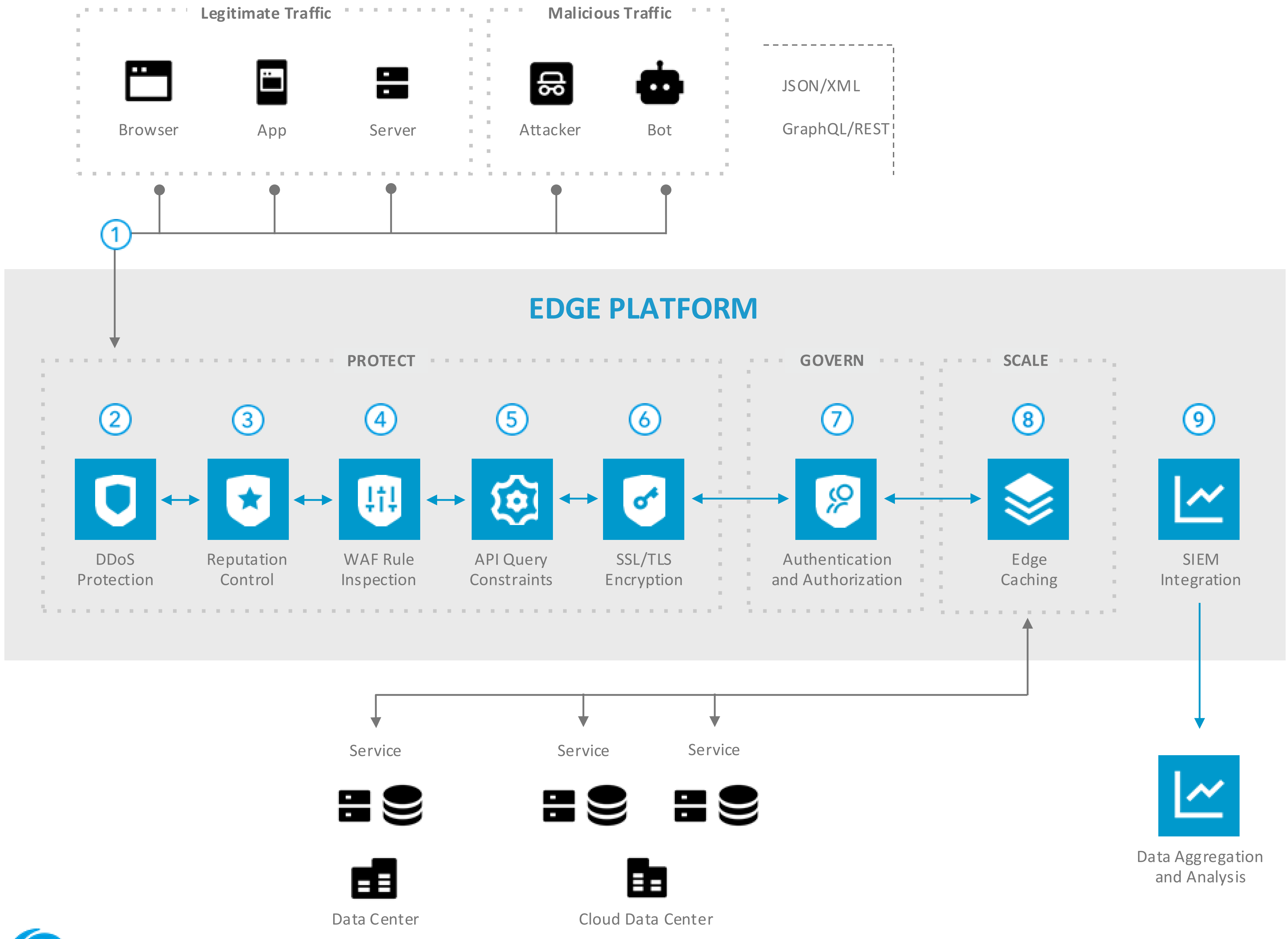
IMPROVE APPLICATION AND API SECURITY

Reference Architecture



OVERVIEW

Application 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 applications and APIs from DDoS, application, and credential stuffing attacks. Application and 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 applications and APIs through Akamai Connected Cloud.
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 application and API requests for malicious content and block attack tools based on device fingerprinting.
5. Positive security model based on individual application and API specifications helps to prevent data extraction and insertion. Protect back-end microservices and applications from DoS attacks.
6. SSL/TLS encryption prevents sensitive data exposure during transmission.
7. API Gateway validates API requests to ensure legitimate consumers can access APIs.
8. Application and 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 ▶ App & API Protector or Bot Manager

Govern ▶ API Gateway

Scale ▶ Ion

SIEM Integration ▶ SIEM connector

Akamai

Published 11/24