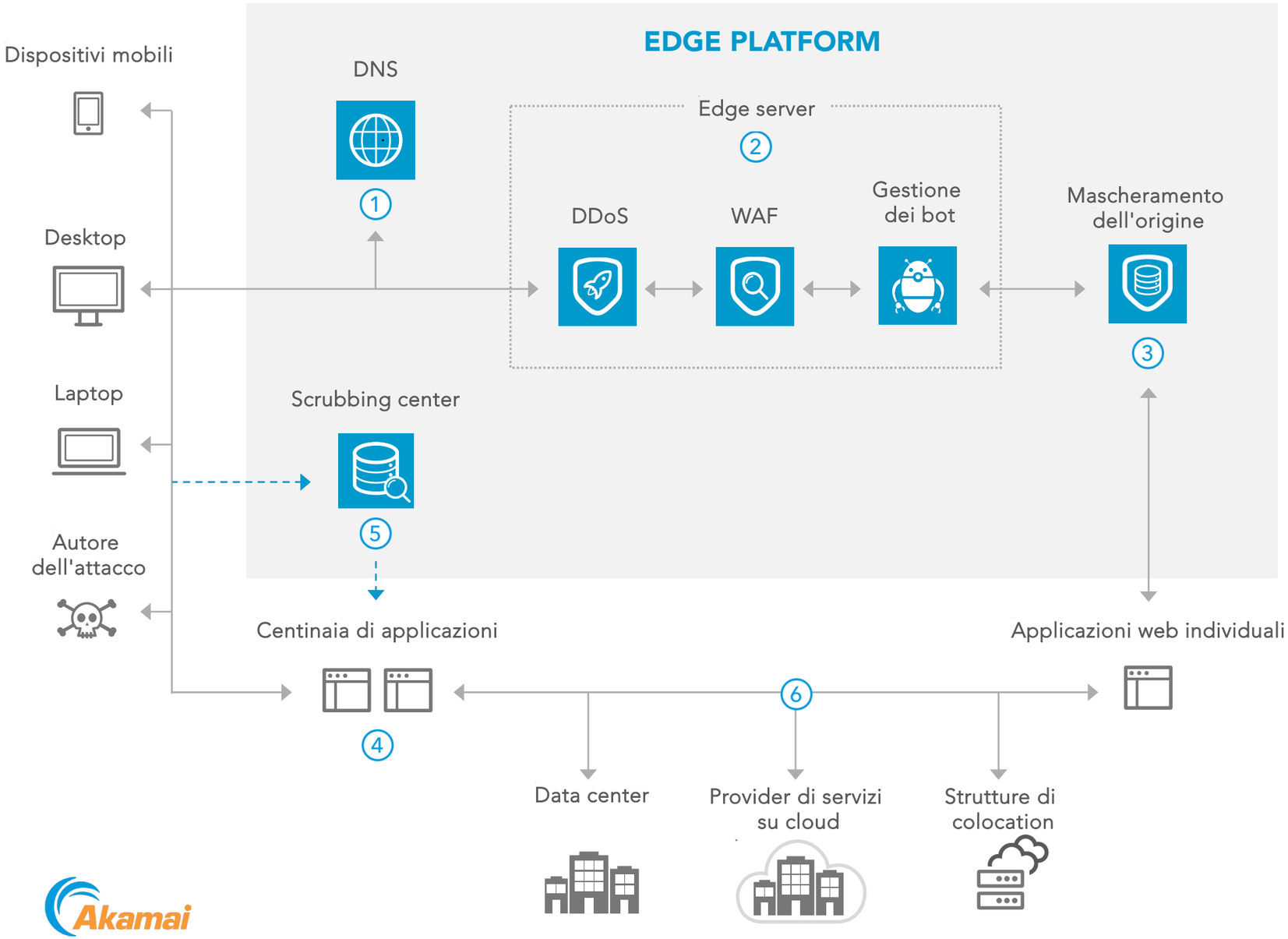
PROTEZIONE CONTRO GLI ATTACCHI DDoS

Architettura di riferimento



PANORAMICA

Akamai mitiga il rischio di attacchi DDoS con una protezione rapida ed efficace, concepita per contrastare i più imponenti e sofisticati attacchi DDoS, ovunque siano state implementate le applicazioni (nei data center, sull'infrastruttura del cloud pubblico o in strutture di colocation).

1. I client eseguono una ricerca DNS sulla base del servizio DNS di Akamai, che ha assorbito anche gli attacchi DDoS più imponenti.
2. Gli edge server ispezionano automaticamente il traffico CDN per rilevare attacchi DDoS, alle applicazioni web e bot, bloccando eventualmente le minacce dannose.
3. Akamai instrada il traffico CDN tramite gli edge server designati per consentire ai clienti di bloccare il traffico proveniente da altre fonti e impedire ai malintenzionati di eludere la protezione basata sull'edge.
4. Il traffico non CDN viene solitamente instradato direttamente all'origine in base alle informazioni di routing del protocollo BGP (Border Gateway Protocol).
5. I clienti possono instradare il traffico tramite gli scrubbing center di Akamai (always-on oppure on-demand), se gli attacchi DDoS vengono bloccati tramite i controlli di mitigazione proattiva o la mitigazione attiva del SOC.
6. I servizi di scrubbing DDoS e CDN di Akamai possono proteggere le applicazioni implementate nei data center, sull'infrastruttura del cloud pubblico o in strutture di colocation.

PRODOTTI PRINCIPALI

DNS ▶ Edge DNS

DDoS/WAF ▶ Kona Site Defender o Web Application Protector

Bot ▶ Bot Manager

Scrubbing center ▶ Prolexic Routed

Data di pubblicazione: 03/20