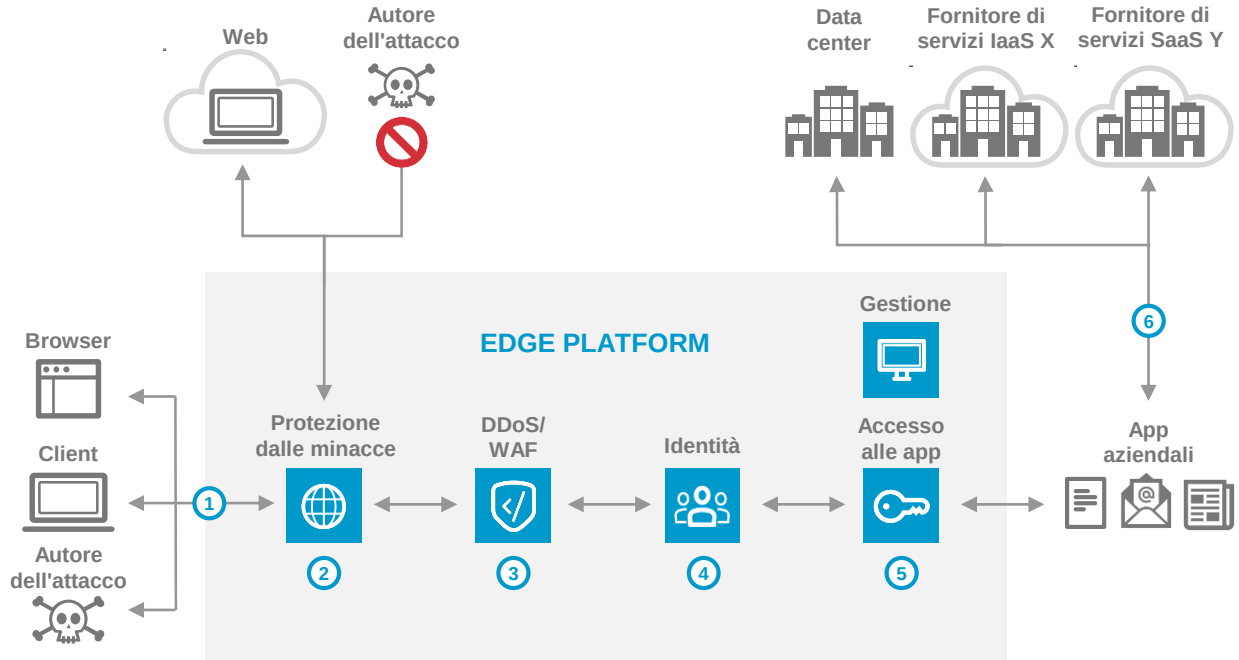
SICUREZZA ZERO TRUST

Architettura di riferimento



PANORAMICA

Un'architettura di sicurezza Zero Trust minimizza il rischio di penetrazione del perimetro di rete, con spostamenti laterali ed esfiltrazione di dati da parte di malintenzionati. Basato sul principio del privilegio minimo e del rifiuto per impostazione predefinita, il modello Zero Trust vi consente di proteggere gli utenti e di fornire l'accesso tramite una sola serie di controlli di sicurezza e degli accessi, anche quando si adattano risorse limitate per soddisfare le esigenze aziendali.

1. Gli utenti accedono alle applicazioni aziendali e al web tramite l'Akamai Intelligent Edge Platform.
2. La protezione dalle minacce difende gli utenti da malware, phishing e contenuti web dannosi, fornendo, al contempo, visibilità all'azienda.
3. Per le applicazioni aziendali, gli edge server bloccano automaticamente gli attacchi DDoS a livello di rete ed esaminano le richieste web per bloccare eventuali minacce dannose, come gli attacchi SQL injection, XSS e RFI.
4. L'identità dell'utente viene stabilita tramite appositi archivi Akamai, in sede o sul cloud.
5. In base all'identità dell'utente e ad altri segnali relativi alla sicurezza, l'accesso viene fornito solo alle applicazioni richieste e non all'intera rete aziendale.
6. L'Akamai Intelligent Edge Platform instrada gli utenti autorizzati e autenticati alle applicazioni aziendali pertinenti.

PRODOTTI PRINCIPALI

Protezione dalle minacce ► Enterprise Threat Protector
DDoS/WAF ► Kona Site Defender o Web Application Protector
Accesso a identità e applicazioni ► Enterprise Application Access

Akamai