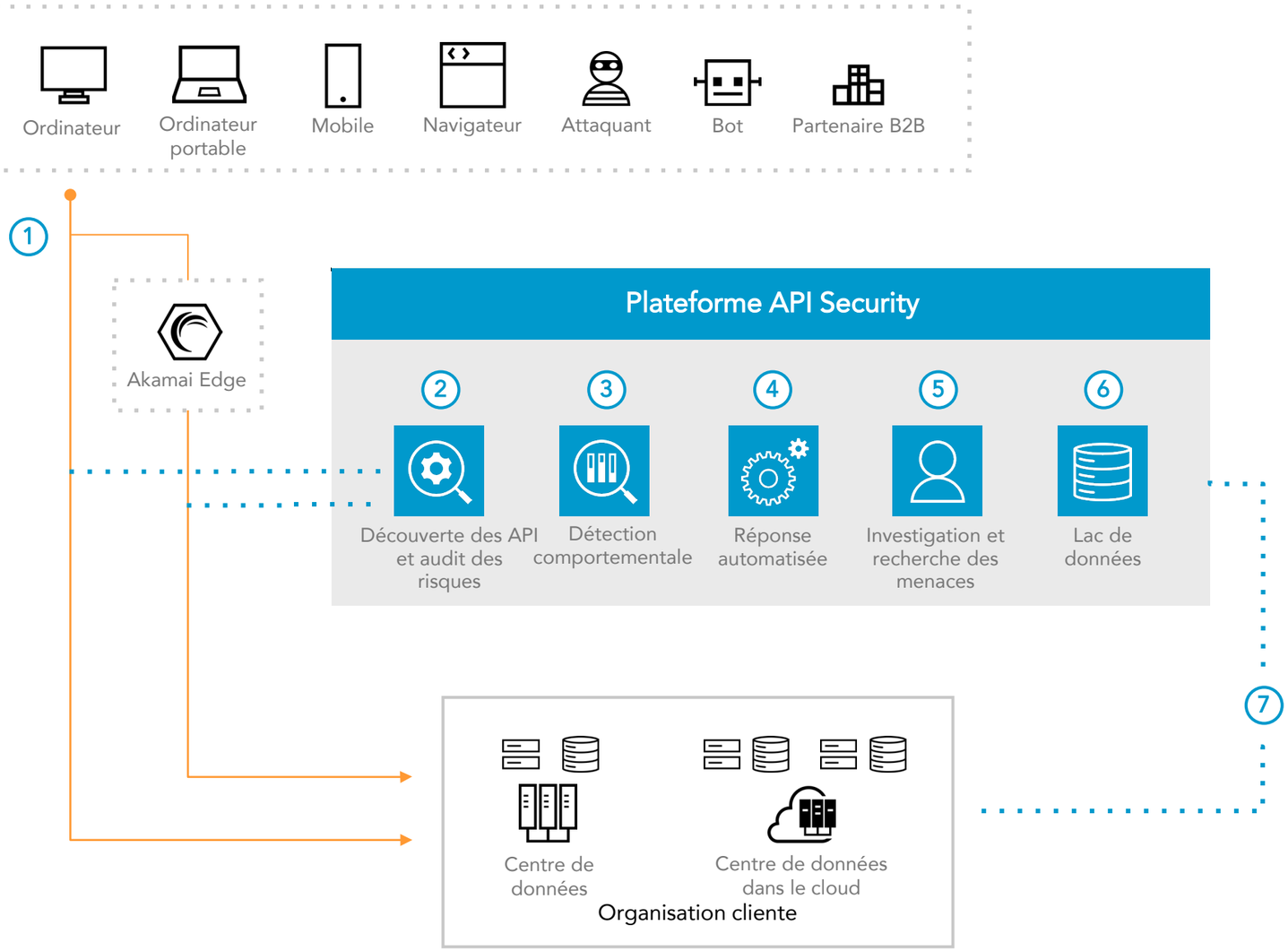
API SECURITY

Fonctionnement de la solution



PRÉSENTATION

La solution Akamai API Security découvre et audite toutes les API et surveille leur activité à l'aide d'analyses comportementales afin de détecter et réagir aux menaces et aux abus. Elle fournit des détections contextuelles pour protéger contre les abus de logique et les attaques d'API que les solutions basées sur les signatures ne peuvent pas détecter.

1. Le trafic provient de l'organisation du client et/ou traverse la plateforme en bordure de l'Internet d'Akamai
2. Une copie de ce trafic alimente la plateforme API Security, où toutes les API sont découvertes
3. Les détections comportementales établissent un modèle de comportement normal afin de détecter les anomalies et les abus de logique
4. Les réponses automatisées peuvent envoyer des informations critiques aux équipes de sécurité ou bloquer le trafic en bordure d'Akamai
5. Les équipes de sécurité peuvent utiliser le contexte comportemental pour enquêter et rechercher des menaces dans le trafic API ou utiliser un service de recherche de menaces géré.
6. L'activité historique des API est stockée dans notre lac de données et soutient les initiatives d'investigation et de recherche des menaces.
7. API Security offre également une visibilité complète sur les API et l'activité des API de l'organisation cliente

PRODUITS CLÉS

Protection des API ► Akamai API Security

Recherche des menaces gérée ► Akamai API Security ShadowHunt

Rendez-vous sur akamai.com/products/api-security

Publication : 04/24