

Cloudflare WAF

WAF для захисту сучасних додатків

Проблеми безпеки додатків

Додатки є критично важливими для бізнесу, тому вони постійно стають об'єктами атак зловмисників, що призводить до зростання проблем з безпекою в організаціях.

Занепокоєння охоплюють широкий спектр питань: від захисту від нових експлойтів нульового дня, виявлення спроб обходу захисту, зменшення ризику використання вкрадених облікових даних, що призводить до захоплення акаунтів, до виявлення витоків даних та навіть сканування завантаження шкідливого програмного забезпечення у застосунки.

Ці занепокоєння поєднуються з необхідністю забезпечити, щоб захист застосунків був частиною ширшої, уніфікованої стратегії безпеки, яка також захищає API, зупиняє ботів і знижує ризики на стороні клієнта. Усе це має відбуватися без зайвого навантаження на команди управління.



Cloudflare WAF

Вебфайрвол Cloudflare (WAF) є наріжним каменем нашого портфоліо передових рішень для захисту застосунків, що забезпечує їх безпеку та продуктивність. Тільки WAF від Cloudflare надає повну видимість безпеки, забезпечує багаторівневий захист від атак OWASP і нових експлойтів, виявляє обходи та нові атаки за допомогою машинного навчання, блокує захоплення облікових записів, виявляє витоків даних тощо, легко інтегруючись у ширші робочі процеси корпоративної безпеки. Наші потужні можливості захисту застосунків, такі як безпека API та управління ботами, повністю інтегровані з нашим WAF, використовуючи ту саму потужну систему правил, яка працює на одній із найбільш підключених глобальних хмарних платформ у світі.



Видимість та виявлення атак

Ми пропонуємо диференційовану аналітику безпеки для візуалізації всього трафіку, незалежно від того, чи він захищений, чи ні. Вона інформує команди безпеки про невідомі атаки та засоби захисту, які вони повинні створити. Він відображає оцінки атак WAF, оцінки ботів та аналітику сканування контенту.



Швидкий захист від нових атак

Зі щорічною появою десятків тисяч вразливостей наш WAF оперативно впроваджує нові керовані правила, які блокують експлойти нововиявлених (нульового дня) вразливостей. Ці правила ефективно нейтралізують загрози та підкріплюються оцінками атак, створеними на основі машинного навчання, що дозволяє виявляти спроби обходу захисту.



Перша десятка загроз OWASP

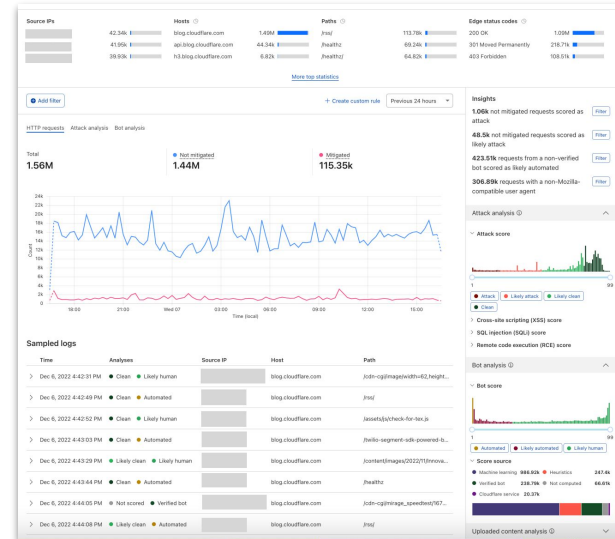
Атаки вимагають багаторівневого захисту, в тому числі від відомих типів атак з першої десятки списку OWASP.

Наш базовий набір правил OWASP регулярно оновлюється і розроблений таким чином, щоб працювати як єдине ціле для оцінки загрози і виконання дій на основі цієї оцінки. Цей набір правил можна конфігурувати відповідно до вимог безпеки та ризиків.

Чому брандмауер вебдодатків Cloudflare

- **Cloudflare захищає ефективніше.** Ми забезпечуємо більш ефективний захист WAF за допомогою багаторівневого захисту:
 - Аналітика безпеки
 - Кілька керованих наборів правил
 - Кастомні правила
 - Виявлення за допомогою машинного навчання
 - Виявлення чутливих даних
 - Перевірка вкрадених облікових даних
 - Розширене обмеження швидкості
 - Сканування завантаження шкідливого програмного забезпечення
- **Cloudflare реагує швидше.** Ми швидше захищаємо від експлоїтів. Для основних вразливостей, таких як Log4j, ми створили кілька керованих правил на один робочий день швидше, ніж інші постачальники WAF.
- **Cloudflare забезпечує комплексну інтеграцію захисту застосунків.** Наш WAF органічно поєднаний з іншими елементами портфоліо захисту, зокрема безпекою API та управлінням ботами. Усі ці функції реалізуються в єдиному рішенні, яке працює на одній із найбільш глобальних хмарних платформ світу.

Аналітика безпеки WAF



WAF для безпеки підприємства

Інтегрований з SIEM, готовий до SOC

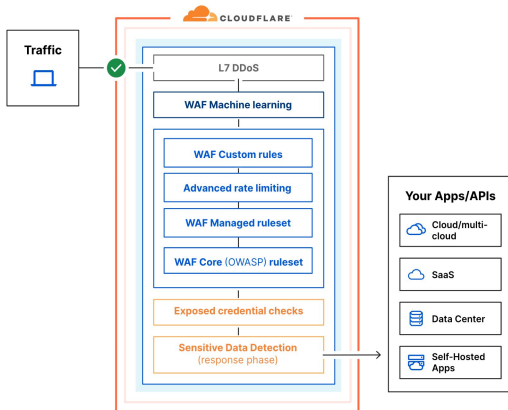
Завдяки API Cloudflare та інтеграції необроблених журналів можна легко інтегруватися з SIEM або забезпечити роботу операційного центру безпеки (SOC) за допомогою аналітики, наданої Cloudflare.

DevSecOps стало простіше

Наша готова інтеграція з Terraform значно спрощує впровадження захисту застосунків у підході DevOps.

За підтримки Cloudforce One

Система безпеки додатків Cloudflare отримує дані про загрози від Cloudforce One, нашої команди по боротьбі із загрозами, блокуючи загрози за допомогою нових виявлень, заснованих на нових даних і TTP.



Лідерство Cloudflare

Організації отримують більш ефективний рівень безпеки застосунків, використовуючи глобальну мережу Cloudflare як корпоративний периметр безпеки. Портфоліо захисту застосунків Cloudflare здобуло визнання за свою потужність та широкий функціонал. Gartner визнала Cloudflare лідером у 2022 році в Magic Quadrant™ для захисту вебзастосунків і API (WAAP). Компанію також відзначено як лідера в The Forrester Wave™ для WAF. WAF від Cloudflare отримав нагороду "Вибір клієнтів 2022" за версією Gartner. Frost & Sullivan відзначила Cloudflare як інноваційного лідера у сфері глобального комплексного захисту веб-застосунків у 2020 році, а IDC та Forrester назвали компанію лідером у захисті від DDoS-атак у 2021 році.



Безпека вебдодатків

Багаторівневий захист за допомогою декількох наборів правил WAF.	<p>Зупиняє шкідливі дані в будь-якому компоненті запиту за допомогою кількох наборів правил:</p> <ol style="list-style-type: none"> 1. Правила, які управляються Cloudflare. 2. Базовий набір правил OWASP. 3. Користувацькі набори правил для зупинки будь-якої атаки. <p>Нові керовані правила протестовані на величезних обсягах трафіку, щоб гарантувати мінімальну кількість помилкових спрацьовувань.</p>
Оновлені правила для захисту від нульового дня	<p>Правила постійно оновлюються командами безпеки Cloudflare для захисту від нових атак та експлоїтів вразливостей нульового дня до того, як будуть доступні патчі або оновлення.</p>
Виявлення за допомогою машинного навчання	<p>Зупиняйте спроби обходу за допомогою моделей машинного навчання, які доповнюють багаторівневі набори правил. Для правил доступні чотири різні оцінки атак: загальна оцінка WAF-атаки, оцінка XSS-атаки, оцінка SQLi-атаки, оцінка RCE-атаки.</p>
Набори правил для основних платформ CMS та електронної комерції, орієнтованих на конкретну платформу	<p>Отримуйте готовий захист без додаткових витрат для платформ, таких як WordPress, Joomla, Plone, Drupal, Magento, IIS та інших.</p>
Спеціальна конфігурація правил	<p>Під час розгортання правил або наборів правил виберіть один з варіантів: «Дозволити», «Блокувати», «Керована перевірка», «JS-перевірка», «Пропустити», «Залогувати», «Показати капчу» та «Користувацькі відповіді».</p>
Розширене обмеження швидкості	<p>Зупиняйте зловживання, DDoS-атаки та спроби перебору паролів, обмежуючи швидкість для IP-адрес, атрибутів заголовків (ключі, cookie, токени), ASN або країн.</p>
Канали розвідки загроз	<p>Блокуйте з'єднання з IP-адрес відомих відкритих SOCKS-проксі-серверів, VPN, бот-мереж, командних серверів, джерел шкідливого програмного забезпечення та анонімайзерів.</p>
Виявлення чутливих даних	<p>Виявлення відповідей, що містять конфіденційні дані, такі як персональні дані, фінансова інформація, номери кредитних карток або секретні дані, такі як ключі API.</p>
Відкриті перевірки облікових даних	<p>Виявляйте атаки перебору паролів із використанням викрадених облікових даних до захоплення акаунтів користувачів.</p>
Сканування завантаження контенту	<p>Сканування вмісту WAF перевіряє завантажені файли на наявність шкідливого програмного забезпечення. Пом'якшення наслідків здійснюється за допомогою користувацьких правил WAF.</p>
SSL/TLS	<p>Повністю розвантажте та налаштуйте SSL-трафік для вашої програми.</p>
Менше хибних спрацьовувань	<p>Нові правила були протестовані на величезних обсягах трафіку, щоб забезпечити найменшу кількість помилкових спрацьовувань.</p>
Підтримка gRPC та WebSocket	<p>Проксі та захист трафіку для кінцевих точок gRPC та WebSocket.</p>
Налаштовувані сторінки блоків	<p>Налаштовуйте сторінки блокування з відповідними деталями для відвідувачів.</p>
Повна інтеграція з більш широким набором продуктів Cloudflare	<p>Покращуйте продуктивність застосунків, спрямовуйте трафік за географічним принципом і використовуйте переваги периферійних обчислень.</p>

Видимість, звітність та програмованість

Аналітика безпеки	Візуалізація всіх потенційних атак з оцінкою машинного навчання.
Ведення журналу в реальному часі та доступ до необроблених лог-файлів	Отримуйте повну видимість для точного налаштування WAF; проводьте детальний аналіз усіх запитів до WAF.
Логуювання корисного навантаження	Реєструйте та шифруйте шкідливе навантаження для аналізу інцидентів.
Інтеграції SIEM	Завантажуйте журнали безпосередньо в існуючий SIEM.
Інтеграція з Terraform	Впроваджуйте безпеку додатків у робочі процеси CI/CD.

Управління

Керування з єдиної консолі	Оптимізоване управління за допомогою єдиної консолі для розгортання та управління глобальною безпекою та продуктивністю додатків.
Управління на рівні облікового запису	Заощаджуйте час на керування WAF завдяки єдиній конфігурації WAF на рівні облікового запису для всіх доменів.
Висока доступність з SLA	100% гарантія безвідмовної роботи, включаючи фінансові штрафи за порушення SLA
Немає необхідності в обладнанні, ПЗ або налаштуванні	Розгортання за допомогою простої зміни DNS
Сертифікація PCI	Cloudflare має сертифікацію постачальника послуг 1-го рівня
Авторизований FedRAMP	Наш набір рішень Cloudflare для уряду має захист застосунків та авторизацію FedRAMP.

iIT Distribution є офіційним Value Added дистриб'ютором, який постійно розвивається у сфері проєктної дистрибуції складних B2B рішень в Україні, Польщі та країнах Балтії. Ми представляємо програмні рішення від провідних світових постачальників. Наша місія полягає в тому, щоб забезпечити організації будь-якого розміру сучасними можливостями IT-інфраструктури, забезпечуючи їхній захист відпереважаючих загроз інформаційної безпеки.

E-mail: sales.ua@iitd.io | **Більше інформації на сайті:** <https://iitd.ua/>

