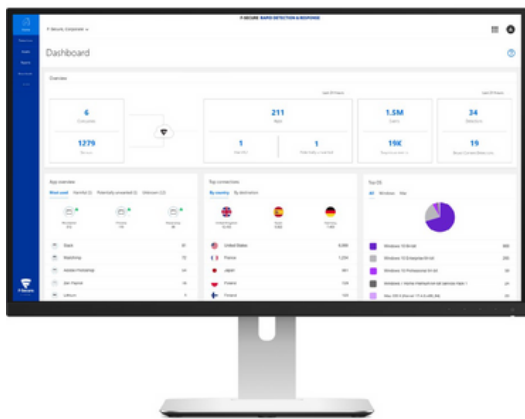


# F-SECURE RAPID DETECTION & RESPONSE

Solución de detección y respuesta en el endpoint para detener los ataques dirigidos con automatización y orientación



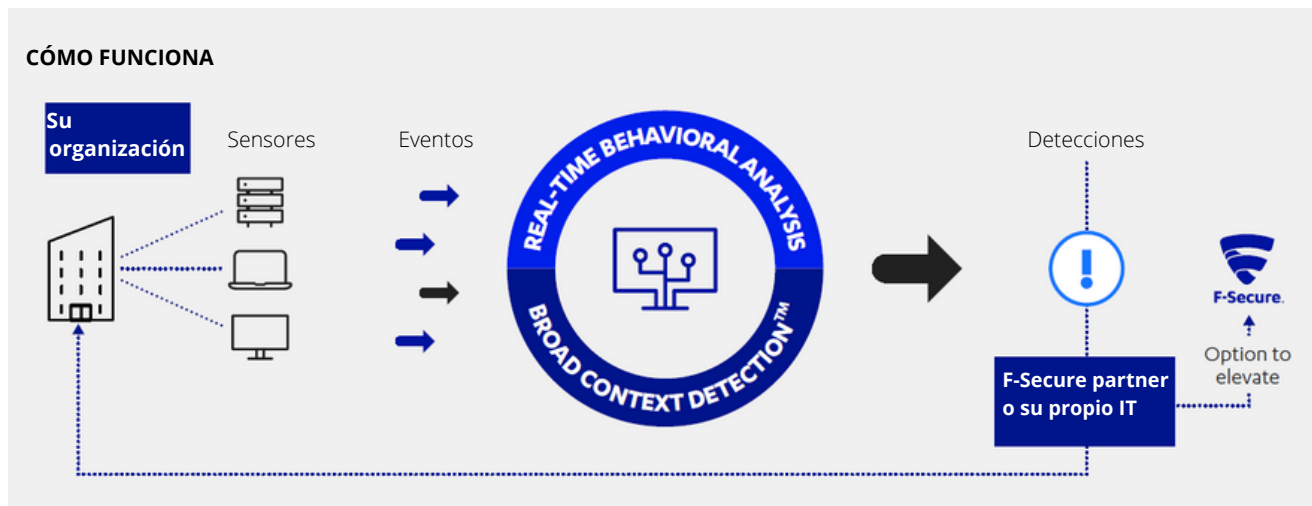
La prevención efectiva de amenazas antes del compromiso es la piedra angular de la ciberseguridad, pero no se puede confiar únicamente en las medidas preventivas para mantener su empresa y sus datos a salvo de las tácticas, técnicas y procedimientos que los adversarios utilizan en los ataques dirigidos.

F-Secure Rapid Detection & Response es una solución de detección y respuesta de endpoints (EDR) líder en el sector que aprovecha las tecnologías de análisis y de aprendizaje automático más avanzadas para proteger a su organización contra las amenazas e infracciones cibernéticas avanzadas. Con la identificación automática de amenazas avanzadas de la solución, la visibilidad contextual de su

## BENEFICIOS CLAVE:

- Obtener una visibilidad inmediata de los potenciales no deseados o aplicaciones perjudiciales y servicios en la nube
- Identificar automáticamente las amenazas avanzadas con niveles de riesgo y la criticidad del anfitrión para facilitar la priorización
- Visualizar los ataques en un contexto más amplio con todos los detecciones y anfitriones en una línea de tiempo
- Detener los ataques rápidamente con una guía incorporada o automatizada
- Acciones de respuesta basadas en un calendario predefinido
- Resolver los casos difíciles con el análisis de incidentes a petición y las investigaciones de los cazadores de amenazas de clase mundial
- Reduzca los gastos de gestión con la nube nativa y solución de seguridad de endpoint de un solo cliente
- Opción de subcontratar la vigilancia avanzada de amenazas a un proveedor de servicios gestionados certificado

seguridad y guía incorporada con la opción de automatizar las acciones de respuesta a distancia, su equipo puede detectar y detener los ataques dirigidos de forma rápida y eficiente. La solución es administrada por su propio equipo de TI o por un proveedor de servicios de EDR certified, y siempre estará respaldado por los cazadores de amenazas de clase mundial de F-Secure, lo que permite resolver incluso los casos más difíciles.



## Visibilidad proactiva de su entorno informático

Obtener una amplia visibilidad de las aplicaciones en su entorno de TI y los servicios en la nube reducirá la exposición a las amenazas avanzadas y la fuga de datos. La solución EDR le permite listar inmediatamente todos los procesos activos que se ejecutan en los puntos finales de su red para identificar las aplicaciones no deseadas, desconocidas y dañinas. Puede restringir fácilmente las aplicaciones y los servicios en la nube potencialmente dañinos, incluso antes de que se produzcan filtraciones de datos.

- Identifica todas las aplicaciones dañinas o no deseadas, y los destinos extranjeros de los diferentes servicios de la nube
- Aprovecha los datos de reputación de F-Secure para identificar aplicaciones potencialmente dañinas
- Restringe las aplicaciones potencialmente dañinas y la nube servicios incluso antes de que ocurran las infracciones de los datos

## Acciones de respuesta remota con automatización

Las acciones de respuesta automatizada pueden utilizarse para reducir el impacto de los ataques cibernéticos dirigidos, conteniéndolos las 24 horas del día cuando los niveles de riesgo son suficientemente altos. La automatización, basada en horarios predefinidos, ha sido diseñada específicamente para apoyar a los equipos que sólo están disponibles durante las horas de trabajo, teniendo en cuenta también la criticidad de las detecciones.

- Acciones de respuesta automatizadas basadas en la criticidad, los niveles de riesgo y el calendario predefinido
- Los niveles de criticidad y riesgo que ofrece la solución permiten establecer prioridades en las medidas de respuesta
- Contenga los ataques rápidamente, incluso si su equipo sólo está disponible durante el horario de trabajo

## Los cazadores de amenazas de clase mundial te respaldan

Algunas detecciones requieren un análisis más profundo de las amenazas y la orientación de expertos en seguridad cibernética especializados. Para estos casos difíciles, la solución tiene incorporado un servicio único de "Elevación a F-Secure". Ofrece un análisis profesional de incidentes de métodos y tecnologías, rutas de red, orígenes del tráfico y plazos de una detección de contexto amplio™ para proporcionar asesoramiento experto y una mayor orientación de respuesta siempre que se produzca un ataque.

- Guía de respuesta paso a paso incorporada y remoto acciones para detener los ataques
- Guía y apoyo para los proveedores de servicios gestionados certificados a través de acciones de respuesta
- Único análisis de amenazas de Elevate to F-Secure y experto el servicio de orientación te respalda

## Gestión basada en un solo cliente y en la nube

Herramientas de monitoreo livianas y discretas diseñadas para la detección de anomalías, desplegables en todas las computadoras Windows y MacOS relevantes dentro de su organización. Los sensores están diseñados para funcionar con cualquier solución de protección de puntos finales y funcionan con las soluciones de seguridad de puntos finales de F-Secure en una infraestructura de administración y cliente único.

- Los sensores de peso ligero se despliegan en todas las computadoras relevantes dentro de su organización
- Infraestructura de gestión y cliente único con las soluciones de seguridad de endpoint de F-Secure
- Los sensores recogen datos de comportamiento de los dispositivos finales sin comprometer la privacidad de los usuarios.

[fsecure.com/business](https://fsecure.com/business) | [twitter.com/fsecure](https://twitter.com/fsecure) | [linkedin.com/fsecure](https://linkedin.com/fsecure)

