RATE LIMIT

gocache
your apps safe.
your audience happy.

Rate Limit

Bloqueie IPs que fazem uso abusivo de sua aplicação

Estima-se que um terço do tráfego da internet é automatizado. Parte considerável deste tráfego pode mirar sua aplicação com propósitos de encontrar vulnerabilidades, roubar conteúdo, roubar credenciais, tirá-las do ar ou simplesmente buscam usá-la de forma legítima, porém em um ritmo que causa danos à sua sustentação.

Com o Rate Limit da GoCache você tem uma poderosa ferramenta para mitigar o impacto de atividades que geram grandes volumes de requisições, a partir de regras granulares o suficiente para evitar falsos positivos.

Bloqueie acessos volumétrico que podem gerar indisponibilidades e comprometer sua operação digital

Principais casos de uso

Com o Rate Limit da GoCache você conta com uma ferramenta que te permite desenvolver estratégias proteção contra ataques como:

Mitigação de DDoS na camada de aplicação

Ataques DDoS na camada de aplicação obrigatoriamente precisam enviar uma quantidade excessiva de requisições. Você pode criar regras que bloqueiam IPs que apresentem uma taxa excessiva de requisições, atenuando os efeito do ataque.

Proteção de APIs contra mal uso

Alguns usuários de suas APIs podem enviar uma taxa de requisições que exija um consumo excessivo de recursos, aumentando o risco de impactar outros clientes por instabilidade e indisponibilidade. Você pode criar regras que ajudam a manter o tráfego dentro do limite que cada API suporta.

Credential Stuffing

Credential Stuffing testam diversas combinações de credenciais para encontrar valores válidos, de forma que possam invadir contas de usuários para realizar ações criminosas. Você pode limitar taxas específicas para áreas de login.

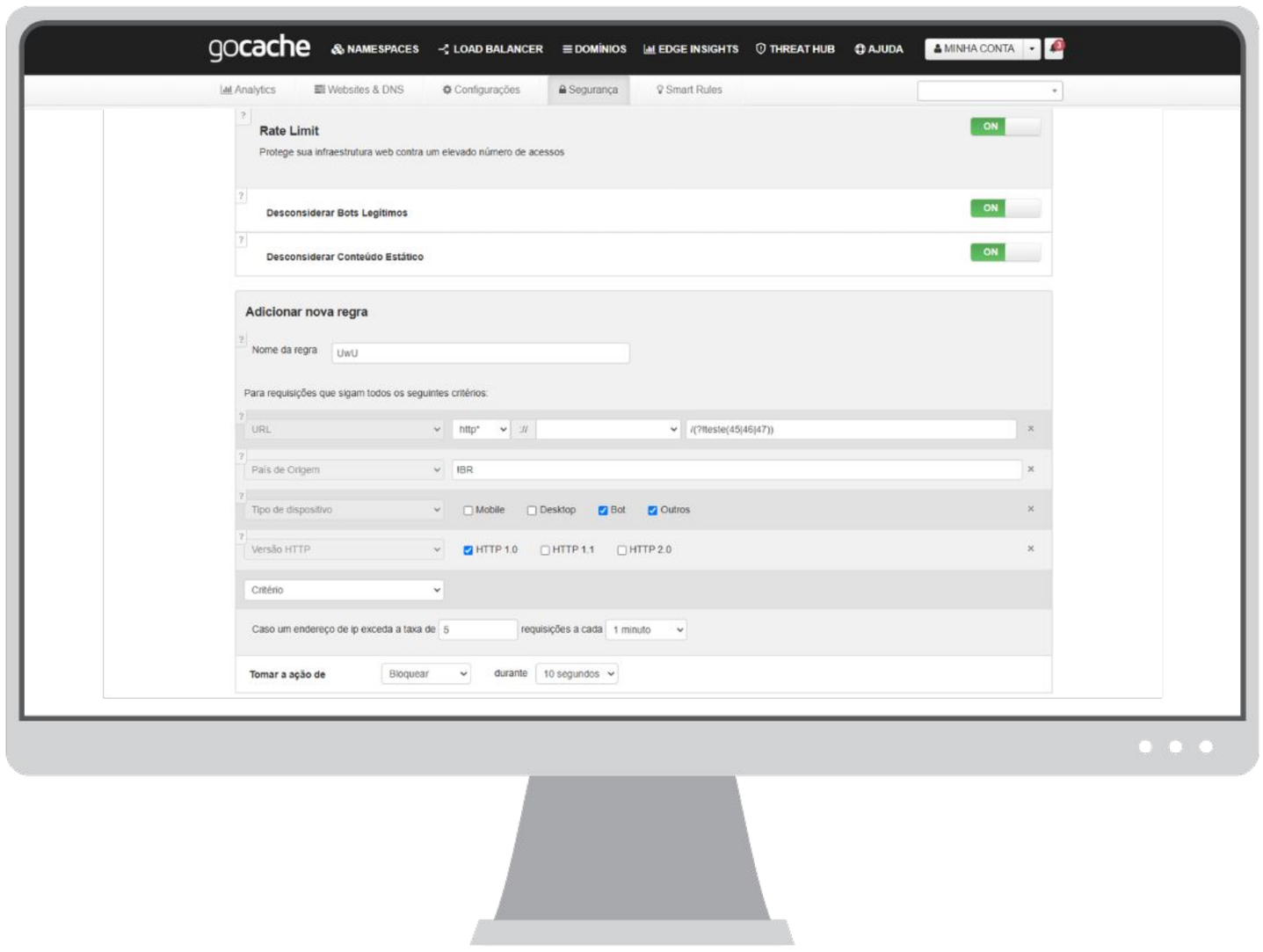
Proteção contra scraping

Concorrentes podem estar de olho em seu conteúdo mesmo que seu negócio não seja mídia. Por exemplo, catálogos de produtos são difíceis de enriquecer, sendo atrativo buscar as informações no vizinho. Você pode limitar a taxa de visualização desse conteúdo.

Como funciona

Flexibilidade para criação de regras

Combine múltiplos critérios e uso de regex em cada regra para criar uma estratégia efetiva de proteção.



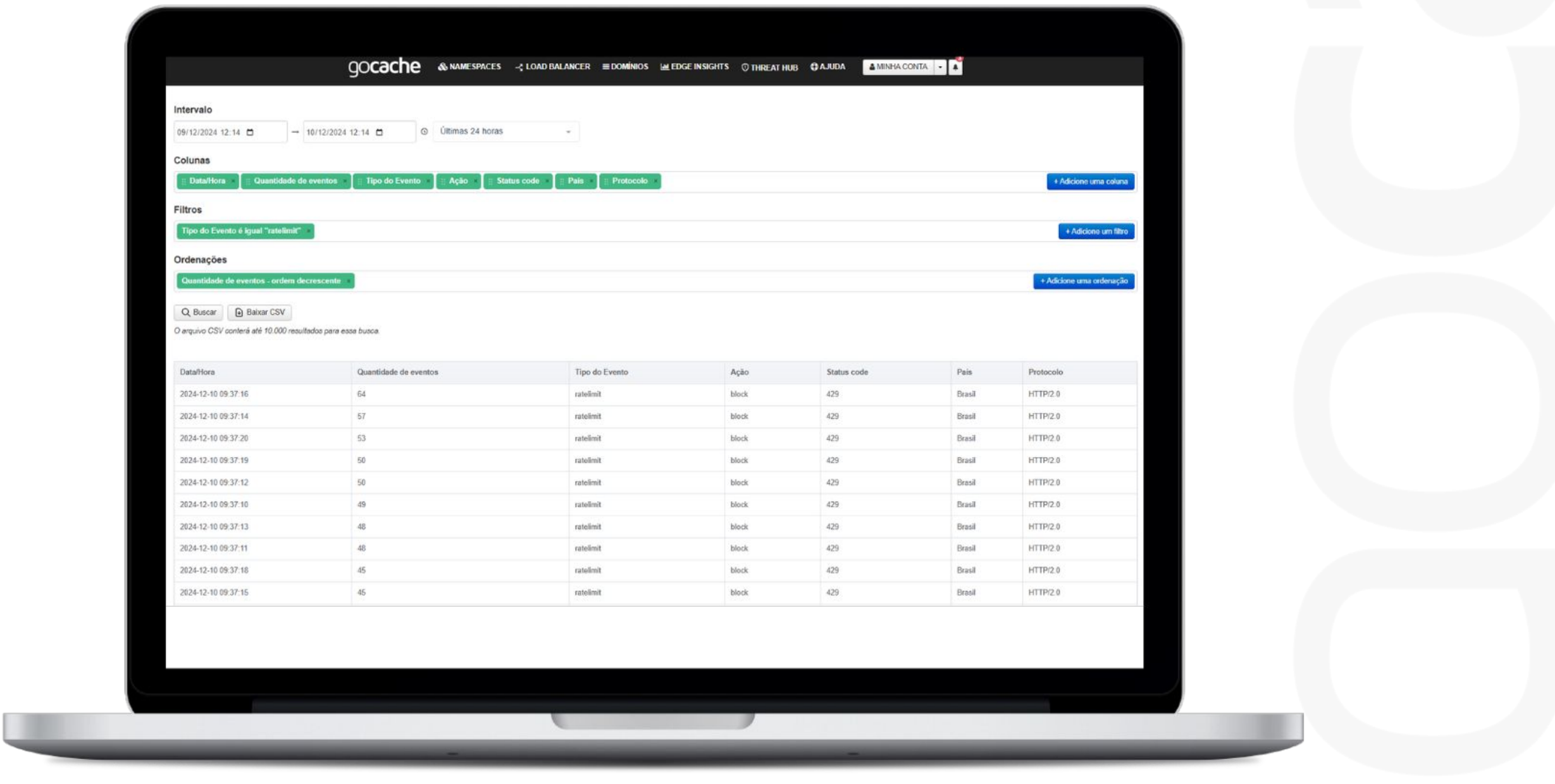
Múltiplas opções de ação

Você pode escolher se bloqueia, desafia ou apenas gera logs para cada regra criada

Análise sobre diferentes recortes

Você pode escolher se bloqueia, desafia ou apenas gera logs para cada regra criada

Analise os resultados do Rate Limit, seja dentro de um recorte gerencial ou de operações através do Analytics, Edge Insights, Threat Hub, ou integrando com um SIEM de sua preferência



Bloqueie, desafie e monitore, transformando dados em decisões estratégicas

gocache