# 10 considerazioni fondamentali sulla gestione dei bot

eBook

## SOMMARIO

# Introduzione

Vi state chiedendo quanto sia diventato difficile il problema dei bot? Provate ad acquistare un biglietto per Taylor Swift o un nuovo paio di Air Jordan. E questi sono solo eventi pubblicitari. I bot stanno diventando sempre più invasivi e dannosi in tutti i settori.

Ciò che è peggio per chi cerca risposte è che il gioco della gestione dei bot è cambiato. A dire il vero, è sempre stato in evoluzione. La gestione dei bot viene spesso descritta come una corsa agli armamenti, o un gioco tra gatto e topo, in cui le aziende implementano sistemi di difesa e i creatori di bot continuano a trovare modi per aggirarli. Ma ora non sono solo gli stessi bot a evolversi. Anche l'ambiente che li circonda si sta evolvendo. Ad esempio, le imprese non hanno più a che fare solo con singoli attori o anche con gruppi coordinati. Ora è possibile noleggiare un bot per una settimana, come con Airbnb. Allo stesso modo, le soluzioni non possono limitarsi a segmentare i bot in categorie di bot legittimi e dannosi. Oggi c'è una vera e propria zona grigia.

Questa evoluzione dei bot e dell'ambiente che li circonda ha reso il compito di selezionare il software di gestione dei bot più difficile che mai. È necessario determinare non solo cosa è stato efficace contro i bot di ieri, ma cosa sarà efficace contro quelli di oggi e di domani.

Questa guida delinea alcune delle considerazioni principali per la scelta di un software di gestione dei bot da acquistare. Usatela per orientarvi e prendere una decisione di acquisto informata.

# 1 Competenza sofisticata

Le soluzioni di gestione dei bot, per definizione, rilevano i bot. In altre parole, cercano segnali di automazione e altri indicatori che le richieste non provengano da un essere umano. Tuttavia, oltre a essersi evoluti e a essere diventati sempre più sofisticati, i bot sono diventati anche più specializzati. Oggi i bot vengono progettati per scopi mirati come lo scraping di contenuti dal vostro sito, il furto dell'inventario durante gli eventi pubblicitari e il credential stuffing per acquisire il controllo degli account dei vostri clienti, tra gli altri casi di utilizzo. E spesso ciò che rileva un tipo di bot specializzato non ne rileva altri. Dovete sapere se il fornitore è in grado di bloccare i bot specifici che vi riguardano, non solo i bot di base e generici.

**Considerazioni:**

- il fornitore dispone di sistemi di rilevamento specializzati per i bot basati su casi di utilizzo aziendale?
- Il fornitore può dimostrare la propria esperienza rispetto al vostro problema con bot specifici?
- Quanti altri clienti del fornitore stanno affrontando gli stessi problemi? Potete trarre vantaggio da ciò che il fornitore ha imparato da quei clienti?
- Il fornitore offre rapporti, servizi o altre funzionalità per supportare ulteriormente la vostra battaglia contro bot dannosi specializzati?

# 2 Intelligence

L'efficacia di una soluzione di gestione dei bot è proporzionale alla sua capacità di riconoscere le caratteristiche dei bot che sta monitorando. Anche se alcuni fornitori affermano di rilevare il 99,9% dei bot, è impossibile misurarne oggettivamente l'efficacia. I bot cambiano continuamente, quindi quelli rilevati ieri probabilmente hanno appreso come eludere il rilevamento oggi. Un criterio migliore per valutare gli strumenti di gestione dei bot è il modo in cui il fornitore aggiorna le proprie funzionalità di rilevamento dei bot. È necessaria una soluzione in grado di rilevare i bot più sofisticati (non solo i soliti sospetti) e di estrarre dal set di dati più grande disponibile. Tenete presente che molti strumenti di intelligenza artificiale (AI) e apprendimento automatico (ML) sono open source, quindi la quantità di dati, la pulizia dei dati e la velocità con cui la soluzione fornisce i dati agli algoritmi sono considerazioni sottovalutate quando si valuta l'AI/ML di una soluzione. Le informazioni dovrebbero includere indicatori di fiducia e punteggi di rischio per ogni accesso e per tutti i domini. Inoltre, soluzioni efficaci dovrebbero adottare un approccio su più fronti per il rilevamento dei bot, utilizzando i metodi più recenti.

**Considerazioni:**

- chiedete dettagli su come il fornitore aggiorna le proprie funzionalità di rilevamento dei bot. I fornitori con grandi clienti che attraggono i criminali disporranno di una maggiore esperienza e di set di dati più completi su cui sviluppare le proprie funzionalità, compresi i segnali di rischio e fiducia da valutare e più rilevamenti di anomalie dei dispositivi, tra gli altri. La mancanza di trasparenza dovrebbe essere un segnale.
- Il fornitore utilizza l'AI/ML per supportare la soluzione? Quanto sono sofisticati questi modelli? E, altrettanto importante: quanti dati inserisce il fornitore in questi modelli? Gli autori di attacchi utilizzano sicuramente l'AI. Dovreste farlo anche voi.
- Tuttavia, l'AI non basta. Il fornitore dispone di un team di esperti qualificati come ricercatori della sicurezza e analisti di intelligence sulle minacce che cercano costantemente nuove tecniche di attacco e monitorano le community di hacker per assicurarsi di essere sempre un passo avanti?

# 3 Protezione resiliente

Quando un bot sofisticato viene bloccato, in realtà non scompare in modo permanente, ma continua a presentarsi con forme sempre diverse nel tentativo di aggirare i vostri sistemi di rilevamento. Molte soluzioni sono in grado di rilevare i bot (o almeno alcuni di loro) in un primo momento, ma perdono efficacia quando questi iniziano a mutare. Akamai ha osservato i bot mutare nel giro di poche ore. I cicli di sviluppo tradizionali sono troppo lenti per stare al passo. Assicuratevi che la soluzione scelta apprenda e si evolva nel tempo, preferibilmente utilizzando automaticamente l'apprendimento automatico. Ciò dovrebbe includere funzioni di difesa preventive che rendano più difficile per i criminali ottenere informazioni che utilizzeranno per eludere le vostre difese.

**Considerazioni:**

- cercate una soluzione con le tecnologie di rilevamento dei bot più sofisticate (come l'analisi del comportamento degli utenti e modelli di apprendimento specifici del cliente). Queste rimarranno efficaci più a lungo nel tempo via via che i bot muteranno.
- Scoprite se la soluzione include tattiche difensive come l'offuscamento di JavaScript, che rende più difficile per i criminali decodificare i bot che riescono ad aggirare le vostre difese.
- Verificate con altri clienti che hanno già implementato la soluzione che quest'ultima mantenga la sua efficacia nel tempo.

# 4 Falsi positivi e falsi negativi

Quando una soluzione per la gestione dei bot indica di avere bloccato un bot, come potete avere la certezza di non aver effettivamente bloccato un utente legittimo? Molti fornitori ignorano volutamente i falsi positivi. Se non dispongono di una soluzione che assegni un punteggio ai bot rispetto a ogni rilevamento, potrebbero non essere in grado di rilevare i bot grigi, provocando decisioni binarie di tipo "sì/no". Spesso inoltre, tali fornitori preferiscono dimostrare ai clienti di aver bloccato un gran numero di "bot"," anche se il relativo tasso di falsi positivi è elevato, il che significa che stanno bloccando i bot ma anche traffico valido: utenti o bot "legittimi" che sono utili per la vostra azienda. D'altro canto, un tasso di falsi negativi basso sembra ottimo finché non ci si rende conto che è così basso perché il fornitore ha dovuto ridurre l'efficacia complessiva della soluzione per assicurarsi di non bloccare gli utenti, finendo per consentire l'accesso a bot a cui non dovrebbe consentirlo. Se desiderate bloccare i bot dannosi senza interferire con le attività aziendali e senza abbassare il livello di protezione, dovete accertarvi che il fornitore che state per scegliere come partner prenda sul serio aspetti come l'accuratezza e l'impatto dei falsi positivi e dei falsi negativi.

**Considerazioni:**

- Il fornitore lascia a voi l'incombenza di ottimizzare i falsi positivi/negativi o investe in funzionalità e servizi per collaborare con voi?
- La soluzione apprende dai modelli di traffico tra i siti e si autoregola per ridurre il carico sul vostro team?
- Il fornitore vi suggerisce di utilizzare un CAPTCHA invece di altre azioni? Questo è spesso un indizio inequivocabile. Gli utenti non sopportano questi programmi, ma per i fornitori è più facile offrire un CAPTCHA che mettere a punto delle regole per ridurre al minimo i falsi positivi.
- La soluzione vi consente di comprendere perché una richiesta è stata contrassegnata come proveniente da un bot? Oppure vi mette semplicemente davanti al fatto compiuto? Dovete pretendere che la soluzione offra la possibilità di verificare le azioni adottate, con una visibilità granulare delle richieste e la possibilità di visualizzare le modifiche nelle impostazioni prima di metterle in produzione.

# 5 Azioni flessibili

La tentazione di pensare di dovervi preoccupare esclusivamente di bloccare i bot dannosi consentendo quelli legittimi, è forte. Ma l'ambiente è diventato molto più complesso di così. Molti operatori di bot hanno imparato come ridurre i segnali di rischio abbastanza da posizionare i propri bot in una zona grigia, sapendo che la maggior parte delle organizzazioni preferirebbe rischiare di consentire un bot dannoso piuttosto che rischiare di bloccare un utente legittimo. La vostra soluzione dovrebbe fornire una serie di azioni sofisticate in modo da poter andare oltre al semplice blocco o consentire di includere azioni come sfide crittografiche e l'MFA incrementale. E la vostra soluzione dovrebbe includere anche azioni per affrontare altri tipi di situazioni, ad esempio con i bot legittimi. Potreste avere la necessità di rallentare i bot dei vostri partner durante i periodi di traffico intenso e di consentirli immediatamente durante le ore non di punta. Potete anche scegliere azioni diverse per i bot nella stessa categoria nota: ad esempio, i retailer possono consentire ai più comuni bot di coupon di controllare il proprio sito, bloccando quelli con cui, invece, non desiderano avere relazioni commerciali. Dovete pretendere la flessibilità necessaria per intervenire in modo diverso sui vari tipi di bot in base all'impatto che producono sul business e sull'IT, soprattutto quando tale impatto dipende da fattori come posizione, ora del giorno o stagionalità. Oltre a ciò, avrete bisogno di una soluzione che non blocchi semplicemente tutti i bot (e, così facendo, insegni loro a cambiare tattiche di elusione) ma che crei invece ostacoli, rendendo nel complesso le attività dei criminali più difficili e più costose.

**Considerazioni:**

- La soluzione consente di creare diverse categorie a seconda dei vari tipi di bot o permette solo di classificarli come legittimi o dannosi? Consente anche di creare azioni diverse per i bot della stessa categoria, come motori di ricerca o aggregatori finanziari?
- Quali tipi di azioni condizionali supporta la soluzione? Supporta azioni avanzate, come la possibilità di rallentare e offrire contenuti alternativi che aiutano a configurare meglio il vostro traffico? Include azioni come una sfida crittografica?
- Che grado di flessibilità offre la soluzione per gestire i diversi bot in cui solitamente vi imbattete? È solo l'ennesimo strumento preconfigurato e poco flessibile oppure è in grado di eseguire con precisione azioni mirate in base all'ora del giorno, alla percentuale di traffico o all'URL?
- La soluzione è in grado di introdurre problemi ad alta intensità di risorse che aumentino i costi per gli operatori di bot e rallentano gli attacchi ad alto volume oltre solo un difficile 403?

# 6 Distribuzione

Per una qualsiasi soluzione di gestione dei bot, il tempo necessario per avviare la soluzione e la velocità con cui è possibile modificarla dovrebbero essere considerazioni fondamentali. Gli addetti agli acquisti dovrebbero diffidare di qualsiasi soluzione che richieda modifiche alle applicazioni esistenti o che influisca sulle performance delle applicazioni. I ritardi nella distribuzione possono essere costosi e se necessitate di apportare modifiche alle vostre applicazioni ogni volta che eventi aziendali lo richiedono, come le vendite flash, ciò richiederà solo più risorse.

**Considerazioni:**

- La soluzione funziona in tempo reale senza influire sulle performance delle applicazioni esistenti?
- Richiede di apportare modifiche alle applicazioni esistenti?
- Consente di aumentare o diminuire la scalabilità per far fronte a eventi imprevisti come attacchi volumetrici o eventi previsti come vendite flash?

# 7 Visibilità e rapporti

Ogni soluzione di gestione dei bot è in grado di mostrarvi delle statistiche generali in merito al vostro traffico bot, ma a voi serve ben altro. Dalla pianificazione dell'infrastruttura alla redazione di rapporti destinati ai livelli manageriali, le statistiche generali sono un ottimo ausilio, ma non offrono il livello di granularità necessario per analizzare il traffico bot. Inoltre non sono in grado di garantire che la soluzione adottata utilizzi la strategia corretta. Se la soluzione rischia di bloccare i vostri utenti, non è quella che vi serve. Necessitate di rapporti dettagliati che supportino la vostra azienda e vi aiutino a comprendere meglio in che modo le modifiche alle soglie di rischio influiscono sulle performance.

**Considerazioni:**

- La soluzione offre la possibilità di creare rapporti che consentono di puntare l'attenzione su specifici bot, botnet o caratteristiche di bot? È in grado di riferire sui diversi segmenti di punteggio, quali bot stanno attaccando quali endpoint e mostrare quali azioni sono state intraprese?
- Consente di analizzare sia picchi di traffico che singole richieste? Talvolta è necessario analizzare i dettagli della singola richiesta per capire come comportarsi.
- La soluzione è in grado di confrontare il vostro traffico bot con quello di altri operatori del settore?
- In che modo la creazione dei rapporti si integra con le funzionalità di altre soluzioni di sicurezza? Avete la possibilità di analizzare il vostro traffico in maniera olistica oppure ogni visualizzazione è a se stante?

# 8 Protezione delle API

Indipendentemente dal fornitore o dalla soluzione, le tecnologie di rilevamento dei bot più sofisticate, attualmente, si basano sull'iniezione di codice JavaScript e sull'analisi delle risposte dei client. Ma che fare per proteggere le vostre API quando client basati sulle stesse non rispondono al codice JavaScript? Se avete l'esigenza di esporre le vostre API per supportare app mobili o altre terze parti, vi serve una soluzione che vi aiuti a proteggerle esattamente come proteggete le vostre pagine web. Il rischio altrimenti è che i bot (e i problemi che ne derivano) si spostino semplicemente dalle vostre pagine web alle vostre API.

**Considerazioni:**

- Che tipo di protezioni offre il fornitore per le API? Solo la gestione della quota e la limitazione della velocità?
- Cercate una funzionalità mobile in grado di incorporare le funzionalità di rilevamento bot più sofisticate nelle vostre app mobile.
- Sebbene non sempre efficace quanto altri metodi di rilevamento attivi, un approccio basato sulla reputazione può rivelarsi una buona opzione per proteggere le API che supportano terze parti prive di accesso a una funzionalità mobile come SDK.

# 9 Sito completo o singola pagina

Se il vostro sito web è composto da più di una pagina, molto probabilmente sarà soggetto a svariati problemi di bot, ciascuno correlato alle diverse parti del sito. Lo scraping di prezzi può avere un grande impatto sulle pagine dei prodotti. Lo scraping di contenuti può pregiudicare i vostri contenuti digitali a valore aggiunto. Nel frattempo, continuano a verificarsi attacchi di abuso di credenziali nei confronti delle pagine di accesso. Eppure alcune soluzioni di gestione dei bot sono progettate per affrontare un solo problema. Accertatevi che la soluzione che state valutando possa aiutarvi ad affrontare tutti i vostri problemi di bot, che riguardino l'intero sito o solo determinate pagine.

**Considerazioni:**

- Su che cosa si focalizza la soluzione, su singole pagine o sull'intero sito web? In che modo viene implementata, per le singole pagine o per l'intero sito?
- La soluzione è in grado di aiutarvi ad affrontare tutti i vostri problemi di bot, dall'abuso di credenziali, al web scraping, all'aggregazione di contenuti?

# 10 Servizi gestiti

Dovete essere in grado di gestire i bot per controllarne l'impatto sul vostro business, ma questa attività è tutt'altro che semplice. E benché la vostra organizzazione disponga di personale competente, talvolta potreste avere bisogno di aiuto dall'esterno, ad esempio di esperti che conoscano e comprendano i vostri problemi. Inoltre, assumere personale per queste posizioni sta diventando sempre più difficile. Cosa succede se una parte dei vostri talenti se ne va? Chiunque è in grado di leggere una richiesta HTTP e creare una firma per bloccare il traffico, ma questo non significa saper risolvere il problema. Ciò che vi serve è qualcuno in grado di correlare i bot ai vostri problemi di base e quindi progettare e implementare una strategia per risolverli.

**Considerazioni:**

- Disponete di competenze interne specializzate nella gestione dei bot che vi consentano di sfruttare al meglio la soluzione prescelta?
- Il fornitore che state valutando offre anche servizi professionali oppure vende solo prodotti per la gestione dei bot?
- È possibile accedere in qualsiasi momento al monitoraggio proattivo e a risorse specialistiche supplementari in caso di emergenza?

# Siate proattivi, non reattivi

È meglio investire nella gestione dei bot prima che diventino un problema e prima che la prossima ondata di evoluzione renda le difese esistenti una debole imitazione di quelle precedenti. Tenete conto di queste considerazioni durante la ricerca delle vostre opzioni. Akamai Bot Manager può contribuire a fornirvi le garanzie di cui avete bisogno. Per ulteriori informazioni, richiedete la guida personalizzata di un attacco simulato.

**Scoprite di più**