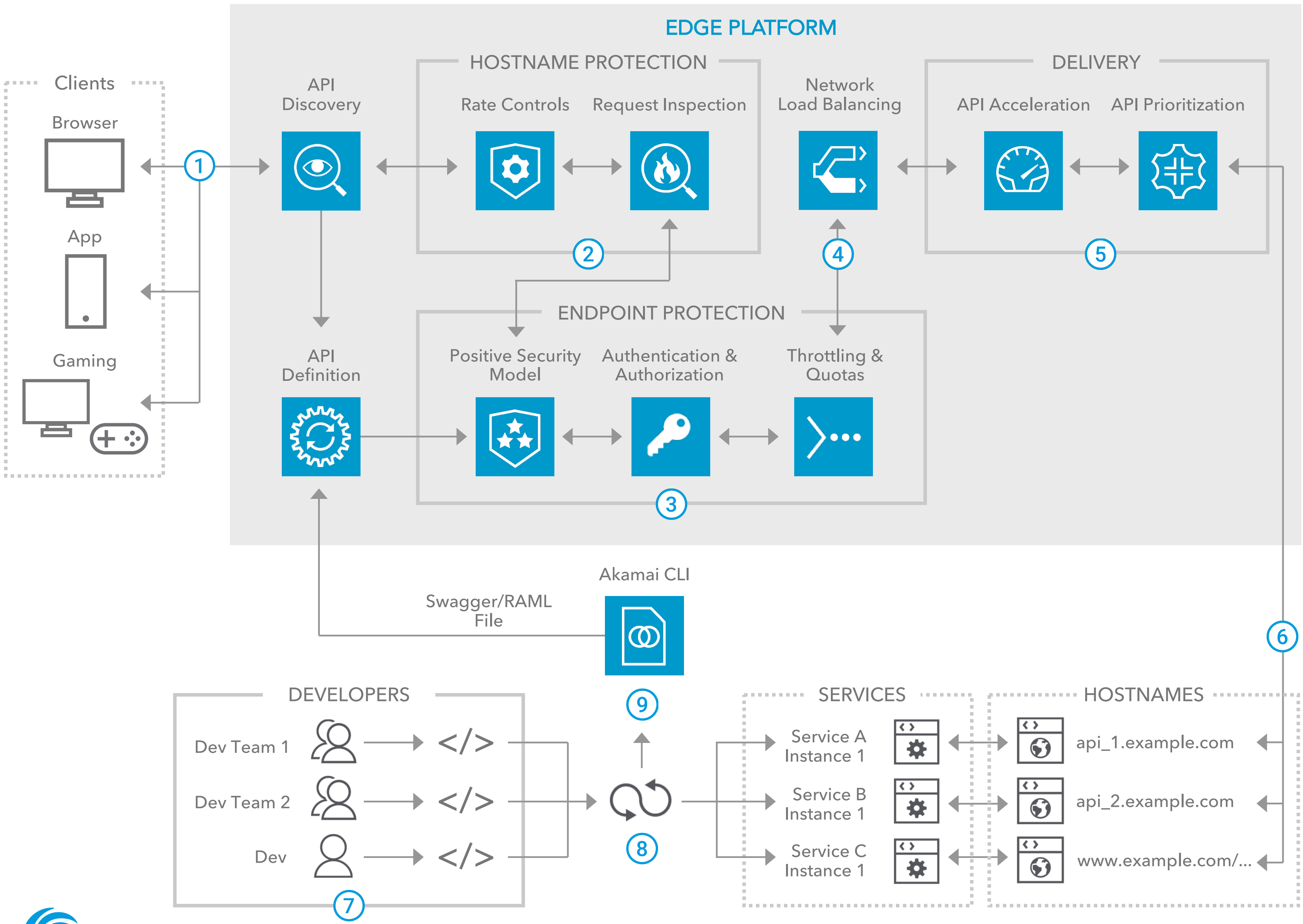
MODERN API ARCHITECTURE

Reference Architecture (Hostnames)



OVERVIEW

APIs have quickly emerged as a standard way of building and connecting apps, as every day more organizations are adopting modern app architectures. Regardless of the architecture, Akamai can provide APIs and digital businesses with higher availability, improved user experience, and a strong security posture.

1. Clients connect to the APIs through the edge platform. Hostname-level protection is applied to all API traffic to discover new API endpoints.
2. Akamai can inspect all API traffic and protect hostnames against DDoS and application attacks.
3. Registering API definitions enables more granular protection for individual API endpoints, with a positive security model, authentication, authorization, and throttling/quotas.
4. Load balancing determines to which origin the request should be routed, considering performance and availability.
5. APIs are accelerated via protocol and route optimization. Prioritize API traffic to deal with use cases like heavy load.
6. The edge provides the ability to optimize settings and apply controls to the API traffic, considering your app architecture.
7. Development teams create/update APIs based on their app needs without having to worry about security.
8. Code is compiled as part of the CI/CD process, the Swagger/RAML file is created with the API definitions, and services are updated.
9. Automatically register and update API definitions using the Akamai CLI for up-to-date endpoint-level protections.

KEY PRODUCTS

API discovery and profiling, hostname protection ▶ App & API Protector

API definition, endpoint protection ▶ App & API Protector, API Gateway

Network load balancing ▶ Global Traffic Management

Delivery ▶ Ion or API Acceleration, API Prioritization Cloudlet

CI/CD process ▶ Akamai CLI

Akamai

Published 02/22