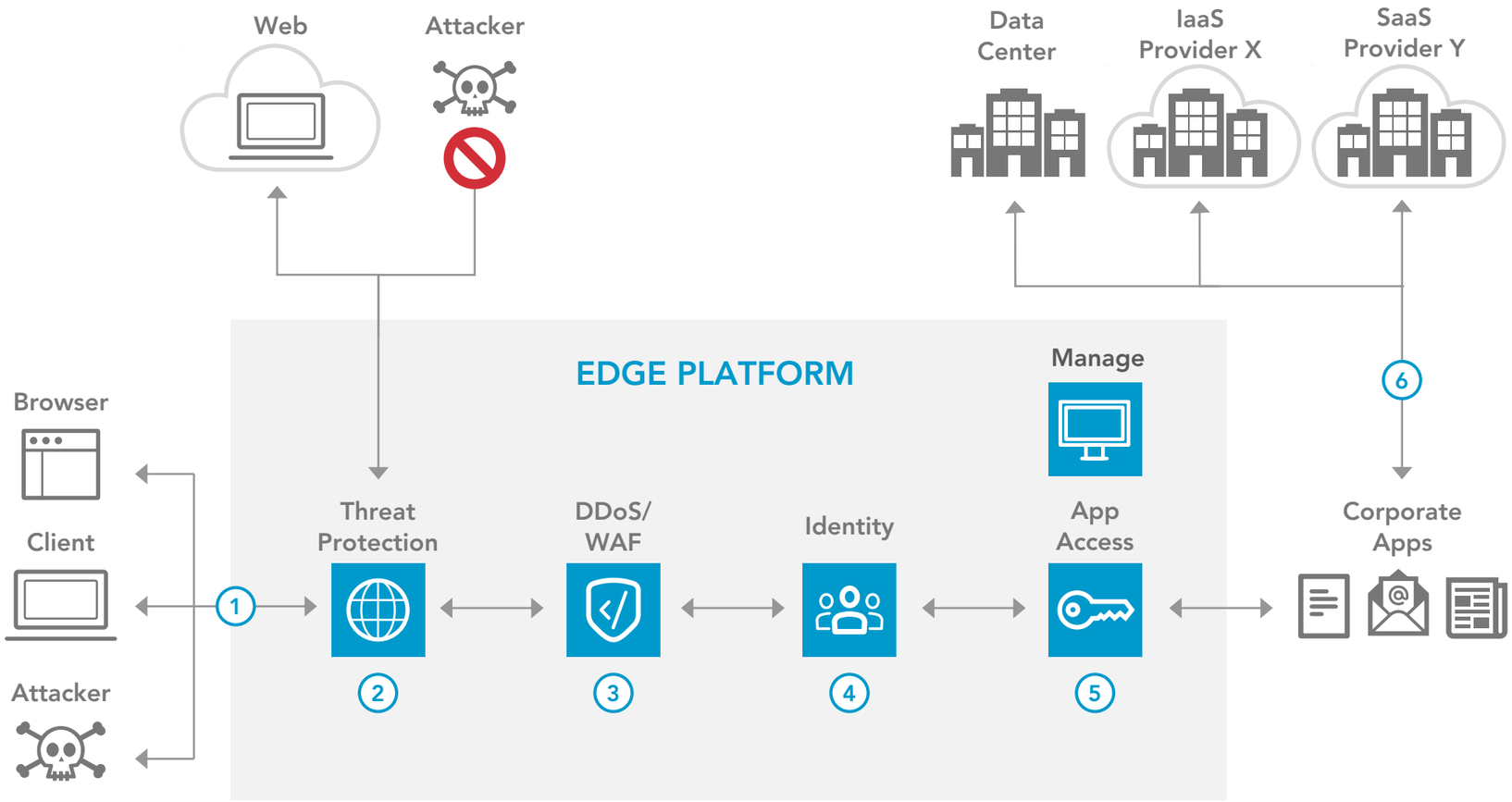
ZERO TRUST SECURITY

Reference Architecture



OVERVIEW

A Zero Trust security architecture minimizes the risk of malicious actors penetrating the perimeter, moving laterally, and exfiltrating data. Based on least privilege and default deny, Zero Trust lets you protect users and provide access through a single set of security and access controls, even as you scale finite resources to the needs of the business.

1. Users access corporate applications and the web through the Akamai Intelligent Edge Platform.
2. Threat protection defends users from malware, phishing, and malicious web content, while providing visibility to the enterprise.
3. For corporate applications, edge servers automatically drop network-layer DDoS attacks and inspect web requests to block malicious threats like SQL injections, XSS, and RFI.
4. Identity of the user is established using on-premises, cloud-based, or Akamai identity stores.
5. Based on the user's identity and other security signals, access is provided only to required applications, and not the entire corporate network.
6. The Akamai Intelligent Edge Platform routes authorized and authenticated users to the relevant corporate applications.

KEY PRODUCTS

Threat protection ▶ Enterprise Threat Protector
DDoS/WAF ▶ Kona Site Defender or Web Application Protector
Identity and application access ▶ Enterprise Application Access

Akamai