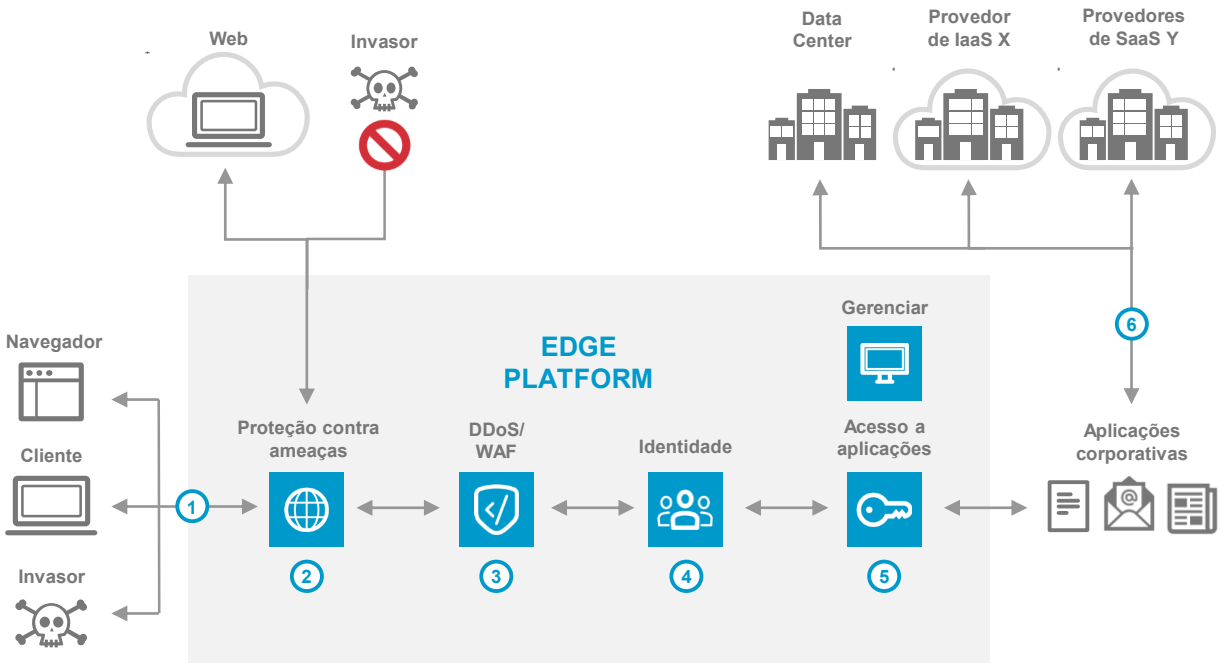
SEGURANÇA ZERO TRUST

Arquitetura de referência



VISÃO GERAL

Uma arquitetura de segurança Zero Trust minimiza o risco de agentes mal-intencionados penetrarem no perímetro, moverem-se lateralmente e extraírem dados. Com base no privilégio mínimo e na negação padrão, o Zero Trust permite que você proteja os usuários e forneça acesso por meio de um conjunto único de controles de segurança e acesso, mesmo quando você escalona recursos finitos de acordo com as necessidades da empresa.

1. Os usuários acessam aplicações corporativas e a Web por meio da Akamai Intelligent Edge Platform.
2. A proteção contra ameaças protege os usuários contra malware, phishing e conteúdo malicioso da Web, ao tempo em que fornece visibilidade para a empresa.
3. Para aplicações corporativas, os servidores de borda derrubam automaticamente ataques DDoS na camada de rede e inspecionam solicitações da Web para bloquear ameaças maliciosas, como injeções de SQL, XSS e RFI.
4. A identidade do usuário é estabelecida usando armazenamentos de identidade locais baseados em nuvem ou da Akamai.
5. Com base na identidade do usuário e em outros sinais de segurança, o acesso é fornecido apenas para as aplicações necessárias, e não para toda a rede corporativa.
6. A Akamai Intelligent Edge Platform encaminha usuários autorizados e autenticados para as aplicações corporativas relevantes.

PRINCIPAIS PRODUTOS

Proteção contra ameaças ► Enterprise Threat Protector
DDoS/WAF ► Kona Site Defender ou Web Application Protector
Acesso a identidades e aplicações ► Enterprise Application Access

Akamai