

# McAfee Investigator

## Transforme a los analistas en expertos investigadores

McAfee® Investigator ayuda a los analistas a cerrar más casos en menos tiempo y con mayor confianza en determinar el origen del problema. Con las alertas clasificadas comienza el análisis realizado por especialistas para recoger datos acreditativos, interpretar las pruebas y presentar las conclusiones necesarias para validar las amenazas y responder de forma rápida y global.

### Dificultades de las operaciones de seguridad

Los problemas que generan los enormes volúmenes de datos y su tiempo de conservación complican la tarea de evaluar con precisión la importancia y alcance de una alerta. Los analistas a menudo ignoran las alertas porque carecen del contexto o del conocimiento para decidir si deberían tratarse como incidentes formales.

En consecuencia, las investigaciones de los incidentes seleccionados pueden prolongarse en el tiempo y requerir un amplio conocimiento de los vectores de ataque para llegar hasta el fondo del problema. Estas tendencias implican una mayor necesidad de disponer de analistas experimentados en operaciones de seguridad y, sin embargo, hay una escasez de expertos disponibles.

### Nuevos análisis investigativos

Para enfrentarse a este problema, los equipos de operaciones de seguridad deben simplificar y agilizar

la clasificación y la investigación de alertas para que su personal existente y los nuevos analistas puedan hacer más.

McAfee Investigator pone al alcance de cualquier equipo de operaciones de seguridad unas investigaciones guiadas que incluyen clasificación, recopilación exhaustiva de datos y análisis avanzados. Como oferta de seguridad como servicio (SaaS), los sistemas especializados y las herramientas de captura para endpoints se integran con las fuentes de datos y sistemas de administración de la seguridad existentes para ofrecer una rápida rentabilización con un mínimo esfuerzo.

Estos análisis interactivos proporcionan orientación actualizada permanentemente para que los responsables de la respuesta a incidentes puedan investigar a fondo el malware, las amenazas a través de la red y los indicadores de peligro, en menos tiempo y con mayor precisión.

### Principales ventajas

- **Reduzca el tiempo de permanencia:** la exploración de los datos del caso aumenta las posibilidades de detectar el origen del problema en lugar de corregir un síntoma.
- **Pase de alertas a casos:** reduzca el tiempo dedicado a las investigaciones manuales y de prioridad baja.
- **Preste atención a lo desconocido:** céntrate en los artefactos y datos únicos que requieren interpretación y decisiones humanas.
- **Mejore la clasificación:** procese más casos en menos tiempo y con mayor calidad.
- **Reduzca la fatiga de los analistas:** aproveche al máximo el tiempo limitado, la energía y la capacidad cognitiva.
- **Desarrolle las aptitudes de los analistas:** los analistas reciben formación a través de manuales e información relevante sobre las cuestiones e hipótesis adecuadas dentro del flujo de trabajo.

### Descubra información útil a una velocidad asombrosa

McAfee Investigator mejora la clasificación de manera inmediata permitiendo que las operaciones de seguridad automaticen la asignación de prioridades a determinadas situaciones para gestionarlas de manera inmediata. Para estas y otras alertas que desea explorar un analista, McAfee Investigator recopila, organiza, resume y muestra las alertas, la actividad, las pruebas y la inteligencia reunida sobre un ataque potencial.

Se recopilan datos en segundo plano y se incluyen solo los que son importantes para llevar a cabo una investigación sobre amenazas específica que permitirá tomar una decisión. Los datos de las soluciones de administración de eventos e información de seguridad (SIEM) pueden complementarse con datos de los endpoints, sin necesidad de agentes de detección y respuesta para endpoints (EDR) en cada nodo. Este modelo sustituye la información aislada por visibilidad contextual de los indicadores de peligro, tácticas, técnicas, procedimientos y relaciones.

Un motor de análisis de datos y aprendizaje automático compara las pruebas con referencias conocidas y fuentes de inteligencia sobre amenazas. Procesa los artefactos y aumenta la información sospechosa fundamental.

Gracias a la recopilación y priorización automáticas de los datos adecuados, McAfee Investigator reduce el esfuerzo y aumenta la velocidad con la que los analistas pueden determinar el riesgo y urgencia del incidente. Los analistas pueden adoptar decisiones de clasificación precisas de forma más rápida y poner el foco en las amenazas más importantes.

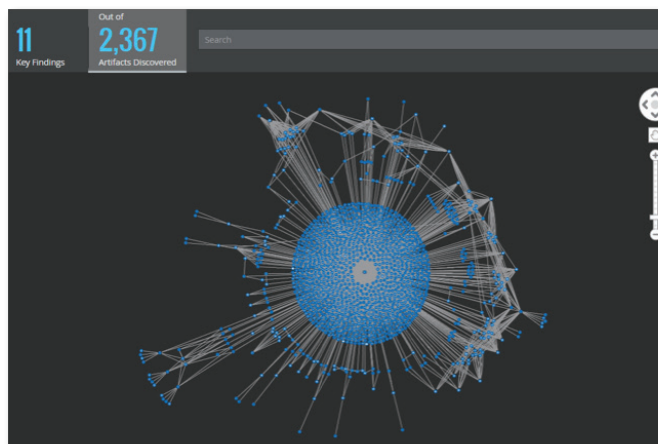


Figura 1. McAfee Investigator recopila miles de elementos de prueba.

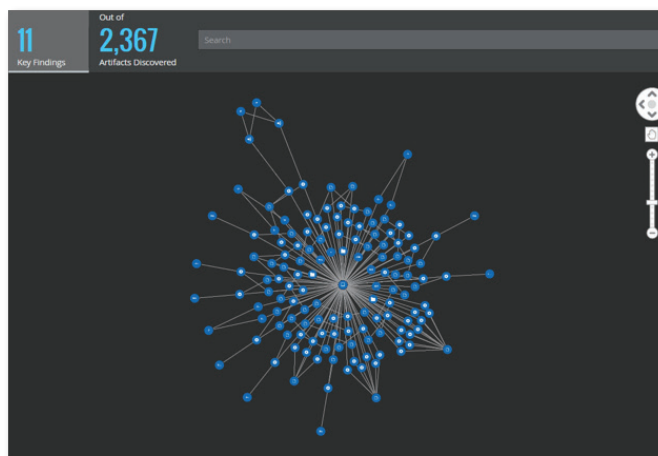


Figura 2. McAfee Investigator aplica entonces análisis y asesoramiento especializado para presentar las conclusiones que importan.

### Principales ventajas (continuación)

- **Aumente el valor de los sistemas actuales:** se mejoran las fuentes de datos y análisis existentes para centrar objetivos y aumentar la precisión.

### Características principales

- Recopilación precisa de datos bajo demanda
- Agente de recopilación de datos en los endpoints diferenciado
- Interpretación de los datos recopilados con asesoramiento especializado e inteligencia artificial
- Visualizaciones interactivas
- Hipótesis multivector para explorar datos factibles
- Referencias para inteligencia institucional
- La gestión de casos dirige al personal y permite compartir la información en todas las investigaciones

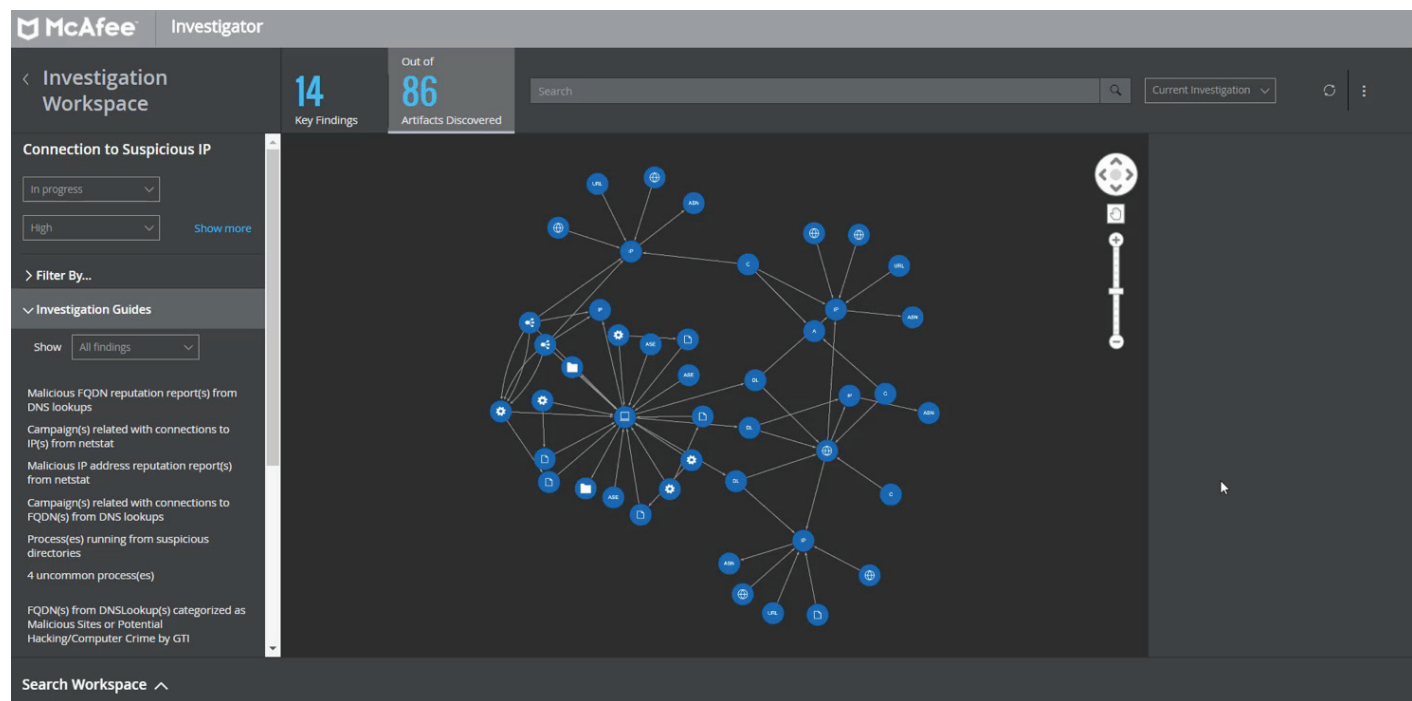


Figura 3. El espacio de trabajo convierte en obvias y fáciles de analizar las conclusiones principales.

A nivel organizativo, los beneficios son muchos. Al elevar la clasificación de meras revisiones de alertas a casos contextuales, todos los analistas aumentan su eficacia, se gestionan un mayor número de casos por parte de analistas de Nivel 1, y los analistas dedican el tiempo a las actividades de mayor valor.

### Oriente las investigaciones a partir de conocimientos especializados

Cuando se elige un incidente para llevar a cabo una investigación detallada, los analistas emplean manuales interactivos que les indican lo que es importante mientras

los evalúan y determinan su alcance. Los manuales de investigación no se basan en scripts ni en código estático. El sistema simula el proceso del pensamiento humano, explorando muchas hipótesis en paralelo para conseguir la máxima velocidad y exactitud.

Los manuales en lenguaje natural se han realizado con una combinación de experiencia de los investigadores de Foundstone® e inteligencia artificial. Esta es una de las formas mediante las que McAfee Investigator incorpora la asociación hombre-máquina.

## FICHA TÉCNICA

El espacio de trabajo estructura la información y los hallazgos sobre los casos para que los analistas planteen las cuestiones adecuadas. Esta exploración focalizada y multivector se traduce en el cierre de casos eficaz y preciso con un alto grado de confianza de que los analistas han identificado la causa fundamental.

### **Adapte experiencia y capacidad**

El espacio de trabajo interactivo de McAfee Investigator impulsa los flujos de trabajo y la navegación a través de datos en un único entorno cognitivo. Este modelo aumenta la eficacia, reduce la sobrecarga de información generada a partir de la gran multitud de tipos de alertas y elimina la necesidad de revisar varias pantallas.

El espacio de trabajo enseña a los analistas inexpertos y de nivel intermedio a implementar los procesos de pensamiento de analistas avanzados, generando experiencia sin formación adicional.

### **Aproveche las herramientas y datos existentes**

McAfee Investigator trabaja con un sistema SIEM y con el software McAfee® ePolicy Orchestrator® para añadir análisis avanzados a las fuentes de datos, referencias, correlaciones y alertas existentes. Un agente diferenciado recopila nuevos datos de endpoints que resultan fundamentales para realizar una interpretación precisa de pruebas discretas. La integración entre McAfee Investigator y McAfee Active Response permite a los analistas examinar el impacto de una amenaza en todos los endpoints en tiempo real. Una fuente constante de información de actividad comparte los datos con las herramientas de terceros para incorporarlos en los flujos de trabajo actuales, lo que agiliza los procesos y mejora la colaboración. Los servicios profesionales facilitan la incorporación y la activación correctas.

## FICHA TÉCNICA

### Más información

Con McAfee Investigator, cuando tiene una sospecha, no necesita dedicar horas a recopilar datos e incluso más tiempo a interpretarlos. El motor de análisis avanzado que utiliza McAfee Investigator inspecciona y clasifica las alertas de amenazas dentro de una interfaz basada en el contexto para escalar las operaciones de seguridad. McAfee Investigator automatiza el uso de conocimientos especializados en investigaciones de centros de operaciones de seguridad, lo que permite a los analistas trabajar de forma más inteligente, rápida y con un mayor grado de precisión.

Esta es la verdadera asociación hombre-máquina.

Para obtener más información, visite

[www.mcafee.com/es/products/investigator.aspx](http://www.mcafee.com/es/products/investigator.aspx).

Las funciones y ventajas que ofrecen las tecnologías de McAfee dependen de la configuración del sistema y es posible que necesiten la activación de hardware, software o servicios. Encontrará más información en [mcafee.com/es](http://mcafee.com/es). Ningún sistema informático puede ser totalmente seguro.

Los casos de reducción de costes y tiempo que se describen son ejemplos de cómo un producto determinado de McAfee, en las circunstancias y configuraciones especificadas, puede afectar a costes futuros y ofrecer un ahorro de tiempo y dinero. Las circunstancias y los resultados variarán. McAfee no garantiza ninguna reducción de costes.



Avenida de Bruselas nº 22  
Edificio Sauce  
28108 Alcobendas, Madrid, España  
+34 91 347 85 00  
[www.mcafee.com/es](http://www.mcafee.com/es)

McAfee y el logotipo de McAfee, ePolicy Orchestrator y Foundstone son marcas comerciales o marcas comerciales registradas de McAfee LLC, o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Copyright © 2018 MAYO 2018