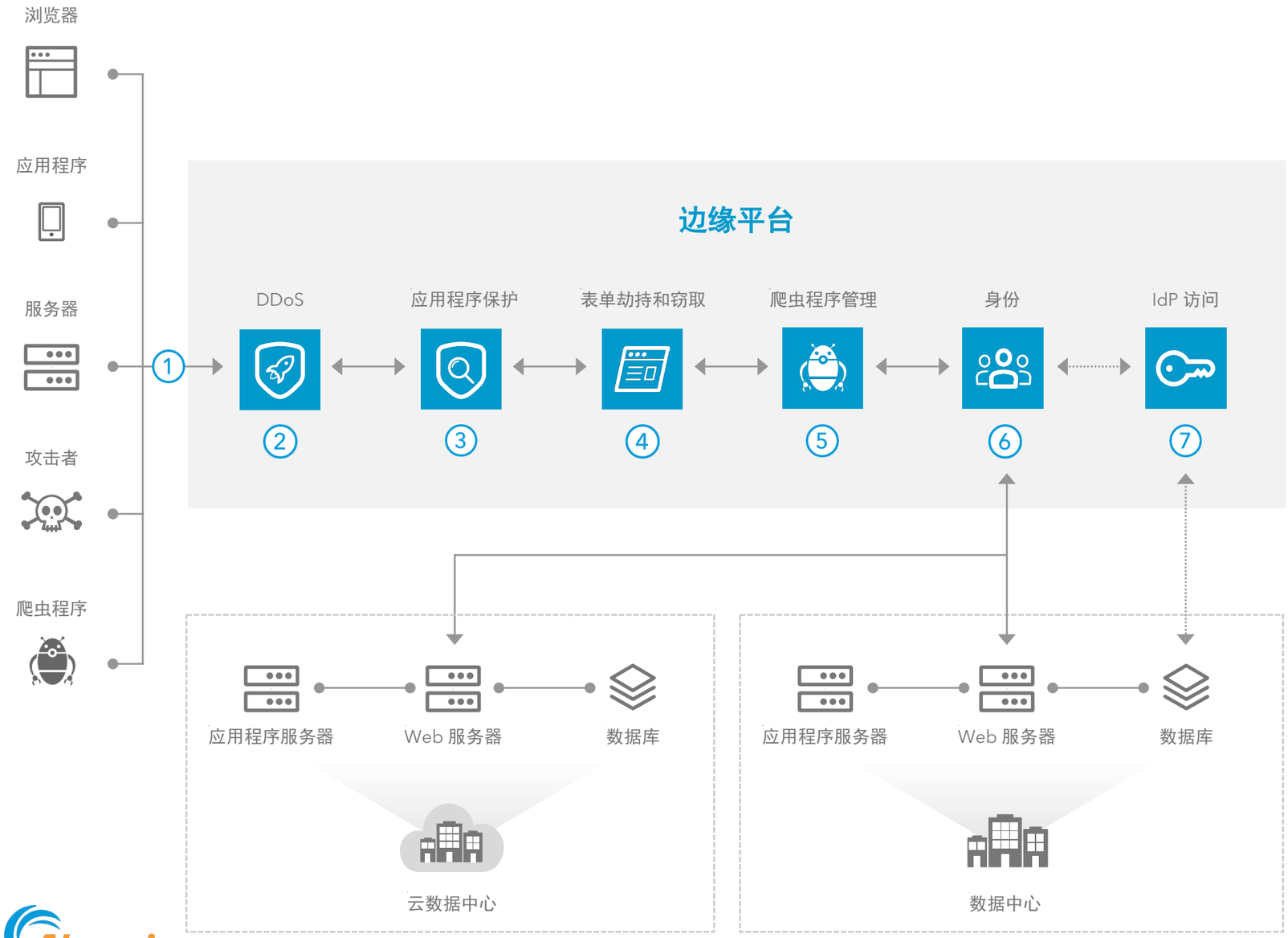
防止在线欺诈和网络犯罪

参考架构



概述

金融机构是具有吸引力的攻击目标。这些机构对于老练的犯罪分子特别有吸引力，这些攻击者会不断地更换攻击媒介来规避检测。一旦被攻击成功侵入，不仅仅是带来监管负担，更重要的是会降低消费者的信任度。

Akamai 解决方案通过以下方式建立安全态势，从而在面对不断变化的威胁时保持领先，并保护消费者的个人财富，同时让新用户注册过程变得更加轻松。

1. Akamai Intelligent Edge Platform 支持通过双向 TLS 及其他网络控件进行应用程序访问，还支持出色的 API 身份验证和授权方法。
2. 除了构成重大威胁外，DDoS 有时还会使攻击目标分散注意力，导致无法发现攻击者的真实目的。边缘服务器可自动阻止网络层 DDoS 泛洪攻击并防范应用程序层攻击。
3. 通过 Web 请求检查和主动安全模型（使用 API 配置文件中定义的特定参数）来保护应用程序数据。
4. 深入检查和分析页面，确保发现被入侵的脚本并保护数据。
5. 使用相应的功能来识别最新的复杂爬虫程序，以防止撞库攻击和可能的帐户接管 (ATO)。
6. 边缘的客户身份和访问管理 (CIAM) 可保护敏感信息，以确保出色的性能、个性化、数据保护以及对复杂监管环境的有力支持。
7. 可选择将凭据存储在本地目录或第一方应用程序中。

关键产品

DDoS、应用程序和表单劫持防护 ▶ Kona Site Defender

爬虫程序管理 ▶ Bot Manager

身份和应用程序访问 ▶ Identity Cloud 和 Enterprise Application Access

发布时间：2020 年 5 月