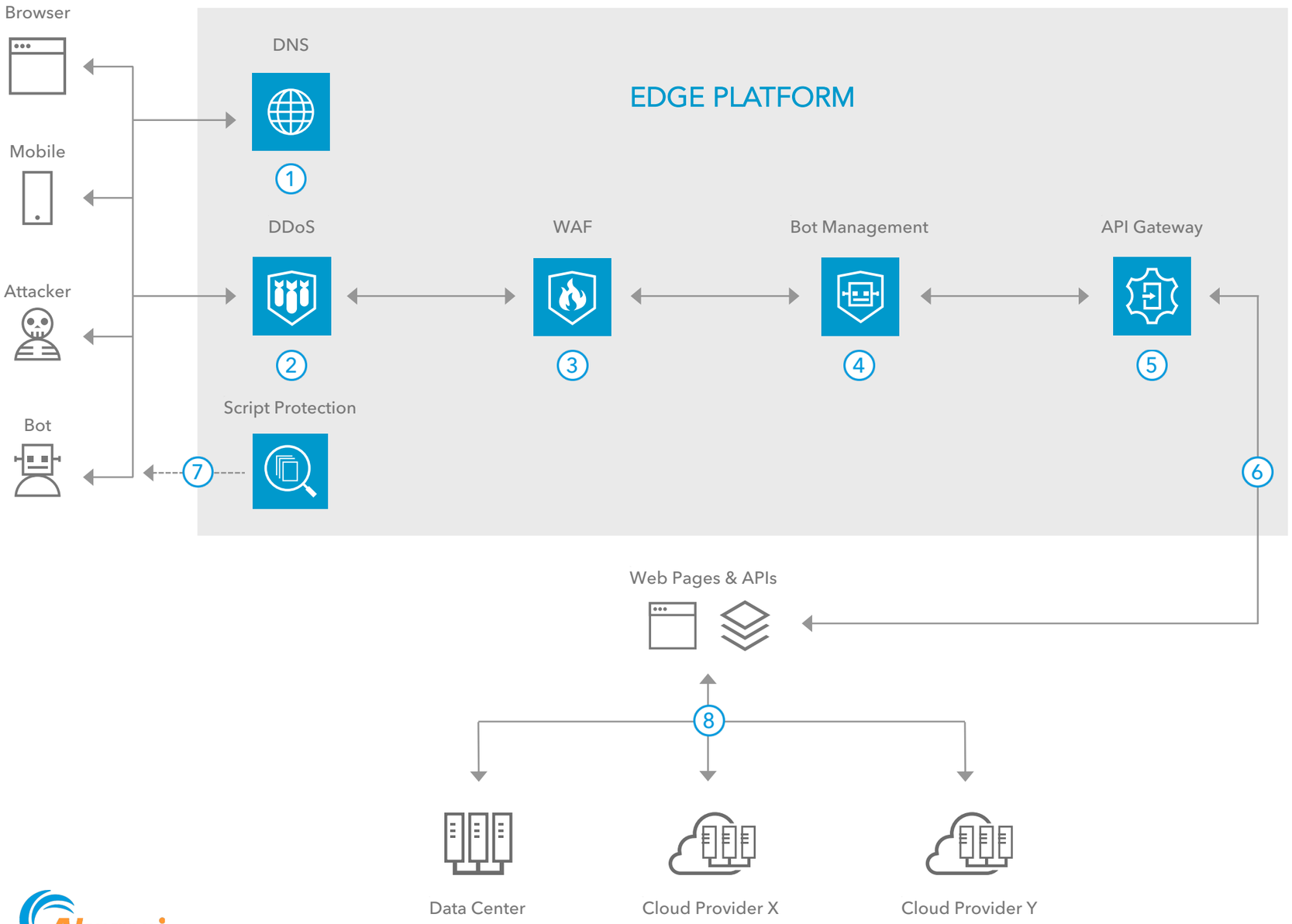
SECURING MULTI-CLOUD

Reference Architecture



OVERVIEW

Migrating to the cloud is the just first step in the cloud journey. The next step employs multiple cloud providers in unison to leverage their different capabilities where they make sense for your business, applications, and developer teams.

Security teams responsible for protecting applications deployed across multi-cloud environments need a single set of security controls to maintain a consistent security posture, and they need to scale their staff and resources to meet the demands of the business.

1. Authoritative DNS resolves client lookup requests while protecting against the largest DDoS attacks.
2. Edge servers automatically drop network-layer DDoS attacks and respond to application-layer DDoS attacks within seconds.
3. Web application firewall inspects web requests and blocks malicious threats like SQL injections, XSS, and RFI.
4. Bot management identifies and manages bot traffic with a variety of advanced and conditional actions.
5. API gateway governs API traffic by authenticating, authorizing, and controlling requests from API consumers like mobile apps.
6. Akamai Intelligent Edge Platform routes legitimate browser and mobile (and specified bot) traffic to the web application.
7. Script protection monitors the behavior of third-party scripts to identify and mitigate web skimming and Magecart-style attacks.
8. Web applications can be deployed in any combination of on-premises or cloud data centers, from one or multiple providers.

KEY PRODUCTS

DNS ▶ Edge DNS
DDoS ▶ Kona Site Defender or Web Application Protector
WAF ▶ Kona Site Defender or Web Application Protector
API protection ▶ Kona Site Defender or Web Application Protector
Bot management ▶ Bot Manager
API gateway ▶ API Gateway
Script protection ▶ Page Integrity Manager

Published 08/20