Engineer

Побудувала ліміти запитів і захист від зловживань

Побудувала засоби протидії зловживанням за принципом fail-closed — 22 обмежувачі частоти на Redis, Cloudflare Turnstile, ідемпотентність запитів та прив'язку до origin — щоб платформа відсікала ботів і напливи, а не довіряла тим, хто її викликає.

2025

22

обмежувачів частоти, які в разі збою блокують доступ

Ситуація. Публічний каталог компаній і фахівців стає мішенню того самого дня, коли запускається. Скраперам потрібні дані, спам-акаунтам — охоплення, а ендпоінтом, обслуговування якого коштує платформі реальних грошей, — пошук, експорт, усе, що звертається до зовнішнього API, — варто зловживати вже тому, що викликати його нічого не коштує. Ніхто з них не має злого наміру саме щодо цієї платформи; це просто звичайна погода у відкритому інтернеті.

Завдання. Для дорогих і вразливих до зловживань шляхів потрібні були обмеження, які витримують тиск, зокрема й тоді, коли недоступна залежність самого обмежувача.

Дія. Обмежувачів частоти запитів тут 22, і кожен налаштований під той шлях, який захищає, а не один глобальний ліміт на все, бо спроба входу, пошук і масовий експорт стають зловживанням за дуже різної частоти. Стан зберігається в Redis, тож ліміт спільний для всіх інстансів, а не окремий у кожному процесі, де його легко обійти. Найважливіше рішення — що відбувається, коли Redis недоступний: обмежувачі закриваються (fail closed). Трафік відхиляють, а не пропускають не дивлячись, — це менш зручна відповідь, зате єдина, яку можна обґрунтувати. Доповнюють їх Cloudflare Turnstile на шляхах, де варто перевіряти відвідувача, 351 рядок проміжного

шару ідемпотентності, щоб повторений запис не перетворився на два, блокування за origin, що відкидає запити, які прийшли не через парадні двері, і власна перевірка відвідувачів (challenge) на самому каталозі.

Результат. Зловживати тепер дорого для зловмисника й дешево для платформи, а збій у власному сховищі обмежувача обертається відмовою, а не відчиненими дверима. Так, закриття при збої означає, що проблема з Redis стає видимою для користувачів, — це прийнято свідомо, бо інакше проблема з Redis стала б проблемою з рахунками.

Застосуйте цей досвід у своєму проєкті

Використайте «Побудувала ліміти запитів і захист від зловживань» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Та частина, якої користувач не бачить: де зберігаються дані, які діють правила і як інші системи можуть із нею взаємодіяти.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Побудувала ліміти запитів і захист від зловживань — 22 обмежувачів частоти, які в разі збою блокують доступ

Переглянути наші послуги Зв'язатися з нами →

Боти та скрапери не дають спокою?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з безпеки. Тут задіяні Backend-розробка, API та інтеграції, Надійність і резервне копіювання, Мережі та VPN, Безпека та Оптимізація продуктивності. І, до речі, ми добре вміємо Backend- та API-розробка, Надійність та моніторинг (SRE), Безпека та керування доступом та Безпека ШІ-агентів.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть робочий процес, наявні інтерфейси та користувачів, яким потрібна зміна. Ми можемо визначити перевірюваний результат і спосіб передачі, який дасть вашій команді змогу підтримувати його.

Дивитися, скільки це коштує Зв'язатися з нами →

Боти та скрапери не дають спокою?

Запитайте про рішення в роботі «Побудувала ліміти запитів і захист від зловживань». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/portfolio/built-fail-closed-rate-limiting-and-anti-abuse/