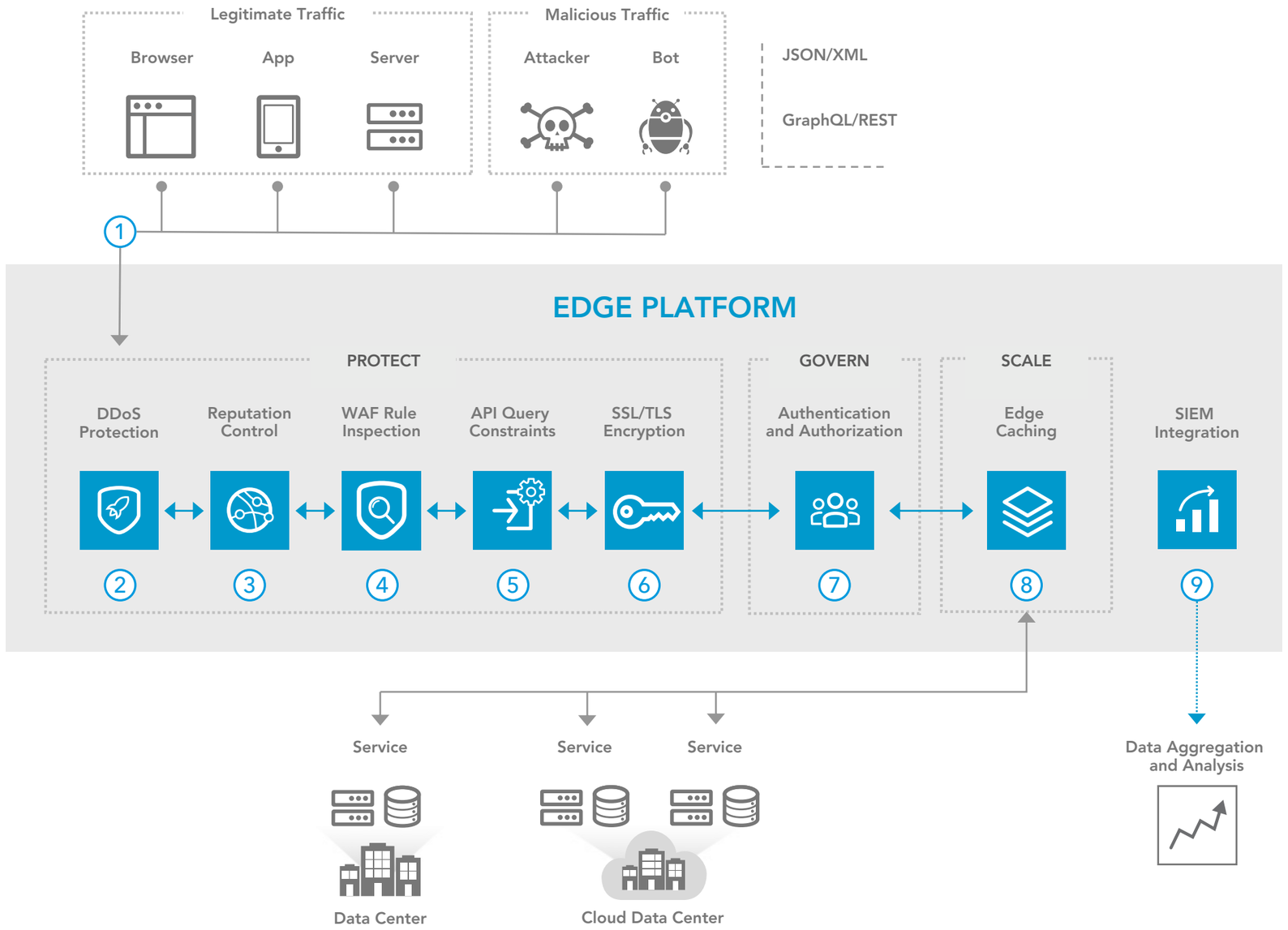
IMPROVE API SECURITY

Reference Architecture



OVERVIEW

API security often gets overlooked, or applied inconsistently. This leaves you vulnerable to malicious attacks, data breaches, and loss of revenue and brand value. Akamai solutions protect your APIs from DDoS, application, and credential stuffing attacks.
API protection is enforced at the Edge, far away from your infrastructure, improving your security posture across a broad and fragmented attack surface.

1. Legitimate consumers and malicious actors access APIs through the Akamai Intelligent Edge Platform.
2. Edge servers automatically drop network-layer DDoS attacks and protect the application layer from DDoS and application attacks.
3. Stop traffic from malicious actors based on their specific reputation score, which is derived from Akamai's visibility into prior behavior of their IP addresses.
4. Automatically inspect API requests for malicious content and block attack tools based on device fingerprinting.
5. Positive security model based on individual API specifications to prevent data extraction and insertion. Protect back-end microservices and applications from DoS-type attacks.
6. SSL/TLS encryption to prevent sensitive data exposure during transmission.
7. API Gateway validates API requests to ensure legitimate consumers can access APIs.
8. API responses can be served from cache to improve performance and reduce infrastructure and bandwidth costs.
9. Capture, retain, and deliver security information and events to your SIEM application in real time.

KEY PRODUCTS

Protect ▶ Kona Site Defender, Web Application Protector, or Bot Manager
Govern ▶ API Gateway
Scale ▶ Ion or Dynamic Site Accelerator
SIEM integration ▶ SIEM Connector

Published 08/19