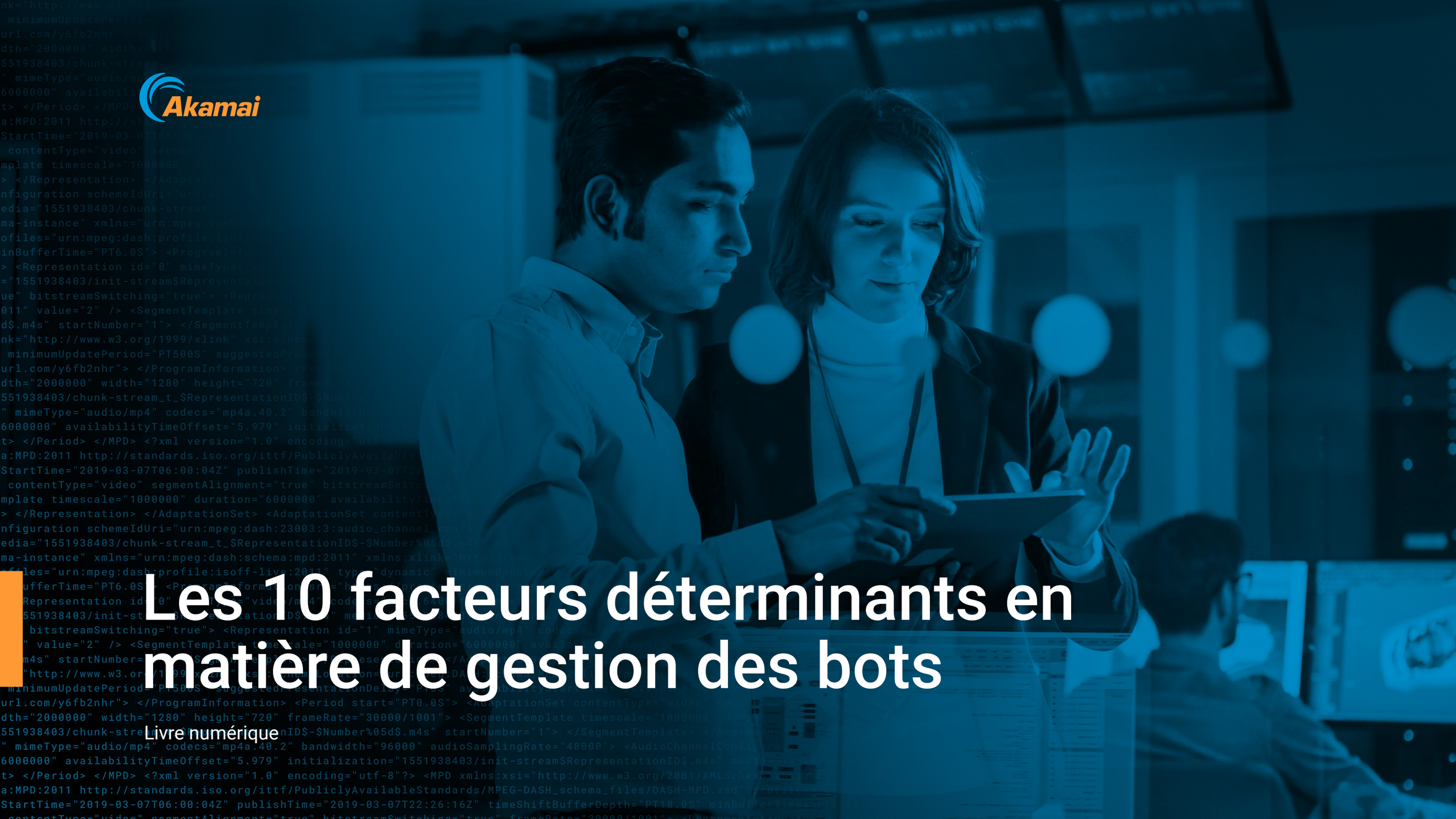

Les 10 facteurs déterminants en matière de gestion des bots

Livre numérique

TABLE DES MATIÈRES

Introduction 03

1. Expertise sophistiquée 04
2. Collecte de renseignements 05
3. Protection renforcée 06
4. Faux positifs et faux négatifs 07
5. Plan d'actions flexibles 08
6. Déploiement 09
7. Visibilité et création de rapports 10
8. Protection des API 11
9. Site ou page 12
10. Services gérés 13

Introduction

Savez-vous à quel point la question des bots est devenue problématique ? Essayez d'obtenir un billet pour un concert de Taylor Swift ou une nouvelle paire de baskets Air Jordans. Et il ne s'agit là que d'événements très médiatisés. Les bots sont de plus en plus omniprésents et nuisibles dans tous les secteurs d'activité.

Ce qui est encore plus difficile pour ceux qui sont en quête de réponses, c'est que la gestion des bots a changé. En réalité, cela a toujours été le cas. La gestion des bots est souvent décrite comme une véritable bataille d'armes ou un jeu du chat et de la souris entre les entreprises qui établissent des défenses et les créateurs de bots qui continuent à trouver des moyens de les contourner. Mais aujourd'hui, ce ne sont pas seulement les bots eux-mêmes qui évoluent. L'environnement qui les entoure évolue également. Par exemple, les entreprises n'ont plus seulement à faire face à des individus seuls, ni même à des groupes coordonnés. Il est désormais possible de louer un bot pour la semaine, comme on le ferait avec un Airbnb. De même, les solutions ne peuvent pas se contenter de segmenter les bots en deux catégories : les bienveillants et les malveillants. La zone grise est trop importante aujourd'hui.

Cette évolution des bots et de l'environnement qui les entoure a rendu la sélection d'un logiciel de gestion des bots plus difficile que jamais. Vous devez non seulement déterminer ce qui était efficace contre les bots d'hier, mais aussi ce qui le sera contre ceux d'aujourd'hui et de demain.

Ce guide présente quelques-unes des principales considérations à prendre en compte par les acheteurs qui choisissent un logiciel de gestion des bots. Il vous aidera à faire le tri et à prendre une décision d'achat éclairée.

1 Expertise sophistiquée

Les solutions de gestion des bots, au sens propre du terme, détectent les bots. En d'autres termes, elles recherchent des signes d'automatisation et d'autres indicateurs permettant de déterminer que le demandeur n'est pas un humain. Toutefois, au fur et à mesure de leur évolution et de leur sophistication, les bots se sont également spécialisés. Les bots sont désormais conçus pour des objectifs ciblés, tels que la récupération de contenu sur votre site, la mise en réserve de vos stocks lors d'événements populaires et le credential stuffing pour prendre le contrôle des comptes de vos clients, entre autres cas d'utilisation. Souvent, la détection d'un type de bot spécialisé ne permet pas de détecter les autres. Vous devez donc déterminer si le fournisseur est en mesure d'arrêter les bots spécifiques auxquels vous êtes confronté, et pas seulement les bots de base à usage général.

Facteurs déterminants :

- Le fournisseur dispose-t-il de moyens de détections spécialisés pour les bots en fonction des scénarios d'utilisation professionnels ?
- Le fournisseur peut-il justifier de son expertise en ce qui concerne le problème spécifique que vous rencontrez avec les bots ?
- Combien d'autres clients du fournisseur sont confrontés aux mêmes problèmes ? Pourrez-vous bénéficier de ce que le fournisseur a appris de ces clients ?
- Le fournisseur propose-t-il des rapports, des services ou d'autres fonctionnalités pour vous aider dans votre lutte contre les bots spécialisés et hostiles ?

2 Collecte de renseignements

La qualité d'une solution de gestion des bots dépend de sa capacité à reconnaître les caractéristiques des bots qu'elle surveille. Certains fournisseurs affirment qu'ils détectent 99,9 % des bots, mais il est impossible d'en mesurer objectivement l'efficacité. Les bots évoluent en permanence, si bien que ce que vous avez détecté hier a probablement trouvé un moyen d'échapper à la détection aujourd'hui. Un meilleur critère d'évaluation des outils de gestion des bots est la manière dont le fournisseur renseigne ses capacités de détection des bots.
Il vous faut une solution capable de détecter les bots les plus sophistiqués (et pas seulement ceux que l'on soupçonne habituellement) et tirer parti de l'ensemble de données le plus vaste. Rappelez-vous que la plupart des outils d'intelligence artificielle (IA) et d'apprentissage machine (ML) sont Open Source, si bien que la quantité de données, la qualité des données et la rapidité avec laquelle la solution alimente les algorithmes en données sont des éléments sous-estimés lors de l'évaluation de l'IA/du ML d'une solution. Les informations doivent inclure des indicateurs de confiance et des scores de risque pour chaque connexion, dans tous les domaines. En outre, les solutions efficaces devraient adopter une approche à plusieurs niveaux pour la détection des bots, en utilisant les méthodes les plus récentes.

Facteurs déterminants :

- Demandez des détails sur la façon dont le fournisseur renseigne ses capacités de détection des bots. Les fournisseurs ayant des clients majeurs qui attirent les pirates auront plus d'expérience et des bases de données plus complètes sur lesquelles ils pourront s'appuyer pour développer leurs compétences, notamment en ce qui concerne les signaux de risque et de confiance à évaluer et les détections d'anomalies plus nombreuses, entre autres. Un manque de transparence devrait vous alerter.

- Le fournisseur utilise-t-il l'IA/le ML pour appuyer sa solution ? Ces modèles sont-ils sophistiqués ? Et, ce qui est tout aussi important, quelle quantité de données le fournisseur introduit-il dans ces modèles ? Les pirates utilisent certainement l'IA. Vous devriez en faire autant.

- Mais l'IA ne suffit pas. Le fournisseur dispose-t-il d'une équipe d'experts qualifiés, tels que des chercheurs en sécurité et des analystes des renseignements sur les menaces, qui recherchent en permanence de nouvelles méthodes d'attaque et gardent un œil sur les communautés de pirates pour s'assurer que vous avez toujours une longueur d'avance ?

3 Protection renforcée

Lorsque vous bloquez un bot sophistiqué, il ne disparaît pas définitivement. Il revient sans cesse et mute constamment afin d'échapper à votre système de détection. De nombreuses solutions de gestion des bots peuvent détecter les bots (ou du moins certains d'entre eux) dans un premier temps, mais perdent ensuite de leur efficacité lorsque les bots commencent à muter. Akamai a constaté que les bots mutaient en l'espace de quelques heures. Toutefois, les cycles de développement traditionnels sont trop lents pour tenir la cadence. Assurez-vous donc que la solution que vous choisissez apprend et évolue au fil du temps, de préférence en utilisant l'apprentissage automatique. La solution doit inclure des défenses préventives qui compliquent la tâche des pirates qui cherchent à obtenir des informations qu'ils utiliseront pour échapper à vos défenses.

Facteurs déterminants :

- Recherchez une solution équipée des technologies de détection des bots les plus sophistiquées (comme l'analyse du comportement des utilisateurs et les modèles d'apprentissage spécifiques aux clients). Leur efficacité durera plus longtemps même lorsque les bots muteront.
- Vérifiez si la solution inclut des tactiques défensives telles que la dissimulation JavaScript, qui rend plus difficile pour les pirates d'effectuer de la rétro-ingénierie sur les bots pour contourner vos défenses.
- Demandez des preuves ou des références d'autres clients ayant déployé la solution afin de savoir si elle reste efficace dans le temps.

4 Faux positifs et faux négatifs

Quand une solution de gestion des bots indique avoir bloqué un bot, comment savez-vous que le système n'a pas en fait bloqué un utilisateur légitime ? Beaucoup de fournisseurs jouent avec les faux positifs. S'ils ne disposent pas d'une solution qui évalue les bots en fonction de chaque détection, ils peuvent ne pas être en mesure de détecter les bots « gris », ce qui les conduit à prendre des décisions binaires de type oui/non. Souvent, ces fournisseurs préfèrent montrer à leurs clients qu'ils ont bloqué de nombreux « bots », même si leur taux de faux positifs est élevé, ce qui signifie qu'ils bloquent des bots, mais aussi du trafic valide (des utilisateurs humains ou des bots bienveillants qui ont de la valeur pour votre entreprise). En revanche, un faible taux de faux négatifs peut sembler intéressant jusqu'à ce que vous réalisiez que ce taux est aussi faible parce que le fournisseur a dû réduire l'efficacité globale de la solution pour s'assurer qu'elle ne bloquait pas les utilisateurs humains, et qu'elle laisse donc passer des bots qu'elle aurait dû bloquer. La solution doit bloquer les bots malveillants sans entraver l'activité de l'entreprise, mais elle ne doit pas non plus affaiblir la protection de l'entreprise. Vous devez donc être sûr que le fournisseur avec lequel vous collaborez se soucie de l'exactitude et de l'impact des faux positifs et faux négatifs.

Facteurs déterminants :

- Le fournisseur vous laisse-t-il gérer les faux positifs/négatifs ou cherche-t-il au contraire à développer des compétences et des services pour travailler en collaboration avec vous ?
- La solution exploite-t-elle les modèles de trafic entre les sites et s'adapte-t-elle automatiquement pour réduire la charge de travail de votre équipe ?
- Le fournisseur suggère-t-il d'utiliser un CAPTCHA au lieu d'autres actions de défi ? C'est souvent mauvais signe. Les utilisateurs détestent cette solution, mais il est plus facile pour un fournisseur de proposer un programme CAPTCHA que d'adapter ses règles afin de réduire le nombre de faux positifs.
- Avez-vous la possibilité de savoir pourquoi la solution a identifié une requête comme provenant d'un bot ? Ou s'agit-il d'une boîte noire ? Vérifiez que les actions entreprises peuvent être vérifiées grâce à une visibilité granulaire des requêtes et que les changements apportés à vos paramètres peuvent être visualisés avant de les mettre en production.

5 Plan d'actions flexibles

On pourrait être tenté de penser qu'il suffit de bloquer les bots malveillants et de laisser passer les autres. Mais l'environnement est devenu beaucoup plus complexe que cela. De nombreux opérateurs de bots ont compris qu'ils pouvaient abaisser suffisamment leurs signaux de risque pour placer leurs bots dans une zone grise, car ils sont conscients que la plupart des entreprises préfèrent prendre le risque de laisser passer un bot malveillant plutôt que de bloquer l'accès à un utilisateur légitime. Votre solution doit prévoir un ensemble d'actions sophistiquées afin que vous puissiez non seulement bloquer ou autoriser, mais aussi inclure des actions de défi telles que les défis cryptographiques et l'authentification multifactorielle par paliers. Par ailleurs, votre solution doit également inclure des actions permettant de faire face à d'autres types de situations, par exemple avec les bots bienveillants. Il se peut que vous souhaitiez ralentir les bots de vos partenaires pendant les périodes de fort trafic et laisser passer ces bots immédiatement pendant les périodes creuses. Vous pouvez également choisir des actions différentes pour les bots d'une même catégorie connue. Par exemple, si vous êtes un détaillant, vous pouvez laisser les bots de bons de réduction les plus populaires consulter votre site tout en bloquant ceux avec lesquels vous ne souhaitez pas travailler. Vous avez besoin de flexibilité pour appliquer différentes actions sur des types de bots variés en fonction de leur impact sur l'entreprise et l'informatique, notamment lorsque celui-ci varie en fonction de l'endroit, de l'heure de la journée ou de la saison. Plus encore, vous aurez besoin d'une solution qui ne se contente pas de bloquer tous les bots (et qui, dans la foulée, leur apprend à changer de tactique d'évasion), mais qui, au contraire, crée des obstacles, rendant la tâche plus difficile et plus coûteuse pour les pirates.

Facteurs déterminants :

- La solution vous permet-elle de créer différentes catégories selon le type de bot ou les bots sont-ils simplement considérés comme bienveillants ou malveillants ?
  Peut-elle également mettre en place des actions différentes pour les bots d'une même catégorie, comme les moteurs de recherche ou les agrégateurs financiers ?
- Quels types d'actions conditionnelles la solution prend-elle en charge ? Prend-elle en charge des actions avancées, telles que le ralentissement et la distribution d'un contenu alternatif, vous permettant de mieux structurer votre trafic ? Comprend-elle des actions telles qu'un défi cryptographique ?
- Quel est le degré de flexibilité de la solution concernant la gestion des différents bots que vous rencontrez ? Applique-t-elle une mesure unique ou entreprend-elle des actions selon le moment de la journée, le pourcentage du trafic ou l'URL ?
- La solution permet-elle de remédier aux problèmes de ressources qui rendent la tâche des opérateurs de bots plus onéreuse et de ralentir les attaques à fort volume de requêtes en dehors de l'affichage d'une simple erreur 403 ?

6 Déploiement

Pour toute solution de gestion des bots, le temps nécessaire au lancement de la solution et la rapidité avec laquelle vous pouvez la modifier doivent être des éléments essentiels à prendre en compte. Les acheteurs doivent se méfier de toute solution qui nécessite une modification de leurs applications existantes ou qui a un impact sur les performances des applications. Les retards de déploiement peuvent être coûteux, et si vous devez apporter des modifications à vos applications chaque fois que des événements commerciaux l'exigent, comme des ventes flash, cela ne fera que mobiliser davantage de ressources.

Facteurs déterminants :

- La solution fonctionne-t-elle en temps réel sans affecter les performances de vos applications existantes ?
- Exige-t-elle que vous apportiez des modifications à vos applications existantes ?
- Peut-elle évoluer en fonction d'événements imprévus tels que des attaques en masse ou d'événements attendus tels que des ventes flash ?

7 Visibilité et création de rapports

Toutes les solutions de gestion des bots peuvent fournir des statistiques détaillées sur votre trafic de bots, mais ce n'est pas suffisant. Ces statistiques détaillées sont intéressantes pour prévoir des infrastructures ou faire remonter des rapports à votre chaîne de gestion, mais elles n'offrent pas la granularité requise pour analyser votre trafic de bots. Elles ne vous apportent pas non plus la preuve nécessaire pour vous assurer que la solution a entrepris les actions appropriées. Avec une solution qui peut bloquer vos utilisateurs, la dernière chose que vous voulez, c'est une boîte noire. Vous avez besoin de rapports détaillés pour soutenir votre activité et vous aider à mieux comprendre l'impact des modifications des seuils de risque sur les performances.

Facteurs déterminants :

- La solution propose-t-elle des fonctions de création de rapports vous permettant de zoomer sur des bots, des botnets ou des caractéristiques de bots en particulier ? Peut-elle rendre compte des différents segments de notation, des bots qui attaquent tel ou tel point de terminaison, et montrer quelles actions ont été entreprises ?
- Peut-elle vous permettre d'enquêter sur les pics de trafic et examiner les requêtes individuelles ? Il est parfois nécessaire d'accéder aux détails des requêtes pour savoir quelle action entreprendre.
- La solution peut-elle comparer votre trafic de bots à celui d'autres entreprises du secteur ?
- Dans quelle mesure les rapports correspondent-ils à ceux des autres solutions de sécurité ? Pouvez-vous analyser votre trafic de manière globale ou existe-t-il des vues distinctes ?

8 Protection des API

Quels que soient le fournisseur et la solution, les technologies de détection des bots les plus sophistiquées actuellement reposent sur l'injection de code JavaScript et sur l'analyse de la réponse client. Mais que faire de vos API lorsque les clients basés sur les API ne répondent pas à JavaScript ? Si vous devez présenter des API pour prendre en charge des applications pour mobile ou d'autres tierces parties, il vous faut une solution de protection de vos API similaire à celle de vos pages Web. Sans quoi, vos bots (et vos problèmes de bots) migreront simplement de vos pages Web vers vos API.

Facteurs déterminants :

- Quel type de protection le fournisseur vous propose-t-il pour vos API ? S'agit-il seulement d'une gestion des quotas et d'une limitation du débit ?
- Recherchez une fonctionnalité mobile qui intègre les détections de bots les plus sophistiquées du fournisseur dans vos applications pour mobile.
- Bien qu'elle ne soit pas toujours aussi efficace que les autres solutions de détection active, une approche basée sur la réputation peut être une bonne option pour protéger les API qui prennent en charge des parties tierces, lesquelles peuvent ne pas avoir accès à une fonctionnalité mobile telle qu'un SDK.

9 Site ou page

Si votre site Web comprend plusieurs pages, vous êtes probablement confronté à plusieurs problèmes de bots, chacun affectant différentes parties de votre site. L'extraction de prix peut avoir un impact important sur vos pages de produits. L'extraction de contenu peut nuire à votre contenu digital à valeur ajoutée. Par ailleurs, les attaques par vol d'identifiants contre vos pages de connexion persistent. Certaines solutions de gestion des bots sont conçues pour ne traiter qu'un seul problème. Assurez-vous que votre solution de gestion vous permet de traiter l'ensemble de vos problèmes de bots, qu'ils touchent l'intégralité de votre site ou uniquement des pages spécifiques.

Facteurs déterminants :

- Sur quoi la solution se concentre-t-elle : des pages individuelles ou l'intégralité du site Web ?
  Comment se déploie-t-elle : en amont des pages individuelles ou de l'intégralité du site Web ?
- La solution vous permet-elle de traiter l'ensemble de vos problèmes de bots, qu'il s'agisse de vol d'identifiants, d'extraction Web ou d'agrégation de contenu ?

10 Services gérés

Vous devez gérer les bots afin de contrôler leur impact sur votre entreprise et ses activités. Mais la gestion des bots n'est pas simple. Et bien que vous ayez peut-être de l'expertise dans votre entreprise, vous avez parfois besoin d'une aide supplémentaire : il vous faut des experts qui comprennent vos problèmes de bots. De plus, il est de plus en plus difficile de pourvoir ces postes. Que se passera-t-il lorsque certains de vos talents partiront ? Tout le monde peut examiner une requête HTTP et créer une signature pour bloquer le trafic, mais le problème n'est pas résolu pour autant. Il vous faut un interlocuteur qui peut relier les bots à vos principaux problèmes, mais aussi concevoir et mettre en œuvre une stratégie pour résoudre ces problèmes.

Facteurs déterminants :

- Disposez-vous en interne de l'expertise spécifique aux bots nécessaire pour exploiter pleinement une solution ?
- Le fournisseur de gestion des bots propose-t-il des services professionnels ou se contente-t-il de vendre des produits ?
- Pouvez-vous accéder à tout moment à une surveillance proactive ainsi qu'à des ressources spécialisées supplémentaires en cas d'urgence ?

Adopter une attitude proactive, et non réactive

Il est préférable d'investir dans la gestion des bots avant qu'ils ne deviennent un problème et que la prochaine vague d'évolution ne réduise les défenses existantes à une pâle imitation de ce qu'elles étaient auparavant. Tenez compte de ces facteurs déterminantes lorsque vous étudiez vos options. Akamai Bot Manager peut vous apporter les garanties dont vous avez besoin. Pour en savoir plus, demandez une présentation personnalisée d'une attaque simulée.

En savoir plus