

Enterprise Application Access y Secure Enterprise Browser de Akamai



Las soluciones tradicionales de Edge de servicio de seguridad (SSE) prometen una protección completa, pero a menudo suelen traducirse en seguridad fragmentada, procesos complejos y experiencias frustrantes para el usuario, lo que tiene un impacto directo en la productividad. Muchas organizaciones se ven atrapadas en la gestión de marcos de políticas complejas y en los cuellos de botella que generan los proxy, mientras intentan defenderse de amenazas web cada vez más sofisticadas.

Enterprise Application Access y Secure Enterprise Browser de Akamai

Enterprise Application Access y Secure Enterprise Browser de Akamai, con tecnología Seraphic, abordan los casos de uso de SSE más importantes: acceso seguro a las aplicaciones, seguridad web y protección de datos. Todo ello con un enfoque centrado en el rendimiento. Esta combinación proporciona acceso de red Zero Trust (ZTNA) a aplicaciones empresariales privadas, así como seguridad avanzada para las aplicaciones SaaS y el acceso a Internet. Además, elimina las brechas de cobertura que suelen presentar las plataformas tradicionales.

En lugar de intentar abarcar todo, esta solución se centra en los requisitos de seguridad básicos, lo que resulta en un rendimiento superior, una menor complejidad operativa y un coste total de propiedad más bajo.

Características y capacidades clave

Acceso seguro (ZTNA para aplicaciones privadas)

- **Control de acceso basado en identidades**, que sustituye el acceso amplio a la red por permisos granulares basados en la identidad para aplicaciones empresariales.
- **Aplicación de políticas dinámicas** basadas en la identidad del usuario, el nivel de seguridad del dispositivo y una evaluación de los riesgos en tiempo real.
- **Integración con proveedores de identidad**, que aprovecha los marcos de identidad empresarial existentes y facilita el acceso sin complicaciones a aplicaciones privadas.
- **Prevención frente a la pérdida de datos** mediante análisis de contenido en tiempo real y la aplicación de políticas para aplicaciones privadas.
- **Compatibilidad con aplicaciones privadas multinube** y acceso seguro a las aplicaciones internas tanto en entornos híbridos como nativos de la nube.

Ventajas para su empresa

- ✓ **Obtenga mejores resultados de SSE** con soluciones especializadas centradas en casos de uso concretos, y no en abordar varios dominios de seguridad. Este enfoque garantiza un rendimiento superior en el acceso a aplicaciones, la seguridad del navegador y la protección de datos actual, tanto en dispositivos gestionados como no gestionados.
- 📊 **Controle el intercambio de datos en herramientas de IA generativa** con visibilidad en tiempo real y la aplicación de políticas de datos en ChatGPT y Copilot, entre otras plataformas. Así, podrá impulsar la productividad sin poner el riesgo la propiedad intelectual ni el cumplimiento normativo.
- 🕒 **Genere valor más rápido** con una implementación y gestión simplificadas, frente a las implementaciones completas de SSE. Esta propuesta cubre los casos de uso clave que impulsan la mayoría de las iniciativas SSE, incluidos los nuevos requisitos de gobernanza.
- 👤 **Optimice la experiencia del usuario** y aproveche el navegador que ya utiliza, sin imponer nuevas interfaces, navegadores especializados ni sacrificar el rendimiento de las aplicaciones, algo habitual en las plataformas SSE tradicionales.
- 📈 **Reduzca la complejidad y los costes de SSE** con una arquitectura optimizada que ofrece funciones básicas de seguridad web y acceso seguro, sin necesidad de licencias completas de plataforma, servicios profesionales exhaustivos ni una gestión continua y compleja.

- **Acceso tanto sin cliente como basado en el cliente**, capaz de adaptarse a distintos escenarios de usuario sin la complejidad de las VPN tradicionales.
- **Entrega optimizada para el rendimiento** gracias a la infraestructura global de Akamai en el Edge.

Seguridad web y protección de datos (SaaS y acceso a Internet)

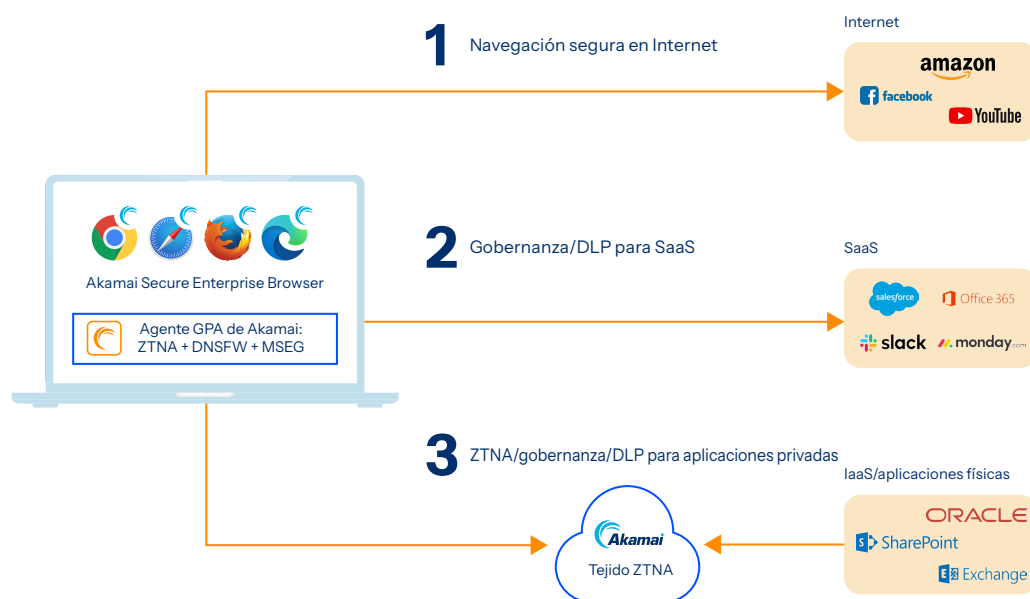
- **Control del acceso a aplicaciones SaaS** mediante políticas basadas en el nivel de seguridad del dispositivo para sistemas en la nube.
- **Anticipación avanzada a amenazas**, como ataques web sofisticados, de día cero y basados en la identidad, sin retrasos en la detección.
- **Prevención integral frente a la pérdida de datos** con análisis del contenido en tiempo real, enmascaramiento de datos confidenciales y la aplicación de políticas en aplicaciones SaaS, navegadores web y LLM con IA.
- **Seguridad independiente del navegador**, que transforma cualquier navegador en un navegador seguro de nivel empresarial para el acceso a SaaS e Internet.
- **Protección a nivel de sesión**, con seguridad de identidad y gestión cifrada de sesiones.
- **Seguridad de las aplicaciones SaaS**, que extiende la protección a herramientas de colaboración modernas, como Slack, Teams y otras aplicaciones en la nube.

Capacidades de reemplazo de SSE

- **Protección directa de SaaS y web**, que elimina la necesidad de soluciones CASB independientes.
- **Prevención de amenazas integrada**, que sustituye la funcionalidad de puerta de enlace web segura.
- **Seguridad nativa del navegador**, que ofrece ventajas de aislamiento remoto del navegador sin sacrificar el rendimiento.

Arquitectura SSE optimizada

En lugar de implementar una plataforma de SSE rígida, esta solución ofrece resultados de SSE mediante dos componentes optimizados que trabajan de forma coordinada.



Seguridad de red distribuida en el Edge: El acceso Zero Trust a aplicaciones empresariales privadas, distribuido desde Akamai Cloud, elimina las brechas de seguridad de red que abordan las soluciones SSE, al tiempo que ofrece un rendimiento superior gracias a su red global de puntos de presencia. Esto sustituye tanto la puerta de enlace web segura como los componentes ZTNA de las plataformas SSE tradicionales para el acceso interno a aplicaciones.

Protección de datos a nivel de navegador: La seguridad avanzada del navegador ofrece una protección integral para aplicaciones SaaS y el acceso a Internet, lo que evita la pérdida de datos y proporciona una seguridad web avanzada directamente en el punto de interacción de cada usuario. Al proteger el navegador —el lugar donde los usuarios acceden tanto a aplicaciones SaaS autorizadas como a contenido general de Internet—, elimina la necesidad de recurrir a soluciones tradicionales, como CASB, SWG y RBI, al tiempo que mejora el rendimiento y la experiencia del usuario.

Esta arquitectura ofrece las prestaciones clave de SSE (acceso seguro, protección web y seguridad de datos), sin los desafíos habituales, como el redireccionamiento del tráfico, la degradación del rendimiento y la gestión compleja de políticas.

Para obtener más información sobre Enterprise Application Access y Secure Enterprise Browser de Akamai, con tecnología Seraphic, **póngase en contacto con su representante de Akamai o envíe un correo electrónico a sales@akamai.com.**