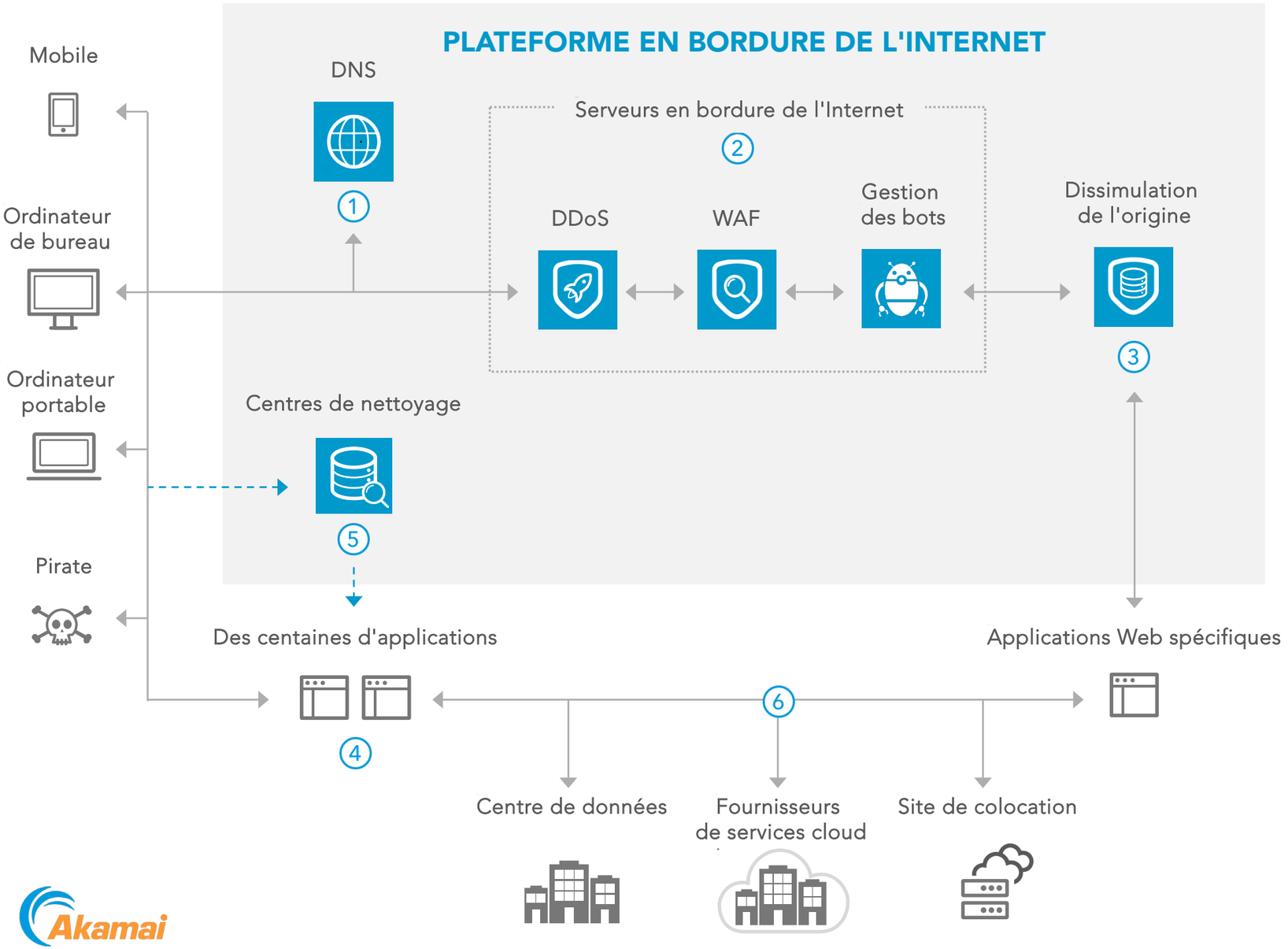
PROTECTION DDoS

Architecture de référence



PRÉSENTATION

Akamai limite le risque d'attaques DDoS grâce à une protection rapide et efficace conçue pour contrer les attaques DDoS les plus massives et sophistiquées, que les applications soient déployées dans le centre de données, une infrastructure de cloud public ou un site de colocation.

1. Les clients effectuent une recherche DNS sur le service DNS d'Akamai, en mesure d'absorber même les attaques DDoS les plus importantes.

2. Les serveurs en bordure de l'Internet inspectent automatiquement le trafic CDN pour détecter les attaques DDoS, les attaques de type bot et les attaques ciblant les applications Web, et bloquent les menaces malveillantes.

3. Akamai achemine le trafic CDN par le biais des serveurs désignés en bordure de l'Internet, ce qui permet aux clients de supprimer le trafic en provenance d'autres sources et d'empêcher les hackers de contourner la protection basée sur la bordure de l'Internet.

4. Le trafic non CDN est généralement acheminé directement vers l'origine en fonction des annonces de routage BGP du client.

5. Les clients peuvent acheminer le trafic via les centres de nettoyage d'Akamai (de manière automatique ou à la demande), où les attaques DDoS sont bloquées grâce à des contrôles d'atténuation proactifs ou une atténuation active du SOC.

6. Les services de nettoyage des attaques DDoS et basés sur le CDN d'Akamai assurent la protection des applications déployées dans les centres de données des clients, l'infrastructure de cloud public ou dans les sites de colocation.

PRODUITS CLÉS

DNS ▶ Edge DNS

DDoS/WAF ▶ Kona Site Defender ou Web Application Protector

Bots ▶ Bot Manager

Centres de nettoyage ▶ Prolexic Routed

Publication : 03/20