Dez principais considerações sobre o gerenciamento de bots

e-book

ÍNDICE

Introdução		03
1.	Conhecimento sofisticado	04
2.	Inteligência	05
3.	Proteção resiliente	06
4.	Falsos positivos e negativos	07
5.	Ações flexíveis	08
6.	Implantação	09
7.	Visibilidade e geração de relatórios	10
8.	Proteção de APIs	11
9.	Website x página	12
10.	Serviços gerenciados	13

Introdução

Quer saber quão difícil o problema dos bots se tornou? Tente comprar um ingresso para Taylor Swift ou um novo par de Air Jordans. E esses são apenas grandes eventos. Os bots estão se tornando cada vez mais difundidos e perniciosos em todos os setores.

E o pior para quem procura respostas é que o jogo de gerenciamento de bots mudou. Na verdade, sempre esteve mudando. O gerenciamento de bots é frequentemente descrito como uma corrida armamentista ou um jogo de gato e rato, com empresas erguendo defesas e criadores de bots continuando a encontrar maneiras de contorná-las. Mas agora não são apenas os próprios bots que estão evoluindo. O ambiente ao seu redor também está evoluindo. Por exemplo, as empresas já não lidam apenas com agentes individuais, nem mesmo com grupos coordenados. Hoje é possível alugar um bot por uma semana, como você faria com um Airbnb. Da mesma forma, as soluções não podem simplesmente segmentar os bots em categorias de bons e ruins. Há muitas áreas nebulosas atualmente.

Essa evolução dos bots e do ambiente ao seu redor tornou a tarefa de selecionar um software de gerenciamento de bots mais difícil do que nunca. Você precisa não apenas determinar o que foi eficaz contra os bots de ontem, mas também o que será eficaz contra os bots de hoje e de amanhã.

Este guia descreve algumas das principais considerações para compradores que escolhem um software de gerenciamento de bots. Use-o para ajudar você a manter o foco e tomar uma decisão de compra informada.

1 Conhecimento sofisticado

As soluções de gerenciamento de bots, por definição, detectam bots. Em outras palavras, elas procuram sinais de automação e outros indicadores de que o solicitante não é humano. No entanto, à medida que os bots evoluíram e se tornaram mais sofisticados, também se tornaram mais especializados. Os bots agora são projetados para fins específicos, como extrair conteúdo de seu website, acumular seu inventário durante grandes eventos e preencher credenciais para assumir o controle de contas de clientes, entre outros casos de uso. E muitas vezes, as detecções para um tipo de bot especializado não detectam outros. Você precisa saber se o fornecedor pode impedir os bots específicos que você está enfrentando, não apenas os bots básicos e de uso geral.

Considerações:

- O fornecedor possui detecções especializadas para bots com base em casos de uso de negócios?
- O fornecedor pode demonstrar sua experiência no problema específico do bot que você enfrenta?
- Quantos dos outros clientes do fornecedor estão enfrentando os mesmos problemas? Você se beneficiará com o que o fornecedor aprendeu com esses clientes?
- O provedor oferece relatórios, serviços ou outros recursos para suportar ainda mais sua batalha contra bots adversários e especializados?

2 Inteligência

A eficácia de uma solução de gerenciamento de bots depende da sua capacidade de reconhecer as características dos bots que está monitorando. Embora alguns fornecedores possam alegar a detecção de 99,9% dos bots, é impossível medir a eficácia da solução objetivamente. Os bots estão sempre mudando. Dessa maneira, o que você capturou ontem provavelmente aprendeu como escapar dessa detecção realizada hoje. Um critério melhor para avaliar as ferramentas de gerenciamento de bots é como o fornecedor informa sobre seus recursos de detecção de bots. Você precisa de uma solução que possa detectar os bots mais sofisticados (não apenas os suspeitos óbvios) e que consiga extraí-los do maior conjunto de dados. Muitas ferramentas de inteligência artificial (IA) e de aprendizado de máquina (ML) são de código aberto, portanto, a quantidade de dados, a limpeza dos dados e a velocidade com que a solução alimenta os algoritmos com os dados são uma consideração subestimada ao avaliar a IA/ML de uma solução. As informações devem incluir indicadores de confiança e pontuações de risco em cada login, em todos os domínios. Além disso, soluções eficazes devem adotar uma abordagem multifacetada para a detecção de bots usando os métodos mais recentes.

Considerações:

- Peça informações sobre como o fornecedor informa sobre seus recursos de detecção de bots. Os fornecedores com grandes clientes que são atraentes para os invasores terão mais experiência e conjuntos de dados mais abrangentes sobre os quais poderão desenvolver suas capacidades, incluindo quais sinais de risco e de confiança avaliar, mais detecções de anomalias de dispositivos, entre outros. A falta de transparência deve servir de alerta.
- O fornecedor usa IA/ML para oferecer suporte à solução? Qual é o nível de sofisticação dos modelos? E isso também é muito importante: quantos dados o fornecedor alimenta nesses modelos? Os invasores certamente estão usando IA. Você também deveria estar.
- No entanto, a IA não é suficiente. O fornecedor possui uma equipe de especialistas qualificados, como pesquisadores de segurança e analistas de inteligência contra ameaças, que procuram constantemente novas técnicas de ataque e monitoram comunidades de hackers para garantir que você esteja sempre um passo à frente?

3 Proteção resiliente

Quando você bloqueia um bot sofisticado, ele não vai embora permanentemente. Ele continua voltando e mudando, em uma tentativa de contornar suas detecções. Muitas soluções de gerenciamento de bots podem detectá-los (ou pelo menos alguns deles) inicialmente, mas depois os perdem quando eles começam a passar por mutações. A Akamai observou bots sofrerem mutações em questão de horas. Os ciclos de desenvolvimento tradicionais são lentos demais para acompanhar isso. A solução selecionada deve aprender e evoluir com o tempo, de preferência usando o aprendizado de máquina automaticamente. Isso deve incluir defesas preventivas, que dificultem para os invasores obter informações que usarão para escapar de suas defesas.

Considerações:

- Procure uma solução com as tecnologias mais sofisticadas de detecção de bots (como análise de comportamento do usuário e modelos de aprendizado específicos do cliente). Elas permanecerão eficazes por mais tempo, à medida que os bots passarem por mutações.
- Descubra se a solução inclui táticas defensivas, como ofuscação de JavaScript, o que torna mais difícil para os invasores fazerem a engenharia reversa de bots que podem escapar de suas defesas.
- Peça comprovações ou referências de outros clientes que implantaram a solução para ver se a solução permaneceu eficaz ao longo do tempo.

4 Falsos positivos e negativos

Quando uma solução de gerenciamento de bots mostra que bloqueou um bot, como você sabe que o sistema realmente bloqueou um bot e não um usuário legítimo? Muitos fornecedores são bem descuidados com os falsos positivos. Se eles não tiverem uma solução que avalie os bots em todas as detecções, poderão não conseguir detectar bots indefinidos, levando a decisões binárias de sim/não. E muitas vezes, esses fornecedores gostam de mostrar aos clientes que bloquearam muitos “bots”, mesmo que a taxa de falsos positivos seja alta. Isso significa que estão interrompendo os bots, mas também o tráfego válido, os humanos ou bots "bons" que são valiosos para sua empresa. Por outro lado, uma taxa baixa de falsos negativos parece ótima até você perceber que a taxa de falsos negativos é tão baixa porque o fornecedor teve que reduzir a eficácia geral da solução para garantir que ela não estava bloqueando usuários humanos, porém acaba deixando entrar os bots que não deveria. Você deseja bloquear bots mal-intencionados sem atrapalhar seus negócios, mas também não quer diminuir sua proteção. Você precisa confiar que o fornecedor com o qual está fazendo uma parceria se preocupa com a precisão e o impacto dos falsos positivos ou negativos.

Considerações:

- O fornecedor deixa você responsável pelo ajuste de falsos positivos e negativos ou investe em recursos e serviços para trabalhar em colaboração com você?
- A solução aprende com os padrões de tráfego nos websites e se ajusta automaticamente para reduzir a carga de sua equipe?
- O fornecedor sugere o uso de CAPTCHA em vez de outras ações de desafio? Muitas vezes, isso é o que entrega o jogo dele. Os usuários odeiam os CAPTCHAs, mas é mais fácil para um fornecedor oferecê-los que ajustar as regras para minimizar falsos positivos.
- Você pode visualizar por que a solução sinalizou uma solicitação como proveniente de um bot? Ou ela é uma caixa preta? Veja se é possível verificar as ações realizadas com visibilidade granular das solicitações e visualizar alterações nas suas configurações antes de colocá-las em produção.

5 Ações flexíveis

É tentador pensar que você só precisa se preocupar em bloquear bots mal-intencionados e deixar passar os bons. Mas o ambiente se tornou muito mais complexo do que isso. Muitos operadores de bots aprenderam como reduzir os sinais de risco o suficiente para colocar seus bots em uma área indefinida, sabendo que a maioria das organizações prefere arriscar e permitir a entrada de um bot mal-intencionado do que arriscar bloquear um usuário legítimo. Sua solução deve fornecer um conjunto de ações sofisticadas para que você possa ir além do bloqueio e permissão, e incluir também ações desafiadoras, como desafios criptográficos e autenticação multifatorial intensificada.
E sua solução também deve incluir ações para lidar com outros tipos de situações, como bots bons. Você pode querer desacelerar os bots parceiros durante horários de tráfego intenso e deixá-los passar imediatamente fora dos horários de pico. Você também pode escolher ações diferentes para bots na mesma categoria conhecida. Por exemplo, se você é um varejista, pode permitir que os bots de cupons mais populares verifiquem seu website, enquanto bloqueia aqueles com os quais você não deseja fazer negócios. Você precisa de flexibilidade para adotar diferentes ações para diferentes tipos de bots com base nos impactos que eles causam nos negócios e na TI, especialmente quando esses impactos variam com base na localização, na hora do dia ou na sazonalidade. Mais do que isso, você precisará de uma solução que não bloqueie simplesmente todos os bots (e, ao fazer isso, os ensine a mudar as táticas de evasão), mas que crie obstáculos, tornando-os mais difíceis e mais caros para os invasores.

Considerações:

- A solução permite que você crie diferentes categorias para diferentes tipos de bots, ou apenas os divide entre bons e ruins? Ela também consegue criar ações diferentes para bots da mesma categoria, como mecanismos de busca ou agregadores financeiros?
- A quais tipos de ações condicionais a solução oferece suporte? A solução oferece suporte a ações avançadas, como lentidão e entrega de conteúdo alternativo, que ajudam você a moldar melhor o tráfego? Inclui ações como um desafio criptográfico?
- Qual é a flexibilidade da solução para gerenciar os diferentes bots que você observa? Ela é padronizada ou pode aplicar ações cirurgicamente com base na hora do dia, por porcentagem de tráfego ou por URL?
- A solução pode inserir problemas que consomem muitos recursos, tornando-a mais cara para os operadores de bots e retardando ataques de alto volume de solicitações além de apenas um hard 403?

6 Implantação

Quando se trata de uma solução de gerenciamento de bots, o tempo que fornecedor leva para lançar a solução e com que rapidez você pode modificá-la devem ser considerações fundamentais. Os compradores devem ter cuidado com soluções que exijam modificação em aplicações existentes ou que afetem o desempenho das aplicações. Atrasos na implantação podem custar caro. Se você precisar fazer alterações em aplicações sempre que eventos de negócios exigirem, como vendas-relâmpago, isso exigirá mais recursos.

Considerações:

- A solução funciona em tempo real sem afetar o desempenho das aplicações existentes?
- Isso exige que você faça alterações em aplicações existentes?
- Ela pode ser ampliada ou reduzida para acomodar eventos imprevistos, como ataques volumétricos ou eventos esperados, como vendas-relâmpago?

7 Visibilidade e geração de relatórios

Todas as soluções de gerenciamento de bots podem mostrar estatísticas de alto nível sobre o tráfego de bots, mas você precisa de mais que isso. Para o planejamento da infraestrutura ou para a geração de relatórios da sua cadeia de gerenciamento, as estatísticas de alto nível são excelentes, mas não apresentam a granularidade necessária para analisar o tráfego de bots. Elas também não apresentam as provas de que você precisa para confiar que a solução realizou as ações certas. Quando se trata de uma solução que pode bloquear seus usuários, você não quer uma caixa preta. Você precisa de relatórios detalhados para apoiar seus negócios e ajudar você a entender melhor como as alterações nos limites de risco afetam o desempenho.

Considerações:

- A solução oferece recursos de geração de relatórios que permitem que você visualize em mais detalhes os bots específicos, as botnets ou as características dos bots? Ela pode relatar diferentes segmentos de pontuação, quais bots estão atacando quais endpoints e mostrar quais ações foram tomadas?
- Você pode investigar o pico de tráfego e analisar solicitações individuais? Às vezes, você precisa ver os detalhes das solicitações para saber o que fazer.
- A solução pode mostrar como o tráfego do seu bot se compara a outros no setor?
- Como os relatórios se relacionam aos das outras soluções de segurança? Você pode analisar seu tráfego de forma abrangente ou há visualizações separadas?

8 Proteção de APIs

Independentemente do fornecedor ou da solução, as tecnologias mais sofisticadas de detecção de bots disponíveis atualmente dependem da injeção de código JavaScript e da análise da resposta do cliente. Mas o que você faz com suas APIs quando os clientes baseados em API não respondem ao JavaScript? Se você precisa expor APIs para oferecer suporte a aplicações móveis ou outros terceiros, precisará de uma solução que possa ajudá-lo a proteger essas APIs assim como protege suas páginas da Web. Caso contrário, seus bots (e seus problemas de bots) simplesmente migrarão de suas páginas da Web para suas APIs.

Considerações:

- Que tipo de proteções o fornecedor oferece para APIs? Apenas o gerenciamento de cotas e a limitação de taxa?
- Procure uma funcionalidade móvel que possa incorporar as detecções de bot mais sofisticadas do fornecedor em suas aplicações móveis.
- Embora nem sempre seja tão eficaz quanto outras detecções ativas, uma abordagem baseada em reputação pode ser uma boa opção para proteger APIs que oferecem suporte a terceiros que podem não ter acesso a um SDK.

9 Website x página

Se o seu website for mais que somente uma página, você provavelmente sofrerá vários problemas de bots e cada um deles afetará partes diferentes de seu website. A captura de preços pode ter um grande impacto nas páginas dos produtos. A captura de conteúdo pode prejudicar o conteúdo digital de valor agregado. Enquanto isso, ataques de abuso de credenciais em suas páginas de login continuam acontecendo. Mas quando se trata de soluções de gerenciamento de bots, algumas são projetadas para abordar apenas um problema. A sua solução de gerenciamento deve ajudar você a resolver todos os seus problemas de bots, independentemente de eles afetarem todo o website ou apenas páginas específicas.

Considerações:

- Em que a solução se concentra: páginas individuais ou todo o website?
  Como ela é implantada: na frente de páginas individuais ou de todo o website?
- A solução pode ajudar você a resolver todos os problemas de bots, sejam eles abuso de credenciais, captura da Web ou agregação de conteúdo?

10 Serviços gerenciados

Você precisa gerenciar os bots para controlar os impactos deles sobre você e sua empresa, mas o gerenciamento de bots não é fácil. Embora você possa ter pessoal especializado em sua empresa, às vezes, você precisa de ajuda extra: você precisa de especialistas que entendam seus problemas de bots. Além disso, preencher esses cargos está se tornando cada vez mais difícil. O que acontece quando alguns dos seus talentos vão embora? Qualquer pessoa pode examinar uma solicitação HTTP e criar uma assinatura para bloquear o tráfego, mas isso não resolve o problema. O que você precisa é de alguém que possa relacionar os bots aos seus principais problemas, e projetar e implementar uma estratégia para resolver esses problemas.

Considerações:

- Você conta com pessoal especializado com conhecimento específico sobre bots necessário para aproveitar ao máximo qualquer solução?
- O fornecedor de gerenciamento de bots oferece serviços profissionais ou apenas vende produtos?
- Você tem acesso a monitoramento proativo e recursos especializados complementares em caso de emergência a qualquer momento?

Seja proativo, não reativo

Você se sairá melhor investindo no gerenciamento de bots antes que os bots se tornem um problema e antes que a próxima onda de evolução torne as defesas existentes uma fraca imitação do que eram antes. Leve essas informações em consideração ao pesquisar suas opções. O Akamai Bot Manager pode a fornecer as garantias que você precisa. Para saber mais, solicite um passo a passo personalizado de um ataque simulado.

Saiba mais

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções da Akamai para computação em nuvem, segurança e entrega de conteúdo em akamai.com e akamai.com/blog ou siga a Akamai Technologies no Twitter e no LinkedIn. Publicado em 09/23