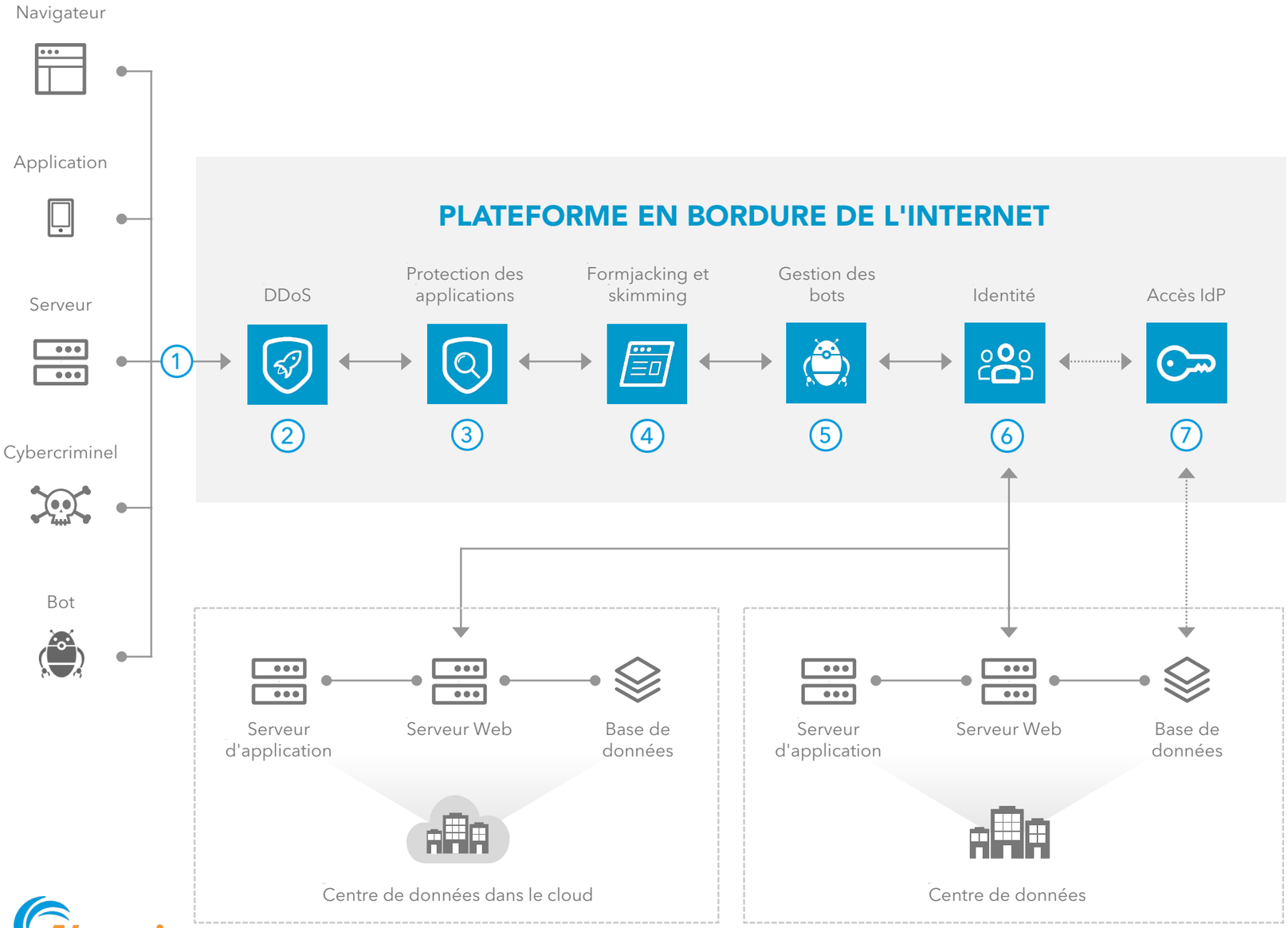
# PRÉVENEZ LA FRAUDE ET LA CYBERCRIMINALITÉ EN LIGNE

## Architecture de référence




## PRÉSENTATION

Les institutions financières sont des cibles attrayantes. Elles attirent des criminels dotés d'outils sophistiqués, qui changent constamment de vecteur d'attaque pour éviter d'être détectés. Les attaques réussies génèrent de nouvelles contraintes réglementaires et, de manière plus significative encore, ébranlent la confiance des utilisateurs.

Voici comment les solutions Akamai créent une stratégie de sécurité pour garder une longueur d'avance sur les menaces en constante évolution et protéger le patrimoine des utilisateurs, tout en facilitant les nouvelles souscriptions.

1. L'Akamai Intelligent Edge Platform prend en charge l'accès aux applications par le biais du protocole TLS mutuel et d'autres contrôles réseau, ainsi que les principales formes d'authentification et d'autorisation des API.
2. En plus de constituer une menace sérieuse, les attaques DDoS peuvent parfois détourner les cibles des véritables motivations des cybercriminels. Les serveurs en bordure de l'Internet bloquent automatiquement les attaques DDoS au niveau de la couche réseau et déjouent les attaques de la couche applicative.
3. Protection des données des applications par le biais d'inspections de requêtes Web et de modèles de sécurité positifs, qui utilisent des paramètres spécifiques définis dans le fichier de configuration de l'API.
4. Inspection et analyse approfondies des pages afin de découvrir les scripts malveillants et de protéger les données.
5. Protection contre toutes les tentatives de vols d'identifiants et les éventuels piratages de compte, basée sur des fonctionnalités qui identifient les bots les plus récents et les plus sophistiqués.
6. La gestion des identités et des accès client (CIAM) en bordure de l'Internet sécurise les informations sensibles pour garantir les performances, la personnalisation, la protection des données et la conformité à un environnement réglementaire complexe.
7. Possibilité de stocker les identifiants dans un répertoire sur site ou dans une application tierce.

## PRODUITS CLÉS

Protection contre les attaques DDoS, les attaques des applications et le formjacking ► Kona Site Defender

Gestion des bots ► Bot Manager

Accès aux identités et aux applications ► Identity Cloud et Enterprise Application Access

Publication : 05/20