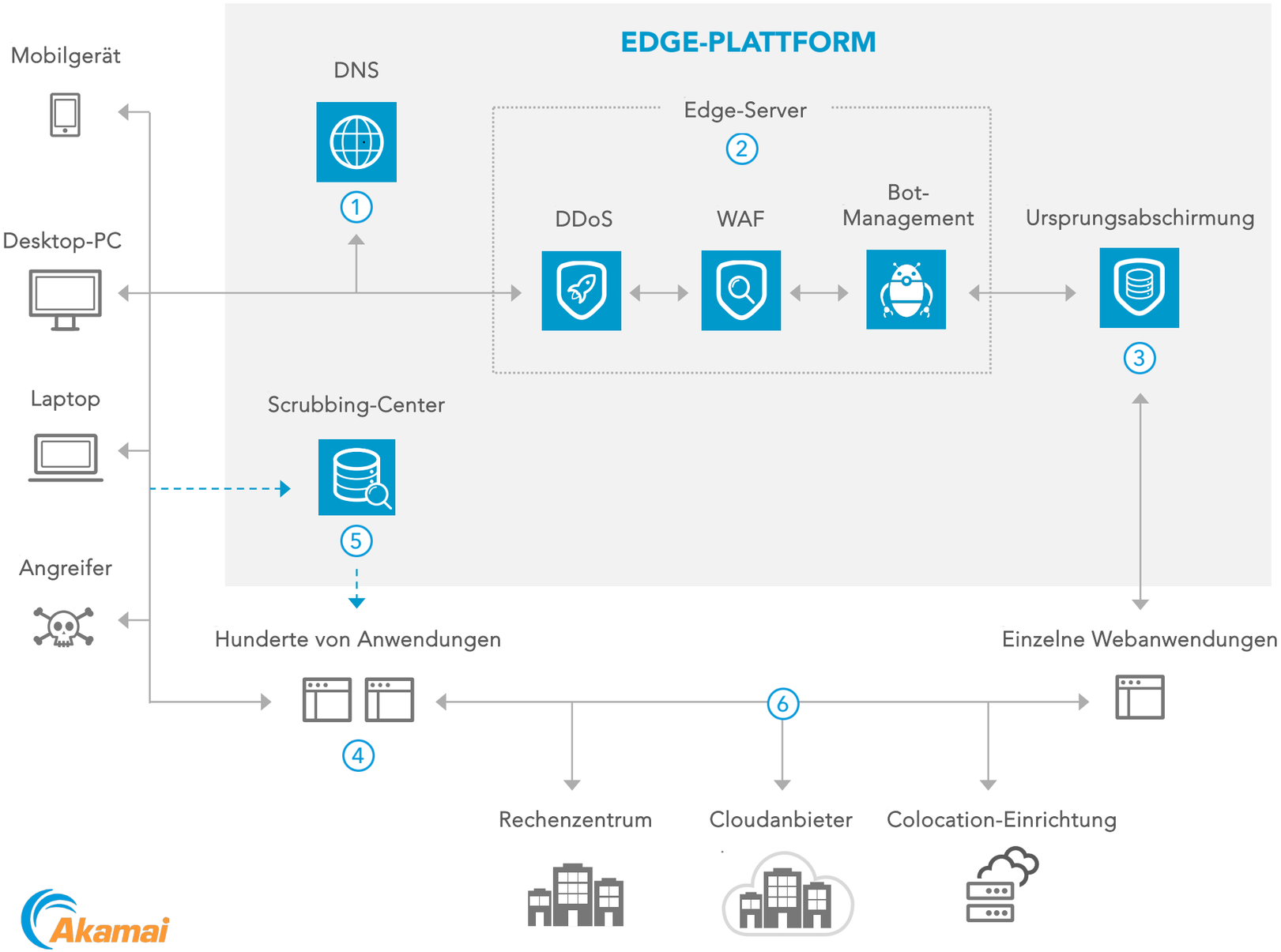
DDoS-SCHUTZ

Referenzarchitektur



ÜBERBLICK

Akamai verringert das Risiko von DDoS-Angriffen mit schnellem und effektivem Schutz, der selbst die größten und komplexesten DDoS-Angriffe abwehrt – unabhängig davon, ob Anwendungen im Rechenzentrum, in der Public Cloud oder in einer Colocation-Einrichtung bereitgestellt werden.

1. Mithilfe des DNS-Service von Akamai führen Clients eine DNS-Abfrage durch. Dieser Service konnte bereits die größten DDoS-Angriffe abfangen.
2. Edge-Server überprüfen CDN-Traffic automatisch auf DDoS-, Webanwendungs- und Bot-Angriffe und blockieren schädliche Bedrohungen.
3. Akamai leitet CDN-Traffic über ausgewählte Edge-Server weiter, sodass Kunden Traffic von anderen Quellen zurückweisen und Angreifer daran hindern können, den edgebasierten Schutz zu umgehen.
4. Nicht-CDN-Traffic wird in der Regel gemäß BGP-Routenankündigungen des Kunden direkt an den Ursprung weitergeleitet.
5. Kunden können Traffic über Scrubbing-Center von Akamai weiterleiten (durchgehend oder bei Bedarf), wo DDoS-Angriffe durch proaktive Abwehrmechanismen oder aktive SOC-Abwehr blockiert werden.
6. Anwendungen, die in Kundenrechenzentren, Public Clouds oder Colocation-Einrichtungen bereitgestellt werden, können sowohl durch CDN- als auch DDoS-Scrubbing-Dienste von Akamai geschützt werden.

HAUPTPRODUKTE

DNS ▶ Edge DNS
DDoS/WAF ▶ Kona Site Defender oder Web Application Protector
Bot-Management ▶ Bot Manager
Scrubbing-Center ▶ Prolexic Routed

Veröffentlicht: März 2020