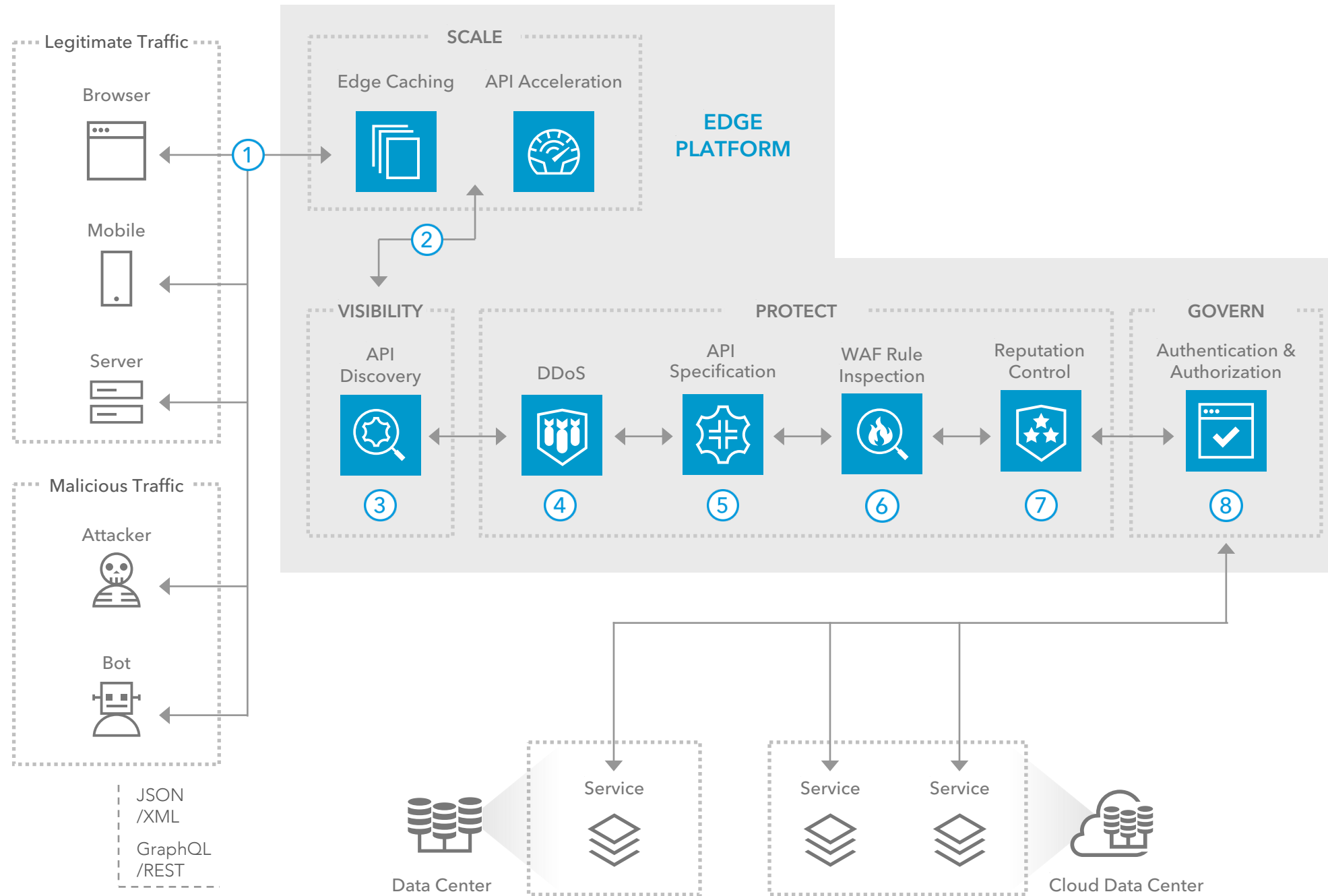


API DISCOVERY & SECURITY

Reference Architecture



OVERVIEW

Protecting APIs can be a significant hurdle when organizations lack visibility. After all, you can't protect what you can't see. With Akamai, automatic API discovery and profiling finds both protected and unprotected APIs — including their endpoints, definitions, and resource and traffic characteristics. Once identified, Akamai provides broad API protections against DDoS and injection attacks, and provides authentication and authorization at the edge.

- 1 Legitimate consumers (and malicious actors attempt to) access APIs through the Akamai Intelligent Edge Platform
- 2 Edge caching + API acceleration improves scalability and performance for all API traffic
- 3 API discovery and profiling capabilities inspect traffic to find both protected and unprotected API endpoints, their traffic, and risk profile to quickly apply protections
- 4 Automatically drop network-layer DDoS attacks and set rate limits to protect against application-layer DoS and other automated or excessive bot traffic
- 5 Positive API security allows for the ability to take action on API requests that violate predefined specifications
- 6 Inspect API requests for injection attacks such as SQL injections, XSS, file inclusion, and command injections
- 7 Stop traffic from malicious actors based on a reputation score derived from Akamai's visibility into prior malicious behavior
- 8 API Gateway validates API requests to ensure only legitimate consumers can access APIs

KEY PRODUCTS

- Edge caching, API acceleration ▶ API Acceleration
- API discovery and profiling ▶ Kona Site Defender
- DDoS protection, API specification, WAF rule inspection ▶ Kona Site Defender
- Reputation control ▶ Client Reputation
- Authentication and authorization ▶ API Gateway