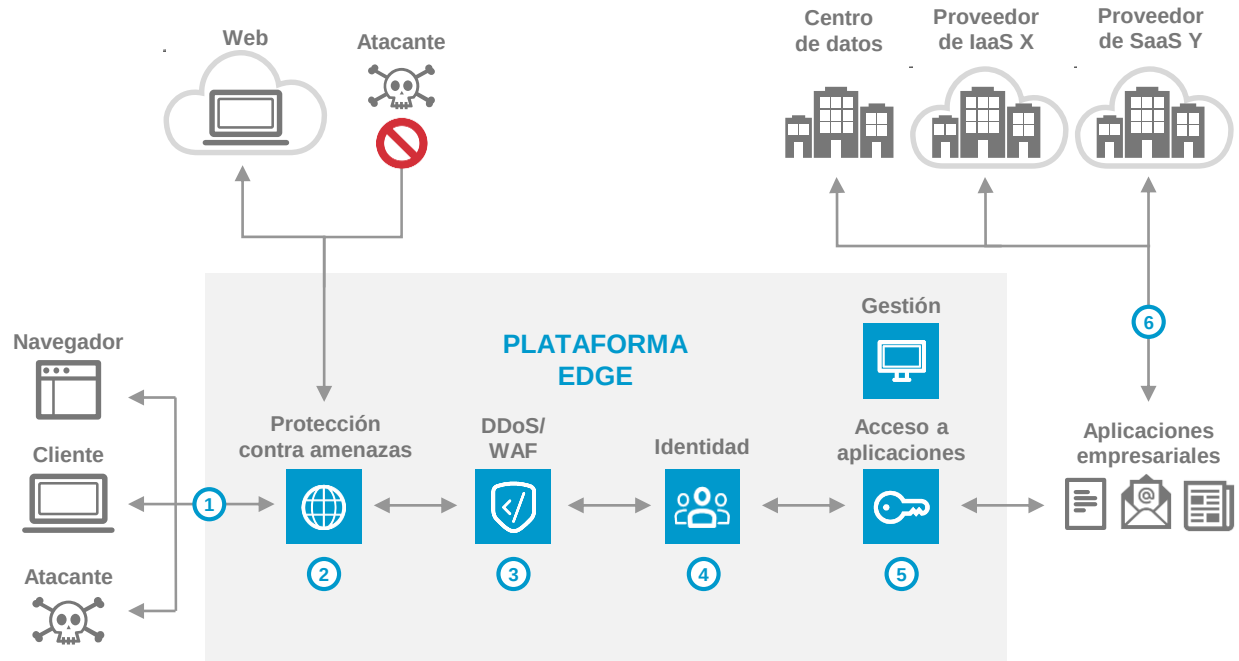
SEGURIDAD ZERO TRUST

Arquitectura de referencia



DESCRIPCIÓN GENERAL

La arquitectura de seguridad Zero Trust reduce al mínimo el riesgo de que los agentes maliciosos traspasen el perímetro y, una vez dentro, se desplacen lateralmente y extraigan datos. Este modelo, basado en el mínimo privilegio y la denegación predeterminada, le permite proteger a los usuarios y proporcionar acceso mediante un conjunto único de controles de seguridad y acceso, incluso a medida que escala los recursos finitos según las necesidades de su empresa.

1. Los usuarios acceden a las aplicaciones empresariales y a la Web a través de Akamai Intelligent Edge Platform.
2. La protección contra amenazas defiende a los usuarios contra el malware, el phishing y el contenido web malicioso, además de proporcionar visibilidad a la empresa.
3. Los servidores del borde de Internet bloquean automáticamente los ataques DDoS dirigidos a la capa de red e inspeccionan las solicitudes web para bloquear las amenazas maliciosas, como inyecciones SQL, XSS y RFI.
4. La identidad del usuario se establece con almacenes de identidades locales, en la nube o de Akamai.
5. En función de la identidad del usuario y otras señales de seguridad, se proporciona acceso únicamente a las aplicaciones requeridas y no a toda la red corporativa.
6. Akamai Intelligent Edge Platform dirige los usuarios autorizados y autenticados a las aplicaciones corporativas correspondientes.

PRODUCTOS CLAVE

Protección contra amenazas ► Enterprise Threat Protector
DDoS/WAF ► Kona Site Defender o Web Application Protector
Identidad y acceso a aplicaciones ► Enterprise Application Access

Akamai