

Web Application Firewall (WAF)

Protege tu sitio y aplicaciones web

Seguridad continua

Con los servicios gestionados de WAF analizamos los sitios web **de forma recurrente** para revisar si han aparecido vulnerabilidades que los afecten y que continúan siendo **seguros**.

Arquitectura Cloud

Sin la instalación de servidores o infraestructuras adicionales, WAF despliega el servicio en la zona geográfica más adecuada según el servicio a proteger.

Permite implementar actualizaciones y mejoras de forma **rápida y sin interrupciones**.

Protección de datos

En los sitios web, uno de los objetivos de los ciberdelincuentes son los **datos de clientes o de la compañía**.

Proteger la página de la compañía es importante para **cuidar de la marca y su reputación**.



Aumenta la disponibilidad de los servicios web

Eliminar una vulnerabilidad en un sitio web puede ser complejo técnicamente y requerir semanas de trabajo de programación, durante las cuales **el servicio está inactivo**.

WAF permite proteger los sitios sin tener que modificar el código aumentando la disponibilidad de los servicios.



Protección contra ataques web y DDoS

WAF proporciona seguridad a los servicios web, defendiéndolos ante las amenazas y protegiéndolos ante ataques conocidos y desconocidos.

Podrás protegerte contra ataques de DDoS sin importar el tamaño o duración del ataque.



Protección contra Bots

Existen millones de Bots programados para escanear la web y encontrar sitios y servicios vulnerables para ser atacados de forma automatizada.

Contar con un sistema WAF es esencial para protegerse ante estas amenazas crecientes.



Protección de APIs y aplicaciones móviles

No solo es importante proteger los clásicos sitios web, el acceso a las API o aplicaciones móviles pueden y deben protegerse con WAF.



Análisis de vulnerabilidades web

ANCO ofrece un análisis gratuito de las vulnerabilidades más conocidas, que ayudará al cliente a ver la utilidad del servicio.



Aprendizaje automático

WAF protege de ataques conocidos (protección negativa basada en firmas) y de ataques de día 0 (protección positiva).



Bloqueo por reputación o geolocalización

WAF bloquea el acceso a los sitios protegidos desde IPs maliciosas o establece filtros para evitar conexiones desde países con alto índice de origen de ataques.



Protección de sesión y contra robo de datos

Protege las sesiones de los usuarios con el cifrado de cookies nativo o la protección contra ataques por manipulación de parámetros.

Además, identifica si la salida de datos contiene datos confidenciales (como tarjetas de crédito, etc) y los oculta de forma automática, protegiéndolos.



Firewall JSON y XML

WAF es capaz de proteger aplicaciones y servicios basados en JSON y XML gracias a la inspección profunda (Deep Inspection) de paquetes intercambiados en estos formatos.

Detecta y detiene posibles violaciones de confidencialidad de los datos.



Mantén tu negocio a salvo con seguridad preventiva

¿Cómo proteger tu infraestructura y anticiparte a cualquier riesgo? Identifica amenazas, cubre vectores de ataque y forma en ciberseguridad a tus empleados para una defensa completa.

¡Nosotros nos encargamos de todo!

[Descubre más aquí →](#)