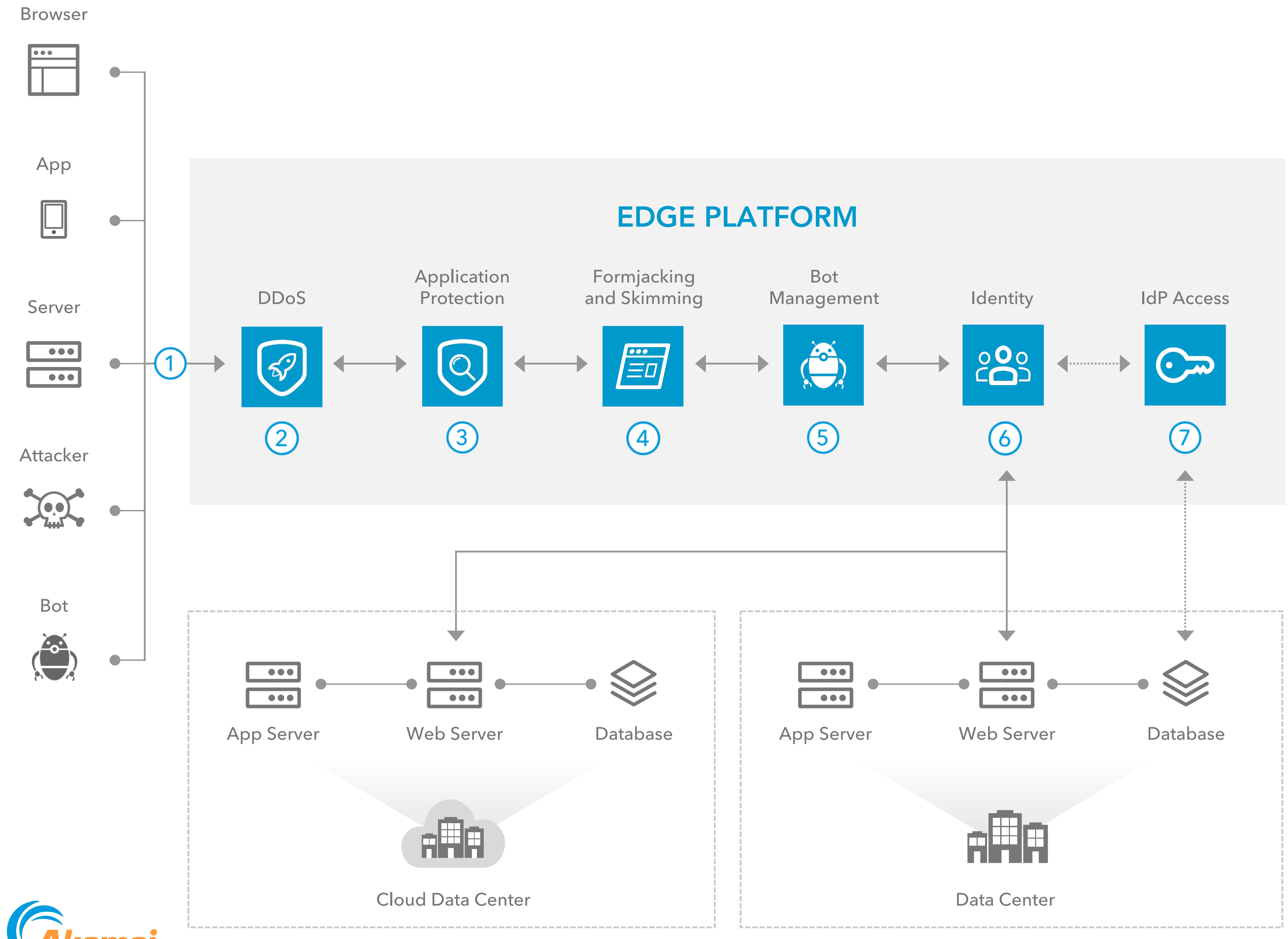
PREVENT ONLINE FRAUD AND CYBERCRIME

Reference Architecture



OVERVIEW

Financial institutions are appealing targets. They attract sophisticated criminals who constantly change attack vectors to avoid detection. Successful attacks introduce regulatory burdens and, more important, erode consumer trust.

Here's how Akamai solutions create a security posture to stay ahead of ever-changing threats and protect consumers' personal wealth, even as it makes new sign-ups easier.

1. The Akamai Intelligent Edge Platform supports application access through mutual TLS and other network controls, as well as leading forms of API authentication and authorization.

2. In addition to being a substantial threat, DDoS can sometimes distract targets from an attacker's true goals. Edge servers automatically drop network-layer DDoS floods and protect against application-layer attacks.

3. Protect application data through both web request inspections and positive security models, which use specific parameters defined in the API configuration file.

4. Deep inspection and analysis of the pages to uncover compromised scripts and protect data.

5. Protect against credential abuse attempts and possible account takeover (ATO), using capabilities that identify the newest and most sophisticated bots.

6. Customer identity and access management (CIAM) at the edge secures sensitive information to ensure performance, personalization, data protection, and support for a complex regulatory environment.

7. Option to store credentials in an on-premises directory or in a first-party application.

KEY PRODUCTS

DDoS, application, and formjacking protection ▶ Kona Site Defender

Bot management ▶ Bot Manager

Identity and application access ▶ Identity Cloud and Enterprise Application Access

Published 05/20