arsenet
soluciones para empresas

FORTINET
MSSP GOLD PARTNER

Seguridad Gestionada
WAF (Web Application Firewall)

WAF es Seguridad específica para entornos Web:
Firmas basadas en el "OWASP Top 10", riesgos más críticos en aplicaciones Web, SQL Injection, Cross-Site Scripting (XSS), Security Misconfiguration.

Desde
20 € /mes

OWASP	Descripción Web Application Firewall	Técnicas de mitigación
SQL Injection	Los defectos en inyecciones de SQL se producen cuando los datos que no son de confianza se envían a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar a la víctima para que ejecute involuntariamente los comandos o acceded a los datos no autorizados.	Las firmas contra SQL injection construyen automáticamente una barrera, permitiendo una validación de solicitud comprensiva para cumplir estrictamente con la URL y sus parámetros. La aplicación mejorada del motor de detección de firmas añade una capa secundaria para caracteres atípicos y cadenas conocidas de inyección código.
Cross-Site Scripting (XSS)	Las fallas de XSS ocurren cuando una aplicación toma los datos de un atacante y los envía a un navegador web sin validación adecuada. XSS permite a dichos atacantes ejecutar secuencias de comandos en el navegador de la víctima, el cual puede secuestrar sesiones de usuario, desfigurar sitios web, o redirigir al usuario a sitios maliciosos (phishing).	El motor de detección de firmas incluye varias firmas (anti)XSS. El proceso de solicitud de validación, asegura que sólo caracteres relevantes puedan ser introducidos.
Security Misconfiguration (Configuración de seguridad indebida)	Una buena seguridad requiere tener una configuración definida e implementada para la aplicación, frameworks, servidor de aplicaciones, servidor web, servidor de base de datos, y la plataforma. Todos estos ajustes se deben definir, implementar, y mantener ya que muchos de ellos no se envían con valores seguros por defecto. Esto incluye mantener todo el software actualizado, incluyendo todas las librerías de código utilizadas por la aplicación.	Con el uso reglas basadas en firmas, se bloqueará cualquier intento realizado por un atacante para explotar una aplicación web mal configurada o desactualizada.
Otros aspectos	**Web Application Firewall** orientado a aplicaciones webs, también cuenta con firmas para la detección y bloqueo de solicitudes de números de tarjetas de crédito, troyanos y robots que intenten aprovecharse de vulnerabilidades de la web. Por otro lado, cuenta con un apartado de restricciones (Constraints), en los que se pueden introducir parámetros o rangos de permiso a ciertos tipos de variables, tales como límite de contenido de una página, límite de contenido de las cabeceras, número total de parámetros en la URL, cantidad de cookies en una solicitud, etc.	