Telematicos

CONSULTORÍA TECNOLÓGICA

CENTINELA

SEGURIDAD GESTIONADA PARA HOSTING

Cortafuegos inteligente con IA especializada en ciberseguridad, desarrollado y operado por Telematicos.

PROTECCIÓN ACTIVA 24/7



FICHA DE PRODUCTO

Su web, vigilada las 24 horas por un guardián que nunca duerme.

Detecta los ataques, los bloquea en cuestión de un minuto y le explica en lenguaje claro qué ha pasado, sin que usted tenga que hacer nada.

~14.000 ataques bloqueados en los últimos 30 días	**+9.000** direcciones hostiles distintas neutralizadas	**+500** dominios protegidos	**≈ 1 min** tiempo mediano entre la petición hostil y el bloqueo

Datos reales de producción: 4 servidores en funcionamiento continuo, últimos 30 días.

8 capas de defensa

IA propia sin enviar datos a terceros

24/7 todo el año

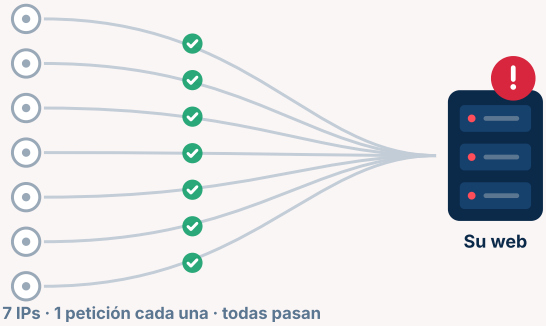
telematicos.es
916 55 72 42 · info@telematicos.es

POR QUÉ CENTINELA

Un firewall que entiende lo que ve

Un cortafuegos convencional mira cada visita por separado. Los ataques actuales no funcionan así: **cientos de direcciones distintas atacan a la vez**, cada una con una sola petición, repartidas entre muchas webs y cuentas de correo. Centinela **analiza todo el servidor a la vez** (web, correo, FTP, panel, SSH…), cruza la información y decide con reglas, memoria histórica e inteligencia artificial.

SIN CENTINELA Firewall convencional



Cada dirección hace una sola petición. Ninguna parece sospechosa por sí misma, así que **todas pasan**.

CON CENTINELA Visión de conjunto



Centinela cruza todas las peticiones del servidor, reconoce el patrón común y **bloquea el ataque completo**.

PASO 1
Vigila

Lee en tiempo real el tráfico de todas las webs, el correo y los accesos al servidor, sin instalar nada en el sitio del cliente.

PASO 2
Decide

Reglas locales, correlación entre dominios, reputación histórica de cada atacante y, en los casos dudosos, una IA que lo analiza.

PASO 3
Actúa y le informa

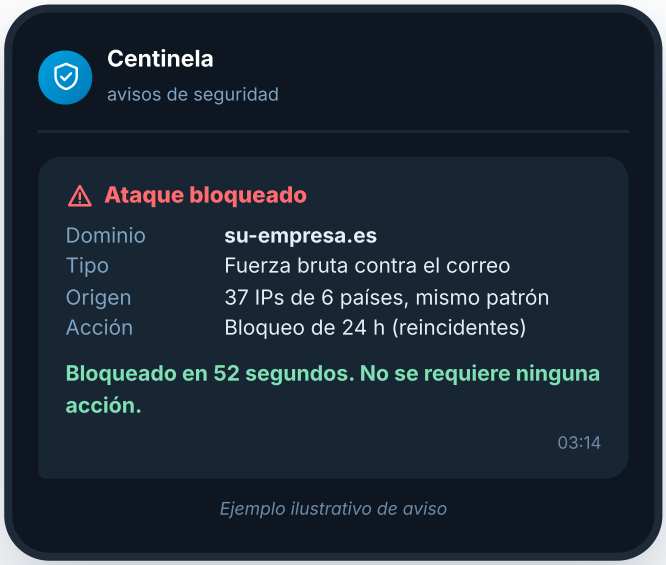
Bloquea al atacante, avisa por email o Telegram y deja constancia del motivo, el dominio afectado y las pruebas.

TRANSPARENCIA TOTAL

Sabrá qué ha pasado, en lenguaje claro

Cada bloqueo queda registrado con su motivo y sus pruebas. Y si lo desea, le avisamos al momento, sin jerga técnica.

- Motivo del bloqueo, país y red de origen
- Web o buzón atacado y prueba de la petición
- Avisos por email, Telegram o webhooks (Slack, Discord…)
- Informes en PDF por dominio, listos para el cliente final



Ejemplo ilustrativo de aviso

Ocho capas de defensa trabajando juntas

Cada capa cubre un frente distinto. Lo que una no ve, lo detecta otra, y todas comparten lo que aprenden.

1 Cortafuegos web inteligente

- Bloquea inyección SQL, XSS, ejecución remota de código y Log4j.
- Frena el robo de ficheros sensibles (.env, .git, copias de seguridad) y los escáneres de vulnerabilidades.
- Rutas trampa (honeypot): quien las toca queda bloqueado al instante.

2 Protección del correo

- Fuerza bruta contra buzones, incluso repartida entre muchas IPs, y ataques «de rociado» contra muchas cuentas.
- Avisa de cuentas comprometidas que envían spam: evita acabar en listas negras.
- Detecta accesos acertados tras una larga serie de fallos (posible brecha).

3 Defensa ante saturación (DDoS)

- Detecta asedios de botnets (miles de IPs pidiendo una sola cosa cada una), Slowloris, inundaciones y acaparamiento de conexiones.
- Mitigación controlada: límites temporales que caducan solos, sin alterar la configuración del cliente.
- Pantalla «Ataques en curso» con el estado en directo.

4 Correlación y reputación

- Cruza señales entre dominios y servicios: un atacante que prueba suerte en 20 webs se ve como lo que es.
- Memoria histórica por IP, subred y red de origen.
- Bloqueo escalado a reincidentes: 1 h → 24 h → 7 días → permanente.

5 IA que decide… y que revisa

- Interviene solo en los casos ambiguos, no en cada visita.
- Segunda revisión «en frío» de cada bloqueo; explica cada decisión en lenguaje claro.
- Si la IA no está disponible, el resto de capas sigue protegiendo.

6 Antimalware y control de ficheros

- Integración con Imunify: escaneo semanal automático y cuarentena automática si se confirma malware.
- Detecta webshells, ficheros sospechosos y procesos o tareas que intentan persistir.
- Histórico por dominio con descarga de lo aislado.

7 Inteligencia compartida

- Un atacante detectado en un servidor se bloquea también en el resto.
- Un único panel para todos los servidores.
- Vigilancia de los propios nodos: si uno deja de responder, se detecta y se autorrepara con escalado prudente.

8 Panel, avisos e informes

- Panel web en tiempo real: bloqueos, incidentes, países, redes y dominios.
- Avisos por email, Telegram y webhooks (Slack, Discord…).
- Informes en PDF por dominio, redactados por IA en lenguaje no técnico, listos para el cliente final.

Siempre bajo control

- Modo de prueba antes de activar bloqueos
- Lista blanca respetada por todas las detecciones
- Desbloqueo inmediato desde el panel
- Registro auditable: quién, cuándo y por qué
- Actualizaciones firmadas con vuelta atrás automática

VENTAJAS

Lo que gana con Centinela

Protección que no depende de usted
Funciona sola, todos los días del año. Sin configurar reglas ni revisar registros.

Sin ralentizar su web
Analiza los registros del servidor y no se interpone en cada visita: no añade latencia a sus clientes.

Transparencia total
Cada bloqueo queda registrado con motivo, país, red de origen, web atacada y prueba de la petición.

Privacidad por diseño
La IA se ejecuta en infraestructura propia: los registros de sus webs no se envían a servicios de terceros.

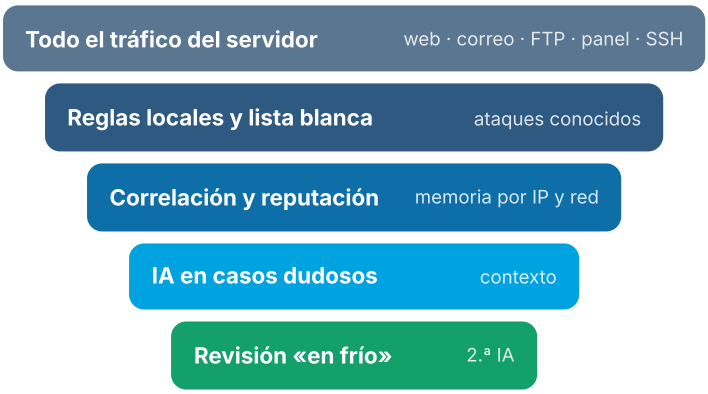
Menos falsos bloqueos
Una segunda IA revisa cada bloqueo a posteriori, y buscadores y servicios legítimos están protegidos por lista blanca.

Siempre al día
Actualizaciones gestionadas por nosotros, con vuelta automática a la versión anterior si algo falla.

CÓMO DECIDE

Cada petición pasa por varios filtros

Las reglas y la memoria resuelven la gran mayoría de casos. La inteligencia artificial se reserva para los dudosos, donde realmente aporta valor.



Si la IA no estuviera disponible, las capas anteriores siguen protegiendo.

REINCIDENTES

Quien insiste, lo paga

Centinela recuerda a cada atacante por su IP, su subred y su red de origen. Cada nueva intentona endurece el bloqueo.



Y gracias a la inteligencia compartida, un atacante detectado en un servidor queda bloqueado también en todos los demás.

Desbloqueo inmediato desde el panel si fuera necesario

COMPARATIVA

Centinela frente a un firewall convencional

CAPACIDAD	FIREWALL CONVENCIONAL	CENTINELA
Detecta ataques repartidos entre cientos de IPs	✗	✓
Cruza señales entre webs, correo, FTP y panel	✗	✓
Recuerda a los reincidentes y endurece el bloqueo	Parcial	✓
Entiende el contexto de un caso dudoso (IA)	✗	✓
Revisa a posteriori sus propios bloqueos	✗	✓
Indica qué web y qué cliente están siendo atacados	✗	✓
Informe del incidente apto para el cliente final	✗	✓
Aísla malware confirmado automáticamente	✗	✓

RESPUESTAS CLARAS

Preguntas frecuentes

¿Ralentiza mi web?
No. Centinela analiza los registros del servidor; no se coloca entre el visitante y su web.

¿Puede bloquear a un cliente legítimo?
Es poco probable y se corrige al instante: lista blanca, buscadores protegidos, revisión posterior por IA y desbloqueo con un clic.

¿Y si la IA deja de funcionar?
El resto de capas (reglas, correlación y reputación) sigue protegiendo sin interrupción.

¿Tengo que instalar algo?
No. Es un servicio gestionado: la protección y sus actualizaciones corren de nuestra cuenta.

¿Se envían mis datos fuera?
No. La IA funciona en infraestructura propia; los registros de sus webs no se envían a plataformas de IA de terceros.

¿Cómo sé lo que está pasando?
Con el panel en tiempo real, los avisos por email o Telegram y los informes en PDF por dominio.

Ficha técnica

Sistemas	Linux (Debian, Ubuntu, RHEL y derivados)	Servicios vigilados	Web, correo (SMTP/IMAP), FTP, SSH, panel, DNS
Panel de hosting	Plesk, con detección automática de dominios	Direcciones	IPv4 e IPv6
Bloqueo	CSF / Juggernaut, sin modificar su configuración	Avisos	Email, Telegram y webhooks
Servidores web	Apache y nginx	Integración	Métricas Prometheus, registros JSON auditables
Antimalware	Integración con Imunify	Actualización	Gestionada, firmada y con vuelta atrás automática

Puesta en marcha sin sobresaltos

1 — Alta del servidor
Detección automática de los dominios alojados en Plesk. No hay que instalar nada en las webs.

2 — Modo de prueba
Centinela observa y registra sin bloquear, para validar la lista blanca con su tráfico real.

3 — Bloqueo activo
Se activan las detecciones y mitigaciones, con desbloqueo inmediato desde el panel.

Protección continua
Vigilancia 24/7 y actualizaciones firmadas gestionadas por nosotros.

Incluido en el plan de mantenimiento web Avanzado. Centinela forma parte de nuestro nivel de máxima seguridad, junto con antimalware, copia externa y técnico personalizado.

DEJE QUE CENTINELA LOS VEA VENIR

¿Quiere más información?

Hable con nuestro equipo técnico: le explicamos cómo Centinela puede proteger sus webs y su correo, sin compromiso.

916 55 72 42
info@telematicos.es
telematicos.es

CONTACTE CON NOSOTROS →