



USE CASE

Média : protéger ses applications et ressources des attaques automatisées

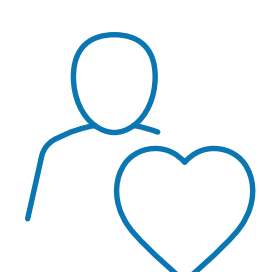
Un diffuseur de contenus met à disposition de ses clients un portail en ligne leur permettant de gérer leurs abonnements de manière autonome. Via ce portail, les utilisateurs peuvent enrichir leurs offres, consulter leurs factures, participer à des jeux ou défis, voter lors d'événements, ou encore modifier les paramètres de leur compte. Ce portail est devenu la cible de nombreux bots, dont certains très sophistiqués. Ces attaques ont permis de mener diverses actions malveillantes telles que des tentatives de force brute, du credential stuffing, des votes frauduleux, la création massive de faux comptes ou encore des modifications non autorisées d'abonnements. Les solutions anti-bots « best effort » déjà en place n'ont pas permis de contenir efficacement ces attaques.

Besoin du client



Détection avancée, impact minimal

Une solution de protection contre les bots à la fois puissante et intelligente, capable de détecter et bloquer les bots les plus avancés sans impacter les utilisateurs légitimes.



Expérience utilisateur préservée

Le maintien d'une expérience utilisateur fluide et inchangée, notamment sans recours à des mécanismes intrusifs comme les CAPTCHA.



Supervision SOC assurée

Un service opéré et supervisé par un centre de sécurité (SOC), et non une solution en libre-service.

Solution

F5 Distributed Cloud Bot Defense détecte et bloque les bots, y compris les plus avancés, grâce à des modèles de machine learning (supervisés et non-supervisés) et à l'expertise d'analystes SOC. La solution exploite la télémétrie applicative du client pour repérer les évolutions des bots (bot retooling) et ajuster les politiques de protection quasi en temps réel. Les données sont collectées à plusieurs points du plan de données (**Distributed Cloud WAAP, BIG-IP, CDN et connecteurs vers d'autres environnements**) afin de déterminer si une requête vient d'un humain ou d'un bot, sans perturber l'expérience des utilisateurs légitimes, tout en préservant les performances du portail.

