USE CASE

Administration publique : sécuriser les accès aux services numériques face au credential stuffing et aux attaques par force brute

Un client de l'administration publique centrale, équipé de BIG-IP on-premise, voyait son application de réservation de services ministériels ciblée par des bots spécialisés. Ces derniers monopolisaient les créneaux disponibles pour les revendre via des agences externes.

Résultat : un accès dégradé pour les citoyens, des coûts en hausse et une satisfaction utilisateur en baisse. L'analyse a confirmé l'usage d'outils d'automatisation sophistiqués, spécialement conçus pour contourner l'application du client.

Besoin du client

Empêcher les accès non autorisés par des bots

Bloquer les tentatives d'accès malveillantes menées par des utilisateurs non humains afin de protéger l'application et ses services.

Déjouer les bots qui imitent les comportements humains

Identifier et contrer les bots capables de reproduire des interactions humaines et d'adapter continuellement leurs méthodes pour contourner la sécurité.

Solution

F5 Distributed Cloud Bot Defense permet de détecter et de bloquer les bots, même les plus sophistiqués. La solution combine machine learning supervisé et non supervisé, expertise SOC et télémétrie applicative pour identifier les évolutions des menaces et ajuster la sécurité en quasi temps réel.

Connectée à **F5 Distributed Cloud WAAP, BIG-IP, au CDN et à d'autres plans de données**, elle distingue les utilisateurs légitimes des bots sans ajouter de friction, comme des CAPTCHA.

Dans le contexte du client, la solution **s'appuie sur le BIG-IP déjà en place dans le datacenter on-premise**. Résultat : les bots sophistiqués sont bloqués, les points de terminaison applicatifs sont protégés, et le problème est résolu rapidement grâce à une protection automatisée pilotée par le machine learning et l'IA.