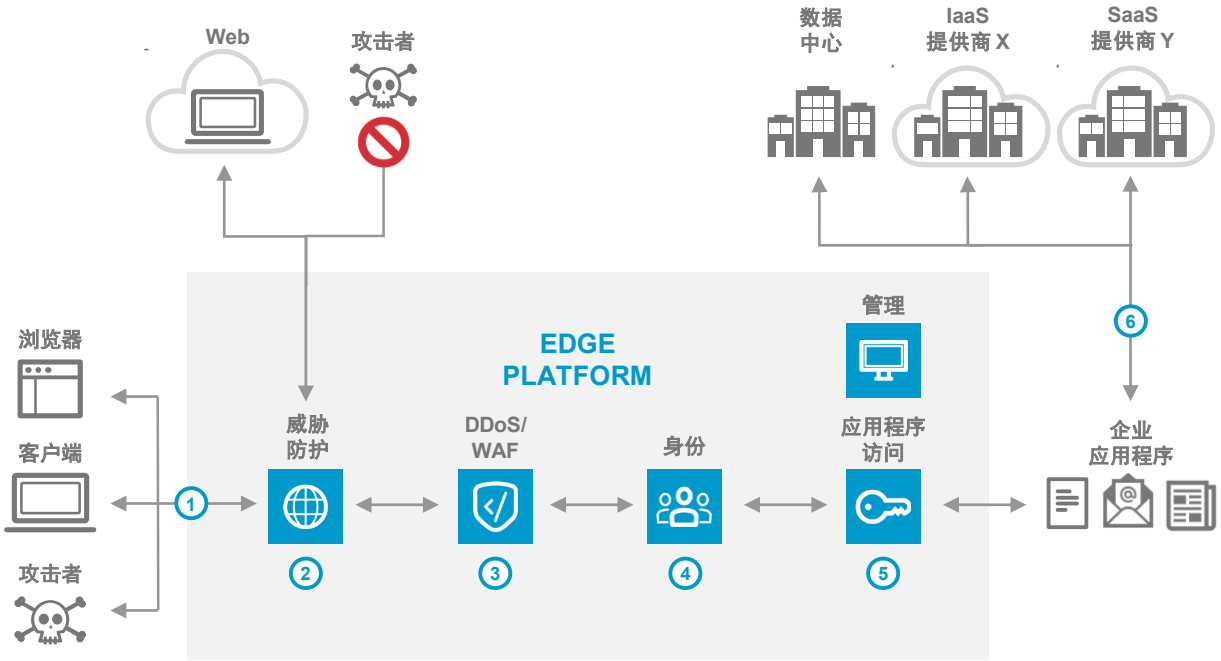
ZERO TRUST 安全

参考架构



概览

Zero Trust 安全架构最大限度地降低了恶意攻击者渗入边界、横向移动和泄露数据的风险。Zero Trust 基于最低权限和默认拒绝，支持您通过一组安全和访问控制保护用户和提供访问，即使您根据业务需求扩展有限的资源也是如此。

1. 用户可通过 Akamai Intelligent Edge Platform 访问公司应用程序和 Web。
2. 威胁防护可保护用户免受恶意软件、网络钓鱼和恶意 Web 内容的攻击，同时为企业提供可见性。
3. 对于企业应用程序，边缘服务器自动阻止网络层 DDoS 攻击并检查 Web 请求以阻止 SQL 注入、XSS 和 RFI 等恶意威胁。
4. 使用本地、基于云的或 Akamai 身份存储确定用户身份。
5. 根据用户的身份和其他安全信号，仅提供所需应用程序（而不是整个企业网络）的访问权限。
6. Akamai Intelligent Edge Platform 将授权和验证的用户路由到相关的企业应用程序。

关键产品

威胁防御 ▶ Enterprise Threat Protector
DDoS/WAF ▶ Kona Site Defender 或 Web Application Protector
身份和应用程序访问 ▶ Enterprise Application Access

Akamai