
	Social Media Brand Impersonations		✓	✓
ACI	Social Media			✓
	Dark Web Monitoring			✓
	Technical Intelligence			✓
	IoC Reputation Lookup (IP/Domain/Hash/CVE)			✓
	Dark Web Marketplace Monitoring (Stealer Logs)			✓
	OSINT Cyber Threats			✓
Delivery	Executive Reporting	✓	✓	✓
	24×7 Portal Access	✓	✓	✓
	Analyst Support		✓	✓
	Realtime Alerting		✓	✓
	Orchestration/Integrations (Ticketing/SOAR)		✓	✓

Ліцензування FortiRecon

NUMBER OF ASSETS	EASM	EASM & BP	EASM, BP & ACI
Up to 500	FC2-10-RNSVC-533-02-DD	FC2-10-RNSVC-534-02-DD	FC2-10-RNSVC-535-02-DD
Up to 1000	FC3-10-RNSVC-533-02-DD	FC3-10-RNSVC-534-02-DD	FC3-10-RNSVC-535-02-DD
Up to 2000	FC4-10-RNSVC-533-02-DD	FC4-10-RNSVC-534-02-DD	FC4-10-RNSVC-535-02-DD
Up to 10 000	FC5-10-RNSVC-533-02-DD	FC5-10-RNSVC-534-02-DD	FC5-10-RNSVC-535-02-DD
Up to 50 000	FC6-10-RNSVC-533-02-DD	FC6-10-RNSVC-534-02-DD	FC6-10-RNSVC-535-02-DD
Up to 100 000	FC7-10-RNSVC-533-02-DD	FC7-10-RNSVC-534-02-DD	FC7-10-RNSVC-535-02-DD

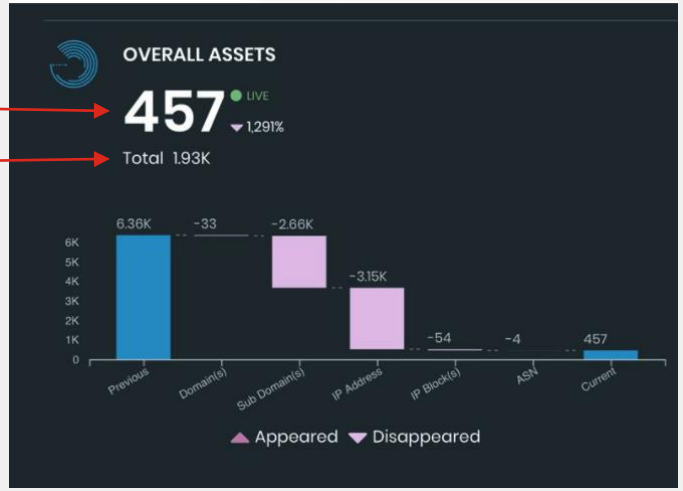
FORTIRECON TAKEDOWN SERVICE		
PRODUCT	SKU	DESCRIPTION
Service Credits - 5 Takedowns	FRN-TKD-5	License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.
Service Credits - 10 Takedowns	FRN-TKD-10	License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.
Service Credits - 50 Takedowns	FRN-TKD-50	License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.

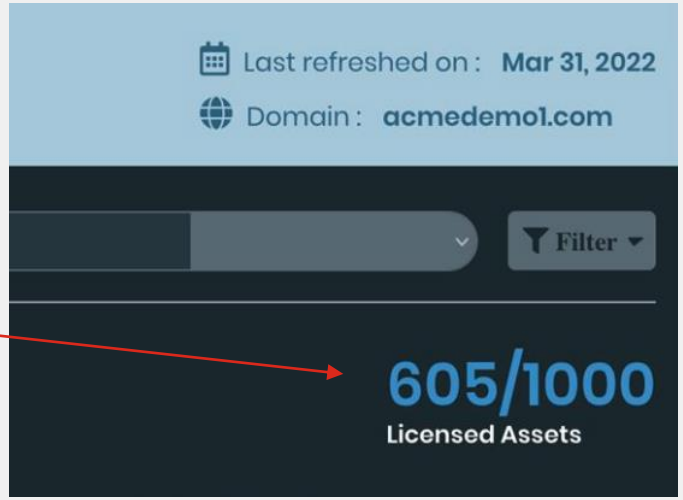
Кількість ативів в ліцензії

- Таксономія- як визначити актив :
  - ASN – BGP Autonomous System Number
  - IP address
  - IP block
  - Domain
  - Subdomain
- EASM - Dashboard
  - Live asset (457)
  - Total of asset scan (1930)
- Потрібна ліцензія на 457 активів? Як порахувати?

Кількість ативів в ліцензії

- В цьому прикладі EASM dashboard показує:
  - Total number of live assets: **457**
  - Total number of scanned assets: **1930**
- Ліцензія розраховується як сума загальної кількості живих активів (457) і 10 % решти сканованих активів
- 10% призначені для покриття потенційного зростання
  - Total number of live assets: 457
  - Total number of assets scanned: 1930
  - Remaining assets scanned: 1930 – 457 = 1473 non-live assets
  - (**10% of 1473**) + 457 = **605**





Дякую за увагу!


FORTINET