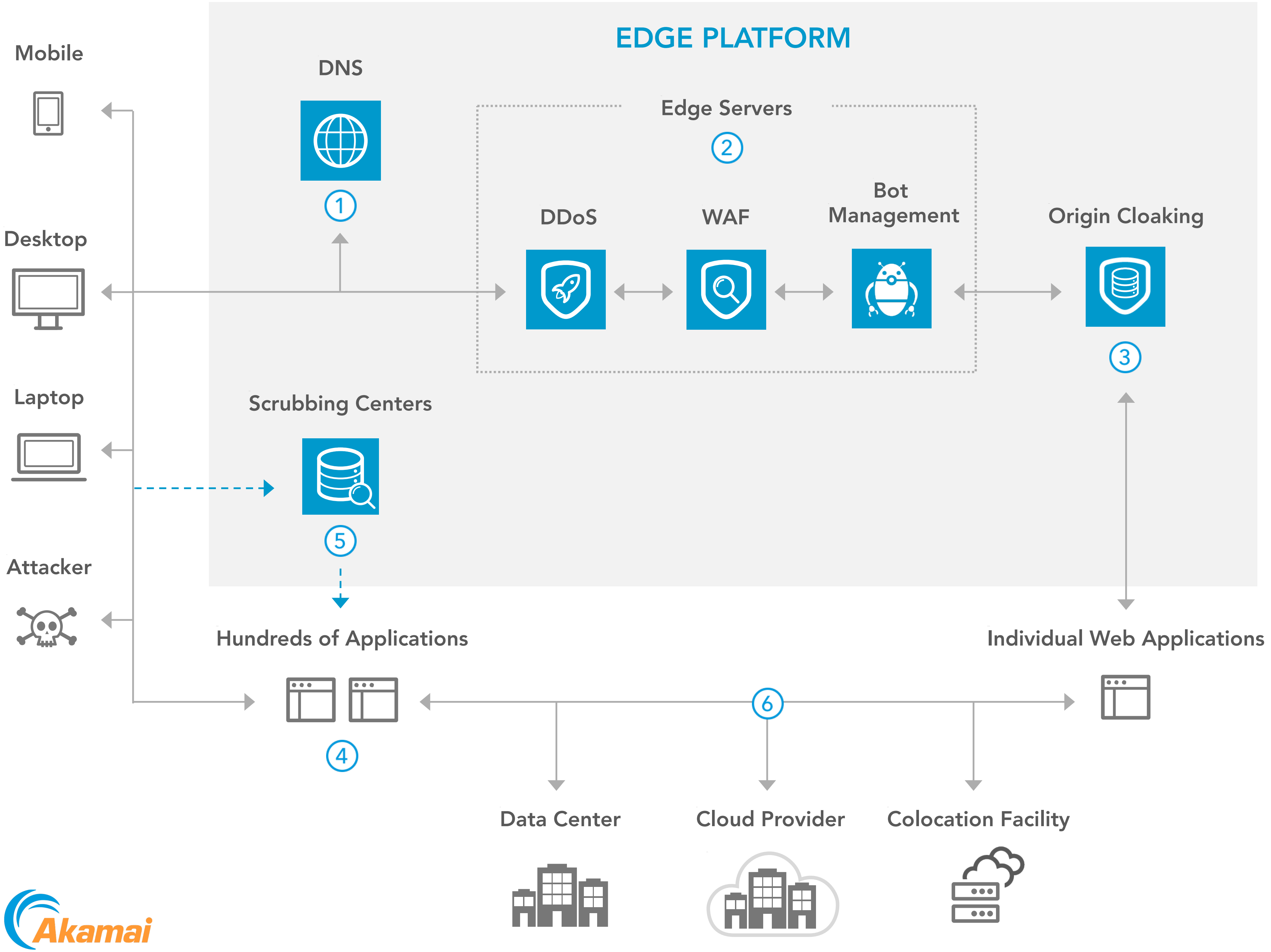
DDoS PROTECTION

Reference Architecture



Akamai

OVERVIEW

Akamai mitigates the risk of DDoS attacks with fast and effective protection designed to counter the largest and most sophisticated DDoS attacks, whether applications are deployed in the data center, public cloud infrastructure, or colocation facility.

1. Clients perform a DNS lookup against Akamai's DNS service, which has absorbed even the largest DDoS attacks.

2. Edge servers automatically inspect CDN traffic for DDoS, web application, and bot attacks — and block malicious threats.

3. Akamai routes CDN traffic through designated edge servers, allowing customers to drop traffic from other sources and prevent attackers from bypassing edge-based protection.

4. Non-CDN traffic is typically routed directly to the origin based on customer BGP route advertisements.

5. Customers can route traffic through Akamai scrubbing centers (always-on or on-demand), where DDoS attacks are blocked through proactive mitigation controls or active SOC mitigation.

6. Both Akamai's CDN-based and DDoS-scrubbing services can protect applications deployed in customer data centers, public cloud infrastructure, or in colocation facilities.

KEY PRODUCTS

DNS ▶ Edge DNS

DDoS/WAF ▶ Kona Site Defender or Web Application Protector

Bot ▶ Bot Manager

Scrubbing Centers ▶ Prolexic Routed

Published 03/20