imperva
a Thales company

SOFTPROM

# IMPERVA – ПРОДУКТОВИЙ ПОРТФЕЛЬ КОРОТКО

Imperva — компанія, яка займається програмним забезпеченням та послугами в галузі кібербезпеки, що забезпечує захист корпоративних даних та додатків. Штаб-квартира компанії знаходиться в Сан-Матео, Каліфорнія. Imperva, по суті, працює у трьох галузях: безпека даних, безпека додатків та Edge/мережева безпека, також є відділ професійних послуг. Місія компанії: «Захист даних та всіх шляхів до них».

## Data Security:

У сфері безпеки даних йдеться про рішення, які дозволяють компаніям захистити свої дані. Однією з двох основних мотивуючих причин проєктів забезпечення безпеки даних є забезпечення дотримання компанією нормативно-правових актів. Друга причина — підвищити безпеку даних організації шляхом їхнього безперервного моніторингу та виявлення аномалій.

### Основні варіанти використання:

- Класифікація даних. Визначення того, де зберігаються дані та їх актуальність. Класифікаційні роботи всередині БД та інших репозиторіях, наприклад, у файлах.

- Моніторинг активності даних (DAM). Проведіть повний аудит доступу до будь-яких даних, щоб гарантувати відповідність нормативним вимогам та здатність розслідувати передбачувані витоки даних.

- Управління правами користувачів. Застосування принципу найменших привілеїв щодо доступу до даних. Забезпечення того, щоб кожен мав мінімальний набір дозволів на доступ до цінних даних.

- Розширена аналітика, яка вивчає використання даних в організації таким чином:

    - Поведінковий аналіз доступу до даних, тобто вивчення звичайної поведінки користувача та виявлення аномалій на основі дефолтних та кастомних моделей.
    - Аналіз на основі шаблонів, який є аналізом використання даних у порівнянні з даними, наданими постачальником сигнатур, і виявлення шкідливої поведінки.
    - Аналіз на основі користувацьких правил, тобто можливість застосовувати власні визначення небажаної поведінки та генерувати інциденти, якщо такі спостерігаються.

- Відповідність нормативним вимогам. Зокрема: GDPR, PCI DSS, HIPPA тощо. Регульована обробка даних, як PII, яка потребує контролю доступу до даних.

- Маскування даних – безпечне використання продакшн даних у середовищах розробки без ризику обробки вихідних цінних даних у незахищених середовищах.

- Реагування на інциденти – підтримка реагування на інциденти з даними за допомогою автоматизації та інтеграції з іншими системами безпеки (Runbooks, SOAR).

- Підтримка автоматизованих процесів, включаючи підтримку доступу до запитів суб'єктів даних у рамках даних, що їх обробляє організація.

**Ключові особливості рішення:**

- Інтеграція з базами даних із використанням агента або без агента (наприклад, нативний аудит).
- Підтримка баз даних як у локальному дата-центрі, так і у хмарі (PaaS та IaaS).
- Підтримка даних як у базах даних, так і у файлах (неструктуровані дані).
- Рішення доступне у вигляді обладнання, віртуальних машин та хмарного сервісу.

## Application Security:

Сфера безпеки додатків / застосунків присвячена захисту веб-додатків на різних рівнях. Головною та найбільш популярною функцією є WAF (брандмауер веб-додатків), який представлений у вигляді хмарної послуги, а також програмного/апаратного забезпечення, яке клієнти можуть встановити у свою інфраструктуру. Пропозиція доповнюється RASP (Runtime Application Self-Protection), який забезпечує захист за допомогою прямої інтеграції з веб-додатком.

**Основні варіанти використання:**

- Захист веб-додатків від відомих і невідомих атак, які зазвичай використовуються в контексті веб-додатків.

- Захист додатків від DoS та DDoS-атак на рівні додатків, метою яких є перевантажити сервер додатків.

- Content Delivery Network (CDN). Прискорює продуктивність додатків за рахунок оптимізації контенту сайту та кешування контенту в точках доступу по всьому світу.

- Управління трафіком, яке генерується ботами (хорошими або поганими), зокрема, запобігання:
  - Веб-скрапінг – автоматичне зчитування вмісту сторінки, наприклад, цін, продуктів тощо.
  - Спаму – розміщення значної кількості марних даних.
  - Кардингу та злому карток – різні зловживання, пов'язані з кредитними картками.
  - Перевантаження сервера та відсутності контролю над поведінкою клієнтів.

- Захист ідентифікаторів клієнтів компанії, виявлення та нейтралізація атак, спрямованих на захоплення облікових записів клієнтів (Account Takeover attacks).

- Захист та контроль середовища браузера, керування кодом, який виконується на стороні браузера та зниження ризику перехоплення даних на стороні браузера (наприклад, атак Magecert).

- Захист API від зловживань, зокрема:
  - API Discovery — сканування (навчання) API.
  - Забезпечення захисту за допомогою застосування позитивної моделі безпеки.
  - Сканування самих інтерфейсів на предмет виявлення їх слабких місць.
  - Видимість конфіденційних даних, що надаються API.

**Ключові особливості рішення:**

- Захист програм доступний на всіх рівнях: у хмарі, локально та на рівні застосунку.
- Можливість застосування позитивної та негативної моделі безпеки.
- Для хмарного сервісу мережа з більш ніж 60 точок доступу розповсюджена по всьому світу.
- Динамічне використання репутаційної інформації, зібраної Imperva.
- Гнучке ліцензування всіх компонентів.
- Рішення, створене з урахуванням низької сукупної вартості володіння.
- Команда SOC працює 24/7/365.

## Edge/Network Security:

Сфера Edge/Захист мережі зосереджена навколо проблеми DDoS-атак. Атаки можуть здійснюватися на різних мережевих рівнях та на різних протоколах додатків. Imperva пропонує чотири основних продукти у своєму портфоліо, які захищають цілі центри обробки даних (мережевий захист від DDoS), окремі сервери (окремий IP-захист від DDoS), веб-додатки (захист веб-додатків від DDoS) та DNS-сервери (DNS) DDoS-захист).

imperva
a Thales company

SOFTPROM

## Основні варіанти використання:

- Захист мереж від DDoS-атак. Це об'ємні атаки, часто розподілені, спрямовані на перевантаження мережної інфраструктури й, як наслідок, блокування доступу до серверів додатків.

- Захист веб-застосунків від DDoS-атак. Маються на увазі атаки на додатки, які прагнуть перевантажити сам сервер додатків, надіславши надмірну кількість запитів до додатків. Наслідком успішної такої атаки є блокування доступу до серверів додатків.

## Ключові особливості рішення:

- Мережа з більш ніж 60 центрів очищення трафіку розкидана по всьому світу (https://www.imperva.com/products/global-network-map/).
- 3-секундний SLA для нейтралізації атаки.
- SLA угода про рівень обслуговування для 100% доступності сервісів при правильному налаштуванні послуги.
- Команда SOC працює 24/7/365.

---

***SOFTPROM — IT ДИСТРИБ'ЮТОР З ДОДАНОЮ ЦІННІСТЮ***
*Софтпром — провідний IT-дистриб'ютор на ринках СНД та Східної Європи, якому довіряють понад 1200 партнерів. Компанія була заснована у 1999 році й сьогодні представлена більш ніж у 30 країнах світу.*

***НАША МІСІЯ***
*Підвищення ефективності роботи клієнтів за рахунок надання високоякісних IT-рішень та послуг.*