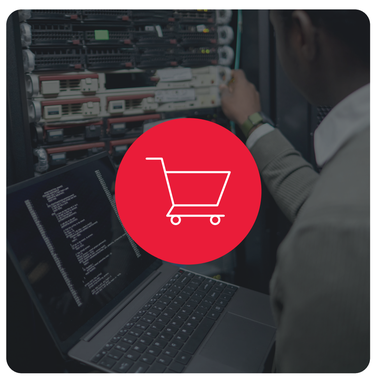

USE CASE

Retail : protéger son portail e-commerce des attaques automatisées

Une entreprise de vente de produits électroniques grand public utilise F5 BIG-IP pour protéger son portail de e-commerce avec Advanced WAF. Le client recevait en continu des alertes provenant d'Advanced WAF. L'analyse des journaux BIG-IP a mis en évidence de nombreuses tentatives de connexion infructueuses, provenant de multiples adresses IP. Les cybercriminels exploitaient des identifiants compromis pour tenter d'accéder à des comptes clients et à des informations sensibles, en s'appuyant sur des bots et des outils d'attaque sophistiqués.

Besoin du client

Trafic filtré en temps réel
Bloquer les tentatives d'accès malveillantes effectuées par des utilisateurs non humains et non autorisés.

Détection des comportements suspects
Déjouer des bots capables d'imiter le comportement humain et d'adapter en permanence leurs techniques.

Architecture existante préservée
S'intégrer à l'architecture BIG-IP existante sans remise en cause du fonctionnement en place.

Solution

F5 Distributed Cloud Bot Defense, associé au connecteur BIG-IP, utilise une instance virtuelle d'obfuscation et de randomisation rendant les signaux de détection imprévisibles, pour empêcher l'analyse et le contournement par les cybercriminels.

Le connecteur s'insère dans le chemin de données entre applications web/mobiles et serveurs d'origine, redirige le trafic à protéger vers le **service Bot Defense**, permet de conserver l'architecture et les flux existants sans modification majeure, tout en bloquant le credential stuffing, la force brute et les abus de logique métier, sans dégrader l'expérience des utilisateurs légitimes.