RESUMO DO PRODUTO DA AKAMAI

# Content Protector

**Proteja sua receita contra ataques de scraper cada vez mais sofisticados**

Quando seu conteúdo é copiado, os invasores ganham e você perde dinheiro. Embora compartilhar conteúdo publicamente seja uma escolha estratégica, é fundamental diferenciar entre o envolvimento do consumidor e as atividades de captura prejudiciais. Concorrentes e invasores podem explorar dados extraídos, minando sua estratégia de preços e prejudicando seus clientes. O Akamai Content Protector identifica e interrompe rapidamente os scrapers, usando detecções adaptadas às ferramentas e técnicas exclusivas de ataques de scraper. Proteja sua empresa e sua receita sem comprometer a velocidade e o desempenho.

Ataques de scraping representam um desafio contínuo para as empresas on-line. Ao contrário das ameaças virtuais típicas que têm pontos de início e término claros, os scrapers podem acessar persistentemente seu site, levando a implicações significativas se não forem interrompidos. Isso inclui:

- **Impacto no desempenho do site:** atividades de scraping persistentes podem tornar seu site mais lento, levando à frustração do usuário e a taxas de conversão reduzidas.
- **Desvantagens competitivas:** os concorrentes podem usar o scraping para monitorar e reduzir seus preços, afetando sua receita.
- **Riscos à reputação:** os contraventores podem usar indevidamente o conteúdo roubado, vendendo produtos falsos com o nome da sua marca.

Esse tipo de ataque existe há vários anos. Mas por que estão piores agora? A urgência de combater scrapers se intensificou recentemente. Os acontecimentos de 2020, incluindo a pandemia e as subsequentes perturbações da cadeia de abastecimento, aumentaram os incentivos financeiros para esse tipo de ataque. Itens de alta demanda, que vão de itens essenciais do dia a dia até produtos de luxo e serviços de viagem, tornaram-se alvos principais para operações sofisticadas de scraping.

Com mais dinheiro em potencial a ser obtido, os operadores de bots começaram a inovar de forma febril, especializando-se em ferramentas (como telemetria) e, em seguida, encadeando-as com ferramentas feitas por outros operadores de bots para criar bots altamente especializados, inéditos em ataques de scraping. Isso torna os scrapers mais perigosos e difíceis de detectar. E, pior ainda, o scraping também pode ocorrer usando outros métodos, como plug-ins, portanto, você precisa de mais do que o gerenciamento de bots para interromper esse tipo de atividade.

Mas você não pode simplesmente bloquear todos os scrapers: os bots de pesquisa procuram conteúdo que você pode querer mostrar em pesquisas públicas, alguns bots de compras para consumidores podem destacar seus produtos em sites de comparação, e os parceiros podem reunir com eficiência as informações mais recentes sobre os produtos para compartilhar com seus clientes.

## BENEFÍCIOS PARA A SUA EMPRESA

**Aumente as taxas de conversão**
Remova os bots que desaceleram seu site e suas aplicações, mantendo mais clientes na página e melhorando as vendas

**Reduza os custos**
Não pague pelo tráfego de bots

**Frustre os falsificadores**
Impeça que os scrapers façam ping em seu site para ver quando o estoque fica disponível, reduzindo a capacidade dos operadores de bots de chegar à próxima etapa em uma cadeia de ataque de acúmulo de estoque

**Frustre os concorrentes**
Interrompa o scraping automatizado que permite que seus concorrentes cubram seus preços e reduzam suas vendas

**Reduza a falsificação**
Impeça que agentes roubem seu conteúdo e se passem por você

**Melhore suas vendas**
Remova o tráfego de bots da análise do site para garantir que você esteja otimizando para usuários reais

Akamai

O Akamai Content Protector tem detecções projetadas exclusivamente para detectar scrapers e interrompê-los. E isso é feito enquanto aproveita a visibilidade da rede Akamai, nossa força global no gerenciamento de bots e no desenvolvimento contínuo de detecções de ponta. Ao atualizarmos sua proteção à medida que as ameaças evoluem, incorporamos automaticamente insights de nossos cientistas de dados e pesquisadores de inteligência contra ameaças, de modo que o Content Protector continua a liderar detecções personalizadas para scrapers.

Depois de parar os scrapers, você pode se concentrar em aproveitar ao máximo sua presença digital, melhorando o desempenho do site e as taxas de conversão e reduzindo o impacto dos concorrentes.

## Principais recursos

- **Detecções:** um conjunto de métodos de detecção com ML que avalia os dados coletados no lado do cliente e no lado do servidor.
  - » **Avaliação no nível do protocolo:** a impressão digital do protocolo avalia como o cliente estabelece a conexão com o servidor nas diferentes camadas do modelo OSI: TCP, TLS e HTTP, verificando se os parâmetros negociados estão alinhados com os esperados dos navegadores web e aplicações móveis mais comuns.
  - » **Avaliação no nível da aplicação:** avalia se o cliente pode executar alguma lógica empresarial escrita em JavaScript. Quando o cliente executa JavaScript, o Content Protector coleta as características dos dispositivos e navegadores e as preferências dos usuários (impressão digital). Esses vários pontos de dados são comparados e verificados em relação aos dados no nível do protocolo para verificar a consistência.
  - » **Interação do usuário:** as métricas comportamentais avaliam se um ser humano interage com o cliente por meio de periféricos padrão, como tela de toque, teclado e mouse. A falta de interação ou interação anormal geralmente está associada ao tráfego de bots.
  - » **Comportamento do usuário:** analisa a jornada do usuário pelo website. As botnets geralmente vão atrás de conteúdos específicos, resultando em um comportamento significativamente diferente do tráfego legítimo.
  - » **Detecção de navegadores sem interface:** um JavaScript personalizado em execução do lado do cliente procurando indicadores deixados para trás por navegadores sem interface, mesmo quando em execução no modo furtivo.
- **Classificação de risco:** fornece uma classificação determinística e prática quanto ao risco baixo, médio ou alto do tráfego com base nas anomalias encontradas durante a avaliação.
- **Ações de resposta:** um conjunto de estratégias de resposta, incluindo a simples ação monitorar e negar, e outras mais avançadas, como o tarpit, que simula um servidor suspenso ou vários tipos de ações de desafio. Os desafios de criptografia geralmente são mais fáceis de usar do que os desafios de CAPTCHA para lidar com possíveis falsos positivos.

**A base do Content Protector: o ecossistema da Akamai**

A Akamai torna a Internet rápida, inteligente e segura. Nossas soluções abrangentes são baseadas na globalmente distribuída Akamai Connected Cloud, gerenciadas pelo unificado e personalizável Akamai Control Center para oferecer visibilidade e controle e contam com o suporte de especialistas de serviços profissionais, que colocam seus negócios em pleno funcionamento rapidamente e inspiram inovações, à medida que as suas estratégias evoluem.

Inscreva-se para uma demonstração ou fale com o time de vendas da Akamai.